TECHNICAL SPECIFICATION

ISO/TS 21719-2

Second edition
2022-10

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 21719-2:2022(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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).

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.

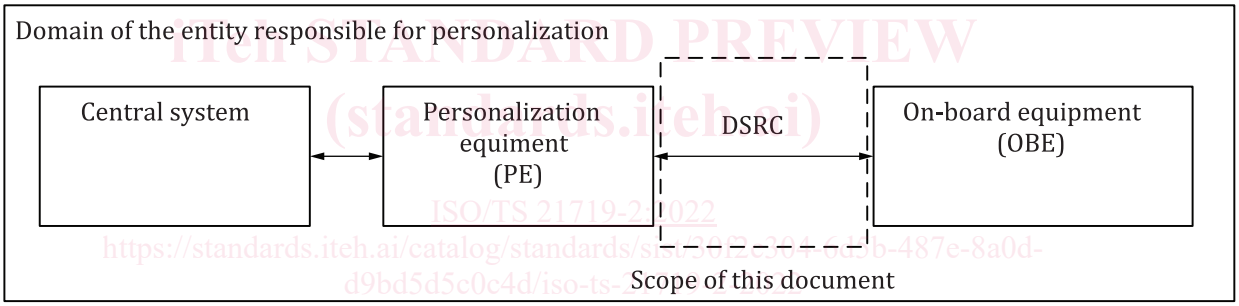
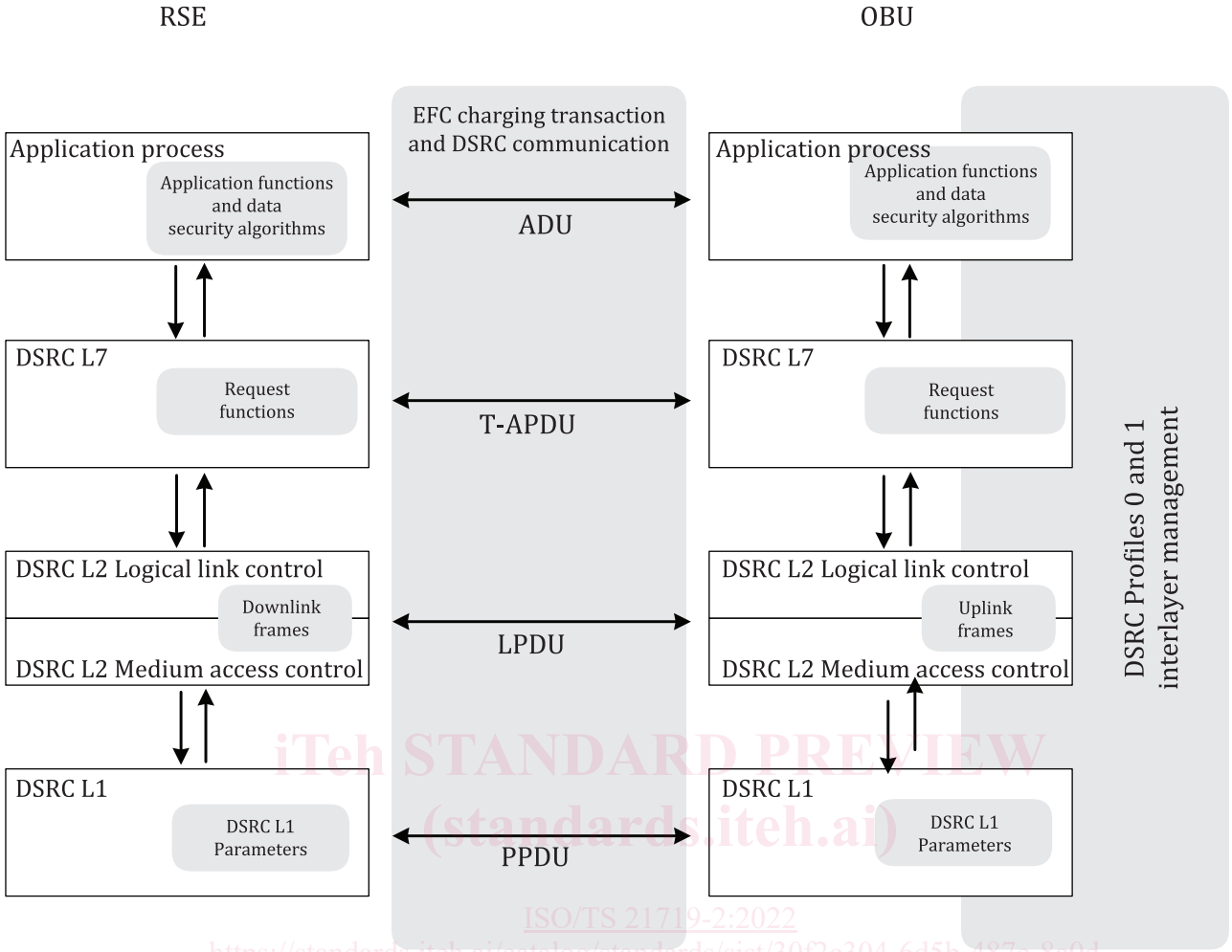


Figure 1 — Scope for this document (box delimited by a dotted line)

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.



