SLOVENSKI STANDARD
SIST EN ISO 14906:2005

01-januar-2005

BUXca Yý U.
SIST ENV ISO 14906:2003

Cestna transportna in prometna telematika (RTTT) – Elektronsko pobiranje pristojbin – Definicija aplikacijskega vmesnika za posebne komunikacije kratkega dosega (ISO 14906:2004)

Road transport and traffic telematics - Electronic fee collection - Application interface definition for dedicated short-range communication (ISO 14906:2004)

iTeh STANDARD PREVIEW
Straßenverkehrstelematik - Elektronische Gebührenerfassung (EFC) - Anforderungen an
die EFC-Schnittstelle für Fahrzeug-Baken-Kommunikation (ISO 14906:2004)
(standards.iteh.ai)

SIST EN ISO 14906:2005
Télématique de la circulation et du transport routier - Perception du télépéage - Définition
de l'interface d'application relative aux communications dédiées a courte portée (ISO
14096:2004)

Ta slovenski standard je istoveten z: EN ISO 14906:2004

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 14906:2005   **en**

SIST EN ISO 14906:2005
https://standards.iteh.ai/catalog/standards/sist/e4f5da3d-95c4-4547-9484-
5691becd0f2c/sist-en-iso-14906-2005

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 14906

September 2004

ICS 35.240.60

English version

Road transport and traffic telematics - Electronic fee collection - Application interface definition for dedicated short-range communication (ISO 14906:2004)

Télématique de la circulation et du transport routier - Perception du télépéage - Définition de l'interface d'application relative aux communications dédiées à courte portée (ISO 14096:2004)

Straßenverkehrstelematik - Elektronische Gebührenerfassung (EFC) - Anforderungen an die EFC-Schnittstelle für Fahrzeug-Baken-Kommunikation (ISO 14906:2004)

This European Standard was approved by CEN on 30 April 2004.

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 Central Secretariat 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 Central Secretariat has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

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

Management Centre: rue de Stassart, 36   B-1050 Brussels

Ref. No. EN ISO 14906:2004: E

Contents

Foreword

This document (EN ISO 14906:2004) has been prepared by Technical Committee CEN/TC 278 "Road Transport and Traffic Telematics (RTTT)", the secretariat of which is held by NEN, in collaboration with Technical Committee ISO/TC 204 "Intelligent Transport Systems (ITS)".

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 March 2005, and conflicting national standards shall be withdrawn at the latest by March 2005.

This document supersedes ENV ISO 14906:1998.

In order to facilitate migration from ENV ISO 14906, equipment procured and installed in accordance with ENV ISO 14906 has been considered when drafting this European Standard. Operation of such equipment and procurement of additional equipment for systems based on such equipment can continue with reference to Directive 93/36/EEG Article 8 item 3c.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

Introduction

This document specifies an application interface for Electronic Fee Collection (EFC) systems, which are based on the Dedicated Short-Range Communication (DSRC). It supports interoperability between EFC systems on an EFC-DSRC application interface level.

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 European Standard. It is not envisaged that the complete set of EFC attributes and functions is present in each piece of EFC equipment, be 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 RSE, or they may reach an agreement to define a new transaction (and contract) that is common to both. Considerations should also be made by each operator that the RSE has sufficient resources to implement such additional EFC transactions.

In order to achieve interoperability, operators should agree on issues like:

— 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 (e.g. as entry tickets or as proof of payment);

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

This document has the following structure. In the first four clauses the scope, normative references, definitions of terms and abbreviations are accounted for. Next, in Clause 5, the EFC Application interface architecture is described in terms of its relation to the DSRC communication architecture, including the addressing of data attributes and of components. In the following Clause 6, the EFC transaction model is introduced, defining the common steps of each EFC transaction, in particular the initialisation phase. Clauses 7 and 8 are dedicated to the detailed specification of the EFC application functions and of the EFC data attributes, respectively. Four annexes provide:

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

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

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

4. Annex D: an informative listing of functional requirements, which can be satisfied by using the tools provided by this document.

