ICS 03.220.20, 35.240.60 PREDBEŽNÁ SLOVENSKÁ TECHNICKÁ NORMA Marec 2019

STN P	**Elektronický výber poplatkov Personalizácia palubného zariadenia (OBE) Časť 2: Používanie špecializovanej komunikácie krátkeho dosahu (ISO/TS 21719-2: 2018)**	**STN P CEN ISO/TS 21719-2** 01 8612

Electronic fee collection - Personalization of on-board equipment (OBE) - Part 2: Using dedicated short-range communication (ISO/TS 21719-2:2018)

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 02/19

Táto predbežná STN je určená na overenie. Pripomienky zasielajte ÚNMS SR najneskôr do februára 2020.

Obsahuje: CEN ISO/TS 21719-2:2018, ISO/TS 21719-2:2018

128191

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN ISO/TS 21719-2

February 2018

ICS 03.220.20; 35.240.60

English Version

Electronic fee collection - Personalization of on-board equipment (OBE) - Part 2: Using dedicated short-range communication (ISO/TS 21719-2:2018)

Perception de télépéage - Personnalisation des équipements embarqués - Partie 2: Utilisation des communications dédiées à courte portée (ISO/TS 21719-2:2018)

Elektronische Gebührenerhebung - Personalisierung von Onboard Einrichtungen - Teil 2: Verwendung von dedizierter Nahbereichskommunikation (ISO/TS 21719-2:2018)

This Technical Specification (CEN/TS) was approved by CEN on 2 February 2018 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. CEN ISO/TS 21719-2:2018 E

Contents

Page

European foreword..... 3

European foreword

This document (CEN ISO/TS 21719-2:2018) has been prepared by Technical Committee ISO/TC 204 "Intelligent transport systems" in collaboration with Technical Committee CEN/TC 278 “Intelligent transport systems”, the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/TS 21719-2:2018 has been approved by CEN as CEN ISO/TS 21719-2:2018 without any modification.

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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **2**
3 Terms and definitions ... **2**
4 Abbreviated terms and symbols ... **5**
5 Conformance ... **6**
5.1 General ... 6
5.2 Base standards ... 6
5.3 Main contents of an EFC Personalization AP ... 6
6 Personalization overview ... **7**
6.1 Process ... 7
6.2 System architecture ... 7
7 OBE requirements ... **7**
7.1 General ... 7
7.2 DSRC lower layer requirements ... 7
7.2.1 Supported DSRC stacks ... 7
7.2.2 CEN DSRC stack ... 8
7.3 OBE personalization functions ... 8
7.3.1 General ... 8
7.3.2 Initialization and termination ... 9
7.3.3 Retrieving OBE identifier ... 9
7.3.4 Writing of data ... 9
7.4 Security requirements ... 11
7.5 Transaction requirements ... 13
8 Personalization equipment requirements ... **13**
8.1 General ... 13
8.2 DSRC lower layer requirments ... 13
8.2.1 Supported DSRC stacks ... 13
8.2.2 CEN DSRC stack ... 13
8.3 PE personalization functions ... 13
8.4 Security requirements ... 14
8.5 Transaction requirements ... 14
Annex A (normative) **Security calculations** ... **15**
Annex B (normative) **PICS proforma** ... **20**
Annex C (normative) **Personalization of ES 200 674-1 compliant OBEs** ... **25**
Annex D (informative) **Transaction example** ... **30**
Annex E (informative) **Security computation example** ... **35**
Bibliography ... **39**

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.

