~~ISO/TC 204/SC~~

ISO/TC 204

ISO/DTS 21719-2

~~Second edition~~

2022-~~02~~05-27

~~ISO/TC 204/WG 5~~

ISO/TC 204/WG 5

Secretariat: ~~ANSI~~ANSI

Electronic fee collection — Personalization of on-board equipment (OBE) — Part 2: Using dedicated short-range ~~comunication~~communication

Perception de télépéage — Personnalisation des équipements embarqués — Partie 2: Utilisation des communications à courte portée

Document type:
Document subtype:
Document stage:
Document language:

Style Definition: List Continue 5: Font: Indent: Hanging: 0.71 cm, Don't add space between paragraphs of the same style

Style Definition: RefNorm

Style Definition: Base_Text: Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

Style Definition: Body Text_Center

Style Definition: Code: Tab stops: 0.57 cm, Left + 1.15 cm, Left + 1.72 cm, Left + 2.3 cm, Left + 2.87 cm, Left + 3.45 cm, Left + 4.02 cm, Left + 4.6 cm, Left + 5.17 cm, Left + 5.74 cm, Left

Style Definition: Dimension_100

Style Definition: Figure Graphic

Style Definition: Figure subtitle

Style Definition: List Continue 1

Style Definition: List Number 1: Tab stops: Not at 0.71 cm

Style Definition: Example indent 2: Tab stops: 2.39 cm, Left

Style Definition: Note indent 2 continued: Tab stops: 3.1 cm, Left

Style Definition: Note indent 2

Style Definition: AMEND Heading 1 Unnumbered: Pattern: 15%

Formatted: Font: 13 pt

Formatted: Font: 13 pt, Bold, Font color: Black

Formatted: Font: 13 pt, Bold, Font color: Black

Formatted: Font: 13 pt, Bold, Font color: Black

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: 13 pt, Font color: Black

Formatted: Font: 13 pt, Bold, Font color: Black

Formatted: Font: 13 pt, Font color: Black

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: 13 pt, Font color: Black, French (Switzerland)

Formatted: Font: Not Bold, French (Switzerland)

Document type:
Document subtype:
Document stage:
Document language:

Formatted

Formatted: Justified, Border: Right: (Single solid line, Blue, 0.5 pt Line width), Tab stops: 16.97 cm, Left

Formatted: Font: 11 pt

Formatted: Font: 11 pt, Not Bold

Formatted: Tab stops: 5.71 cm, Left + Not at 17.2 cm

Formatted: Header

Contents

Page

~~Foreword 4~~

~~Introduction 5~~

~~1 Scope 1~~

~~2 Normative references 1~~

~~3 Terms and definitions 2~~

~~4 Abbreviated terms 4~~

~~5 Conformance 6~~
~~5.1 General 6~~
~~5.2 Base standards 6~~
~~5.3 Main contents of an EFC Personalization AP 6~~
~~5.4 Conformance statement 7~~

~~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 8~~
~~7.2.1 Supported DSRC stacks 8~~
~~7.2.2 CEN DSRC stack 8~~
~~7.3 OBE personalization functions 9~~
~~7.3.1 General 9~~
~~7.3.2 Initialization and termination 9~~
~~7.3.3 Retrieving OBE identifier 10~~
~~7.3.4 Writing of data 10~~
~~7.4 Security requirements 13~~
~~7.5 Transaction requirements 15~~

~~8 Personalization equipment requirements 15~~
~~8.1 General 15~~
~~8.2 DSRC lower layer requirements 15~~
~~8.2.1 Supported DSRC stacks 15~~
~~8.2.2 CEN DSRC stack 15~~
~~8.3 PE personalization functions 15~~
~~8.4 Security requirements 15~~
~~8.5 Transaction requirements 16~~

~~Annex A (normative) Security calculations 17~~

~~Annex B (normative) PICS proforma 22~~

~~Annex C (normative) Personalization of ES 200 674-1-compliant OBE 27~~

~~Annex D (informative) Transaction example 32~~

~~Annex E (informative) Security computation examples 37~~

~~Bibliography 41~~

Foreword vii

Introduction ix

1 Scope ... 1

2 Normative references ... 1

3 Terms and definitions ... 2

4 Abbreviated terms ... 4

5 Conformance ... 6
5.1 General ... 6
5.2 Base standards ... 6
5.3 Main contents of an EFC personalization AP ... 8
5.4 Conformance statement ... 8

6 Personalization overview ... 8
6.1 Process ... 8
6.2 System architecture ... 8

7 OBE requirements ... 9
7.1 General ... 9
7.2 DSRC lower layer requirements ... 9
7.2.1 Supported DSRC stacks ... 9
7.2.2 CEN DSRC stack ... 9
7.3 OBE personalization functions ... 11
7.3.1 General ... 11
7.3.2 Initialization and termination ... 11
7.3.3 Retrieving the OBE identifier ... 12
7.3.4 Writing of data ... 12
7.4 Security requirements ... 15
7.5 Transaction requirements ... 17

