SLOVENSKI STANDARD
oSIST prEN 15509:2013

01-januar-2013

Elektronsko pobiranje pristojbin - Medobratovalnost profila aplikacije za DSRC

Electronic fee collection - Interoperability application profile for DSRC

Elektronische Gebührenerhebung - Interoperable Anwendungsprofile für DSRC

Perception de télépéage - Profil d'application d'interopérabilité pour DSRC

Ta slovenski standard je istoveten z: prEN 15509

ICS:

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

oSIST prEN 15509:2013 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 15509

October 2012

ICS 35.240.60

Will supersede EN 15509:2007

English Version

Electronic fee collection - Interoperability application profile for DSRC

Perception de télépéage - Profil d'application d'interopérabilité pour DSRC

Elektronische Gebührenerhebung - Interoperable Anwendungsprofile für DSRC

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 278.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. prEN 15509:2012: E

Contents

Page

Foreword

This document (prEN 15509:2012) has been prepared by Technical Committee CEN/TC 278 “Road transport and traffic telematics”, the secretariat of which is held by NEN.

This document is currently submitted to the CEN Enquiry.

This document will supersede EN 15509:2007.

Introduction provides details of significant technical changes between this European Standard and the previous edition.

This European Standard defines an Application Profile based on a set of base standards according to the concept of "International Standardised Profiles (ISP)" as defined in ISO/IEC TR 10000-1. The objective is to support technical interoperability between EFC DSRC-based systems in Europe. The principles of Application Profiling and relations to underlying base standards are defined in the Introduction.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

Introduction

CEN/TC 278(/WG 1) has produced a set of standards that supports interoperable electronic fee collection (EFC) dedicated short-range communication (DSRC)-based systems (e.g. EN ISO 14906, a “toolbox” for defining EFC-application transactions). However, these standards are necessary but not sufficient to ensure technical interoperability. This European Standard provides for a coherent set of requirements of the EFC-application that may serve as a common technical platform for EFC-interoperability.

This European Standard defines an Interoperable Application Profile for DSRC-EFC transactions. The main objective is to support technical interoperability between EFC-systems within the scope of this European Standard (as defined in Clause 1 below). A basic description of the EFC-service and an EFC System can be found in ISO 17573.

This European Standard only defines a basic level of technical interoperability for EFC equipment, i.e. on-board unit (OBU) and roadside equipment (RSE) using DSRC. It does not provide a full solution for interoperability, and it does not define other parts of the EFC-system, other services, other technologies and non-technical elements of interoperability.

The first elaboration of this European Standard was based on the experiences from a vast number of implementations and projects throughout Europe. This European Standard makes use of the results from European projects such as CARDME, PISTA and CESARE, as they represent the fruit of European EFC harmonisation and have been used as the basis for several national implementations. The development of a common European Electronic Toll Service (EETS) as a part of the European EFC Directive (2004/52/EC) also calls for the definition of an interoperable EFC-service. This European Standard provides for effective support for the work on the definition of EETS.

For the revision of this European Standard, the following principles have been followed:

- take into the evolution of the base standards;

- keep compatibility with the previous version of this European Standard.

Although there already are numerous existing base standards and specifications, there are specific needs that motivate this Interoperable Application Profile standard.

- Definition of the necessary and sufficient EFC-DSRC requirements to support technical interoperability.

- Provision of a crucial part of the EETS and hence support for the EFC Directive (2004/52/EC), the Commission Decision of 6 October 2009 on the definition of the European Electronic Toll Service and its technical elements complemented by the Guide for the application of the directive on the interoperability of electronic road toll systems

- CARDME/PISTA/CESARE dialects are used in many countries but they need to converge, as the present situation is not cost effective.

- Needed additional DSRC-requirements are made.

- Choice of data elements including vehicle data.

- Extended definition of the use of some data elements, including semantics and coding.

- Clear choices for security implementation.

- It facilitates a complementing test specification (with clear relations between the conformance requirements and evaluation tests).

- Good support for procurements.

The Application Profile is described using the concept of "International Standardised Profiles (ISP)" as defined in ISO/IEC TR 10000-1. The ISP-concept is specifically suited for defining interoperability specifications where a set of base standards can be used in different ways. This is exactly the case in EFC, where a set of base standards allows for different choices that are not interoperable.

The principles of the ISP-concept can be summarised as follows.

- An ISP shall make references only to base standards or other ISPs.

- The profile shall restrict the choice of base standard options to the extent necessary to maximise the probability of interoperability (e.g. chosen classes, conforming subsets, options and parameter values of base standards).

- The ISP shall not copy content of the base standards (in order to void consistency problems with the base standards).

