

DIN CEN ISO/TS 21719-2

ICS 03.220.20; 35.240.60

Ersatz für
DIN CEN ISO/TS 21719-2
(DIN SPEC 4629):2018-07

**Elektronische Gebührenerhebung –
Personalisierung von Onboard Einrichtungen –
Teil 2: Verwendung von dedizierter Nahbereichskommunikation
(ISO/TS 21719-2:2022);
Englische Fassung CEN ISO/TS 21719-2:2022**

Electronic fee collection –

Personalization of on-board equipment (OBE) –

Part 2: Using dedicated short-range communication (ISO/TS 21719-2:2022);

English version CEN ISO/TS 21719-2:2022

Perception de télépéage –

Personnalisation des équipements embarqués –

Partie 2: Utilisation des communications dédiées à courte portée (ISO/TS 21719-2:2022);

Version anglaise CEN ISO/TS 21719-2:2022

Gesamtumfang 51 Seiten

DIN-Normenausschuss Automobiltechnik (NAAutomobil)
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Dieses Dokument (CEN ISO/TS 21719-2:2022) wurde vom Technischen Komitee ISO/TC 204 „Intelligent Transport Systems, in Zusammenarbeit mit dem Technischen Komitee CEN/TC 278 „Intelligente Verkehrssysteme“ ausgearbeitet, dessen Sekretariat von NEN (Niederlande) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 052-02-71 GA „Gemeinschaftsarbeitsausschuss NAAutomobil/DKE: Intelligente Verkehrssysteme“ des DIN-Normenausschusses Automobiltechnik.

Technische Spezifikationen sind nicht Bestandteil des Deutschen Normenwerks.

Eine Technische Spezifikation ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens von DIN noch nicht als Norm herausgegeben wird.

Zur vorliegenden Technischen Spezifikation wurde kein Entwurf veröffentlicht.

Das Präsidium des DIN hat mit seinem Beschluss 1/2004 festgelegt, dass von dem in den Regeln der europäischen Normungsarbeit von CEN/CENELEC verankerten Grundsatz, wonach Europäische Normen in den drei offiziellen Sprachen Deutsch, Englisch und Französisch veröffentlicht werden, in begründeten Ausnahmefällen abgewichen und auf die deutsche Sprachfassung verzichtet werden kann.

Dieses Dokument enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die Englische Fassung von CEN/TS 21719-2:2022.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 12813	siehe	DIN EN ISO 12813
ISO 13141	Siehe	DIN EN ISO 13141
ISO 14816	siehe	DIN EN ISO 14816
ISO 14906	siehe	DIN EN ISO 14906
ISO 17573-1	siehe	DIN EN ISO 17573-1
ISO 17575-1	siehe	DIN EN ISO 17575-1
ISO/TS 19299	siehe	DIN CEN ISO/TS 19299
ISO/TS 21719-1:2018	siehe	DIN CEN ISO/TS 21719-1 (DIN SPEC 4628):2018-07

Eine On-Board Ausrüstung (OBE) ist ein Gerät im Fahrzeug, welches eine oder mehrere Anwendungsinstanzen umfasst, um unterschiedliche ITS-Implementierungen wie z. B. Elektronische Gebührenerhebung (EFC) auszuführen.

Um EFC-Anwendungen in der OBE einem bestimmten Nutzer und/oder Fahrzeug zuzuordnen, sollte eine entsprechende Personalisierung durchgeführt werden. Das bedeutet, dass eindeutige Nutzer bzw. fahrzeugbezogene Daten an die OBE übertragen werden müssen.

Unterschiedliche Kommunikationsmedien könnten zur Übertragung der persönlichen Informationen verwendet werden. Unabhängig vom Medium sollten gemeinsame Prozeduren wie z. B. der allgemeine Rahmen zum Datenaustausch sowie notwendige Security Funktionalitäten angewendet werden, um den Datenschutz und die Integrität sicherzustellen.

Dieses Dokument legt ein vollständiges Anwendungsprofil über dem DSRC-Stack unter Verwendung der in Teil 1 beschriebenen Personalisierungsfunktionalität fest.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

Gegenüber DIN CEN ISO/TS 21719-2 (DIN SPEC 4629):2018-07 wurden folgende Änderungen vorgenommen:

- a) kleinere Korrekturen in den Begriffen und dessen Verweisungen;
- b) kleinere Korrekturen in den Datenfestlegungen.

Frühere Ausgaben

DIN CEN ISO/TS 21719-2 (DIN SPEC 4629): 2018-07

Nationaler Anhang NA (informativ)

Begriffe

Die Benummerung der folgenden Begriffe und Abkürzungen ist identisch mit der Benummerung in der englischen Fassung.