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. The scope of this document comprises specifications of:

— EFC attributes (i.e. EFC application information);

— 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.
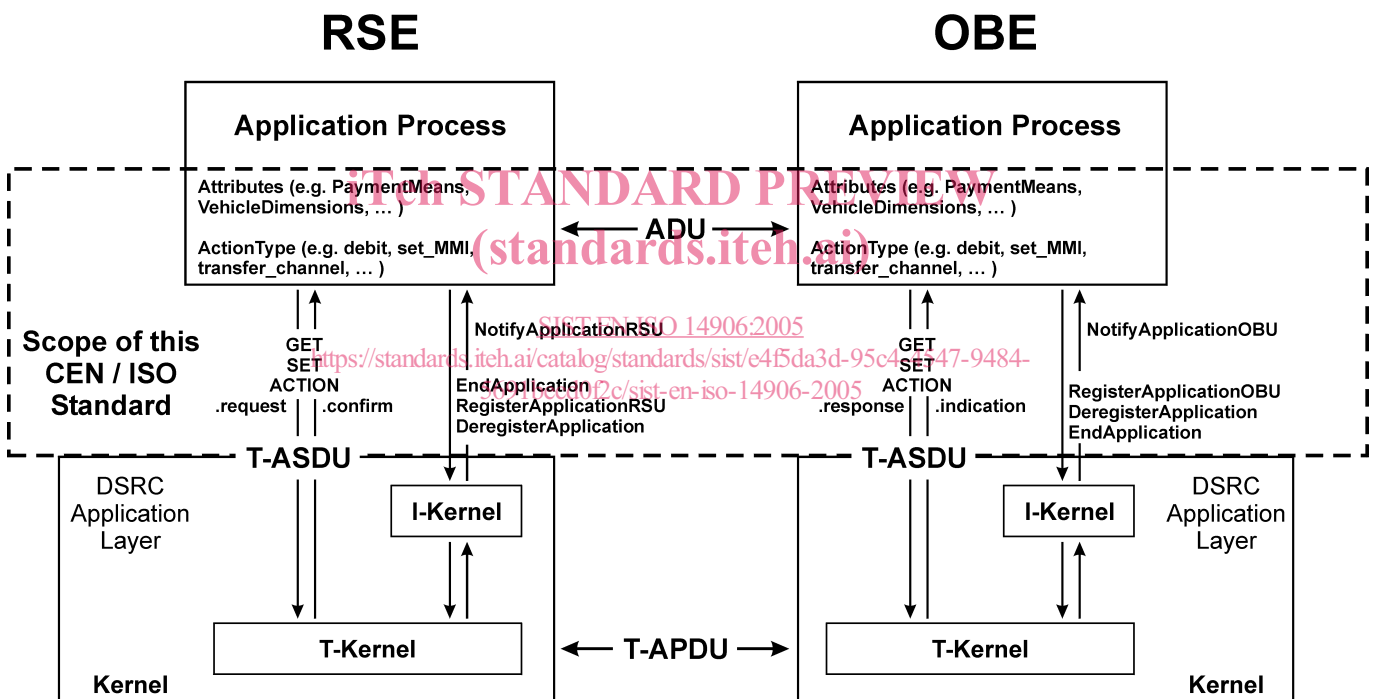

Figure 1 — The EFC application interface

This is an interface standard, adhering to the open systems interconnection (OSI) philosophy (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 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 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.

EN 12834:2003, *Road transport and traffic telematics - Dedicated Short Range Communication (DSRC) – DCRC application layer.*

EN ISO 3166-1, *Codes for the representation of names of countries and their subdivisions - Part 1: Country codes (ISO 3166-1:1997).*

EN ISO/IEC 7812-1, *Identification cards - Identification of issuers - Part 1: Numbering system (ISO/IEC 7812-1:1993).*

ENV ISO[1] 14816:2000, *Road Traffic and Transport Telematics (RTTT) - Automatic Vehicle and Equipment Identification – Numbering and Data Structures (ISO/TR 14816:2000).*

ISO 612, *Road vehicles - Dimensions of motor vehicles and towed vehicles - Terms and definitions.*

ISO 1176, *Road vehicles - Masses - Vocabulary and codes.*

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

ISO 4217, *Codes for the representation of currencies and funds.*

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/DIS 15628:2003, *Transport Information and Control System (TICS) - Dedicated Short-Range Communication (DSRC) – DSRC Application Layer.*

---

[1] Currently being revised.

6

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 carries 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* execute a specific operation during the *transaction*

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

3.4
authenticator
data appended to, or a cryptographic transformation (see 3.8) 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]

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 or/and prevent its unauthorised use

[ISO 7498-2]

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]

3.11
element
in the context of DSRC, a directory containing application information in form of *attributes*

3.12
on-board equipment
equipment located within the vehicle and supporting the information exchange with the *roadside equipment*. It is composed of the *on-board unit* and other sub-units whose presence have to be considered optional for the execution of a *transaction*

3.13
on-board unit
inimum component of an *on-board equipment*, whose functionality always includes at least the support of the DSRC interface

3.14
roadside equipment
Equipment located at a fixed position along the road transport network, for the purpose of communication and data exchanges with the *on-board equipment* of passing vehicles

3.15
service (EFC)
road transport related facility provided by a *service provider*. Normally a type of infrastructure, the use of which is offered to the *user* for which the *User* may be requested to pay

3.16
service primitive (communication)
elementary communication service provided by the Application layer protocol to the application processes

NOTE   The invocation of a service primitive by an application process implicitly calls upon and uses services offered by the lower protocol layers.

