INTERNATIONAL STANDARD

ISO 24100

First edition
2010-05-01

Intelligent transport systems — Basic principles for personal data protection in probe vehicle information services

Systèmes intelligents de transport — Les principes de base pour la protection des données personnelles de sonde

Reference number
ISO 24100:2010(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 24100 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

Introduction

Probe vehicle systems are being investigated and deployed throughout the world. It is expected that the number of practical systems will grow steadily over the next few years. In general, probe data collection systems will incorporate extensive technical measures to minimize the use of personal data and protect any personal data that are used. Nevertheless, because technical measures cannot address every situation, we must address the possibility that situations may arise in which personal data become vulnerable to misuse. Since data collected by such systems can reveal sensitive personal information, it is critical to address consumer requirements for personal data protection through a formal policy for handling these data.

This protection is particularly important because it is difficult to completely eliminate any possibility of probe data being linked to a particular person or vehicle. For example, consider a probe vehicle information service that does not include any personal data within the probe data, but uses personal data to authenticate the data source and ensure data integrity when collecting probe data. In this case, even if personal data are not contained in the collected probe data, probe data senders may still be identified. It is important to have both a system to protect personal data and a set of basic principles that are observed by the probe vehicle information service providers to reassure probe data senders about their personal data and facilitate the creation of information services using useful probe data.

The definition of personal data refers to the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The framework for describing the basic principles is adopted from the eight principles of the said recommendation. The basic principles in this International Standard are examined and developed on the basis of the results of the threat analysis.

This International Standard is promulgated in order to promote the smooth deployment and expansion of probe vehicle information services, in particular the following.

a) If the providers of probe vehicle information services are not consistent in their handling of the privacy aspect of personal data, it could give rise to confusion in the marketplace and generate public mistrust of the services themselves. The development of this International Standard will facilitate the development of standard procedures common to all probe vehicle information service providers.

b) Increasing the transparency of probe vehicle information services will enable drivers to know better in advance how probe data are to be collected and used, which will help dispel their anxieties about the possible misuse of their personal data.

c) Having an International Standard will allow more efficient research and development work on probe vehicle information systems and enhance the universality, commonality and interoperability of these services, thereby facilitating their smooth expansion.

Intelligent transport systems — Basic principles for personal data protection in probe vehicle information services

1 Scope

This International Standard states the basic rules to be observed by service providers who handle personal data in probe vehicle information services. This International Standard is aimed at protecting the personal data as well as the intrinsic rights and interests of probe data senders, i.e., owners and drivers of vehicles fitted with in-vehicle probe systems.

2 Normative references

The following referenced documents are indispensable for the application 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 21217, *Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture*

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
authentication
ensuring that the identity of a subject or resource is the one claimed

3.2
authentication data
data used for the purpose of authentication

3.3
collect
obtain probe packages/data from vehicles

3.4
contextual data
not directly identifiable data to provide information about an individual in combination with other information

NOTE Contextual data require the same level of protection as do personal data.

3.5
cryptography
discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its unauthorized use, establish its authenticity, prevent its undetected modification, and/or prevent its repudiation

3.6
data source
probe data sender from a vehicle to a probe data collector in a probe vehicle system

3.7
data subject
individual from whom personal data are collected, disclosed or used by a probe data collector

3.8
decryption
inverse function of encryption

3.9
encryption
function of transforming data by the discipline of cryptography so as to make the data undecipherable to anyone other than the legitimate sender and receiver

3.10
encryption data
data used for the purpose of encryption

3.11
integrity
safeguarding the accuracy and completeness of information and processing methods

3.12
personal data
data which pertain to an individual and can identify a particular individual, and are handled by probe vehicle systems defined in ISO 22837 when collecting probe data via a communication network

NOTE It also includes data that can be referred to other databases and thereby used to identify a particular individual.

3.13
probe collection
land-side activity that receives probe messages sent by vehicles and extracts probe data from these messages

3.14
probe data
vehicle sensor information formatted as probe data elements and/or probe messages that are processed, formatted and transmitted to a land-based centre for processing to create a good understanding of the driving environment

3.15
probe data collector
party that is responsible for receiving probe messages sent by a probe data sender

NOTE A probe data collector is responsible for probe data at any stage.

3.16
probe data sender
entity that is responsible for sending probe messages to a probe data collector

3.17
probe header
set of data required in order to effect a transmission

NOTE It is (the information) processed at the communication layer, such as a unique communication ID, and includes information on the transmitting/original entity. Personal data may be included depending on the communication medium used.