8 Personalization equipment requirements ... 17
8.1 General ... 17
8.2 DSRC lower layer requirements ... 17
8.2.1 Supported DSRC stacks ... 17
8.2.2 CEN DSRC stack ... 17
8.3 PE personalization functions ... 17
8.4 Security requirements ... 17
8.5 Transaction requirements ... 18

Annex A (normative) Security calculations ... 19

Annex B (normative) PICS proforma ... 24

Annex C (normative) Personalization of OBE conforming to ETSI ES 200 674-1 ... 29

Annex D (informative) Transaction example ... 35

Annex E (informative) Security computation examples ... 40

Bibliography ... 44

Formatted: Tab stops: 5.71 cm, Left + Not at 17.2 cm

Formatted: Header

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.~~

~~In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of documents:~~

~~an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;~~

~~an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.~~

~~An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.~~

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).

This second edition cancels and replaces the first edition (ISO/TS 21719-2:2018), which has been technically revised.

The main changes are as follows:

- addition of subclause 5.4 on Conformance statement;
- minor updating of terms, including the reference to ISO/TS 17573-2 as the primary source.

A list of all parts in the ISO 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.~~www.iso.org/members.html.

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

Formatted: English (United States)

Formatted: Tab stops: 5.71 cm, Left + Not at 17.2 cm

Formatted: Header

Introduction

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

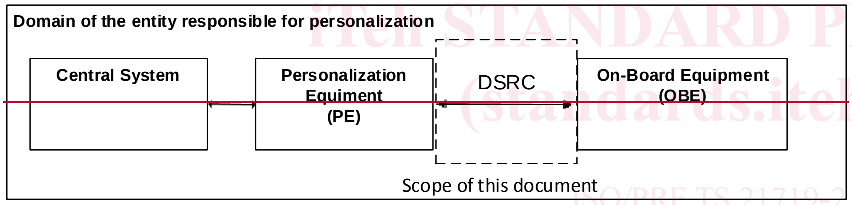
To assign the EFC application in the OBE to a certain user or/and vehicle, personalization is performed. This means that unique user- and vehicle~~-~~-related data~~,~~ needs to be transferred and stored in the OBE.

CEN/TR 16152 assessed many aspects of the personalization process and ~~defin<ed~~defined the overall personalization assets~~;~~: application data, application keys and vehicle data.

Different communication media may be used for transferring the personalization assets to the OBE. An overall message exchange framework and ~~needed~~required security functionality may be applied~~,~~ for all media common procedures, 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~~–~~, TSP), will further be able to outsource ~~parts of,~~partial 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 and is limited to the dedicated short-range communication (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

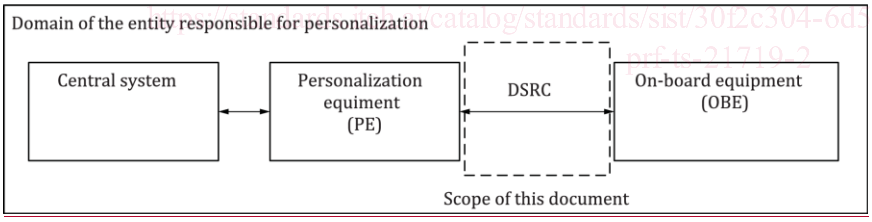

Domain of the entity responsible for personalization
Central system
Personalization equipment (PE)
DSRC
On-board equipment (OBE)
Scope of this document

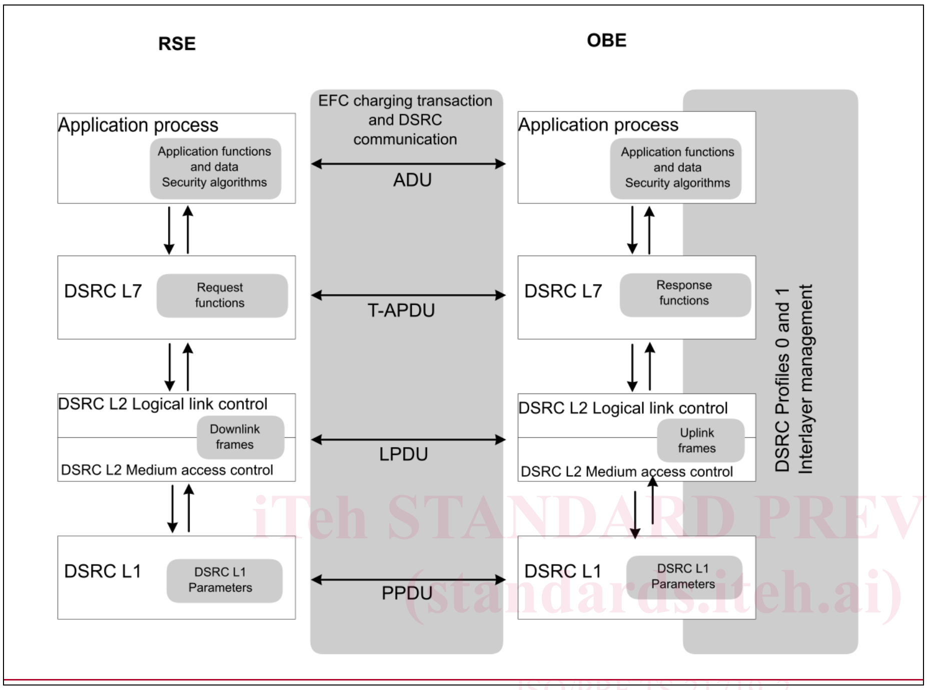
Figure 1 — Scope for this document (box delimited by a dotted line)

