SLOVENSKI STANDARD

SIST EN ISO 14906:2011

01-december-2011

Nadomešča:

SIST EN ISO 14906:2005

Elektronsko pobiranje pristojbin - Definicija aplikacijskega vmesnika za posebne komunikacije kratkega dosega (ISO 14906:2011)

Electronic fee collection - Application interface definition for dedicated short-range communication (ISO 14906:2011)

Elektronische Gebührenerfassung (EFC) - Anforderungen an die EFC-Schnittstelle für Fahrzeug-Baken-Kommunikation (ISO 14906:2011)

Perception du télépéage - Définition de l'interface d'application relative aux communications dédiées à courte portée (ISO 14906:2011)

Ta slovenski standard je istoveten z: EN ISO 14906:2011

ICS:

03.220.20	Cestni transport	Road transport
35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade

SIST EN ISO 14906:2011 en

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 14906

October 2011

ICS 03.220.20; 35.240.60

Supersedes EN ISO 14906:2004

English Version

Electronic fee collection - Application interface definition for dedicated short-range communication (ISO 14906:2011)

Perception du télépéage - Définition de l'interface d'application relative aux communications dédiées à courte portée (ISO 14906:2011)

Elektronische Gebührenerhebung - Anwendungsschnittstelle zur dezidierten Nahbereich-Kommunikation (ISO 14906:2011)

This European Standard was approved by CEN on 20 August 2011.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

This document (EN ISO 14906:2011) has been prepared by Technical Committee ISO/TC 204 "Intelligent transport systems" in collaboration with Technical Committee CEN/TC 278 “Road transport and traffic telematics” the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by April 2012, and conflicting national standards shall be withdrawn at the latest by April 2012.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO 14906:2004.

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, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

Endorsement notice

The text of ISO 14906:2011 has been approved by CEN as a EN ISO 14906:2011 without any modification.

INTERNATIONAL STANDARD

ISO 14906

Second edition
2011-10-15

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 14906:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 14906 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*, in collaboration with Technical Committee CEN/TC 278, *Road transport and traffic telematics*.

This second edition cancels and replaces the first edition (ISO 14906:2004), which has been technically revised.

Introduction

This International Standard specifies an application interface for electronic fee collection (EFC) systems, which are based on dedicated short-range communication (DSRC). It supports interoperability between EFC systems on an EFC-DSRC application interface level. This International Standard 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 International Standard 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 International Standard. 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 International Standard provides the basis for agreements between operators, which are needed to achieve interoperability. Based on the tools specified in this International Standard, 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 revision, 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 of this version of this International Standard.

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 listing of functional requirements, which can be satisfied by using the tools provided by this International Standard.

Annex E 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 F presents an informative mapping table between EFC vehicle data attributes and European registration certificates to ease the task of a service provider when he needs to personalise an OBE by obtaining vehicle data.

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 International Standard can also be used for onboard account systems, in conjunction with ISO/TS 25110, which provides examples of systems based on onboard accounts.

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

1 Scope

This International Standard 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 International Standard 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.

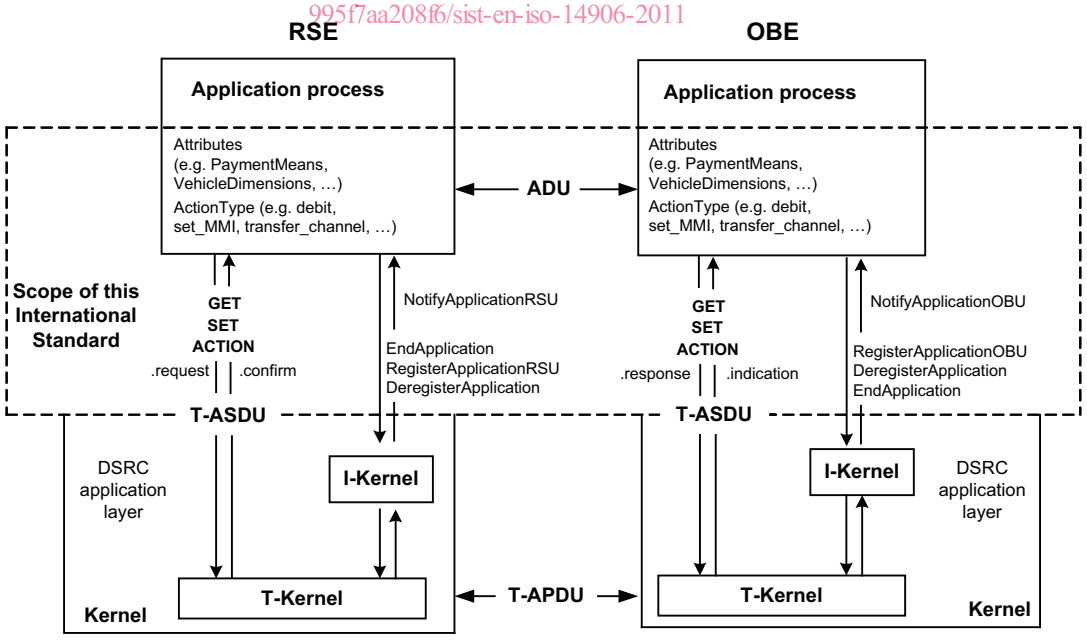

Figure 1 — The EFC application interface

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

This International Standard 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 International Standard.

2 Normative references

The following referenced documents are indispensable for the application 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 and funds*

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

ISO/IEC 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation*

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

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

ISO 15628:2007, *Road transport and traffic telematics — Dedicated short range communication (DSRC) — DSRC application layer*

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.

3.1
access credentials
data that is transferred to on-board equipment (OBE), in order to establish the claimed identity of a roadside equipment (RSE) application process entity

NOTE The access credentials carry information needed to fulfil access conditions in order to perform the operation on the addressed element in the OBE. The access credentials can carry passwords as well as cryptographic based information such as authenticators.

3.2
action
function that an application process resident at the roadside equipment can invoke in order to make the on-board equipment (OBE) execute a specific operation during the transaction

3.3
attribute
application information formed by one or by a sequence of data elements, and that is managed by different actions used for implementation of a transaction

3.4
authenticator
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and/or the integrity of the data unit and protect against forgery

3.5
channel
information transfer path

[ISO 7498-2:1989, definition 3.3.13]

3.6
component
logical and physical entity composing an on-board equipment, supporting a specific functionality

3.7
contract
expression of an agreement between two or more parties concerning the use of the road infrastructure

3.8
cryptography
discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use

[ISO 7498-2:1989, definition 3.3.20]

3.9
data group
collection of closely related EFC data attributes which together describe a distinct part of an EFC transaction

3.10
data integrity
property that data has not been altered or destroyed in an unauthorised manner

[ISO 7498-2:1989, definition 3.3.21]

3.11
element
⟨DSRC⟩ directory containing application information in the form of attributes

3.12
empty list
container for attributeValues (OCTET STRING) with the length equal to zero

3.13
on-board equipment
equipment fitted within or on the outside of a vehicle and used for toll purposes

NOTE The OBE does not need to include payment means.

3.14
on-board unit
minimum component of an on-board equipment, whose functionality always includes at least the support of the DSRC interface