BS ISO 24100:2010

BSI Standards Publication

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

raising standards worldwide™

National foreword

This British Standard is the UK implementation of ISO 24100:2010.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Road transport informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 55209 0

ICS 03.220.01; 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2010

Amendments issued since publication

Date	Text affected

BS ISO 24100:2010

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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Privacy context for probe vehicle systems **4**
5 Reference architecture **5**
6 Personal data included in probe vehicle systems **6**
6.1 Personal data **6**
6.2 Encryption data that can become personal data **7**
6.3 Authentication data that can become personal data **8**
7 The basic principles **8**
7.1 General **8**
7.2 Collection limitation principle **8**
7.3 Data quality principle **9**
7.4 Purpose specification principle **9**
7.5 Use-limitation principle **10**
7.6 Security safeguards principle **10**
7.7 Openness principle **10**
7.8 Individual participation principle **10**
7.9 Accountability principle **10**
Annex A (informative) **Threats to personal data in probe vehicle systems** **11**
Bibliography **23**

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.

INTERNATIONAL STANDARD ISO 24100:2010(E)

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.

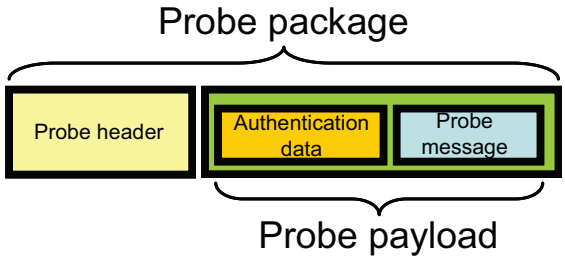

Figure 1 — Model of data transmitted from vehicles

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.