3.18
probe message
structured collation of data elements suitable to be delivered to the onboard communication device for transmission to a land-based centre

NOTE A probe message should not contain any information that identifies the particular vehicle from which it originated or any of the vehicle's occupants, directly or indirectly. In delivering a probe message to be transmitted by the onboard communication device, the onboard data collection system will request that the message be packaged and transmitted without any vehicle- or occupant-identifying information.

3.19
probe package
set of data blocks transmitted from vehicles to probe data collectors

NOTE A probe package includes/constitutes a probe payload and a probe header. Figure 1 shows the overall structure of the probe package.

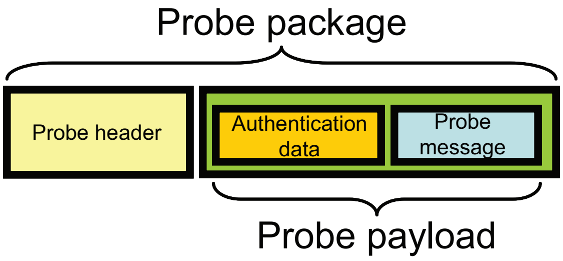

Figure 1 — Model of data transmitted from vehicles

3.20
probe payload
set of data transmitted at the application layer from vehicles to probe data collectors

NOTE A probe payload includes/constitutes probe messages and authentication data. A probe message does not include any personal data, however, personal data may be included in a probe payload.

3.21
probe processing
land-side activity that receives collected probe data from probe collection and processes them

NOTE Probe processing does not receive any information from probe collection that identifies the vehicle or driver.

3.22
probe vehicle system
system consisting of vehicles that collect and transmit probe data and land-based centres that collate and process data from many vehicles to build an accurate understanding of the overall roadway and driving environment

NOTE This International Standard does not refer to the function of “turn off” (sending the probe data by an individual) since some probe vehicle systems have a switch to stop sending probe data and others do not.

3.23
provide
transmit, disseminate or transfer outside a country for disclosure of data

3.24
use
extracting probe data from probe packages, recording and carrying out other operations on probe data including organization, retrieval, consultation and disclosure by providing

4 Privacy context for probe vehicle systems

This International Standard sets out the following items related to probe vehicle systems that collect probe data from private vehicles and process the data statistically to generate useful information that is provided to various end users.

— A *reference architecture* for probe vehicle systems. This International Standard shows probe vehicle systems in which personal data are handled at the time of probe data collection. It should be defined in compliance with the reference architecture in ISO 22837.

— The definition of *personal data* included in probe vehicle systems. This International Standard is defined in reference to the recommendation of the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines).

— The *basic principles* for personal data protection in probe vehicle systems. These principles set out the basic rules for handling personal data properly which should be observed when collecting probe data. They are stipulated in compliance with the eight principles described in the OECD Guidelines.

Figure 2 depicts the context of this International Standard described above.