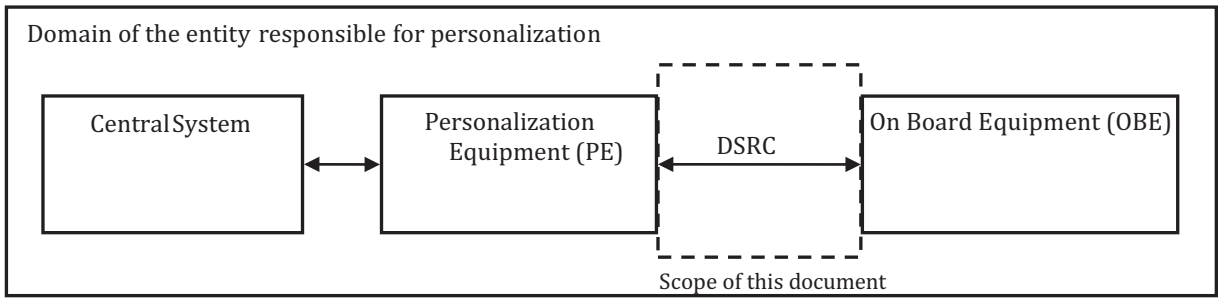

Figure 1 — Scope for this document (box delimited by a dotted line)

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.

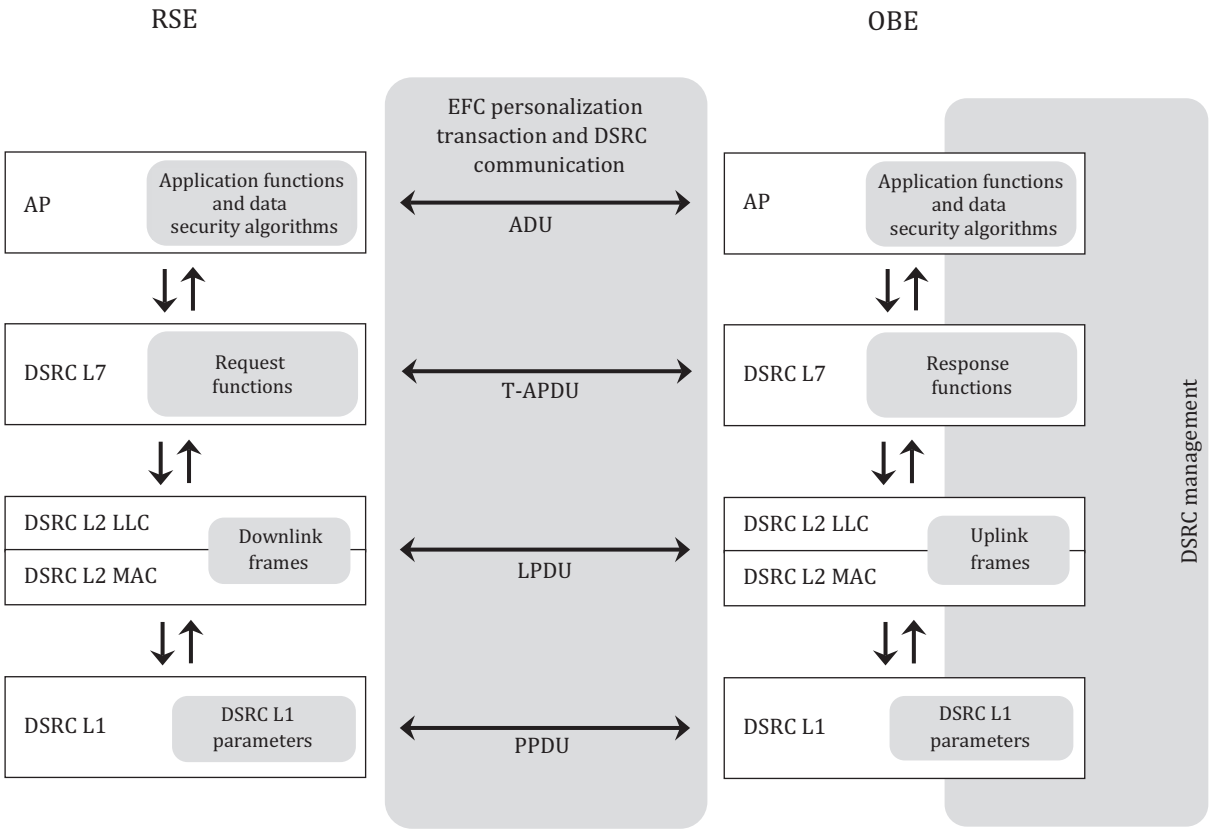

Figure 2 — Relationship between this document and DSRC-stack elements

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*