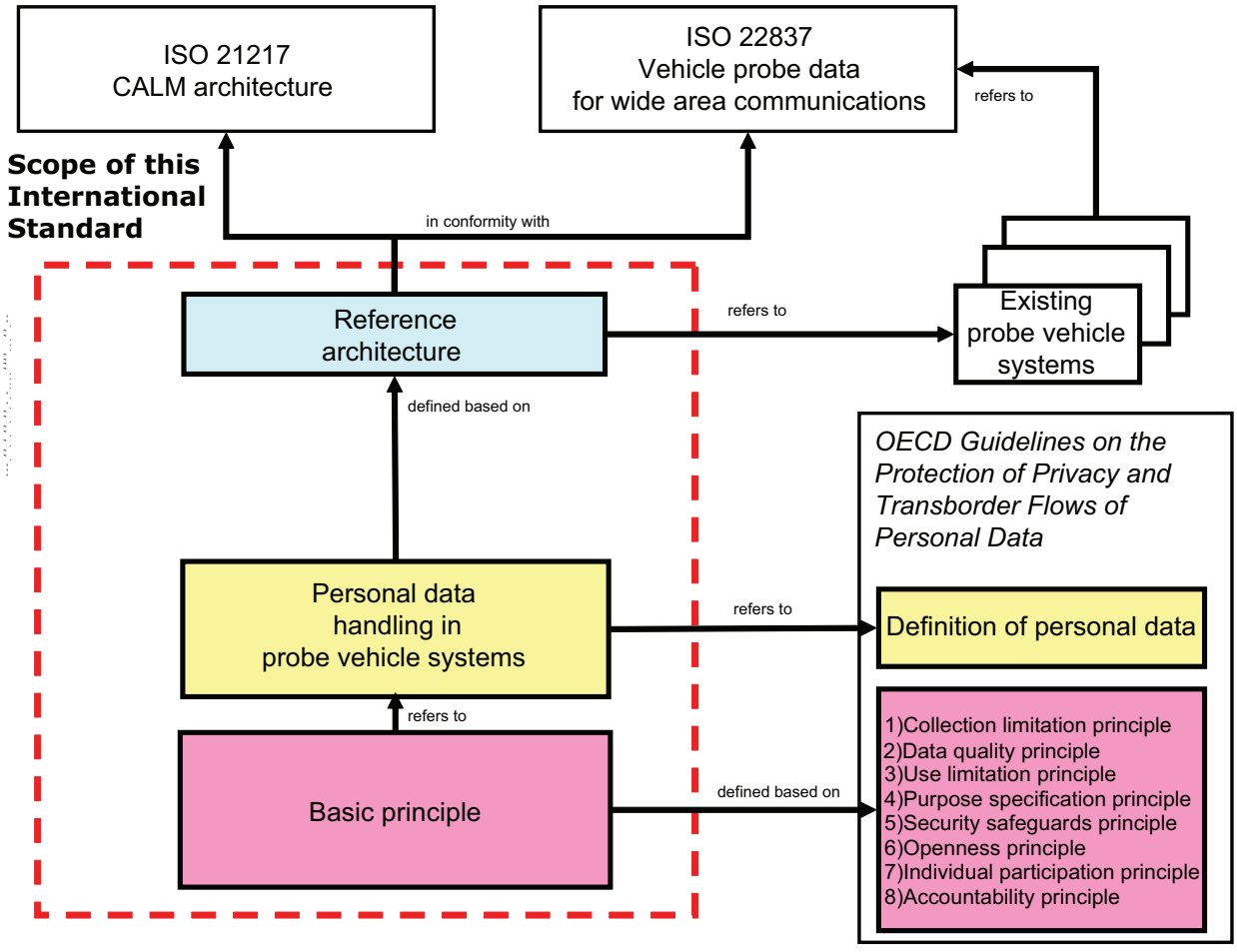

Figure 2 — The relation between this International Standard and related documents

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.

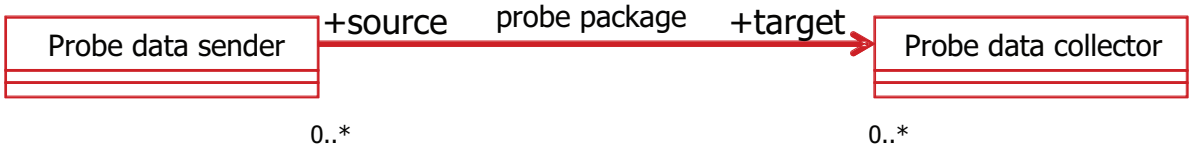

Figure 3 — The conceptual model of probe data collection

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.

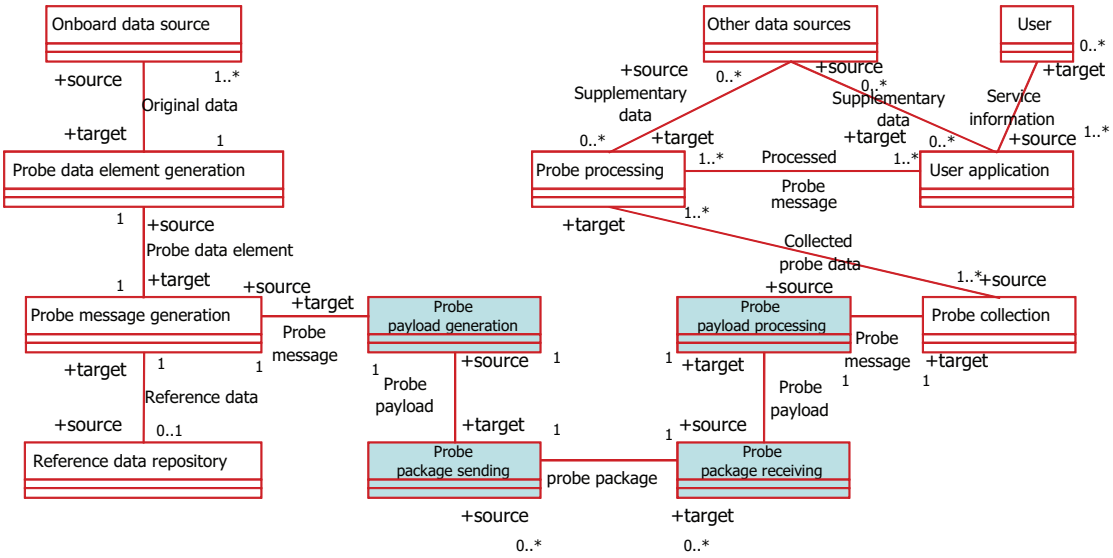

Figure 4 — The reference architecture for the basic principles

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”.