- The profile shall not specify any requirements that would contradict or cause non-conformance to the base standards.

- The profile may contain conformance requirements that are more specific and limited in scope than those of the base standards.

- Conformance to a profile implies by definition conformance to a set of base standards, whereas conformance to that set of base standards does not necessarily imply conformance to the profile.

The use of the Application Profiling concept also provides for a flexible framework towards adoption, migration and use of this European Standard. Toll Chargers, Toll Service Providers and Manufacturers may use this Application Profile as a basis for interoperable use of their equipment, without having to disturb or otherwise affect any EFC-system used locally.

The Interoperable Application Profile is defined in terms of conformance requirements as given in Clause 5. To facilitate easy referencing, testing and look-up, these requirements are divided into two parts; On-Board Unit (OBU) requirements (5.1) and Roadside Equipment (RSE) requirements (5.2).

In addition this European Standard also includes various annexes that provide further detailed specifications as well as background, motivation and examples for the conformance requirements. The intention is that these enhance readability and understanding of this European Standard.

The base standard EN ISO 14906:2011 has been the subject of a revision. The revision of EN 15509 takes into account this fact.

This European Standard is complemented by a set of standards defining Conformity Evaluation of the Conformance Requirements.

EN 15876 defined how to evaluate on-board and roadside equipment for conformity to EN 15509 (this European Standard). EN 15876 consists of the following parts, under the general title "*Electronic fee collection — Evaluation of on-board and roadside equipment for conformity to EN 15509*":

- Part 1: Test suite structure and test purposes;

- Part 2: Abstract test suite.

1 Scope

The scope for this European Standard is limited to

- payment method: Central account based on EFC-DSRC,
- physical systems: OBU, RSE and the DSRC interface between them (all functions and information flows related to these parts),
- DSRC-link requirements,
- EFC transactions over the DSRC interface,
- data elements to be used by OBU and RSE used in EFC-DSRC transactions,
- security mechanisms for OBU and RSE used in EFC-DSRC transactions.

The scope of this European Standard is illustrated in Figure 1.

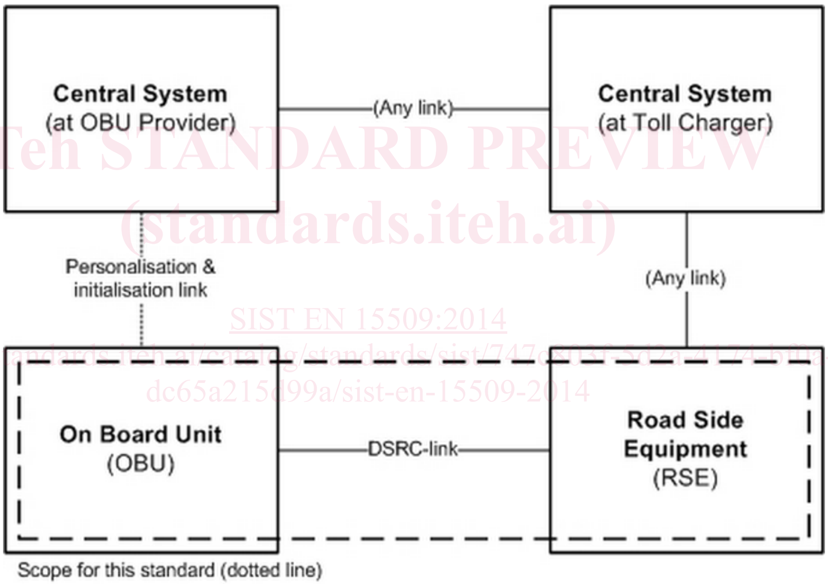

Figure 1 — Scope for this European Standard (within the box delimited with a dotted line)

It is outside the scope of this European Standard to define

- contractual and procedural interoperability requirements (including issues related to a Memorandum of Understanding, MoU),
- conformance procedures and test specification (this is provided in a separate set of standards),
- setting-up of operating organisations (e.g. clearing operator, issuing, trusted third party etc.),
- legal issues,
- other payment methods in DSRC-based EFC (e.g. on-board accounts using integrated circuit cards),

- other basic technologies (e.g. GNSS/CN or video registration based EFC). However, this European Standard may be used for defining the DSRC-EFC parts for the use in applications that implement a mix of different technologies.
- other interfaces or functions in EFC-systems than those specified above (i.e. information flows and data exchange between operators or personalisation, initialisation and customisation of the OBU).

Some of these issues are subject to separate standards prepared by CEN/TC 278, ISO/TC 204 or ETSI ERM.

Figure 2 shows the scope of this European Standard from a DSRC-stack perspective.

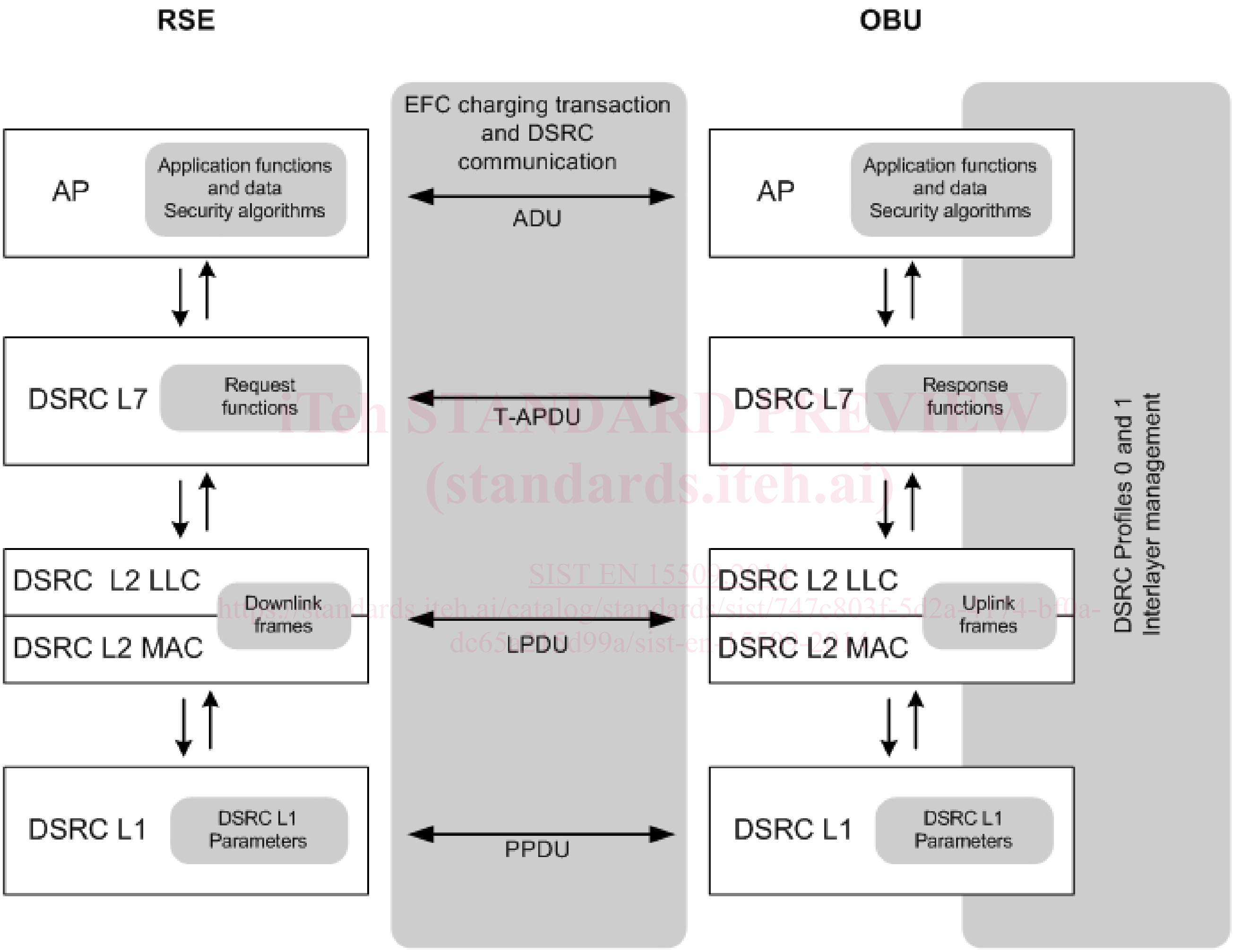

Figure 2 — Relationship between this European Standard and DSRC-stack elements

This European Standard defines an Application Profile based on the ISP-concept. The base standards that this Application Profile is based upon are

- EN ISO 14906 on EFC application interface definition for DSRC (this implies indirect references to EN ISO 14816 on Numbering and data structures),
- EN 12834: on DSRC application layer (L7),
- EN 13372 on DSRC profiles (this implies indirect references to the DSRC L1, L2 and L7 standards: EN 12253, EN 12795 and EN 12834).

The relationship and references between base standards and EN 15509 are illustrated in Figure 3.

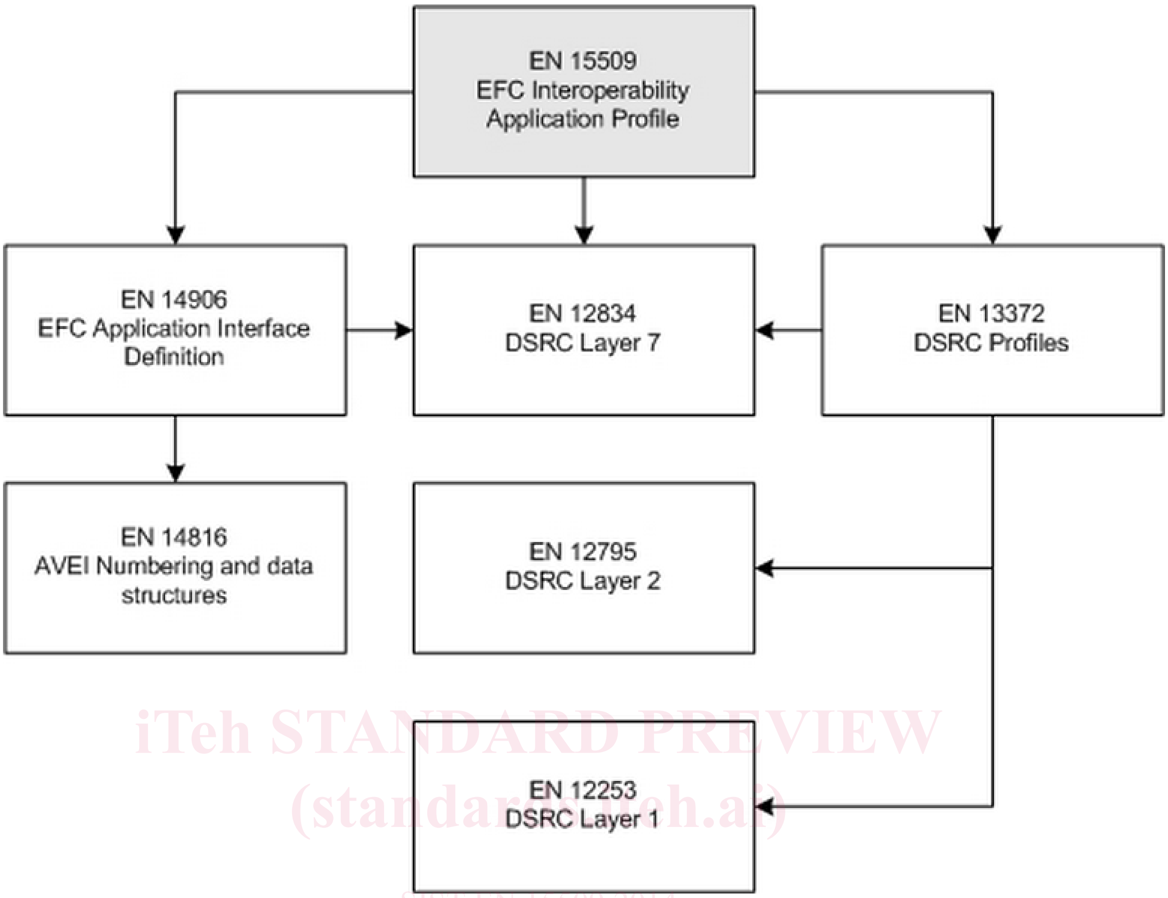

Figure 3 — Relationship and references between base standards and EN 15509

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ANSI X3.92:1981, *American National Standard for Information Systems — Data encryption algorithm*

FprCEN/TS 16439:2012, *Electronic fee collection — Security framework*

EN 12834, *Road transport and traffic telematics — Dedicated Short Range Communication (DSRC) — DSRC application layer*

EN 13372:2004, *Road transport and traffic telematics (RTTT) — Dedicated short-range communication — Profiles for RTTT applications*

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

ETSI TS 102 486-1-1 V1.1.1 (2006-03), *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 1: DSRC data link layer: medium access and logical link control; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification*

ETSI TS 102 486-2-1 V1.1.1 (2006-03) 1), *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 2: DSRC application layer; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification*

ISO/IEC 9646-7, *Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 7: Implementation Conformance Statements*

ISO/IEC 9797-1:1999 2), *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

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

[SOURCE: EN ISO 14906:2011, 3.1]

Note 1 to entry 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* execute a specific operation during the *transaction*

[SOURCE: EN ISO 14906:2011, 3.2]

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*

[SOURCE: EN ISO 14906:2011, 3.3]

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

[SOURCE: EN ISO 14906:2011, 3.4]

1) ETSI TS 102 486-2-1 V1.1.1 (2006-03) is replaced by ETSI TS 102 486-2-1 V1.2.1 (2008-10), *Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 2: DSRC application layer; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification.*

2) ISO/IEC 9797-1:1999 is replaced by ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher.*

3.5
base standard
approved international standard or ITU-T Recommendation

[SOURCE: ISO/IEC TR 10000-1:1998, 3.1.1]

3.6
channel
information transfer path

[SOURCE: ISO 7498-2, 3.3.13, and EN ISO 14906:2011, 3.5]

3.7
component
logical and physical entity composing an *on-board equipment*, supporting a specific functionality

[SOURCE: EN ISO 14906:2011, 3.6]

3.8
contract
expression of an agreement between two or more parties concerning the use of the road infrastructure

[SOURCE: EN ISO 14906:2011, 3.7]

3.9
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

[SOURCE: EN ISO 14906:2011, 3.8]

3.10
data group
collection of closely related EFC data attributes which together describe a distinct part of an EFC transaction

[SOURCE: EN ISO 14906:2011, 3.9]

3.11
data integrity
property that data has not been altered or destroyed in an unauthorised manner

[SOURCE: EN ISO 14906:2011, 3.10]

3.12
element
in the context of DSRC, a directory containing application information in form of *attributes*

[SOURCE: EN ISO 14906:2011, 3.11]

3.13
International Standardised Profile
internationally agreed-to, harmonised document which describes one or more profiles

[SOURCE: ISO/IEC TR 10000-1:1998, 3.1.2]

3.14
interoperability
ability of two or more IT systems to exchange information and to make mutual use of the information that has been exchanged

[SOURCE: ISO/IEC TR 10000-1:1998, 3.2.1]

3.15
mobile roadside equipment
roadside equipment located on-board of special vehicles using or standing near the road transport network or hand-held equipment, for the purpose of communication and data exchanges with the on-board equipment of passing vehicles, within the specific scope of Compliance Checking Communication

[SOURCE: CEN ISO/TS 12813:2009, 3.7]

3.16
on-board equipment
equipment fitted within or on the outside of a vehicle and used for toll purposes

Note 1 to entry The OBE does not need to include payment means.

[SOURCE: EN ISO 14906:2011, 3.13]

3.17
on-board unit
minimum component of an *on-board equipment*, whose functionality always includes at least the support of the DSRC interface

[SOURCE: EN ISO 14906:2011, 3.14]

3.18
profile
set of one or more base standards and/or ISP, and where applicable, the identification of chosen classes, conforming subsets, options and parameters of those base standards, or ISPs necessary to accomplish a particular function

[SOURCE: ISO/IEC TR 10000-1:1998, 3.1.4]

3.19
roadside equipment
equipment located along the road transport network, for the purpose of communication and data exchanges with on-board equipment

[SOURCE: EN ISO 14906:2011, 3.16]

3.20
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

[SOURCE: EN ISO 14906:2011, 3.17]

3.21
service primitive
(communication) elementary communication service provided by the Application layer protocol to the application processes

[SOURCE: EN ISO 14906:2011, 3.18]

Note 1 to entry The invocation of a service primitive by an application process implicitly calls upon and uses services offered by the lower protocol layers.

3.22
session
exchange of information and interaction occurring at a specific EFC station between the *roadside equipment* and the user/vehicle

[SOURCE: EN ISO 14906:2011, 3.19]

3.23
toll charger
legal entity charging toll for vehicles in a toll domain

[SOURCE: EN ISO 14906:2011, 3.20]

3.24
toll service provider
legal entity providing to his customers toll services on one or more toll domains for one or more classes of vehicles

Note 1 to entry In other documents the terms issuer or contract issuer may be used.

Note 2 to entry The Toll Service Provider may provide the OBE or may provide only a magnetic card or a smart card to be used with OBE provided by a third party (like a mobile telephone and a SIM card can be obtained from different parties).

Note 3 to entry The Toll Service Provider is responsible for the operation (functioning) of the OBE with respect to tolling.

[SOURCE: EN ISO 14906:2011, 3.23]

3.25
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

[SOURCE: EN ISO 14906:2011, 3.24]

3.26
transaction counter
data value in the on-board unit that is incremented by the roadside equipment at each transaction

3.27
transaction model
functional model describing the general structure of Electronic Payment Fee Collection transactions

[SOURCE: EN ISO 14906:2011, 3.25]

3.28
user
customer of a Toll Service Provider, one liable for toll, the owner of the vehicle, a fleet operator, a driver etc. depending on the context.

[SOURCE: EN ISO 14906:2011, 3.26]