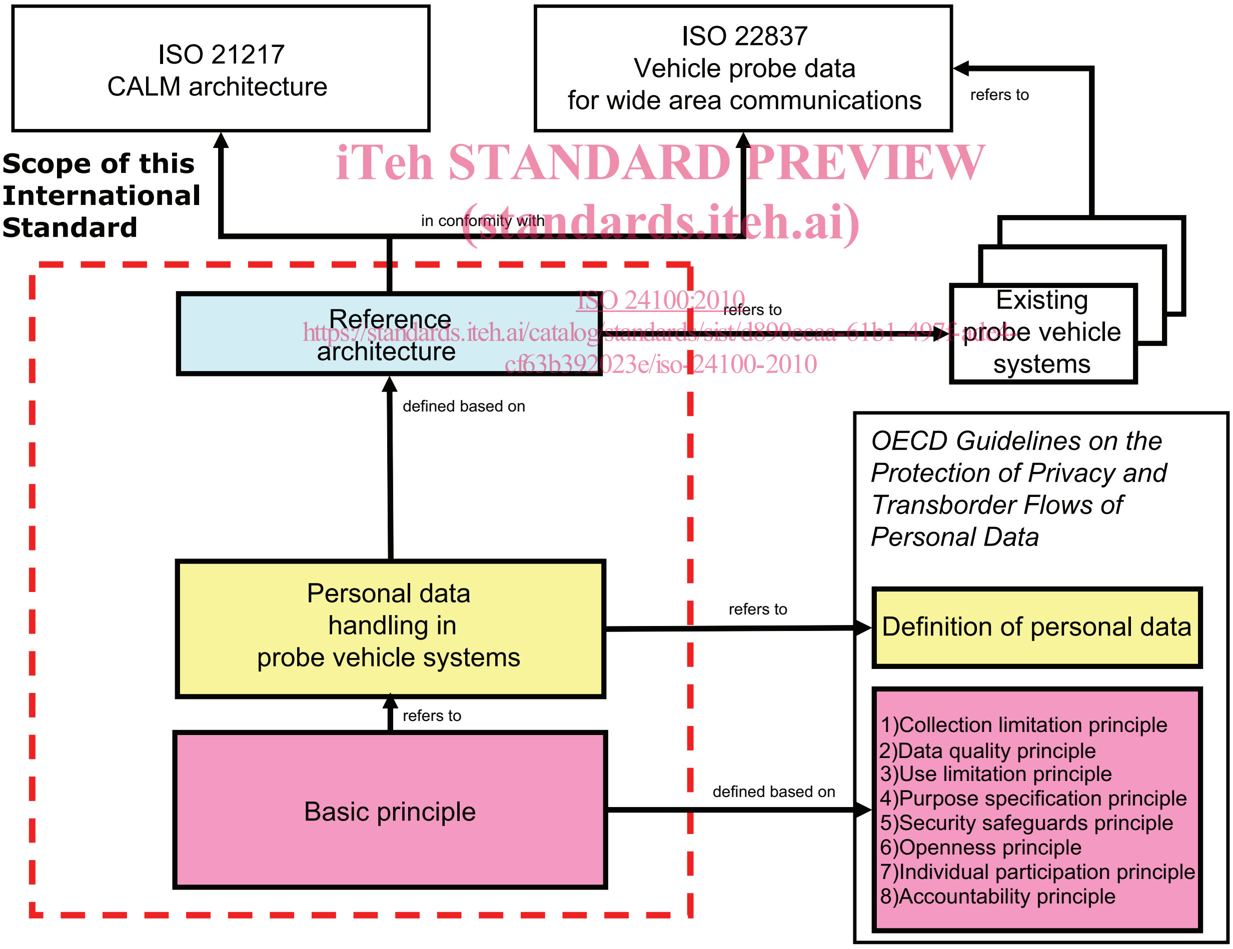
ISO 21217
CALM architecture
ISO 22837
Vehicle probe data
for wide area communications
refers to
Scope of this International Standard
in conformity with
Reference architecture
refers to
Existing probe vehicle systems
defined based on
OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
Personal data handling in probe vehicle systems
refers to
Definition of personal data
refers to
Basic principle
defined based on
1)Collection limitation principle
2)Data quality principle
3)Use limitation principle
4)Purpose specification principle
5)Security safeguards principle
6)Openness principle
7)Individual participation principle
8)Accountability principle

Figure 2 — The relation between this International Standard and related documents

5 Reference architecture

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

Based on the reference architecture defined in ISO 22837, the components of the reference architecture in this International Standard consist of the functions included in probe vehicle systems and the data transmitted between them.

While the reference architecture defined in ISO 22837 forms the basis for the reference architecture in this International Standard, that definition pertains only to probe messages.

The reference architecture in this International Standard, on the other hand, concerns all the data (probe package) transmitted from probe data senders to probe data collectors. A probe package includes data for effecting communication, authentication data and other data. In order to discuss the data in a probe package, it is necessary to have reference architecture that includes all the related concepts. Accordingly, reference architecture that treats all the above-mentioned data should be newly defined by extending the reference architecture described in ISO 22837.

Figure 3 shows the conceptual model of probe data collection.

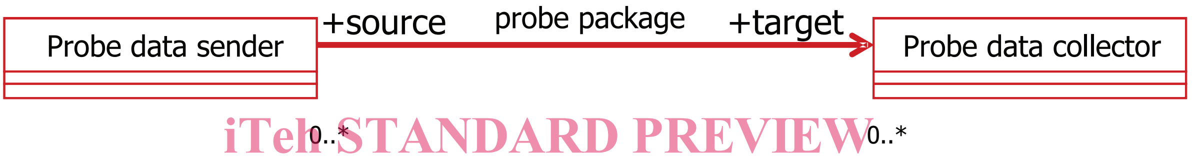

Figure 3 — The conceptual model of probe data collection

Figure 4 shows the reference architecture for the basic principles that include the functions for transmission of a probe message from a probe data sender and receipt of the message by a probe data collector.

