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 ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **2**

3 Terms and definitions **2**

4 Abbreviated terms **4**

5 EFC application interface architecture **5**
5.1 Relation to the DSRC communication architecture 5
5.2 Usage of DSRC application layer by the EFC application interface 7
5.3 Addressing of EFC attributes 7
5.3.1 Basic mechanism 7
5.3.2 Role of the EID 8
5.3.3 Multiple Instances of Attributes 8
5.4 Addressing of components 9

6 EFC Transaction Model **10**
6.1 General 10
6.2 Initialisation Phase 10
6.2.1 Overview 10
6.2.2 EFC application-specific contents of the BST 11
6.2.3 EFC application-specific contents of the VST 12
6.3 Transaction phase 13

7 EFC functions **14**
7.1 Overview and general concepts 14
7.1.1 EFC functions and service primitives 14
7.1.2 Overview of EFC functions 15
7.1.3 Handling of multiple instances 16
7.1.4 Security 18
7.2 EFC functions 21
7.2.1 General 21
7.2.2 GET_STAMPED 21
7.2.3 SET_STAMPED 22
7.2.4 GET_SECURE 23
7.2.5 SET_SECURE 24
7.2.6 GET_INSTANCE 25
7.2.7 SET_INSTANCE 25
7.2.8 GET_NONCE 26
7.2.9 SET_NONCE 27
7.2.10 TRANSFER_CHANNEL 27
7.2.11 COPY 28
7.2.12 SET_MMI 29
7.2.13 SUBTRACT 29
7.2.14 ADD 30
7.2.15 DEBIT 30
7.2.16 CREDIT 31
7.2.17 ECHO 32

8 EFC Attributes **33**
8.1 General 33
8.2 Data group CONTRACT 35
8.3 Data group RECEIPT 38
8.4 Data group VEHICLE 44
8.5 Data group EQUIPMENT 51

8.6 Data group DRIVER 53
8.7 Data group PAYMENT 55
Annex A (normative) **EFC data type specifications** **57**
Annex B (informative) **CARDME transaction** **58**
Annex C (informative) **Examples of EFC transaction types** **92**
Annex D (normative) **Mapping table from LatinAlphabetNo2 & 5 to LatinAlphabetNo1** **104**
Annex E (informative) **Mapping table between EFC Vehicledata attribute and European registration certificate** **105**
Annex F (normative) **Security calculations for DES** **108**
Annex G (informative) **Security computation examples for DES** **113**
Annex H (normative) **Security calculations for AES** **116**
Annex I (informative) **Security computation examples for AES** **121**
Bibliography **123**

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.