TECHNICAL SPECIFICATION

ISO/TS 21719-3

First edition
2021-11

Electronic fee collection — Personalization of on-board equipment (OBE) —

Part 3:
Using integrated circuit(s) cards

Perception de télépéage — Personnalisation des équipements embarqués —

Partie 3: Utilisation de cartes à circuit(s) intégré(s)

Contents

Page

Foreword

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

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

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

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

For an explanation of 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 www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/ TC 278, *Intelligent transport systems*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

A list of all parts in the ISO/TS 21719 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

On-board equipment (OBE) is an in-vehicle device that contains one or more application instances in order to support different intelligent transportation system (ITS) implementations such as electronic fee collection (EFC).

To assign the EFC application in the OBE to a certain user and/or vehicle, personalization is performed. This means that unique user and vehicle related data are transferred to and stored in the OBE.

CEN/TR 16152 assesses many aspects of the personalization process and it defines the overall personalization assets (application data, application keys and vehicle-related data).

Different communication media may be used for transferring the personalization assets to the OBE. An overall message exchange framework and needed security functionality may be applied, for all media common procedures, in order to ensure data protection and integrity.

By standardizing the personalization procedure, compatibility of personalization equipment (PE) is supported. The entity responsible for the personalization, such as a toll service provider, will further be able to outsource parts of, or a complete, personalization to a third party or to another service provider or personalization agent.

The scope of the personalization functionality is illustrated in Figure 1. It is limited to the transfer of data between the PE and the OBE by using integrated circuit(s) cards (ICCs).
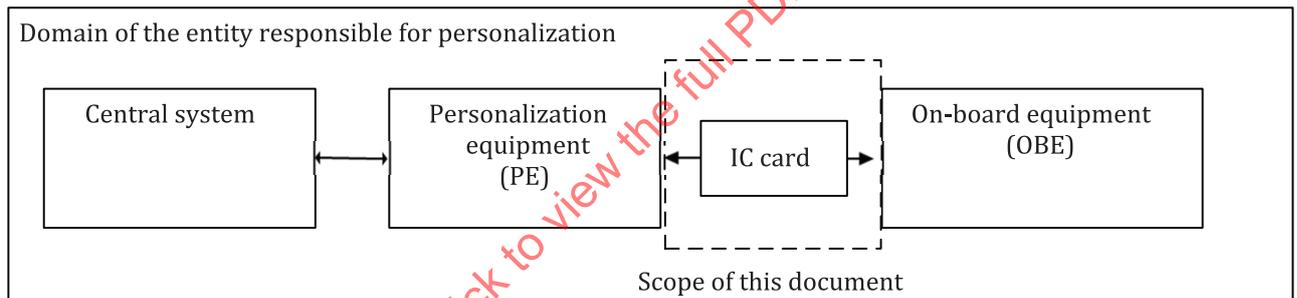
Figure 1 — Scope of this document (box delimited by a dotted line)

This document defines a complete application profile (AP), using ICCs in accordance with the ISO/IEC 7816-3, ISO/IEC 7816-4, ISO/IEC 14443-3, ISO/IEC 14443-4 and the ISO/IEC 15693 series (Table 1), in accordance with the personalization functionality described in ISO/TS 21719-1.

Figure 2 shows the relationship of this document.

There are two interfaces (PE-ICC, ICC-OBE). For further details, see Annex A.

