



SLOVENSKI STANDARD
SIST EN 15509:2008
01-februar-2008

Cestna transportna in prometna telematika - Elektronsko pobiranje pristojbin - Medobratovalnost profila aplikacije za DSRC

Road transport and traffic telematics - Electronic fee collection - Interoperability application profile for DSRC

Straßenverkehrstelematik - Elektronische Gebührenerhebung - Anwendungsprofil für DSRC Interoperabilität

iTeh STANDARD PREVIEW

(transport.iTeh.ai)
Télématique de la circulation et du transport routier - Perception de télépéage - Profil d'application d'interopérabilité pour DSRC

[SIST EN 15509:2008](https://standards.iteh.ai/catalog/standards/sist/569f6cf5-0878-4d2e-ac97-35c47d383042/sist-en-15509-2008)

<https://standards.iteh.ai/catalog/standards/sist/569f6cf5-0878-4d2e-ac97-35c47d383042/sist-en-15509-2008>
Ta slovenski standard je istoveten z: EN 15509:2007

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 15509:2008

en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 15509:2008

<https://standards.iteh.ai/catalog/standards/sist/569f6cf5-0878-4d2e-ac97-55e47d883042/sist-en-15509-2008>

ICS 35.240.60

English Version

Road transport and traffic telematics - Electronic fee collection -
Interoperability application profile for DSRC

Télématique de la circulation et du transport routier -
Perception de télépéage - Profil d'application
d'interopérabilité pour DSRC

Straßenverkehrstelematik - Elektronische
Gebührenerhebung - Anwendungsprofil für DSRC
Interoperabilität

This European Standard was approved by CEN on 22 March 2007.

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 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 Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, 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.

[SIST EN 15509:2008](https://standards.iteh.ai/catalog/standards/sist/569f6c5f-0878-4d2e-ac97-55e47d883042/sist-en-15509-2008)

<https://standards.iteh.ai/catalog/standards/sist/569f6c5f-0878-4d2e-ac97-55e47d883042/sist-en-15509-2008>



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

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

Contents

Page

Foreword.....	4
Introduction	5
1 Scope	6
2 Normative references	10
3 Terms and definitions	10
4 Abbreviations	14
5 Conformance.....	16
5.1 OBU requirements	16
5.1.1 General.....	16
5.1.2 DSRC requirements	16
5.1.3 DSRC L7 and EFC functions.....	16
5.1.4 Data requirements	17
5.1.5 Security requirements	18
5.1.6 Transaction requirements.....	20
5.2 RSE requirements	20
5.2.1 General.....	20
5.2.2 DSRC requirements	20
5.2.3 DSRC L7 and EFC functions.....	20
5.2.4 Data requirements	20
5.2.5 Security requirements	21
5.2.6 Transaction requirements.....	21
Annex A (normative) Data specification	22
Annex B (normative) Security calculations	26
B.1 General.....	26
B.2 Attribute authenticator	26
B.2.1 General.....	26
B.2.2 Authenticator using the attribute Payment Means.....	28
B.3 Access Credentials.....	29
B.3.1 General.....	29
B.3.2 The principle of Access Credentials.....	29
B.3.3 Calculation of Access Credentials.....	29
B.4 Key derivation	30
B.4.1 General.....	30
B.4.2 Calculation of derived Authentication Key	30
B.4.3 Calculation of the Access Key	31
B.5 Transaction Counter.....	31
Annex C (normative) ICS proforma	32
C.1 General.....	32
C.2 Guidance for completing the ICS proforma	32
C.2.1 Purposes and structure	32
C.2.2 Abbreviations and conventions	32
C.3 Instructions for completing the ICS proforma.....	34
C.4 ICS proforma for OBU	35
C.4.1 Identification implementation.....	35
C.4.2 Identification of the standard	35
C.4.3 Global statement of conformance.....	35
C.4.4 ICS proforma for OBU	36

iTeh STANDARD PREVIEW

(standards.iteh.ai)

SIST EN 15509:2008

<https://standards.iteh.ai/catalog/standards/sist/56916cd5-0878-4d2e-ac97-55e47d883042/sist-en-15509-2008>

