INTERNATIONAL STANDARD

ISO 14906

Fourth edition
2022-12

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

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

Reference number
ISO 14906:2022(E)

© ISO 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO 2022 – All rights reserved

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **2**

3 Terms and definitions **2**

4 Abbreviated terms **4**

5 EFC application interface architecture **6**
5.1 Relation to the DSRC communication architecture 6
5.2 Usage of DSRC application layer by the EFC application interface 8
5.3 Addressing of EFC attributes 8
5.3.1 Basic mechanism 8
5.3.2 Role of the Element Identifier (EID) 9
5.3.3 Multiple instances of Attributes 9
5.4 Addressing of components 10

6 EFC transaction model **11**
6.1 General 11
6.2 Initialisation phase 11
6.2.1 Overview 11
6.2.2 EFC application-specific contents of the BST 12
6.2.3 EFC application-specific contents of the VST 13
6.3 Transaction phase 14

7 EFC functions **15**
7.1 Overview and general concepts 15
7.1.1 EFC functions and service primitives 15
7.1.2 Overview of EFC functions 16
7.1.3 Handling of multiple instances 17
7.1.4 Security 19
7.2 EFC functions 22
7.2.1 General 22
7.2.2 GET_STAMPED 22
7.2.3 SET_STAMPED 23
7.2.4 GET_SECURE 24
7.2.5 SET_SECURE 25
7.2.6 GET_INSTANCE 25
7.2.7 SET_INSTANCE 26
7.2.8 GET_NONCE 27
7.2.9 SET_NONCE 28
7.2.10 TRANSFER_CHANNEL 28
7.2.11 COPY 29
7.2.12 SET_MMI 30
7.2.13 SUBTRACT 30
7.2.14 ADD 31
7.2.15 DEBIT 32
7.2.16 CREDIT 33
7.2.17 ECHO 34

8 EFC Attributes **34**
8.1 General 34
8.2 Data group contract 36
8.3 Data group receipt 39
8.4 Data group vehicle 45
8.5 Data group equipment 50

© ISO 2022 – All rights reserved

8.6 Data group driver 52
8.7 Data group payment 54
Annex A (normative) **EFC data type specifications** **56**
Annex B (informative) **CARDME transaction** **57**
Annex C (informative) **Examples of EFC transaction types** **89**
Annex D (informative) **Mapping table from LatinAlphabetNo2, LatinCyrillicAlphabet, LatinGreekAlphabet and LatinAlphabetNo10 to LatinAlphabetNo1** **101**
Annex E (informative) **Mapping table between EFC Vehicledata attribute and European registration certificate** **102**
Annex F (normative) **Security calculations for DES** **105**
Annex G (informative) **Security computation examples for DES** **111**
Annex H (normative) **Security calculations for AES** **114**
Annex I (informative) **Security computation examples for AES** **119**
Bibliography **121**

© ISO 2022 – All rights reserved

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 fourth edition cancels and replaces the third edition (ISO 14906:2018), which has been technically revised. It also incorporates the Amendment ISO 14906:2018/Amd 1:2020.

The main changes are as follows:

— updating of terms and definitions, including reference to ISO/TS 17573-2 as the primary source;

— updating of data definitions, including reference to ISO 17573-3:—[1)] as the primary source;

— addition of a second level of the version identifier (i.e. minor version) of the abstract syntax notation one (ASN.1) module to provide enhanced support to standards that import data types from this document;

— introduction of use of imported ASN.1 types with successors (i.e. including all future minor versions).

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.

1) Under preparation. Stage at the time of publication: ISO/DIS 17573-3:2022.

© ISO 2022 – All rights reserved

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 can potentially 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 the 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 recognizing each others' EFC transactions (including the exchange of security algorithms and keys) and implementing the EFC transactions in each others' RSE, 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. Such issues can be managed by using the following:

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

— EfcContextMark (incl. the ContextVersion), denoting the implementation version; this 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 its capability to accept the new features introduced by this edition of ISO 14906.

This application interface definition can also be used with other DSRC media which do not use 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 provides a detailed description of 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.

This document also includes:

— Annex A, which provides the normative ASN.1 data type specifications (EFC action parameters and attributes);

© ISO 2022 – All rights reserved

— Annex B, which presents an example of a transaction based on the CARDME specification, including bit-level specification;

— Annex C, which presents examples of EFC transaction types, using the specified EFC functions and attributes;

— Annex D, which presents a mapping table from LatinAlphabetNo2 & 5 to LatinAlphabetNo1 to facilitate for a service provider the use of LatinAlphabetNo1 to encode an OBE for data available written with non-Latin1 characters;

— Annex E, which presents a mapping table between EFC vehicle data attributes and European registration certificates to facilitate the task of a service provider in OBE-personalization with vehicle data;

— Annex F, which presents the security calculations according to the data encryption standard (DES).

NOTE 1 Annex F is based on EN 15509:2014, Annex B.

— Annex G, which presents security computations examples for DES;

NOTE 2 Annex G is based on EN 15509:2014, Annex E.

