INTERNATIONAL STANDARD

ISO 14906

Third edition
2018-10

Electronic fee collection — Application interface definition for dedicated short-range communication

Perception du télépéage — Définition de l'interface d'application relative aux communications dédiées à courte portée

Reference number
ISO 14906:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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 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*.

This third edition cancels and replaces the second edition (ISO 14906:2011), which has been technically revised. It also incorporates the Corrigendum ISO 14906:2011/Cor1:2013 and the Amendment ISO 14906:2011/Amd1:2015.

The main changes compared to the previous edition are as follows:

— Inclusion of security calculations according to advanced encryption standard, as recommended in CEN/TR 16968 on security mechanisms (revision of Clause 7 and new Annexes F, G, H and I);

— Update of the normative references, terms and definitions and abbreviated terms clauses and the Bibliography;

— Conversion of the ASN.1 module into an electronic insert;

— Revision of Annex C;

— Removal of Annex D (informative) on functional requirements.

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

This document specifies an application interface for electronic fee collection (EFC) systems, which is based on dedicated short-range communication (DSRC). It supports interoperability between EFC systems on an EFC-DSRC application interface level. This document is intended for DSRC charging applications, but specifically the definition of EFC data elements is valid beyond the use of a DSRC charging interface and might be used for other DSRC applications (e.g. compliance checking communication) and/or on other interfaces (e.g. the application interface of autonomous systems).

This document provides specifications for the EFC transaction model, EFC data elements (referred to as attributes) and functions, from which an EFC transaction can be built. The EFC transaction model provides a mechanism that allows handling of different versions of EFC transactions and associated contracts. A certain EFC transaction supports a certain set of EFC attributes and EFC functions as defined in this document. It is not envisaged that the complete set of EFC attributes and functions be present in each piece of EFC equipment, on-board equipment (OBE) or roadside equipment (RSE).

This document provides the basis for agreements between operators, which are needed to achieve interoperability. Based on the tools specified in this document, interoperability can be reached by operators recognising each others' EFC transactions (including the exchange of security algorithms and keys) and implementing the EFC transactions in each others' RSEs, or they can reach an agreement to define a new transaction (and contract) that is common to both. Considerations should also be made by each operator so that the RSE has sufficient resources to implement such additional EFC transactions.

In order to achieve interoperability, operators should agree on issues such as

— which optional features are actually being implemented and used,

— access rights and ownership of EFC application data in the OBE,

— security policy (including encryption algorithms and key management, if applicable),

— operational issues, such as how many receipts may be stored for privacy reasons, how many receipts are necessary for operational reasons (for example as entry tickets or as proof of payment),

— the agreements needed between operators in order to regulate the handling of different EFC transactions.

In this edition of this document, users are faced with issues related to backward compatibility. This issue can be managed by using the following:

— EfcModule ASN.1 module, including a version number;

— Efc-ContextMark (incl. the ContextVersion), denoting the implementation version, provides a means to ensure co-existence of different implementation versions by means of a look-up table and associated appropriate transaction processing. This will enable the software of the RSE to determine the version of the OBE and his capabilty to accept the new features introduced by this edition of ISO 14906.

Annex A provides the normative ASN.1 specifications of the used data types (EFC action parameters and attributes).

Annex B presents an informative example of a transaction based on the CARDME specification, including bit-level specification.

Annex C presents informative examples of EFC transaction types, using the specified EFC functions and attributes.

Annex D presents an informative mapping table from LatinAlphabetNo2 & 5 to LatinAlphabetNo1 to ease for a Service Provider the use of LatinAlphabetNo1 to encode an OBE for data available wiitten with non-Latin1 characters.

Annex E presents an informative mapping table between EFC vehicle data attributes and European registration certificates to ease the task of a service provider in the OBE personalisation with vehicle data.

Annex F presents the security calculations according to the data encryption standard (DES). This annex is based on EN 15509:2014, Annex B.

Annex G presents the security computations examples for DES. This annex is based on EN 15509:2014, Annex E.

Annex H presents the security calculations for advanced encryption standard (AES). This annex is the adaptation of EN 15509:2014, Annex B for the case of AES.

Annex I presents the security computations examples for AES. This annex is the adaptation of EN 15509:2014, Annex E for the case of AES.

This application interface definition can also be used with other DSRC media which do not use a layer 7 according to ISO 15628/EN 12834. Any DSRC medium which provides services to read and write data, to initialise communication and to perform actions is suitable to be used as a basis for this application interface. Adaptations are medium specific and are not further covered here. As Annex B describes in detail a transaction for central account systems, this document can also be used for on-board account systems, in conjunction with ISO 25110, which provides examples of systems based on on-board accounts.

Electronic fee collection — Application interface definition for dedicated short-range communication

1 Scope

This document specifies the application interface in the context of electronic fee collection (EFC) systems using the dedicated short-range communication (DSRC).

The EFC application interface is the EFC application process interface to the DSRC application layer, as can be seen in Figure 1 below. This document comprises specifications of:

— EFC attributes (i.e. EFC application information) that can also be used for other applications and/or interfaces,

— the addressing procedures of EFC attributes and (hardware) components (e.g. ICC and MMI),

— EFC application functions, i.e. further qualification of actions by definitions of the concerned services, assignment of associated ActionType values and content and meaning of action parameters,

— the EFC transaction model, which defines the common elements and steps of any EFC transaction,

— the behaviour of the interface so as to ensure interoperability on an EFC-DSRC application interface level.

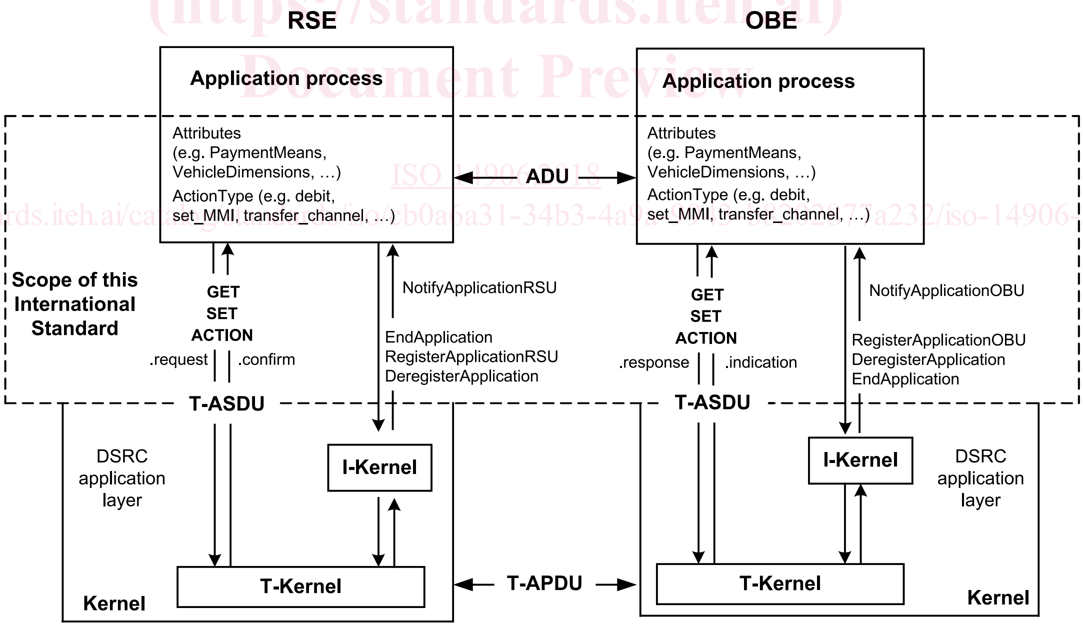

Figure 1 — The EFC application interface

This is an interface standard, adhering to the open systems interconnection (OSI) philosophy (see ISO/IEC 7498-1), and it is as such not primarily concerned with the implementation choices to be realised at either side of the interface.

This document provides security-specific functionality as place holders (data and functions) to enable the implementation of secure EFC transactions. Yet the specification of the security policy (including specific security algorithms and key management) remains at the discretion and under the control of the EFC operator, and hence is outside the scope of this document.

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 612, *Road vehicles — Dimensions of motor vehicles and towed vehicles — Terms and definitions*

ISO 1176, *Road vehicles — Masses — Vocabulary and codes*

ISO 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

ISO 3779, *Road vehicles — Vehicle identification number (VIN) — Content and structure*

ISO 4217, *Codes for the representation of currencies*

ISO/IEC 7812-1, *Identification cards — Identification of issuers — Part 1: Numbering system*

ISO/IEC 8825-2, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) — Part 2*

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

ISO 14816:2005, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure*

ISO 15628:2013, *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 12834:2003, *Road transport and traffic telematics — Dedicated Short Range Communication (DSRC) — DSRC application layer*

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 http://www.electropedia.org/

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

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

3.2
attribute
addressable package of data consisting of a single data element or structured sequences of data elements

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

3.3
authenticator
data, possibly encrypted, that is used for authentication

3.4
channel
information transfer path

[SOURCE: ISO 7498-2:1989, definition 3.3.13]

3.5
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

3.6
data group
class of closely related attributes

[SOURCE: ISO 17575-1:2016, definition 3.10]

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

3.8
Element
DSRC directory containing application information in the form of attributes

3.9
on-board equipment
all required equipment on-board a vehicle for performing required EFC functions and communication services

3.10
on-board unit
single electronic unit on-board a vehicle for performing specific EFC functions and for communication with external systems

3.11
roadside equipment
equipment located along the road, either fixed or mobile

3.12
toll charger
entity which levies toll for the use of vehicles in a toll domain

3.13
toll domain
area or part of a road network where a toll regime is applied

[SOURCE: ISO 17573:2010, definition 3.18]

3.14
toll service
service enabling users to pay toll

3.15
toll service provider
entity providing toll services in one or more toll domains

3.16
transaction
whole of the exchange of information between two physically separated communication facilities

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

3.17
transaction model
functional model describing the structure of electronic payment transactions

4 Abbreviated terms

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

AP	Application Process
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One (ISO/IEC 8824-1)
BST	Beacon Service Table
CCC	Compliance check communication
cf	Confirm
DSRC	Dedicated Short-Range communication
EFC	Electronic Fee Collection
EID	Element Identifier
GNSS	Global Navigation Satellite System
ICC	Integrated Circuit(s) Card
IID	Invoker Identifier
I-Kernel	Initialisation Kernel
ind	Indication
L1	Layer 1 of DSRC (Physical Layer)
L2	Layer 2 of DSRC (Data Link Layer)
L7	Application Layer Core of DSRC
LAC	Localisation Augmentation Communication
LID	Logical Link Control Identifier
LLC	Logical Link Control
LPDU	LLC Protocol Data Unit
MAC	Medium Access Control
MMI	Man-Machine Interface
n.a.	Not applicable
OBE	On-Board Equipment
PDU	Protocol Data Unit
PER	Packed Encoding Rules (ISO/IEC 8825-2)

req	Request
rs	Response
RSE	Roadside Equipment
SAM	Secure Application Module
T-APDU	Transfer-Application Protocol Data Unit
T-ASDU	Transfer-Application Service Data Unit
T-Kernel	Transfer Kernel
VST	Vehicle Service Table

5 EFC application interface architecture

5.1 Relation to the DSRC communication architecture

The DSRC services are provided to an application process by means of the DSRC Application Layer service primitives, which are abstract implementation interactions between a communication service user and a provider. The services are offered by the DSRC communication entities by means of its DSRC Application Layer (EN 12834/ISO 15628) as shown in Figure 2.

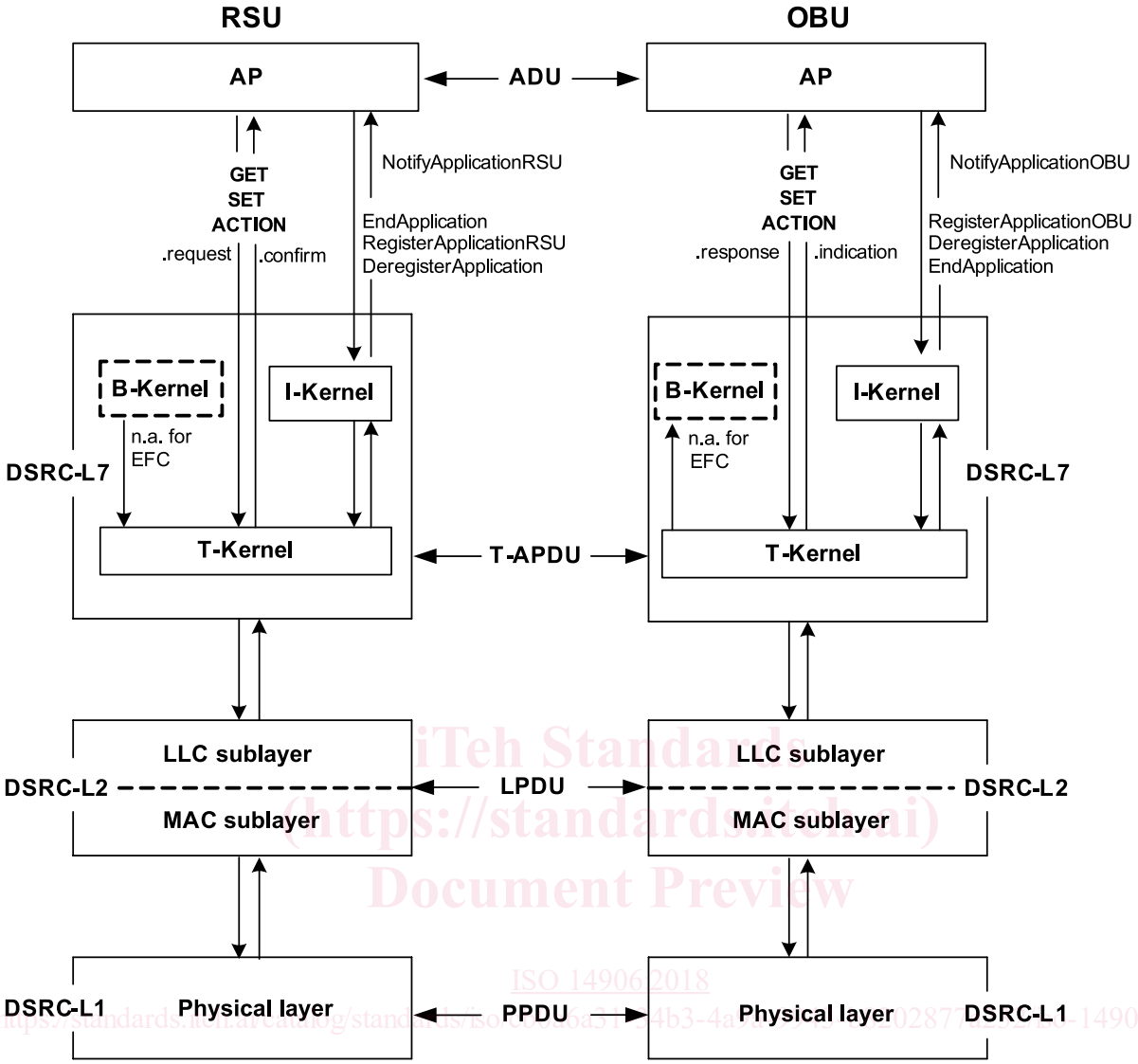

Figure 2 — The EFC application process on top of the DSRC communication stack

NOTE The abbreviated terms used in Figure 2 are defined in Clause 4.

The Transfer Kernel of DSRC Application Layer offers the following services to application processes (see also Figure 2 above):

— GET: The invocation of a GET service request results in retrieval (i.e. reading) of application information (i.e. Attributes) from the peer service user (i.e. the OBE application process), a reply is always expected.

— SET: The invocation of a SET service request results in modification (i.e. writing) of application information (i.e. Attributes) of the peer service user (i.e. the OBE application process). This service may be requested in confirmed or non-confirmed mode, a reply is only expected in the former case.

— ACTION: The invocation of an ACTION service request results in a performance of an action by the peer service user (i.e. the OBE application process). An action is further qualified by the value of the ActionType. This service may be requested in confirmed or non-confirmed mode, a reply is only expected in the former case.

— EVENT-REPORT: The invocation of an EVENT-REPORT service request forwards a notification of an event to the peer service user.