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 DSRC communication profiles as specified in EN 13372 and using the EFC Application Interface according to ISO 14906.

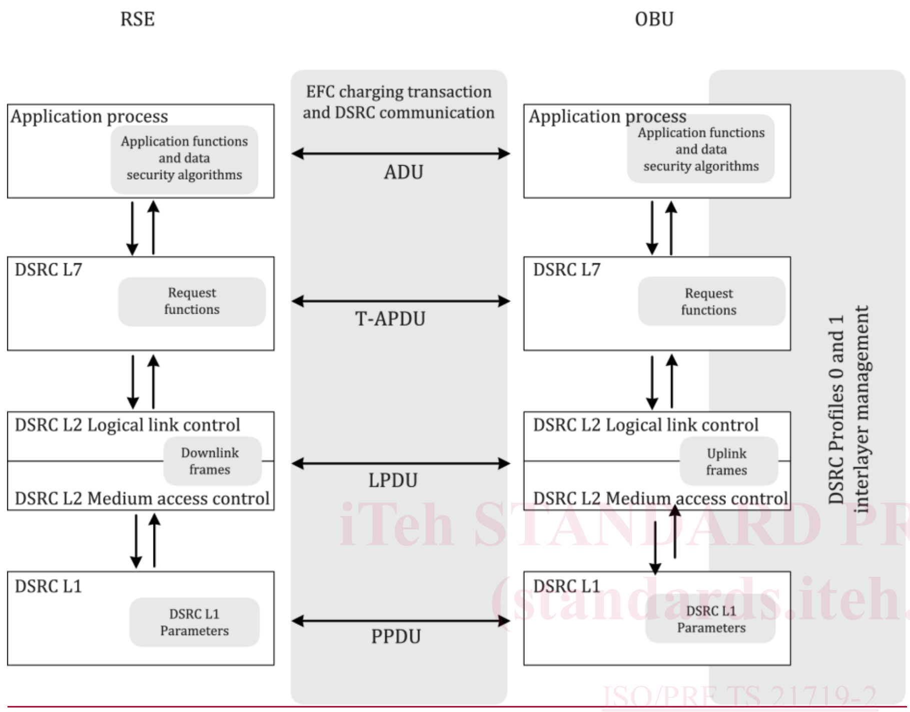
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

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.

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


RSE
OBE
Application process
Application functions and data Security algorithms
EFC charging transaction and DSRC communication
ADU
Application process
Application functions and data Security algorithms
DSRC L7
Request functions
T-APDU
DSRC L7
Response functions
DSRC Profiles 0 and 1 Interlayer management
DSRC L2 Logical link control
Downlink frames
DSRC L2 Medium access control
LPDU
DSRC L2 Logical link control
Uplink frames
DSRC L2 Medium access control
DSRC L1
DSRC L1 Parameters
PPDU
DSRC L1
DSRC L1 Parameters

Formatted: Tab stops: 5.71 cm, Left + Not at 17.2 cm


RSE
OBU
EFC charging transaction and DSRC communication
Application process
Application functions and data security algorithms
ADU
Application process
Application functions and data security algorithms
DSRC L7
Request functions
T-APDU
DSRC L7
Request functions
DSRC L2 Logical link control
Downlink frames
DSRC L2 Medium access control
LPDU
DSRC L2 Logical link control
Uplink frames
DSRC L2 Medium access control
DSRC L1
DSRC L1 Parameters
PPDU
DSRC L1
DSRC L1 Parameters
DSRC Profiles 0 and 1 interlayer management