Key

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

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]

3.7
electronic fee collection

fee collection by electronic means

[SOURCE: ISO/TS 17573-2:2020, 3.70, modified — admitted term removed (listed in Clause 4).]

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)* (3.9), the EID is used to address a toll context, identified by the EFC-ContextMark, in which *attributes* (3.2) 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
all required equipment on-board a vehicle for performing required *electronic fee collection* (*EFC*) (3.7) functions and communication services

[SOURCE: ISO/TS 17573-2:2020, 3.126, modified — admitted term removed (listed in Clause 4).]

3.10
OBE personalization
transferring *personalization assets* (3.11) to the *on-board equipment* (*OBE*) (3.9)

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

3.11
personalization assets
specific data stored in the *on-board equipment* (*OBE*) (3.9) related to the user and the vehicle

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

3.12
personalization equipment
equipment for transferring *personalization assets* (3.11) to the *on-board equipment* (*OBE*) (3.9)

[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
entity providing toll services in one or more toll domains

[SOURCE: ISO/TS 17573-2:2020, 3.206, modified — admitted term removed (listed in Clause 4).]

3.15
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.

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
AVEI	automatic vehicle and equipment identification
BST	beacon service table
CBC	cipher block chaining
DSRC	dedicated short-range communication
EFC	electronic fee collection
EID	element identifier
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

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

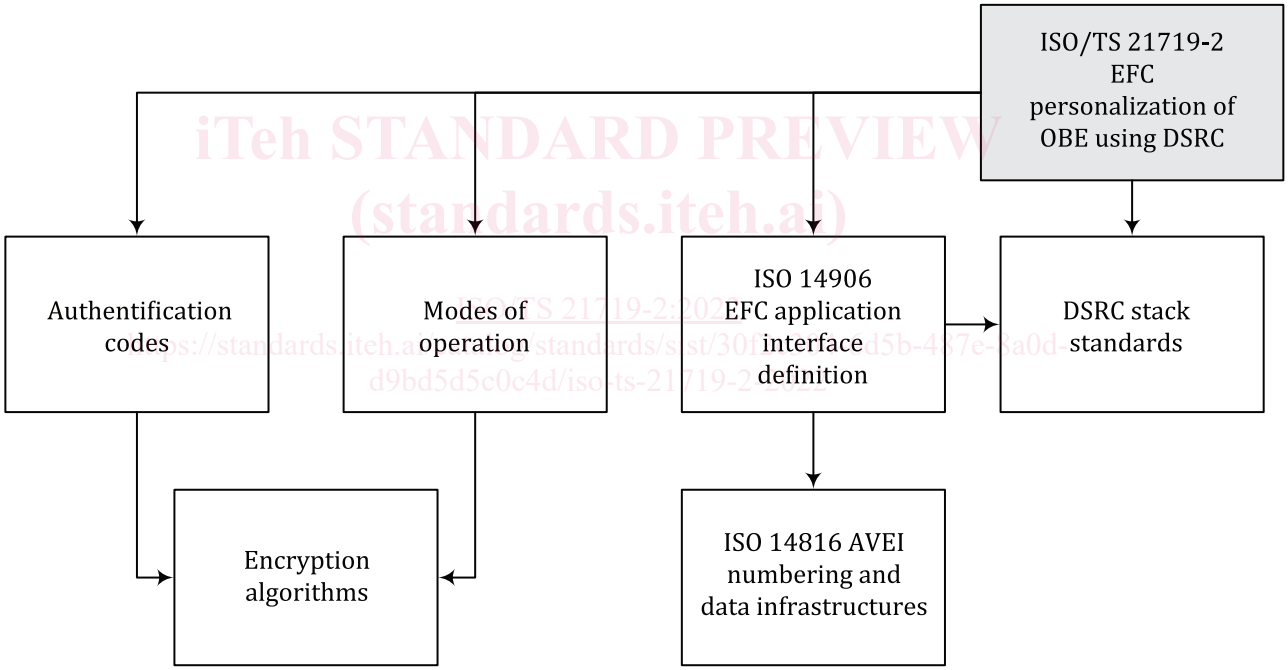
This document defines one application profile (AP). The base standards that this AP is based upon are as follows:

— 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 AP is illustrated in Figure 3.



Key

AVEI automatic vehicle and equipment identification

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.

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

— DSRC lower layer requirements;

— EFC personalization functions;

— security requirements;

— transaction requirements.

5.4 Conformance statement

A supplier of OBE that claims conformity of their OBE to this document shall provide a statement of conformance to this document by completing the protocol implementation conformance statement (PICS) as provided in B.5.

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 data.

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

During personalization, the OBE shall be within the communication range of the PE in order for the data exchange according to this document to take place.

Application data and security keys are transferred to the OBE during the personalization process in an attribute list using standardized DSRC commands according to the requirements in this document.

6.2 System architecture

The overall system architecture is described in ISO/TS 21719-1:2018, 5.2.

For personalization over a DSRC interface, the OBE and PE shall contain a DSRC stack and the application services as described in this document.

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 outside the scope of this document.

7 OBE requirements

7.1 General

This clause contains the normative conformance requirements on the OBE for profile number 1: EFC-DSRC-Personalization Profile 1.

7.2 DSRC lower layer requirements

7.2.1 Supported DSRC stacks

This document supports the DSRC stacks as defined in Table 1.

Table 1 — Supported DSRC stacks

DSRC stack	Application layer	Lower layers	Detailed specifications
CEN-DSRC	ISO 15628 EN 12834	EN 12795 EN 12253	Specification in 7.2.2
Italian DSRC	ETSI/ES 200 674–1:2013, Clause 11 and Annex C	ETSI/ES 200 674–1:2013, Clauses 7 to 10 and Annex C	Specification and implementation example in Annex C
Japanese DSRC	ARIB STD-T75	ARIB STD-T75	
Wave DSRC	IEEE1609.11	IEEE 802.11p IEEE 1609.3/4	

7.2.2 CEN DSRC stack

The following requirements apply for the personalization profile when using the CEN DSRC stack.

The OBE shall comply with EN 15509:2022, 6.1.2 which implicitly requires conformance with the underlying standards as shown in Figure 4.

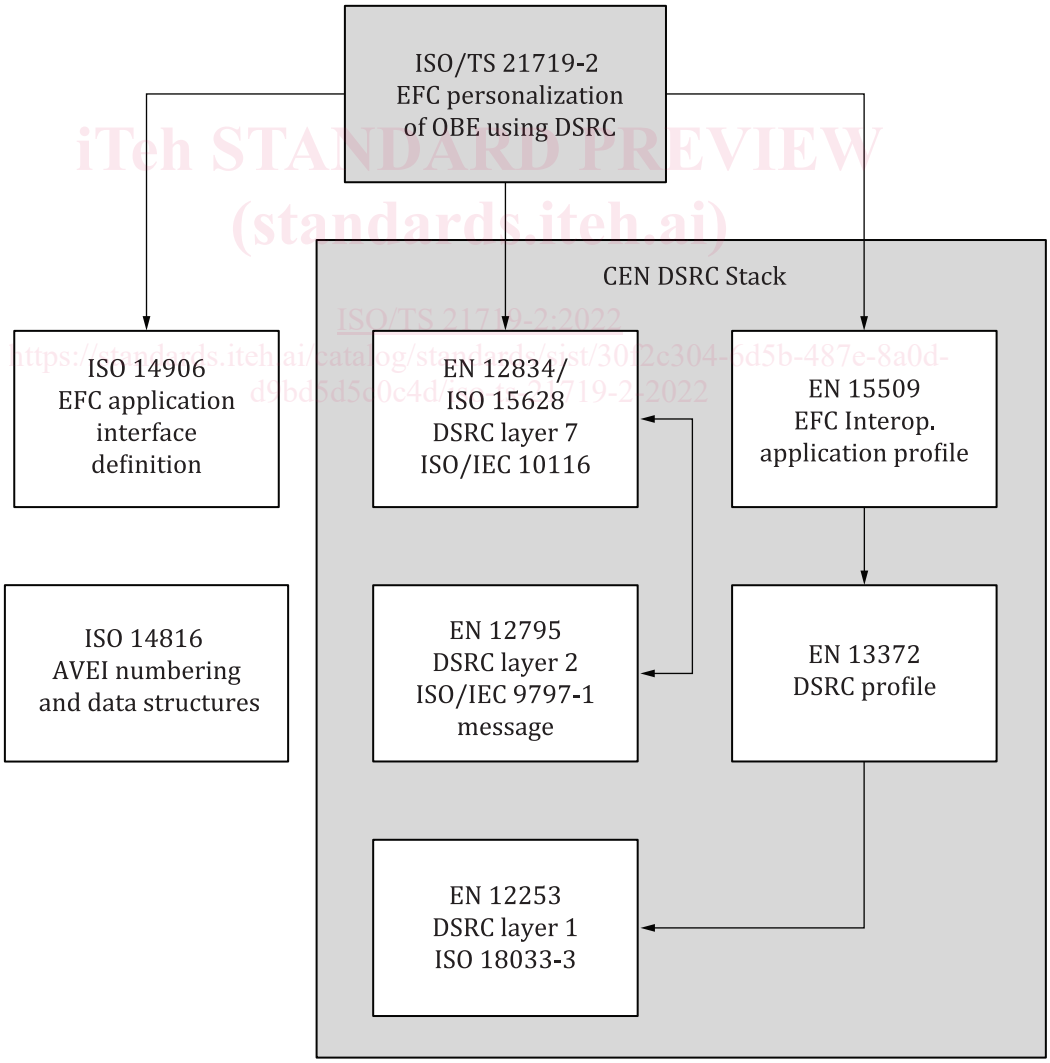


Figure 4 — Relationship and references between standards for the CEN DSRC stack