Table 1 — Other databases

Category	Internal database	External database
Definition	A database[a] that contains information collected by probe data collectors when contracting probe data senders and owned by probe data collectors.	A database made, managed and distributed by public authorities or private sector organizations other than probe data collectors, which contains generally available information.
Examples	— Subscriber registration information — Database of individuals and their passwords	— Maps in which individual residences are identifiable — Address books — Yellow pages — Who is DB[b] — Zone database of Domain Name Server[b]

[a] It should be examined if a database contains any information preserved by a probe data collector.

[b] An Internet database of IP addresses and fully qualified domain names (FQDN) that can identify registered persons and mangers.

Because a probe message, as defined in ISO 22837, is sent in combination with a timestamp and a location stamp at the time probe data are collected, it is possible that a probe data collector might have personal data under certain circumstances, such as a result of collecting probe data from a vehicle on private property. Such probe data that are defined as contextual data also fall under the definition of personal data.

6.2 Encryption data that can become personal data

There are some encryption schemes that identify an individual in the encryption process and other schemes that do not. In cases where an individual is identified in the encryption process, the encryption data used by probe vehicle systems, when decrypting a received probe message, can become personal data.

In cases where encryption data can identify a particular individual directly, they represent personal data. Ordinarily, encryption data consist of character strings (parameters) of symbols, numbers, etc., that have no special meaning. Thus, encryption data alone cannot directly identify a particular individual. Accordingly, encryption data can become personal data in the following situations:

— when an individual is identified in the encryption process and the encryption data can identify an individual directly;

— when an individual is identified in the encryption process, but the encryption data alone cannot identify an individual directly. However, it is possible when the encryption data are cross-checked with other databases that allow comparisons with particular individuals. Such other databases are referred to as encryption data databases.

Definitions and specific examples of encryption data that can become personal data are given in Table 2.

Table 2 — Encryption data that can become personal data

Category	Encryption data that can become personal data
Definitions	In cases where an individual is identified in the encryption process: (1) encryption data that can identify a particular individual directly or (2) encryption data used by someone possessing an encryption data database, though the encryption data cannot identify an individual directly.
Specific examples of definition (2)	Encryption data used in the decryption process by someone possessing an encryption data database in cases where the encryption scheme employs a common key established separately for each probe data sender.

6.3 Authentication data that can become personal data

Authentication is the function for establishing the validity of a claimed identity of a data source as a measure against such threats as data source spoofing and denial of service (DOS) attacks. Authentication data includes information identifying a particular data source.

In cases where authentication data can directly identify an individual, they constitute personal data. However, when authentication data consist of character strings (parameters) of symbols, numbers, etc., without any special meaning, those data alone cannot identify an individual directly. Accordingly, authentication data can become personal data in situations like those noted below:

— when authentication data can identify an individual directly;

— when reference can be made to other databases that allow comparisons between authentication data and particular individuals although the authentication data alone cannot identify an individual directly. Such other databases are referred to as authentication data database.

Definitions and specific examples of authentication data that can become personal data are given in Table 3.

Table 3 — Authentication data that can become personal data

Category	Authentication data that can become personal data
Definitions	(1) Authentication data that can identify an individual directly (2) Authentication data obtained by someone possessing an authentication data database, though the authentication data cannot identify an individual directly
Specific examples	Specific example of (1): authentication data used in a public key encryption system, including a probe data sender's public key Specific example of (2): authentication data used in a password authentication procedure and obtained by someone possessing an authentication data database

7 The basic principles

7.1 General

The basic principles refer to fundamental matters that shall be strictly observed in connection with the proper handling of personal data, in order to protect the personal data of probe data senders.

The basic principles are examined and developed on the basis of the results of the threat analysis for personal data in probe vehicle systems; see Annex A.

The framework for describing the basic principles has adopted the eight principles of the OECD Guidelines.