Key

~~ADU~~	~~Application data unit~~
~~T-APDU~~	~~Transfer-application protocol data unit~~
~~LPDU~~	~~LLC protocol data unit~~
~~PPDU~~	~~physical layer protocol data unit~~
~~DSRC L1~~	~~DSRC layer 1 (physical layer)~~
~~DSRC L2~~	~~DSRC layer 2 (data link layer)~~
~~DSRC L7~~	~~DSRC layer 7 (application layer)~~
ADU	application data unit
T-APDU	transfer-application protocol data unit
LPDU	logical link control (LLC) protocol data unit
PPDU	physical layer protocol data unit
DSRC L1	DSRC layer 1 (physical layer)
DSRC L2	DSRC layer 2 (data link layer)
DSRC L7	DSRC layer 7 (application layer)

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

Formatted: Header

Formatted: Level 1, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: 11.5 pt, English (United Kingdom)

Electronic fee collection — Personalization of on-board equipment (OBE) — Part 2: Using dedicated short-range ~~comunication~~communication

1 Scope

This document defines:

- 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.

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

A protocol information conformance statement (PICS) proforma is provided in Annex B, and security computation examples are provided in Annex E.

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

It is outside the scope of this document to define:

- conformance procedures and test ~~specification~~specifications,
- setting-up of operating organizations (e.g. ~~TSP~~toll service provider, personalization agent, trusted third party), and
- legal issues.

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

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

2 Normative references

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

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.

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

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

Formatted: Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

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

~~FprEN~~EN 15509:2022, Electronic ~~*Fee Collection*~~*fee collection* — Interoperability application profile for DSRC

ETSI~~-~~/ES 200 674-1:~~-~~2013, *Intelligent Transport Systems (ITS) — Road Transport and Traffic Telematics (RTTT) — Dedicated Short Range Communications (DSRC) — Part 1: Technical characteristics and test methods for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band (V2.4.1, 2013-05)*

3 Terms and definitions

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

ISO and IEC maintain terminology 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~~https://www.iso.org/obp

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

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

[SOURCE: ISO/TS 17573-2:2020, 3.4]

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

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

3.3
authentication
security mechanism allowing verification of the provided identity

[SOURCE: ISO/TS 17573-2:2020, 3.15]

3.4

Formatted: Header

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: std_publisher

Formatted: std_documentType

Formatted: std_docNumber

Formatted: std_docPartNumber

Formatted: std_year

Formatted: std_docTitle, Font: Not Italic

Formatted: English (United States)

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Hyperlink, English (United States)

Formatted: Footer

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

[SOURCE: ISO/TS 17573-2:2020, 3.16]

3.5
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]

3.6
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO/TS 17573-2:2020, 3.56]

3.7
electronic fee collection
EFC
fee collection by electronic means

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

3.8
EFC Element
coherent set of data and functionality

Note 1 to entry: The functionality includes, where applicable, the security-related functions and the associated security keys.

Note 2 to entry: EFC Elements are created by the applications and addressed using Element identifiers.

Note 3 to entry: In a given *on-board equipment (OBE)* (3.11), the EID is used to address a toll context, identified by the EFC-ContextMark, in which attributes (3.1) can be addressed unambiguously by AttributeIDs inside an EFC Element of the OBE.

[SOURCE: ISO/TS 17573-2:2020, 3.71]

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

[SOURCE: ISO/TS 17573-2:2020, 3.~~127, modified – Note 1 to entry has been added~~126]

3.10
OBE personalization

Formatted: std_publisher

Formatted: std_documentType

Formatted: std_docNumber

Formatted: std_docPartNumber

Formatted: Source, Line spacing: single, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: std_year

Formatted: std_section

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

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

3.11
personalization assets
specific data stored in the *on-board equipment* (*OBE*) (3.12) related to the user and the vehicle

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

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

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

3.13
profile
set of requirements and selected options from *base standards* (3.5) or international standardized profiles used to provide a specific functionality

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

3.14
toll service provider
TSP
entity providing toll services in one or more toll domains

[SOURCE: ISO/TS 17573-2:2020, 3.206]

3.15
transaction
whole of the exchange of information between two physically separated communication facilities

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

~~5~~4 Abbreviated terms

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

Ack	acknowledgement
AcK	access key
AC_CR	access credentials
ADU	application data unit
APDU	application protocol data unit
AP	application profile
ASN.1	abstract syntax notation one

Formatted: Header

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Footer

AVEI	automatic vehicle and equipment identification
BST	beacon service table
CBC	cipher block chaining
DSRC	dedicated short-range communication
EID	element identifier
EFC	electronic fee collection
ICS	implementation conformance statement
IUT	implementation under test
MAC	message authentication code
OBE	on-board equipment
PE	personalization equipment
PICS	protocol implementation conformance statement
SAM	secure application module
TSP	toll service provider
T-APDU	transfer-application protocol data unit
VST	vehicle service table

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers