TECHNICAL SPECIFICATION

ISO/TS 21719-2

First edition
2018-02

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

Part 2: Using dedicated short-range communication

Perception de télépéage — Personnalisation des équipements embarqués —

Partie 2: Utilisation des communications dédiées à courte portée

Reference number
ISO/TS 21719-2:2018(E)

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

Contents

Page

Foreword

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

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

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

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

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

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

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

Introduction

On-board equipment (OBE) is an in-vehicle device that is able to contain one or more application instances in order to support different intelligent transportation system (ITS) implementations such as electronic fee collection (EFC). Examples of EFC applications are road toll collection/road charging, local augmentation (LAC) or compliance checking (CCC).

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

The CEN/TR 16152 already assessed many aspects of the personalization process and it also defined the overall personalization assets as; application data, application keys and vehicle data.

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

By standardizing the personalization procedure, compatibility of personalization equipment is supported, and the entity responsible for the personalization, e.g. 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.

This document defines a complete application profile using the personalization functionality described in ISO/TS 21719-1, on top of a CEN DSRC stack according to the RTTT communication profiles in EN 13372 and using the EFC Application Interface according to ISO 14906.

This document further defines in the annexes the use of this application profile on top of other DSRC communication stacks that are compliant with the application layer interfaces as defined in ISO 14906 and EN 12834.

This document may be complemented by a set of standards defining conformity evaluation of the conformance requirements.

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

Part 2: Using dedicated short-range communication

1 Scope

This document specifies

— personalization interface: dedicated short-range communication (DSRC),

— physical systems: on-board equipment and the personalization equipment,

— DSRC-link requirements,

— EFC personalization functions according to ISO/TS 21719-1 when defined for the DSRC interface, and

— security data elements and mechanisms to be used over the DSRC interface.

Protcol information conformance statement (PICS) proforma is provided in Annex B, whereas security computation examples are provided in Annex E.

The scope of the personalization functionality is illustrated in Figure 1 and it is limited to the DSRC interface between the personalization equipment (PE) and the OBE.

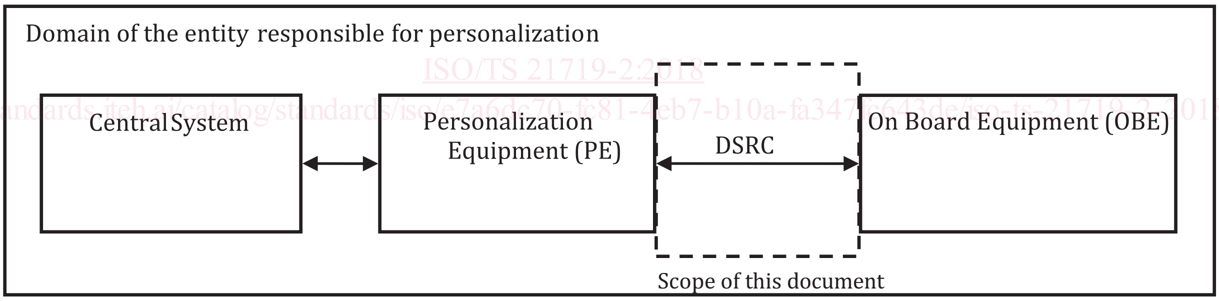
Domain of the entity responsible for personalization
Central System
Personalization Equipment (PE)
DSRC
On Board Equipment (OBE)
Scope of this document

Figure 1 — Scope for this document (box delimited by a dotted line)

It is outside the scope of this document to define

— conformance procedures and test specification (this is provided in a separate set of standards),

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

— legal issues.

NOTE Some of these issues are subject to separate standards prepared by CEN/TC 278, ISO/TC 204 or ETSI ERM.

Figure 2 shows the scope of this document from a DSRC-stack perspective.