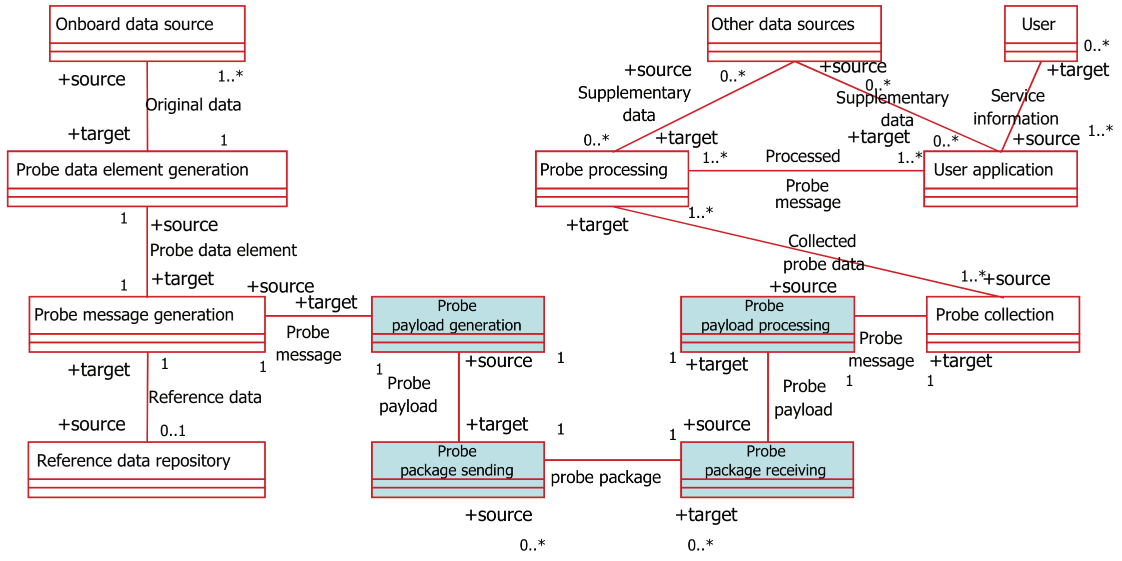

Figure 4 — The reference architecture for the basic principles

NOTE A hand-held mobile phone that has a secondary function as a traffic probe system of a mobile phone without the function of gathering, processing and transmitting probe data in compliance with ISO 22837 is not considered to be a probe vehicle system.

Objects newly added to the reference architecture for the basic principles are listed in a) to d).

a) **Probe package receiving**

Probe package receiving receives the probe package transmitted by probe package sending, extracts the probe payload, excluding the probe header, and sends it to probe payload processing.

b) **Probe package sending**

Probe package sending involves the creation of a probe package and its transmission via the communication medium to a probe data collector. A probe package is created by adding a probe header, representing the information needed for communication, to the probe payload resulting from probe payload generation. It manages the transactions that take place between the communication medium and probe data senders.

c) **Probe payload processing**

According to the data contained in the probe payload received from probe package receiving, probe payload processing first authenticates the probe data sender and ensures data integrity, and then extracts the probe message for transmission to probe collection.

d) **Probe payload generation**

Probe payload generation generates a probe payload consisting of the data in the context of the processing done in the application layer, such as the probe message, authentication data, etc. It manages the authentication procedures for probe data senders and ensures data integrity.

6 Personal data included in probe vehicle systems

6.1 Personal data

Even if data cannot identify an individual directly, if they can do so indirectly, they should be regarded as personal data to be specified in this International Standard as a target of protection, as is mentioned in the OECD Guidelines.

It is therefore necessary to define the personal data to be specified in this International Standard as follows:

Definition of personal data:

Personal data are data that are handled by the probe vehicle systems defined in ISO 22837 when probe data are collected via a communication network, and can identify a particular individual. Personal data also include data that can be referenced to other databases and thereby used to identify a particular individual.

Other databases should be classified into two groups. Table 1 gives the definitions and examples of other databases that should be provided in order to clarify the sentence mentioned in the definition of personal data above: “Personal data also include data that can be referenced to other databases and thereby used to identify a particular individual”.