This document may be supplemented by a set of specifications which define the conformity evaluation of equipment to the conformance requirements contained in this document.
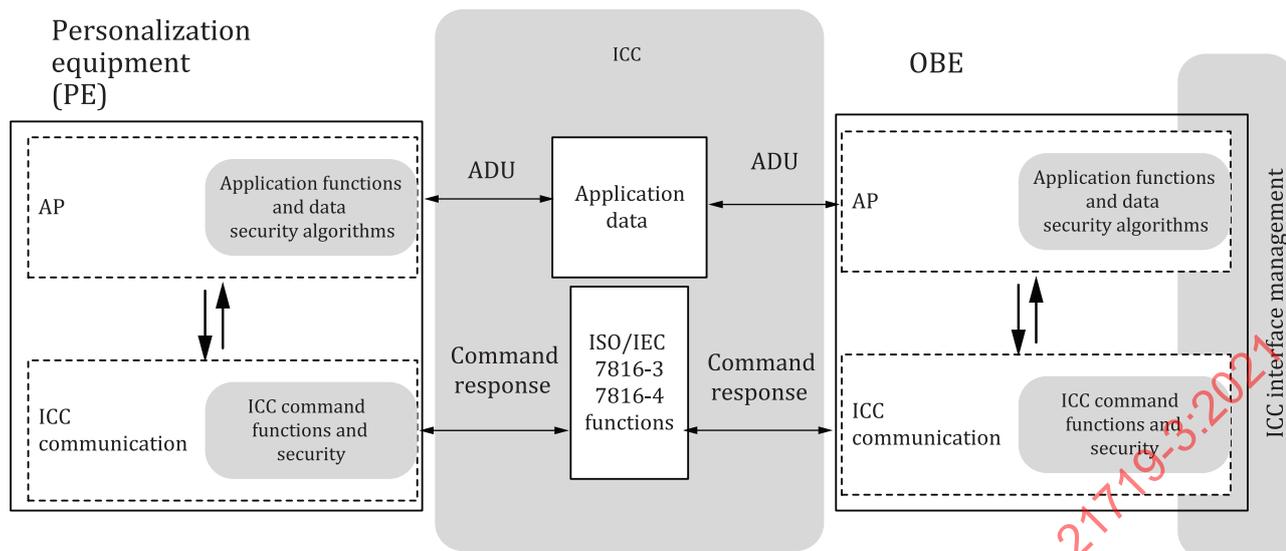
Figure 2 — Relationship between this document and ICC communication

Electronic fee collection — Personalization of on-board equipment (OBE) —

Part 3:
Using integrated circuit(s) cards

1 Scope

This document specifies:

— personalization interface;

— physical systems: on-board equipment (OBE), personalization equipment (PE) and integrated circuit(s) cards (ICCs);

— electronic fee collection (EFC) personalization functions between the PE and the OBE in accordance with ISO/TS 21719-1 when using an ICC;

— data and security elements that are transferred between the PE and the OBE using the ICC.

It is outside the scope of this document to define:

— conformance procedures and test specifications;

— setting-up of operating organizations (e.g. toll service provider, personalization agent, trusted third party, etc.);

— legal issues;

— the exact commands and security functionality within ISO/IEC 7816-4 used by the PE and the OBE, respectively, to interface an ICC.

NOTE   Some of the issues that are outside the scope of this document are the subject of separate standards prepared by CEN/TC 278 and ISO/TC 204.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

ISO/IEC 7816-4, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 14443-3, *Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision*

ISO/IEC 14443-4, *Cards and security devices for personal identification — Contactless proximity objects — Part 4: Transmission protocol*

ISO/IEC 15693 (all parts), *Cards and security devices for personal identification — Contactless vicinity objects*

3 Terms and definitions

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

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

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

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

3.1
attribute
addressable package of data consisting of a single data element or structured sequences of data elements

[SOURCE: ISO/TS 17573-2:2020, 3.13]

3.2
base standard
approved International Standard, Technical Specification or ITU-T Recommendation

Note 1 to entry: This includes but is not limited to approved standard deliverables from ISO, ITU, CEN, CENELEC, ETSI and IEEE.

[SOURCE: ISO/TS 17573-2:2020, 3.23]

3.3
electronic fee collection
EFC
fee collection by electronic means

[SOURCE: ISO/TS 17573-2:2020, 3.70]

3.4
international standardized profile
internationally agreed-to, harmonized document which describes one or more *profiles* (3.9)

[SOURCE: ISO/TS 17573-2:2020, 3.102]

3.5
on-board equipment
OBE
all required equipment on-board a vehicle for performing required *electronic fee collection (EFC)* (3.3) functions and communication services

[SOURCE: ISO/TS 17573-2:2020, 3.126]

3.6
OBE personalization
transferring *personalization assets* (3.7) to the *on-board equipment (OBE)* (3.5)

[SOURCE: ISO/TS 17573-2:2020, 3.123]

3.7
personalization assets
specific data stored in the *on-board equipment (OBE)* (3.5) related to the user and the vehicle

[SOURCE: ISO/TS 17573-2:2020, 3.137]

3.8
personalization equipment
PE
equipment for transferring *personalization assets* (3.7) to the *on-board equipment (OBE)* (3.5)

[SOURCE: ISO/TS 17573-2:2020, 3.138]

3.9
profile
set of requirements and selected options from *base standards* (3.2) or *international standardized profiles* (3.4) used to provide a specific functionality

[SOURCE: ISO/TS 17573-2:2020, 3.146]

3.10
toll service provider
entity providing toll services in one or more toll domains

Note 1 to entry: In other documents, the terms "issuer" or "contract issuer" are sometimes used.