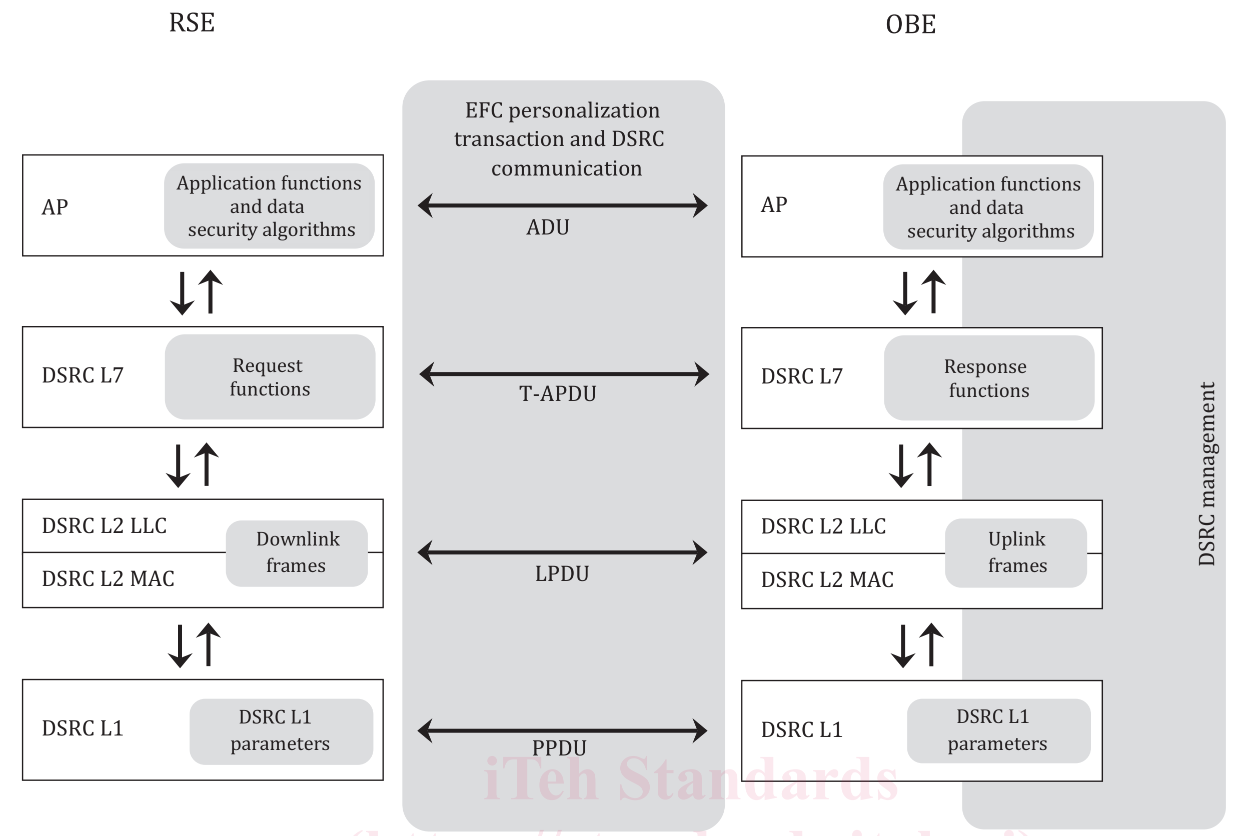

Figure 2 — Relationship between this document and DSRC-stack elements

2 Normative references

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

ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 10116:2017, *Information technology — Security techniques — Modes of operations for an n-bit cipher*

ISO 14906, *Electronic fee collection — Application interface definition for dedicated short-range communication*

ISO 15628, *Intelligent transport systems — Dedicated short range communication (DSRC) — DSRC application layer*

ISO/IEC 18033-3:2010, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

EN 12834, *Road transport and traffic telematics — Dedicated Short Range Communication (DSRC) — DSRC application layer*

EN 15509:2014, *Electronic Fee Collection — Interoperability application profile for DSRC*

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:

— IEC Electropedia: available at www.electropedia.org

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

3.1
access credentials
trusted attestation or secure module that establishes the claimed identity of an object or application

Note 1 to entry: The access credentials carry information needed to fulfil access conditions in order to perform the operation on the addressed element in the OBE. The access credentials can carry passwords, as well as cryptographic based information such as authenticators.

[SOURCE: EN 15509:2014, 3.1]

3.2
attribute
addressable package of data consisting of a single *data element* (3.10) or structured sequences of data elements

[SOURCE: ISO 17575-1:2016, 3.2]

3.3
authentication
security mechanism allowing verification of the provided identity

[SOURCE: EN 301 175 V1.1.1:1998, 3]

3.4
authenticator
data, possibly encrypted, that is used for *authentication* (3.3)

[SOURCE: EN 15509:2014, 3.3]

3.5
base standard
approved International Standard or ITU-T Recommendation

[SOURCE: ISO/IEC TR 10000-1:1998, 3.1.1]

3.6
cryptography
principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorized use

[SOURCE: EN 15509:2014, 3.6]

3.7
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO/TS 19299:2015, 3.24, modified — the term “integrity” has been changed to “data integrity”.]

3.8
data privacy
rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information

[SOURCE: ISO/TS 19299:2015, 3.32]

3.9
electronic fee collection
EFC
fee collection by electronic means

[SOURCE: ISO 12855:2015, 3.6]

3.10
element
DSRC directory containing application information in the form of *attributes* (3.2)

[SOURCE: ISO 14906:2011, 3.11, modified — the definition has been revised.]

3.11
international standardized profile
internationally agreed-to, harmonized document which describes one or more *profiles* (3.16)

[SOURCE: ISO/IEC TR 10000-1:1998, 3.1.2]

3.12
on-board equipment
OBE
required equipment on-board a vehicle for performing required *electronic fee collection* (*EFC*) (3.9) functions and communication services

3.13
OBE personalization
process of transferring *personalization assets* (3.14) to the *on-board equipment* (*OBE*) (3.12)

3.14
personalization assets
specific data stored in the *on-board equipment* (*OBE*) (3.12) related to the user and the vehicle

3.15
personalization equipment
equipment for transferring *personalization assets* (3.14) to the *on-board equipment* (*OBE*) (3.12)

3.16
profile
set of requirements and selected options from *base standards* (3.5) or international standardized profiles used to provide a specific functionality

[SOURCE: ISO/IEC TR 10000-1:1998, 3.1.4 — modified]

3.17
service primitive
elementary communication service provided by the application layer protocol to the application processes

Note 1 to entry: The invocation of a service primitive by an application process implicitly calls upon and uses services offered by the lower protocol layers.