3.17
service provider (EFC)
operator that accepts the user's payment means and in return provides a road-use service to the user

3.18
session
exchange of information and interaction occurring at a specific EFC station between the *roadside equipment* and the user/vehicle

3.19
transaction
whole of the exchange of information between the *roadside equipment* and the *on-board equipment* necessary for the completion of an EFC operation over the DSRC

3.20
transaction model
functional model describing the general structure of Electronic Payment Fee Collection transactions

3.21
user
entity that uses transport services provided by the *Service Provider* according to the terms of a *contract*

4 Abbreviations

For the purpose of this document, the following abbreviations apply throughout the document unless otherwise specified.

4.1
ADU
Application Data Unit

4.2
APDU
Application Protocol Data Unit

4.3
AP
Application Process

4.4
ASN.1
Abstract Syntax Notation One (ISO/IEC 8824-1)

4.5
B-Kernel
Broadcast Kernel

4.6
BST
Beacon Service Table

4.7
cf
Confirm

4.8
DSRC
Dedicated Short-Range communication

4.9
EID
Element Identifier

4.10
EFC
Electronic Fee Collection

4.11
EVENT-RT
EVENT-REPORT

4.12
GPS
Global Positioning System

4.13
ICC
Integrated Circuit(s) Card

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4.14
I-Kernel
Initialisation Kernel

4.15
IID
Invoker Identifier

4.16
ind
Indication

4.17
L1
Layer 1 of DSRC (Physical Layer)

4.18
L2
Layer 2 of DSRC (Data Link Layer)

4.19
L7
Application Layer Core of DSRC

4.20
LID
Logical Link Control Identifier

iTeh STANDARD PREVIEW

(standards.iteh.ai)

4.21
LLC
Logical Link Control

4.22
LPDU
LLC Protocol Data Unit

4.23
MAC
Medium Access Control

4.24
MMI
Man-Machine Interface

4.25
n.a.
Not applicable

4.26
OBE
On-Board Equipment

4.27
OBU
On-Board Unit

4.28
PDU
Protocol Data Unit

10

4.29
PER
Packed Encoding Rules (ISO/IEC 8825-2)

4.30
PPDU
Physical Layer Protocol Data Unit

4.31
req
Request

4.32
rs
Response

4.33
RSE
Roadside Equipment

4.34
RTTT
Road Transport and Traffic Telematics

4.35
SAM
Secure Application Module

4.36
T-APDU
Transfer-Application Protocol Data Unit

4.37
T-ASDU
Transfer-Application Service Data Unit

4.38
T Kernel
Transfer Kernel

4.39
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/DIS 15628).
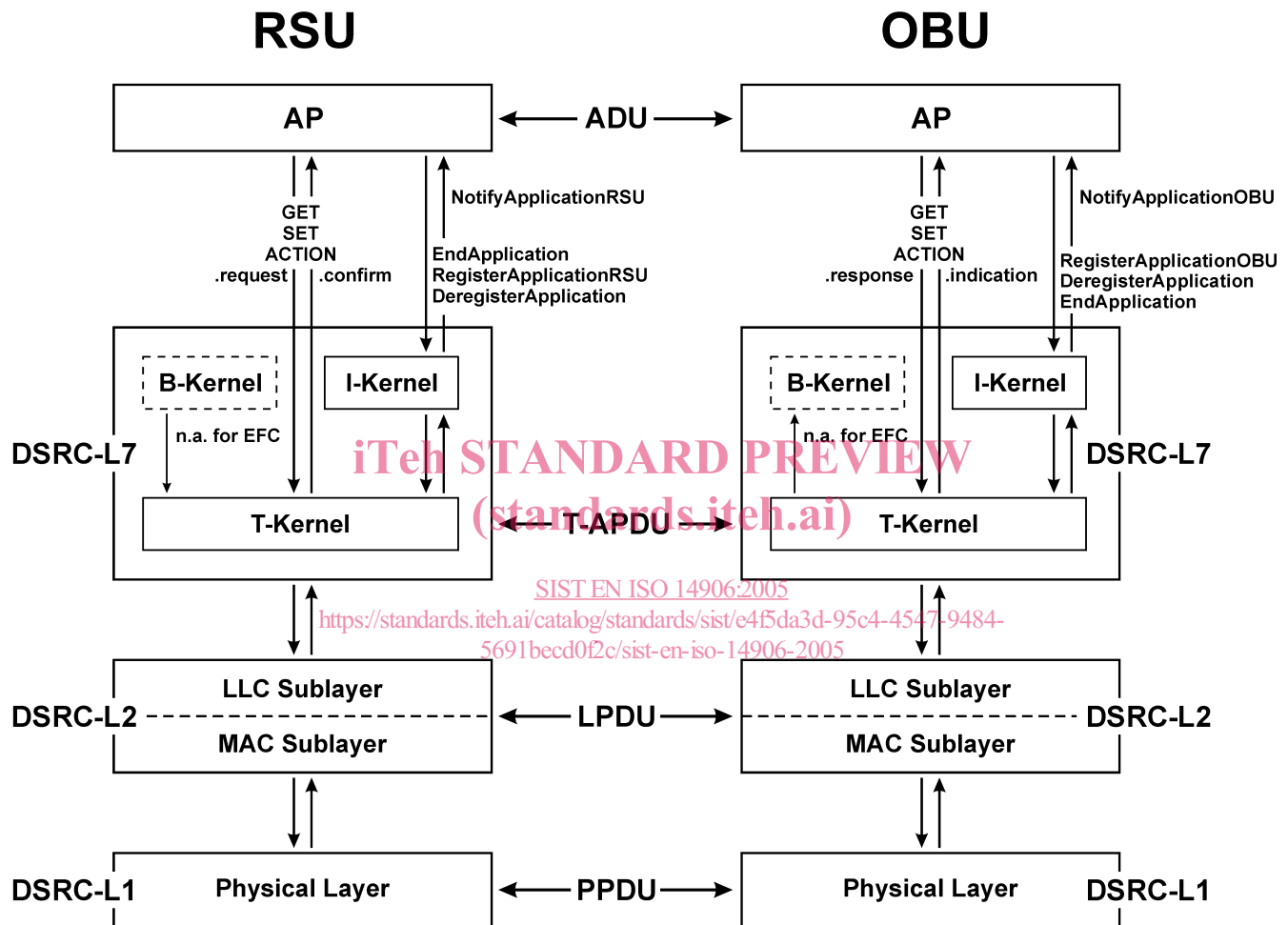

Figure 2 — The EFC application process on top of the DSRC communication stack

NOTE   The abbreviations 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.

— INITIALISATION: The invocation of an initialisation service request by RSE results in an attempt to initialise communication between a RSE and each OBE that has not yet established communication with the concerned RSE. The Initialisation service is only used by the Initialisation Kernel as defined in EN 12834 / ISO/DIS 15628.

5.2 Usage of DSRC application layer by the EFC application interface

EFC uses the following services offered by DSRC Application Layer (as defined in EN 12834 / ISO/DIS 15628):

— The INITIALISATION services:

  — Notify Application RSU   (at RSE);

  — End Application   (at RSE);

  — Register Application RSU (at RSE);

  — Deregister Application   (at RSE and OBE);

  — Notify Application OBU   (at OBE);

  — Register Application OBU(at OBE)

are used to realise the EFC-specific initialisation mechanism (see clause 6);

— The GET service is used to retrieve EFC attributes (For attribute specifications see clause 8);

— The SET service is used to set EFC attributes;

— The ACTION services are applied to realise additional EFC specific functionality needed to support EFC application processes, such as TRANSFER_CHANNEL, SET_MMI and ECHO (see 7.2).

In the following, the EFC-specific usage of the DSRC Layer 7 services is specified in detail.

NOTE   The EVENT-REPORT-service can be implicitly used by EFC application processes. It is e.g. used indirectly as part of an already defined command to release an application process (see EN 12834 / ISO/DIS 15628, Ready Application). However as the EVENT-REPORT-service is not explicitly used by EFC application processes, this service is not further referred to in this document.

5.3 Addressing of EFC attributes

5.3.1 Basic mechanism

EFC Attributes are used to transfer the EFC application-specific information.

EFC Attributes are composed of one or more data elements of specified ASN.1 types. Each data element is associated with, within the context of this document, an unambiguous name.

To each EFC Attribute, an AttributeID is associated. The AttributeId enables to unambiguously identify and address an EFC Attribute.