Note 2 to entry: The toll service provider may provide the *on-board equipment (OBE)* (3.5) or may provide only a magnetic card or a smart card to be used with the OBE provided by a third party (e.g. a mobile telephone and a SIM card can be obtained from different parties).

Note 3 to entry: The toll service provider is responsible for the operation (functioning) of the OBE with respect to tolling.

[SOURCE: ISO/TS 17573-2:2020, 3.206, modified — Notes 1, 2 and 3 have been added.]

3.11
transaction
whole of the exchange of information between two physically separated communication facilities

[SOURCE: ISO/TS 17573-2:2020, 3.211]

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

ADU   application data unit

AP   application profile

ATR   answer-to-reset

AVEI   automatic vehicle and equipment identification

EFC   electronic fee collection

ICC   integrated circuit(s) card

ID   identifier

ICS   implementation conformance statement

IUT   implementation under test

OBE   on-board equipment

PE   personalization equipment

PICS   protocol implementation conformance statement

5   Conformance

5.1   General

This clause describes in general terms what it means to be in conformity with this document.

Annex A provides a PICS proforma that shall be filled in by the concerned equipment supplier or its representative in order to declare conformance of an implementation with this document.

5.2   Base standards

This document defines one application profile (AP). The base standards that this AP is based upon are:

— standards for security functionality, e.g. ISO/IEC 9797-1;

— standards for EFC application definition, notably ISO 14906;

— standards for ICC interface definition, e.g. ISO/IEC 7816-4.

An overview of the relationship and references between base standards and this AP is illustrated in Figure 3.

All requirements specified in this document are either choices made from these base standards or more specific based on the general provisions of these base standards.
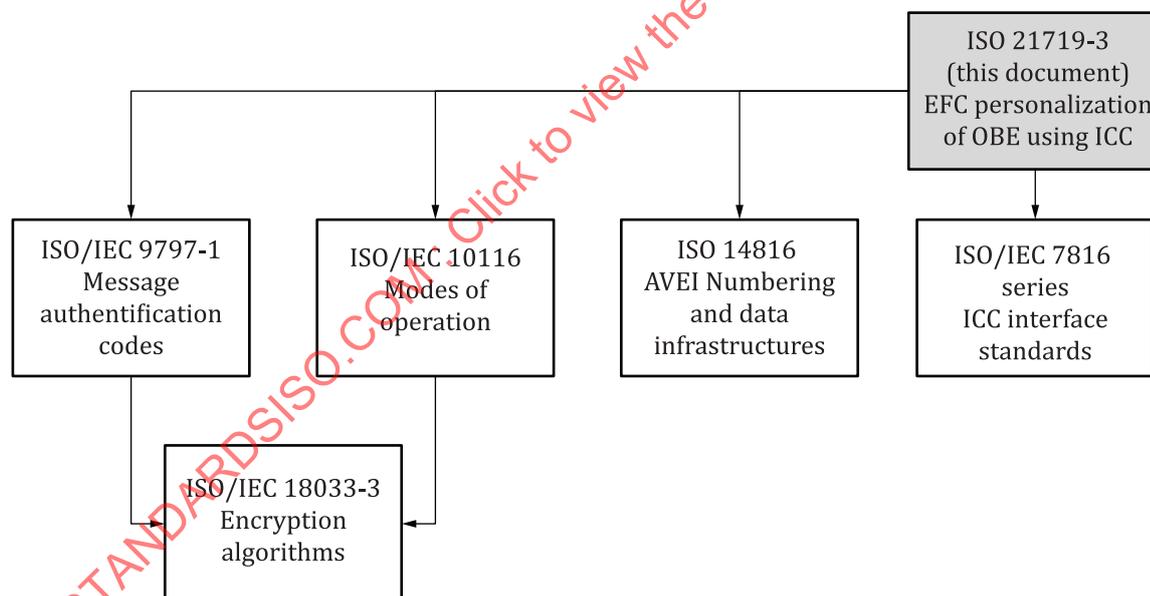
Figure 3 — Relationship and references between base standards and this document

5.3   Main contents of an EFC personalization AP

The conformance requirements of an AP are divided between requirements for OBE and PE. The requirements are listed separately for OBE and PE. This applies for all parts, requirements, PICS and conformance testing.

The conformance requirements of an AP according to this document include the following parts (divided into separate requirements for OBE and PE):

— ICC interface requirements;

— EFC personalization functions;

— security requirements;

— transaction requirements.

6 Personalization overview

6.1 Process

The overall personalization process is described in ISO/TS 21719-1:2018, 5.1.

"Personalization" means that an existing EFC application structure in the OBE is populated with personalization assets such as user or vehicle-related data.

Creation of the EFC application and entering initial data, such as initial security keys, is performed before the personalization and is out of the scope of this document.

During personalization, the ICC is moved between the ICC reader interfaces of the PE and the OBE in order for the data transfer to take place according to this document. Application data and security keys are during the personalization process transferred to the OBE in an attribute list that is stored on the ICC by the PE. Writing and reading of data in the ICC is done by using standardized ICC commands and security functionality according to the ICC interface requirements defined in this document.

6.2 System architecture

The overall system architecture is described in ISO/TS 21719-1:2018, 5.3.

For personalization via the ICC interface, both the OBE and the PE shall contain an ICC reader with ICC communication functionality, and the application services as described in this specification.

Security functionality and secure key storage may either be implemented within the PE or the PE may be connected to a central system where this functionality may reside. This is out of the scope of this document.

7 OBE requirements

7.1 General

This clause contains the conformance requirements on the OBE for personalization data transfer from an ICC.

7.2 ICC interface requirements

7.2.1 General

The OBE shall support at least one of the ICC interfaces as described in Table 1.

Table 1 — Supported ICC interfaces

ICC interface	Application layer	Lower layers
Contact interface	ISO/IEC 7816-4	ISO/IEC 7816-3
Contactless interface	ISO/IEC 7816-4	ISO/IEC 14443-3
		ISO/IEC 14443-4
		ISO/IEC 15693 (all parts)

7.2.2 Case of contact interface

The PE and the OBE shall support suitable application layer commands in ISO/IEC 7816-3 and ISO/IEC 7816-4 in order to support reading and writing application service data for personalization according to this document. No further requirements are defined in this document regarding the ICC communication commands or the ICC security functionality to be used.

7.2.3 Case of contactless interface

The PE and the OBE shall support suitable application layer commands in ISO/IEC 7816-4, ISO/IEC 14443-3, ISO/IEC 14443-4 and the ISO/IEC 15693 series in order to support reading and writing application service data for personalization according to this document. No further requirements are defined in this document regarding the ICC communication commands or the ICC security functionality to be used.

7.3 OBE personalization functions

7.3.1 OBE personalization functions

The PE and the OBE shall offer the following functions in order to support personalization:

— interface between the PE and the ICC:

— initialization of communication with the ICC;

— command and response: writing of data (used to update data in the ICC);

— command and response: reading of data (used to check data in the ICC);

— terminate session with the ICC;

— interface between the OBE and the ICC:

— initialization of communication with the ICC;

— command and response: reading of data (used to update data in the OBE);

— command and response: writing of data (used to update data in the ICC);

— terminate session with the ICC.

7.3.2 Initialization and termination

For the use of an ICC, the PE and the OBE shall provide the following function:

— initialization for establishing communication with certain ICCs in accordance with ISO/IEC 7816-3, ISO/IEC 7816-4, ISO/IEC 14443-3 and the ISO/IEC 15693 series.

After data transmission, the OBE shuts down the power supply to the ICC for terminating the communication.

Security mechanisms for performing the ICC commands are out of the scope of this document.

7.3.3 Writing of data

The main functionality of personalization is to write or update data to already existing data fields (attributes) from the PE to the EFC application in the OBE by the ICC (see Table 2) and to write Lock Flag from the EFC application in the OBE to the PE by the ICC (see Table 4).

Lock Flag proves that the setup was completed successfully.

See Annex B for the flow of writing.

Application attributes are defined with their container types in the application interface standard ISO 14906. Security keys are stored in attributes with container type 2 (octet string).

The ICC contains the personalization parameters as an attribute data structure (octet string) shown in Table 2 to be written into the OBE EFC application. The personalization parameters are assumed to be stored to the ICC memory by the PE, using commands in accordance with ISO/IEC 7816-4.

The OBE shall confirm the PE header whether the authorized PE writes the personalization parameter or not.