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

3.1
Zugriffsbeglaubigung
en access credentials
vertrauliche Bescheinigung oder sicheres Modul, welches die geforderte Identität eines Objektes oder einer Anwendung schafft

[QUELLE: ISO/TS 17573-2:2020, 3.4, modifiziert — anerkannter Begriff wurde gelöscht (in Abschnitt 4 aufgelistet)]

3.2
Attribut
en attribute
adressierbares Datenpaket, welches aus einem einzelnen Datenelement oder strukturierten Sequenzen von Datenelementen besteht

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

3.3
Authentifizierung
en authentication
Sicherheitsmechanismus, der die Überprüfung der gelieferten Identität erlaubt

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

3.4
Authentifikator
en authenticator
Daten, wenn möglich verschlüsselt, die zur *Authentifizierung* (3.3) verwendet werden

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

3.5**Grundnorm**

en base standard

genehmigte internationale Norm, Technische Spezifikation oder ITU-T-Empfehlung

Anmerkung 1 zum Begriff: Dies beinhaltet insbesondere genehmigte Normen von ISO, ITU, CEN, CENELEC, ETSI und IEEE.

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

3.6**Datenintegrität**

en data integrity

Merkmal, dass Daten nicht in unautorisierter Art und Weise verändert oder zerstört wurden

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

3.7**elektronische Gebührenerhebung**

en electronic fee collection

Mautabbuchung mittels Elektronik

[QUELLE: ISO/TS 17573-2:2020, 3.70, modifiziert — anerkannter Begriff wurde gelöscht (in Abschnitt 4 aufgelistet)]

3.8**EFC-Element**

zusammenhängende Menge von Daten und Funktionalitäten

Anmerkung 1 zum Begriff: Die Funktionalität beinhaltet, wenn vorhanden, die sicherheitsrelevanten Funktionen und die dazugehörigen Sicherheitsschlüssel.

Anmerkung 2 zum Begriff: EFC-Elemente werden von den Anwendungen erstellt und adressieren verwendete Elementbezeichner.

Anmerkung 3 zum Begriff: In einer vorhandenen *fahrzeuginternen Einrichtung (OBE)* (3.9) wird die EID dazu verwendet, den Mautinhalt zu adressieren, der von der EFC-ContextMark erkannt wurde und in der *Attribute* (3.2) eindeutig mittels AttributeIDs innerhalb eines EFC-Elementes der OBE adressiert werden können.

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

3.9**fahrzeuginterne Einrichtung**

en on-board equipment

alle notwendigen Ausrüstungen innerhalb eines Fahrzeuges, um notwendige Funktionen zur *elektronischen Gebührenerhebung (EFC)* (3.7) und Kommunikationsdienste durchzuführen

[QUELLE: ISO/TS 17573-2:2020, 3.126, modifiziert — anerkannter Begriff wurde gelöscht (in Abschnitt 4 aufgelistet)]

3.10**OBE-Personalisierung**

en OBE personalization

Übertragung von *Personalisierungsanlagen* (3.11) an eine *fahrzeuginterne Einrichtung (OBE)* (3.9)

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

3.11

Personalisierungsanlagen

en personalization assets

spezielle Daten, bezogen auf den Nutzer und das Fahrzeug, die in einer *fahrzeuginternen Einrichtung (OBE)* (3.9) gespeichert werden

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

3.12

Personalisierungsausrüstung

en personalization equipment

Ausrüstung zur Übertragung von *Personalisierungsanlagen* (3.11) zur *fahrzeuginternen Einrichtung (OBE)* (3.9)

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

3.13

Profil

en profile

Menge von Anforderungen und ausgewählten Optionen aus *Grundnormen* (3.5) oder international normierter Profile, die verwendet werden, um eine bestimmte Funktion zu erfüllen

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

3.14

Maut-Dienstanbieter

en toll service provider

Inстанz, welche Mautdienste in einem- oder mehreren Mautgebiet(en) anbietet

[QUELLE: ISO/TS 17573-2:2020, 3.206, modifiziert — anerkannter Begriff wurde gelöscht (in Abschnitt 4 aufgelistet)]

3.15

Transaktion

en transaction

Gesamtheit eines Informationsaustausches zwischen zwei physikalisch getrennten Kommunikations-einrichtungen

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

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN CEN ISO/TS 19299, *Elektronische Gebührenerhebung — Sicherheitsgrundstruktur*