— Annex H, which presents the security calculations for advanced encryption standard (AES);

NOTE 3 Annex H is an adaptation of EN 15509:2014, Annex B for the case of AES.

— Annex I, which presents the security computations examples for AES.

NOTE 4 Annex I is an adaptation of EN 15509:2014, Annex E for the case of AES.

© ISO 2022 – All rights reserved

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 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. 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. integrated circuit(s) card);

— 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.

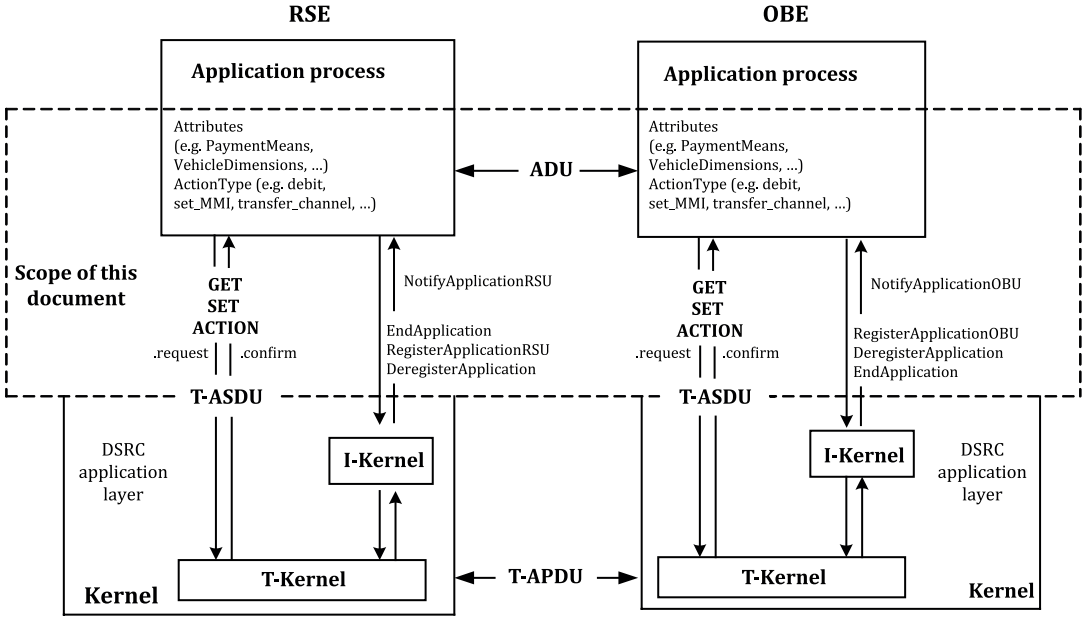


Figure 1 — The EFC application interface

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 realized 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.

© ISO 2022 – All rights reserved

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 code*

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 — Part 2: Specification of Packed Encoding Rules (PER)*

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

ISO 14816, *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 17573-3:—[2)], *Electronic fee collection — System architecture for vehicle-related tolling — Part 3: Data dictionary*

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*

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]

2) Under preparation. Stage at the time of publication: ISO/DIS 17573-3:2022.

© ISO 2022 – All rights reserved

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
authenticator
data, possibly encrypted, that is used for authentication

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

3.4
channel
information transfer path

[SOURCE: ISO/TS 17573-2:2020, 3.30]

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

[SOURCE: ISO/TS 17573-2:2020, 3.53]

3.6
data group
class of closely related *attributes* (3.2)

[SOURCE: ISO/TS 17573-2:2020, 3.55]

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

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

3.8
Element
DSRC directory containing application information in the form of *attributes* (3.2)

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

[SOURCE: ISO/TS 17573-2:2020, 3.126]

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

[SOURCE: ISO/TS 17573-2:2020, 3.127]

© ISO 2022 – All rights reserved

3.11
roadside equipment
fixed or movable electronic fee collection equipment located along or on the road

Note 1 to entry: Roadside equipment (RSE) and roadside unit (RSU) have been used as terms with the same or similar meaning in the standardization of DSRC and DSRC-based EFC within CEN and ETSI. Previously-developed relevant standards used the term "RSU" with the meaning "RSE" as defined in this document.

[SOURCE: ISO/TS 17573-2:2020, 3.161]

3.12
toll charger
entity which levies toll for the use of vehicles in a *toll domain* (3.13)

[SOURCE: ISO/TS 17573-2:2020, 3.194]

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

[SOURCE: ISO/TS 17573-2:2020, 3.201]

3.14
toll service
service enabling users to pay toll

[SOURCE: ISO/TS 17573-2:2020, 3.205]

3.15
toll service provider
entity providing *toll services* (3.14) in one or more *toll domains* (3.13)

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

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

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

3.17
transaction model
functional model describing the structure of electronic payment *transactions* (3.16)

[SOURCE: ISO/TS 17573-2:2020, 3.213]

4 Abbreviated terms

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

ADU	application data unit
AES	advanced encryption standard
AP	application process
APDU	application protocol data unit
ASN.1	abstract syntax notation one
BST	beacon service table

© ISO 2022 – All rights reserved