C.4.5	Profile requirement list for OBU	38
C.5	ICS proforma for RSE.....	41
C.5.1	Identification implementation	41
C.5.2	Identification of the standard	41
C.5.3	Global statement of conformance	41
C.5.4	ICS proforma for RSE.....	42
C.5.5	Profile requirement list for RSE	44
Annex D	(informative) IAP taxonomy and numbering.....	47
D.1	General	47
D.2	Contents of an Interoperable Application Profile (IAP)	47
D.3	IAP referencing and numbering	48
D.3.1	IAP numbering	48
D.3.2	Security levels numbering.....	48
D.3.3	Numbering and referencing examples	48
Annex E	(informative) Security computation examples.....	49
E.1	General	49
E.2	Computation of Attribute Authenticator	49
E.3	Computation of Access Credentials.....	50
E.4	Key derivation.....	51
E.4.1	Authenticator Key.....	51
E.4.2	Access Credentials Key.....	51
Annex F	(informative) Security considerations	53
Annex G	(informative) Inter layer management	55
G.1	General	55
G.2	RSE Inter Layer Management guidelines.....	55
G.3	OBU Inter Layer Management guidelines.....	55
G.4	State Transition Tables	56
Annex H	(informative) Vehicle classification data.....	61
Annex I	(informative) Using this European Standard for other DSRC-based transactions	62
Annex J	(informative) Mounting guidelines for the OBU	63
J.1	General	63
J.2	OBU mounting position	63
J.3	OBU minimum active angle.....	63
Bibliography	65

Foreword

This document (EN 15509:2007) has been prepared by 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 November 2007, and conflicting national standards shall be withdrawn at the latest by November 2007.

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.

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, 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.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST EN 15509:2008](https://standards.iteh.ai/catalog/standards/sist/569f6cf5-0878-4d2e-ac97-55e47d883042/sist-en-15509-2008)

<https://standards.iteh.ai/catalog/standards/sist/569f6cf5-0878-4d2e-ac97-55e47d883042/sist-en-15509-2008>

Introduction

CEN/TC278 (WG1) 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 the standard (as defined in Clause 1 below). A basic description of the EFC-service and an EFC System can be found in CEN/ISO TS 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 elaboration of this European Standard is based on the experiences from a vast number of implementations and projects throughout Europe. The 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.

SIST EN 15509:2008

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). Including structured management of revisions of the standard.
- 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 maximize 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 the standard. Operators, Issuers 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.

(standards.iteh.ai)

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 the 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 the standard.

It is noted that the base standard EN ISO 14906:2004 is subject to a near standing review. The next edition of EN ISO 14906 will incorporate advancements made since its publication such as e.g. the definition of additional Euro classes (i.e. Euro-4 and Euro-5). Hence, such amendments have not been made in this standard as it would jeopardise the consistency with the base standard and violate the ISP-concept.

This European Standard is complemented by a set of standards defining Conformity Evaluation of the Conformance Requirements in this European Standard (not finalised when writing this European Standard).

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.

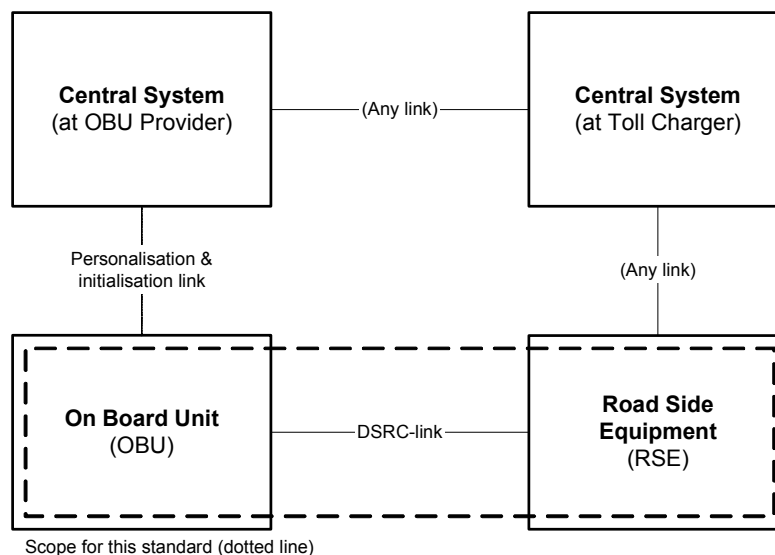


Figure 1 — Scope for this European Standard (within the box delimited with a dotted line)

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 organizations (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.