DIN CEN ISO/TS 21719-1 (DIN SPEC 4628):2018-07, *Elektronische Gebührenerhebung — Personalisierung von Onboard Einrichtungen — Teil 1: Grundstruktur (ISO/TS 21719-1:2018); Englische Fassung*
CEN ISO/TS 21719-1:2018

DIN EN ISO 12813, *Elektronische Gebührenerhebung — Kommunikation zur Übereinstimmungsprüfung für autonome Systeme*

DIN EN ISO 13141, *Elektronische Gebührenerhebung — Kommunikation zur genauen Ortsbestimmung für autonome Systeme*

DIN EN ISO 14816, *Telematik für den Straßenverkehr und Transport — Automatische Identifizierung von Fahrzeugen und Geräten — Nummerierung und Datenstrukturen*

DIN EN ISO 14906, *Elektronische Gebührenerhebung — Anwendungsschnittstelle zur dezidierten Nahbereich-Kommunikation*

DIN EN ISO 17573-1, *Elektronische Gebührenerhebung — Systemarchitektur für fahrzeugbezogene Maut — Teil 1: Referenzmodell*

DIN EN ISO 17575-1, *Elektronische Gebührenerhebung — Definition der Anwendungsschnittstelle für autonome Systeme — Teil 1: Abrechnung*

— Leerseite —

English Version

Electronic fee collection - Personalization of on-board
equipment (OBE) - Part 2: Using dedicated short-range
communication (ISO/TS 21719-2:2022)

Perception de télépéage - Personnalisation des
équipements embarqués - Partie 2: Utilisation des
communications dédiées à courte portée (ISO/TS
21719-2:2022)

Elektronische Gebührenerhebung - Personalisierung
von Onboard Einrichtungen - Teil 2: Verwendung von
dedizierter Nahbereichskommunikation (ISO/TS
21719-2:2022)

This Technical Specification (CEN/TS) was approved by CEN on 6 October 2022 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye 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

European foreword

This document (CEN ISO/TS 21719-2:2022) 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.

This document supersedes CEN ISO/TS 21719-2:2018.

Any feedback and questions on this document should be directed to the users' national standards body/national committee. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/TS 21719-2:2022 has been approved by CEN as CEN ISO/TS 21719-2:2022 without any modification.

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Abbreviated terms	4
5 Conformance	5
5.1 General	5
5.2 Base standards	5
5.3 Main contents of an EFC personalization AP	5
5.4 Conformance statement	6
6 Personalization overview	6
6.1 Process	6
6.2 System architecture	6
7 OBE requirements	6
7.1 General	6
7.2 DSRC lower layer requirements	6
7.2.1 Supported DSRC stacks	6
7.2.2 CEN DSRC stack	7
7.3 OBE personalization functions	8
7.3.1 General	8
7.3.2 Initialization and termination	8
7.3.3 Retrieving the OBE identifier	8
7.3.4 Writing of data	8
7.4 Security requirements	11
7.5 Transaction requirements	12
8 Personalization equipment requirements	13
8.1 General	13
8.2 DSRC lower layer requirements	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	13
8.5 Transaction requirements	13
Annex A (normative) Security calculations	14
Annex B (normative) PICS proforma	19
Annex C (normative) Personalization of OBE conforming to ETSI ES 200 674-1	24
Annex D (informative) Transaction example	29
Annex E (informative) Security computation examples	33
Bibliography	37

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).

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 the Conformance statement;
- minor updating of terms, including a 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.

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 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 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 partial or 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.

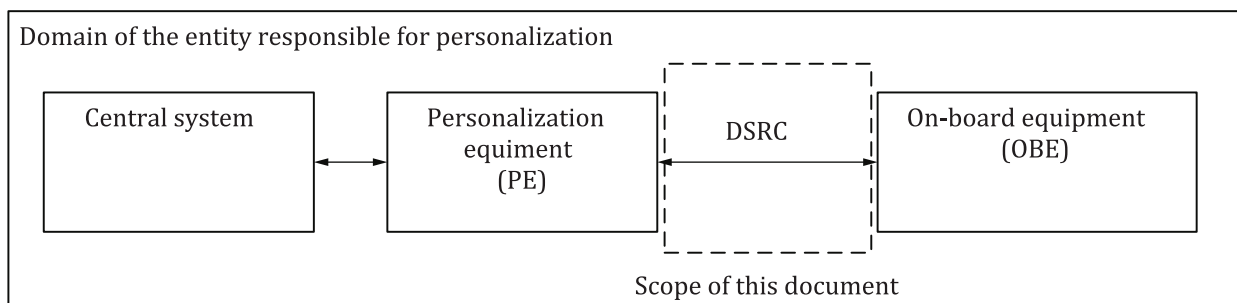


Figure 1 — Scope for this document (box delimited by a dotted line)

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.