Table 2 — Personalization parameters content definition

Parameter	Length (octets)	Definition
Option_indicator request	1	Always present Bit string that describes what optional parameters are present in the personalization parameters. It is defined as follows: b_7 – AttributeList present b_6 – AttributeListEncrypted present b_0 – PE header Table 3 shows the allowed combinations of the option indicator.
PE header	n	Optional Identification data for confirming the authorized PE by the OBE.
AttributeList	n.	Optional An attributeList in accordance with ISO 14906. Either the parameter AttributeList or AttributeListEncrypted shall be present.
AttributeListEncrypted	m.	Optional An octet string that contains an AttributeList that has been padded to even 16 octet blocks and encrypted. Either the parameter AttributeList or AttributeListEncrypted shall be present.

Table 3 — Allowed combinations of option indicators in request

Parameter	Option set 1	Option set 2
b_7 – AttributeList present	X	
b_6 – AttributeListEncrypted present		X

Table 4 — Lock Flag definition

Parameter	Length (octets)	Definition
Option_indicator request	1	Always present Bit string that describes what optional parameters are present in the personalization parameters. It is defined as follows: b_7 – AttributeList present b_6 – AttributeListEncrypted present b_0 – PE header Table 3 shows the allowed combinations of the option indicator.
PE header	n	Optional Identification data for confirming the authorized PE by the OBE.
Lock Flag (Lock Flag proves that the setup was completed successfully)	1.	Optional The setup was completed successfully. 0: initial 1: completed successfully 2: failure Either Lock Flag or Lock Flag Encrypted shall be present.
Lock Flag Encrypted	m.	Optional An octet string that contains Lock Flag that has been padded to even 16 octet blocks and encrypted. Either Lock Flag or Lock Flag Encrypted shall be present.

7.3.4 Reading of data

The main functionality of personalization is the reading by the OBE of the ICC data at the start of setup and the PE reads the Lock Flag of the ICC after the setup.

See Annex B for the flow of reading.

7.4 Security requirements

This document describes security features and mechanisms based on the security framework defined in ISO 19299.

All security functionality for ICC communication is implemented in accordance with ISO/IEC 7816-4 and exact functionality or algorithms are not further specified in this document.

The end-to-end security between the PE and the OBE that is specified within the scope of this document is:

— the OBE ID is installed in the OBE at manufacture;

— the OBE ID and Vehicle Class are input from the PE to the ICC;

— the ICC is inserted into the OBE;

— it is verified whether the OBE ID of the OBE and the OBE ID of the ICC are the same;

— if the numbers are the same, setup is started;

— if the numbers are different, an error will occur and setup is not started;

— when setup is complete, the OBE writes Lock Flag to the ICC.

7.5 Transaction requirements

An OBE conforming to this document shall be able to perform a personalization transaction that includes the functions as described in 7.3.

Annex B provides an example of a personalization transaction when using an ICC.

8 PE requirements

8.1 General

This clause contains the normative conformance requirements on the PE for the ICC reader.

8.2 ICC interface requirements

The PE shall be able to support an ICC interface as described in 7.2.

8.3 PE personalization functions

The PE shall be able to create the personalization parameter and write it to the ICC as specified in 7.3.3.

Annex A
(normative)

Protocol implementation conformance statement (PICS) proforma

A.1 General

In order to evaluate the conformance of a particular implementation, it is necessary to have a statement of those capabilities and options that have been implemented. This is called an "implementation conformance statement (ICS)" or, more specifically when it covers transactions, a "protocol implementation conformance statement (PICS)".

This annex provides a PICS proforma that shall be filled in by the concerned equipment supplier or its representative in order to declare conformance of an implementation with this document.

A.2 Purpose and structure

The purpose of this PICS proforma is to provide a mechanism whereby a supplier of an implementation of the requirements specified in this document can provide information about the implementation in a standardized manner.

The PICS proforma is subdivided into sections for the following categories of information:

— identification of the implementation;

— identification of the protocol;

— global statement of conformance;

— PICS proforma tables.

A.3 Instructions for completing PICS proforma

A.3.1 Definition of support

A capability is said to be supported if the implementation under test (IUT) can:

— generate the corresponding operation parameters (either automatically or because the end user requires that capability explicitly);

— interpret, handle and, when required, make available to the end user the corresponding error or result.

A protocol element is said to be supported for a sending implementation if it is able to generate it under certain circumstances (either automatically or because the end user requires relevant services explicitly).

A protocol element is said to be supported for a receiving implementation if it is correctly interpreted and handled and, when appropriate, made available to the end user.

A.3.2 Status column

This column in the tables indicates the level of support required for conformance. The values are as follows:

m Mandatory support is required.

o Optional support is permitted for conformance to the standard. If implemented, it shall conform to the specifications and restrictions contained in the standard. These restrictions can affect the optionality.

c The item is conditional (support of the capability is subject to a predicate).

c: m The item is mandatory if the predicate is true, optional otherwise.

— The item is not applicable.

i The item is outside the scope of this PICS.

In the PICS proforma tables, every leading item marked "m" shall be supported by the IUT. Sub-items marked "m" shall be supported if the corresponding leading item is supported by the IUT.

A.3.3 Response and support columns

These columns (see Tables A.1 to A.9) shall be completed by the supplier or its representative to indicate the level of implementation of each item.

The proforma has been designed with a support column (see Tables A.4, A.5 and A.9) that shall be completed with the following values:

Y Yes, the item has been implemented.

N No, the item has not been implemented.

— The item is not applicable.

All entries within the PICS proforma shall be made in ink. Alterations to such entries shall be made by crossing out, neither erasing nor making the original entry illegible, and by writing the new entry alongside. All such alterations to records shall be initialized by the person who made them.

A.3.4 Item reference numbers

Each line within the PICS proforma which requires that implementation details be entered is numbered at the left-hand edge of the line. This numbering is included as a mean of uniquely identifying all possible implementation details within the PICS proforma. This referencing is used both inside the PICS proforma and for references from other test specification documents.

The means of referencing individual responses is done in the following sequence:

a) a reference to the smallest individual response enclosing the relevant item;

b) a solidus character ("/");

c) the reference number of the row in which the response appears;

d) if, and only if, more than one response occurs in the row identified by the reference number, implicit labelling of each possible entry as "a", "b", "c", etc., from left to right, with this letter appended to the sequence.

A.4 PICS proforma for OBE

A.4.1 Identification of the implementation

The proforma given in Tables A.1, A.2 and A.3 are to be used to identify the implementation on the OBE side.

Table A.1 — Identification of PICS

Item no.	Question	Response
1	Date of statement (DD/MM/YY)	
2	PICS serial number	
3	ISO/TS 21719-3 version	
4	Other information	

Table A.2 — Identification of the OBE supplier

Item no.	Question	Response
1	Organization name	
2	Contact name	
3	Address	
4	Telephone number	
5	Email address	
6	Other information	

Table A.3 — Identification of the OBE

Item no.	Question	Response
1	Brand name	
2	Type, version	
3	Manufacturer ID	
4	Equipment class	
5	Serial numbers of the supplied unit(s)	
6	OBE ID	
7	Vehicle class	
8	Other information	

A.4.2 Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No) ....

A.4.3 PICS proforma tables

Table A.4 — Implemented ICC interfaces

Item no.	Element	Reference	Status[a]	Support
1	ICC contact interface	7.2.1	o	
2	ICC contactless interface	7.2.1	o	
[a] One of the ICC interfaces shall be implemented.				

Table A.5 — Implemented setup functions

Item no.	Element	Reference	Status	Support
1	Initialization	7.3.2	m	
2	Writing of data	7.3.3	m	
3	Reading of data	7.3.4	m	

A.5   PICS proforma for PE

A.5.1   Identification of the implementation

The proforma given in Tables A.6, A.7 and A.8 are to be used to identify the implementation on the PE side.

Table A.6 — Identification of PICS

Item no.	Question	Response
1	Date of statement (DD/MM/YY)	
2	PICS serial number	
3	ISO/TS 21719-3 version	
4	Other information	

Table A.7 — Identification of the PE supplier

Item no.	Question	Response
1	Organization name	
2	Contact name	
3	Address	
4	Telephone number	
5	Email address	
6	Other information	

Table A.8 — Identification of the PE

Item no.	Question	Response
1	Brand name	
2	Type, version	
3	Serial numbers of the supplied unit(s)	
4	OBE ID	
5	Vehicle class	
6	Other information	

A.5.2   Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No) ....

A.5.3   PICS proforma table

Table A.9 — Implemented ICC interfaces

Item no.	Element	Reference	Status[a]	Support
1	ICC contact interface	7.2	o	
2	ICC contactless interface	7.2	o	
[a] One of ICC interfaces shall be implemented.				