7.2 Collection limitation principle

a) (Limits to data collection)

Before collecting personal data, such as when contracting with the data subject, a probe data collector shall obtain the prior and unambiguous consent of the data subject or inform the data subject of the collection of personal data and the indicated purposes of use and, where appropriate, take other measures required under domestic regulations.

Choice of obtaining the consent or informing the data subject: from a viewpoint of probe vehicle systems, consent is always required when personal data are used in commercial services. However, in cases of

safety and public services, consent is not necessarily required but the knowledge of the data subject may be acceptable.

An example of withdrawing the data subject's consent after contracting: a data subject may withdraw the consent by switching off on-board equipment to send probe data, etc.

b) (Data collection methods)

A probe data collector shall not acquire personal data by fraudulent or other dishonest means.

c) (Data collection without consent)

The provision of a) shall not apply to cases in which the collecting of personal data is based on domestic laws.

d) (Exclusion of probe data capable of identifying an individual from collected probe data)

Probe data collectors shall take reasonable measures to avoid collecting data capable of identifying an individual by referring to a database, in cases where such a possibility exists, and take other measures required under domestic regulations.

An example of a measure for avoiding collection of probe data capable of identifying an individual: probe data is not collected for a certain distance from an origin in order to avoid identification of the location where an engine is started. All probe data stored in an in-vehicle system are deleted when an engine is turned off in order to avoid identification of a destination.

e) (Confirmation of a data subject's consent about probe data collection)

A probe data collector should take suitable measures to confirm the consent of a data subject about probe data collection.

An example of a measure for confirming a data subject's consent about probe data collection: an in-vehicle system is equipped with a mechanism allowing data subjects to choose whether probe data are to be collected or not.

7.3 Data quality principle

A probe data collector shall keep personal data accurate and up to date within the scope necessary for the achievement of the purposes of use.

7.4 Purpose specification principle

a) (Specification of the purposes of use)

When using personal data, a probe data collector shall specify the purposes of use of personal data.

b) (Limits on changing the purposes of use)

A probe data collector shall not change the purposes of use beyond the scope in which new purposes can reasonably be considered to be compatible with the original purposes.

c) (Change of the purposes of use requires prior consent)

Before a probe data collector changes the purposes of use beyond the scope in which new purposes can reasonably be considered to be compatible with the original purposes, it shall inform a data subject of the change or obtain prior and unambiguous consent.

7.5 Use-limitation principle

a) (Use limitation)

A probe data collector shall not use personal data, without obtaining the prior consent of the data subject, beyond the scope necessary for the achievement of the specified purposes of use.

b) (Restriction of disclosure to third parties)

A probe data collector shall not provide personal data to a third party without obtaining the prior consent of the data subject.

c) (Use without consent)

The provisions of a) and b) shall not apply to cases in which the using of personal data is based on domestic laws. Probe data collectors should grant access only to law enforcement authorities as authorized by a domestic court order or equivalent legal instrument.

7.6 Security safeguards principle

Personal data should be protected by security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

7.7 Openness principle

There shall be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data collector.

7.8 Individual participation principle

An individual is entitled:

a) to obtain from a probe data collector, or otherwise, confirmation of whether or not the probe data collector has data relating to him;

b) to have communicated to him, data relating to him:

1) within a reasonable time;

2) at a charge, if any, that is not excessive;

3) in a reasonable manner;

4) in a form that is readily intelligible to him;

c) to be given reasons if a request made under a) and b) is denied, and to be able to challenge such a denial;

d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

7.9 Accountability principle

A probe data collector shall be accountable for complying with measures which give effect to the principles stated above.

Annex A
(informative)

Threats to personal data in probe vehicle systems

Examples of threats to personal data in the process whereby probe data collectors collect data from probe data senders were identified on the basis of the reference architecture for the basic principles.

The threats were examined in relation to the eight principles of the OECD Guidelines.

Examples of threats can be summarised in two ways:

a) threats to personal data in the context of probe vehicle systems;

b) threats occurring in information/communications systems in general and not dependent on probe vehicle systems.

It is proposed that the threats in a) be examined toward developing the basic principles.

Table A.1 classifies examples of a) and Table A.2 classifies examples of b).