[SOURCE: ISO 14906:2011, 3.18, modified — the scope of application has been deleted.]

3.18
toll charger
entity which levies toll for the use of vehicles in a toll domain

[SOURCE: ISO 17573:2010, 3.16, modified — the definition has been revised.]

3.19
toll service provider
entity providing toll services in one or more toll domains

Note 1 to entry: The toll service provider is responsible for the configuration and operation (functioning) of the OBE with respect to tolling.

[SOURCE: ISO 17573:2010, 3.23, modified — the definition has been revised and Notes 1 and 2 have been deleted.]

3.20
transaction
whole of the exchange of information between two physically separated communication facilities

[SOURCE: ISO 17575-1:2016, 3.21]

4 Abbreviated terms and symbols

AC_CR	access credentials (see ISO 14906)
ADU	application data unit (see ISO 14906)
APDU	application protocol data unit (see ISO 14906)
AP	application process (see ISO 14906)
ASN.1	abstract syntax notation one (see ISO/IEC 8824-1)
BST	beacon service table (see ISO 14906)
CCC	compliance check communication (see ISO 12813)
DSRC	dedicated short-range communication
e [key] (value)	encryption of the value using the key
EID	element identifier (see ISO 14906)
EFC	electronic fee collection (see ISO 17573)
IAP	interoperable application profile (see EN 15509)
ICS	implementation conformance statement
ISP	international standardized profile (see ISO/IEC TR 10000-1)
IUT	implementation under test
L1	Layer 1 of DSRC (physical layer)
L2	Layer 2 of DSRC (LLC and MAC layer)
L7	Layer 7 of DSRC (application layer)
LAC	localization augmentation communication (see ISO 13141)
LLC	logical link control (see EN 12795)
LSDU	link service data unit
MAC	media access control (see EN 12795)

OBE	on-board equipment
PE	personalization equipment
PICS	protocol implementation conformance statement
T-APDU	transfer-application protocol data unit
VST	vehicle service table (see ISO 14906)

5 Conformance

5.1 General

This clause describes in general terms what it means to be conformant with (the profile in) this document.

5.2 Base standards

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

- standards for security functionality;
- standards for EFC application definition as, e.g. ISO 14906;
- standards for the DSRC communication stack definition.

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

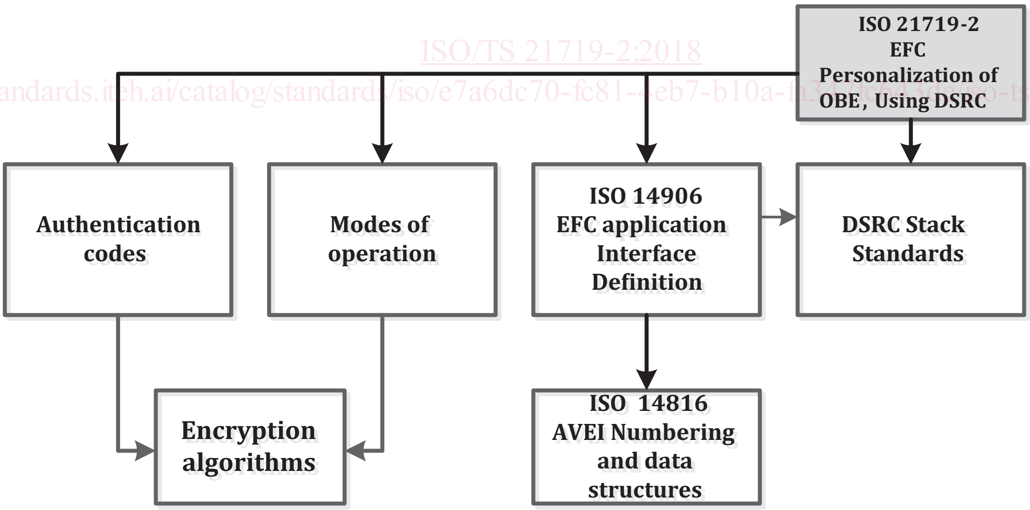

Figure 3 — Relationship and references between base standards and this document

All requirements defined in this document are either choices made from these base standards or more specific and limited requirement based on the general provisions of these standards.

5.3 Main contents of an EFC Personalization AP

The conformance requirements of an AP are divided between requirements for the on-board equipment (OBE) and the personalization equipment (PE). The requirements are listed separately for OBE and PE. This applies for all parts, requirements, PICS and conformance testing.