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.

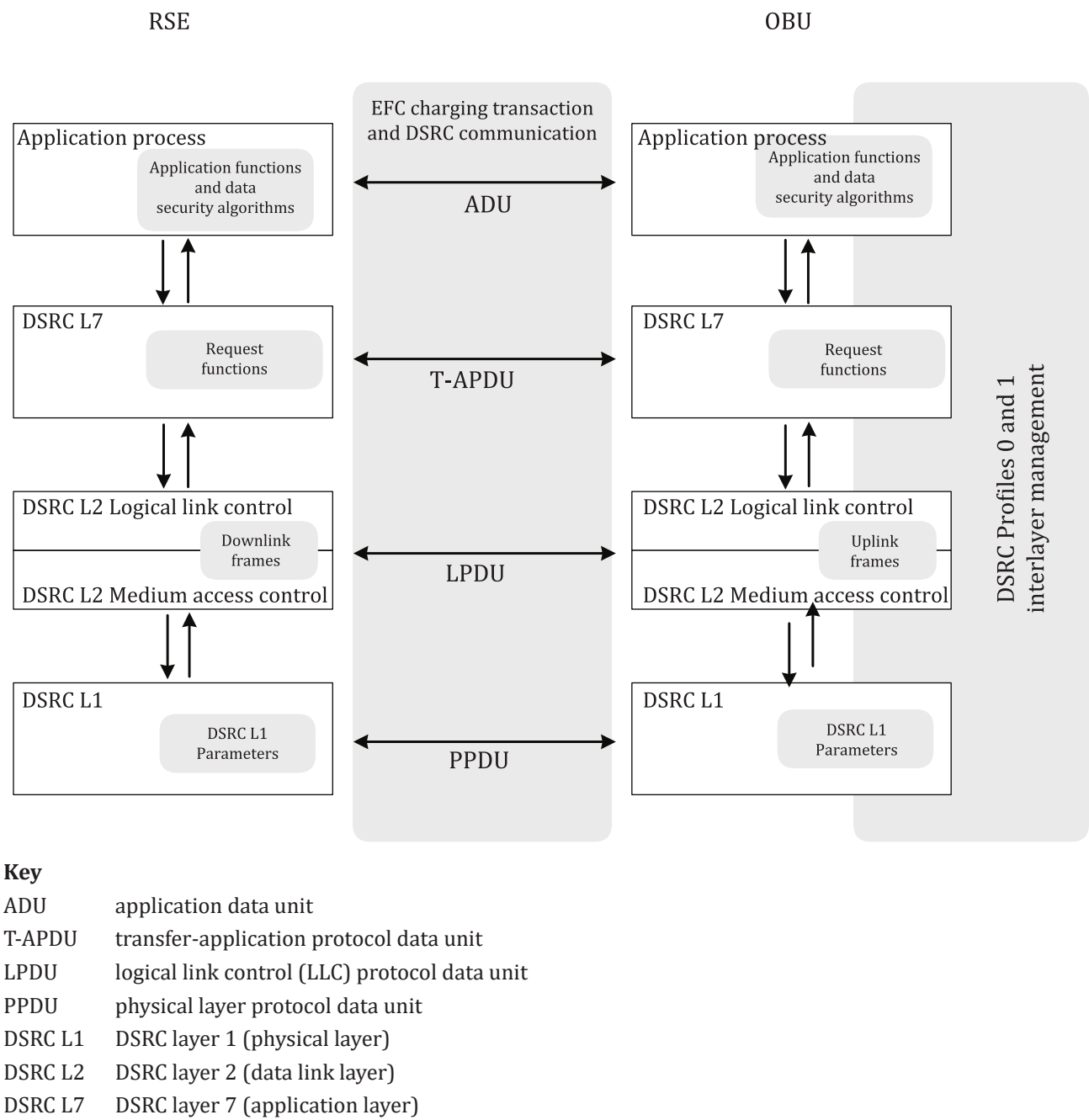


Figure 2 — Relationship between this document and DSRC-stack elements

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

Part 2: Using dedicated short-range 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.

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

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), and
- legal issues.

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

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 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*

EN 15509:2022, *Electronic 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:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 access credentials

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

[SOURCE: ISO/TS 17573-2:2020, 3.4, modified — admitted term removed (listed in Clause 4).]

3.2 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]

3.3 authentication

security mechanism allowing verification of the provided identity

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

3.4 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]