The examples of threats listed in Table A.1 are compared with the types of threat covered by the eight principles of the OECD Guidelines in order to identify threats that will require description in more concrete detail. The result is given in Table A.3, detailed analysis of threats.

Table A.1 — Examples of threats to personal data in the context of probe vehicle systems

No.	Threat	Place where threat occurs in the reference architecture	Overview of threat	Related to the eight principles of the OECD Guidelines
T-4	Use of a communications ID combined with probe data for purposes other than specified	Probe package receiving	An action that threatens the rights or interests of a probe data sender in cases where a communications ID represents personal data. For example, a probe data collector merges a communications ID, which should rightfully be used only for effecting communication, with a probe message and uses it for purposes other than specified.	(2) Data quality principle (3) Purpose specification principle (4) Use limitation principle
T-5	Use of encryption data for purposes other than specified	Probe payload processing	An action that threatens the rights or interests of a probe data sender in cases where the security of communications paths is secured by using an encryption procedure that can identify a particular individual. For example, a probe data collector merges encryption data, which should rightfully be used only for encryption of data on a communications path, with a probe message and uses it for purposes other than specified.	(2) Data quality principle (3) Purpose specification principle (4) Use limitation principle
T-6	Use of authentication data combined with probe data for purposes other than specified	Probe payload processing	An action that threatens the rights or interests of a probe data sender in cases where an authentication procedure is performed which can identify a particular individual. For example, a probe data collector merges authentication data, which should rightfully be used only in the authentication procedure, with a probe message and uses it for purposes other than specified.	(2) Data quality principle (3) Purpose specification principle (4) Use limitation principle
T-7	Use of data, knowable through the operation of a system, for purposes other than specified	Probe processing	An action that threatens the rights or interests of a probe data sender in cases where a probe data collector possesses personal data obtained in the course of distributing or selling in-vehicle devices or in connection with the provisions concerning probe data collection. For example, a probe data collector combines the obtained data with a probe message and uses it for purposes other than specified.	(4) Use limitation principle
T-9	Use of a probe message, from which the identity of a particular individual can be inferred, for purposes other than specified	Probe collection	An action that threatens the rights or interests of a probe data sender in cases where it is possible to infer the identity of a particular individual by cross-checking the place where probe data originated with a database possessed by a probe data collector or by a public body, company or other party. For example, the use of a probe message in such a way by a probe data collector.	(1) Collection limitation principle (4) Use limitation principle

Table A.1 (*continued*)

No.	Threat	Place where threat occurs in the reference architecture	Overview of threat	Related to the eight principles of the OECD Guidelines
T-12	Wrongful acquisition of a communications ID combined with probe data	Probe package receiving	An action that threatens the rights or interests of a probe data sender as a result of a probe data collector having surreptitiously obtained a communications ID that can identify a particular individual.	(1) Collection limitation principle
T-13	Wrongful acquisition of encryption data combined with probe data	Probe payload processing	An action that threatens the rights or interests of a probe data sender as a result of a probe data collector having surreptitiously obtained encryption data that can identify a particular individual.	(1) Collection limitation principle
T-14	Wrongful acquisition of authentication data combined with probe data	Probe payload processing	An action that threatens the rights or interests of a probe data sender as a result of a probe data collector having surreptitiously obtained authentication data that can identify a particular individual.	(1) Collection limitation principle
T-15	Automatic transmission of probe data without reflecting the intention of a probe data sender	Probe package sending	An action that threatens the rights or interests of a probe data sender in cases where probe data is always transmitted from a vehicle regardless of the intention of the probe data sender and even if the sender does not intend to transmit data.	(1) Collection limitation principle (3) Purpose specification principle
T-16	Leakage of personal data due to a software defect	Probe data sender	An action that threatens the rights or interests of a probe data sender owing to the fact that personal data stored in an in-vehicle device is transmitted because of incorrect operation caused by a software defect.	(1) Collection limitation principle

Table A.2 — Threats occurring in information/communications systems in general and not dependent on probe vehicle systems

No.	Threat	Place where threat occurs in RA	Overview of threat	Description in the eight principles of the OECD Guidelines
T-1	Attack on an in-vehicle system	Probe data sender	An action attempting to gain unauthorized access to data stored in an in-vehicle device.	(5) Security safeguards principle
T-2	Tapping or alteration of data on a communications path	Between probe package sending and probe package receiving	An action that threatens the rights or interests of a probe data sender. For example, an unauthorized third party unlawfully obtains a probe package on a communications path between an in-vehicle device and a probe data collector.	(5) Security safeguards principle
T-3	Spoofing on a communications path	Between probe package sending and probe package receiving	An action by an unauthorized third party other than a probe data collector to gain unlawful access to a probe package by using a telecommunications device or some other means.	(5) Security safeguards principle
T-8	An attack on a probe centre system	Probe data collector	An action attempting to gain unauthorized access to data stored in a probe centre system.	(5) Security safeguards principle
T-10	Intentional transmission of bogus information by multiple vehicles	Between probe package sending and probe package receiving	A concerted effort by one or more probe data senders to transmit bogus information to fool police or other authorities into thinking a serious incident has occurred at a certain location in order to leave another location unprotected against criminal or terrorist activity.	(5) Security safeguards principle
T-11	Probe system disturbance due to incorrect information sent from a malfunctioning device	Between probe package sending and probe package receiving	A probe vehicle sends incorrect information due to a device malfunction that causes the probe system to calculate that there is a dangerous situation.	(5) Security safeguards principle

Table A.3 — Detailed analysis of threats

No.	Threat	The OECD Guidelines				
		Collection limitation principle	Data quality principle	Purpose specification principle	Use limitation principle	Security safeguard principle
T-4	Use of a communications ID combined with probe data for purposes other than specified		A threat involving the use of the previous owner's communications ID after a vehicle has been sold to someone else.	A threat involving the use of an obtained communications ID in cases where the purposes of use are not specified. A threat involving the use of an obtained communications ID for purposes other than those consented to, in cases where the purpose of use is changed.	A threat involving the use of a communications ID for purposes exceeding the scope of the purposes of use consented to. A threat involving the merging of an obtained communications ID with a probe message and its provision to a third party without obtaining the data subject's prior consent. A threat involving the merging of an obtained communications ID with a probe message and its provision to a third party without informing the data subject of the relevant legal provisions or obtaining the person's consent.	

Table A.3 (*continued*)

No.	Threat	The OECD Guidelines				
		Collection limitation principle	**Data quality principle**	**Purpose specification principle**	**Use limitation principle**	**Security safeguard principle**
T-5	Use of encryption data for purposes other than specified		A threat involving the use of the previous owner's encryption data after a vehicle has been sold to someone else.	A threat involving the use of obtained encryption data in cases where the purposes of use are not specified. A threat involving the use of obtained encryption data for purposes other than those consented to, in cases where the purpose of use is changed.	A threat involving the use of encryption data for purposes exceeding the scope of the purposes of use consented to. A threat involving the merging of obtained encryption data with a probe message and its provision to a third party without obtaining the data subject's prior consent. A threat involving the merging of obtained encryption data with a probe message and its provision to a third party without informing the data subject of the relevant legal provisions or obtaining the person's consent.	

Table A.3 (*continued*)

No.	Threat	The OECD Guidelines				
		Collection limitation principle	**Data quality principle**	**Purpose specification principle**	**Use limitation principle**	**Security safeguard principle**
T-6	Use of authentication data combined with probe data for purposes other than specified		A threat involving the use of the previous owner's authentication data after a vehicle has been sold to someone else.	A threat involving the use of obtained authentication data in cases where the purposes of use are not specified. A threat involving the use of obtained authentication data for purposes other than those consented to, in cases where the purpose of use is changed.	A threat involving the use of authentication data for purposes exceeding the scope of the purposes of use consented to. A threat involving the merging of obtained authentication data with a probe message and its provision to a third party without obtaining the data subject's prior consent. A threat involving the merging of obtained authentication data with a probe message and its provision to a third party without informing the data subject of the relevant legal provisions or obtaining the person's consent.	

Table A.3 (*continued*)

No.	Threat	The OECD Guidelines				
		Collection limitation principle	**Data quality principle**	**Purpose specification principle**	**Use limitation principle**	**Security safeguard principle**
T-7	Use of data, knowable through the operation of a system, for purposes other than specified				A threat involving the use of personal data for purposes exceeding the scope of the purposes of use consented to. A threat involving the merging of obtained personal data with a probe message and its provision to a third party without informing the data subject of the relevant legal provisions or obtaining the person's consent.	
T-9	Use of a probe message, from which the identity of a particular individual can be inferred, for purposes other than specified	A threat involving the acquisition of probe data that can identify a particular individual without obtaining the data subject's prior consent to such an acquisition.			A threat involving the use of a probe data message, from which a particular individual's identity can be inferred, in a way that contravenes measures taken to deal with such cases. A threat involving the provision to a third party of a probe data message from which a particular individual's identity can be inferred, without obtaining the person's prior consent.	

Table A.3 (*continued*)

No.	Threat	The OECD Guidelines				
		Collection limitation principle	**Data quality principle**	**Purpose specification principle**	**Use limitation principle**	**Security safeguard principle**
T-12	Wrongful acquisition of a communications ID combined with probe data	A threat involving the acquisition of a communications ID that can identify a particular individual without obtaining the data subject's prior consent to such an acquisition. A threat involving the acquisition of a communications ID that can identify a particular individual without obtaining the data subject's prior consent to the purposes of use. A threat involving the acquisition of a communications ID that can identify a particular individual without informing the data subject of the relevant legal provisions or obtaining the person's consent. A threat involving the acquisition of a communications ID that can identify a particular individual other than the person who consented to such an acquisition. A threat involving the acquisition, by some means other than the method consented to, of a communications ID that can identify a particular individual.				

Table A.3 (*continued*)

No.	Threat	The OECD Guidelines				
		Collection limitation principle	**Data quality principle**	**Purpose specification principle**	**Use limitation principle**	**Security safeguard principle**
T-13	Wrongful acquisition of encryption data combined with probe data	A threat involving the acquisition of encryption data that can identify a particular individual without obtaining the data subject's prior consent to such an acquisition. A threat involving the acquisition of encryption data that can identify a particular individual without obtaining the data subject's prior consent to the purposes of use. A threat involving the acquisition of encryption data that can identify a particular individual without informing the data subject of the relevant legal provisions or obtaining the person's consent. A threat involving the acquisition of encryption data that can identify a particular individual other than the person who consented to such an acquisition. A threat involving the acquisition, by some means other than the method consented to, of encryption data that can identify a particular individual.				

Table A.3 (*continued*)

No.	Threat	The OECD Guidelines				
		Collection limitation principle	**Data quality principle**	**Purpose specification principle**	**Use limitation principle**	**Security safeguard principle**
T-14	Wrongful acquisition of authentication data combined with probe data	A threat involving the acquisition of authentication data that can identify a particular individual without obtaining the data subject's prior consent to such an acquisition. A threat involving the acquisition of authentication data that can identify a particular individual without obtaining the data subject's prior consent to the purposes of use. A threat involving the acquisition of authentication data that can identify a particular individual without informing the data subject of the relevant legal provisions or obtaining the person's consent. A threat involving the acquisition of authentication data that can identify a particular individual other than the person who consented to such an acquisition. A threat involving the acquisition, by some means other than the method consented to, of authentication data that can identify a particular individual.				

Table A.3 (*continued*)

No.	Threat	The OECD Guidelines				
		Collection limitation principle	**Data quality principle**	**Purpose specification principle**	**Use limitation principle**	**Security safeguard principle**
T-15	Automatic transmission of probe data without reflecting the intention of a probe data sender	A threat in which probe data, including personal data, continues to be collected under the terms initially agreed to, even though the driver's intention has changed and that change is not reflected in the collection process.		A threat involving the collection of probe data for purposes of use other than those consented to, in cases where the purpose of use is changed.		
T-16	Leakage of personal data due to a software defect					A threat involving the collection of probe data, including personal data, irrespective of whether a probe data sender agrees or not, owing to a software defect.

Bibliography

[1] ISO/IEC 13335-1, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

[2] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*

ICS 03.220.01; 35.240.60

Price based on 23 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.
It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™