The following figure shows the scope of this European Standard from a DSRC-stack perspective.

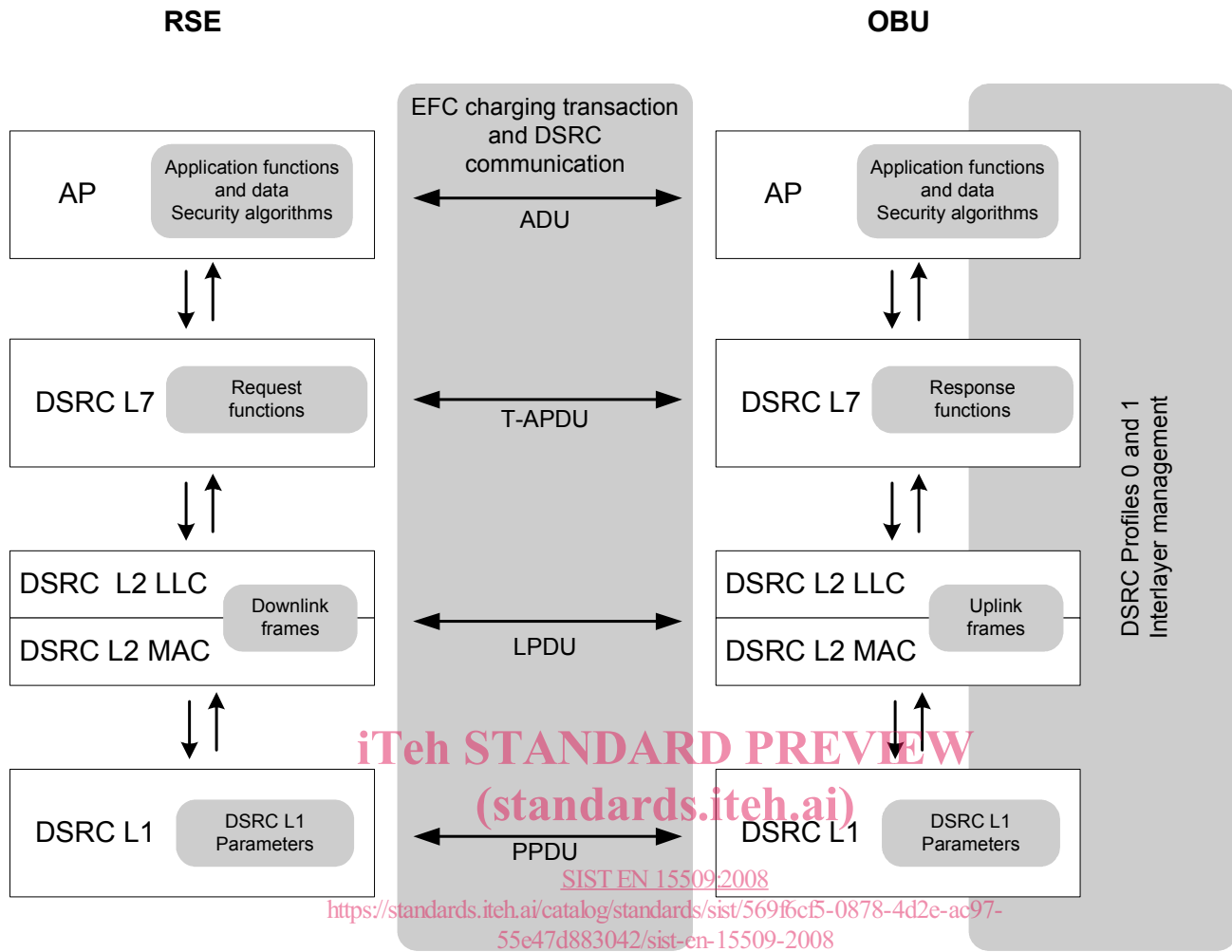
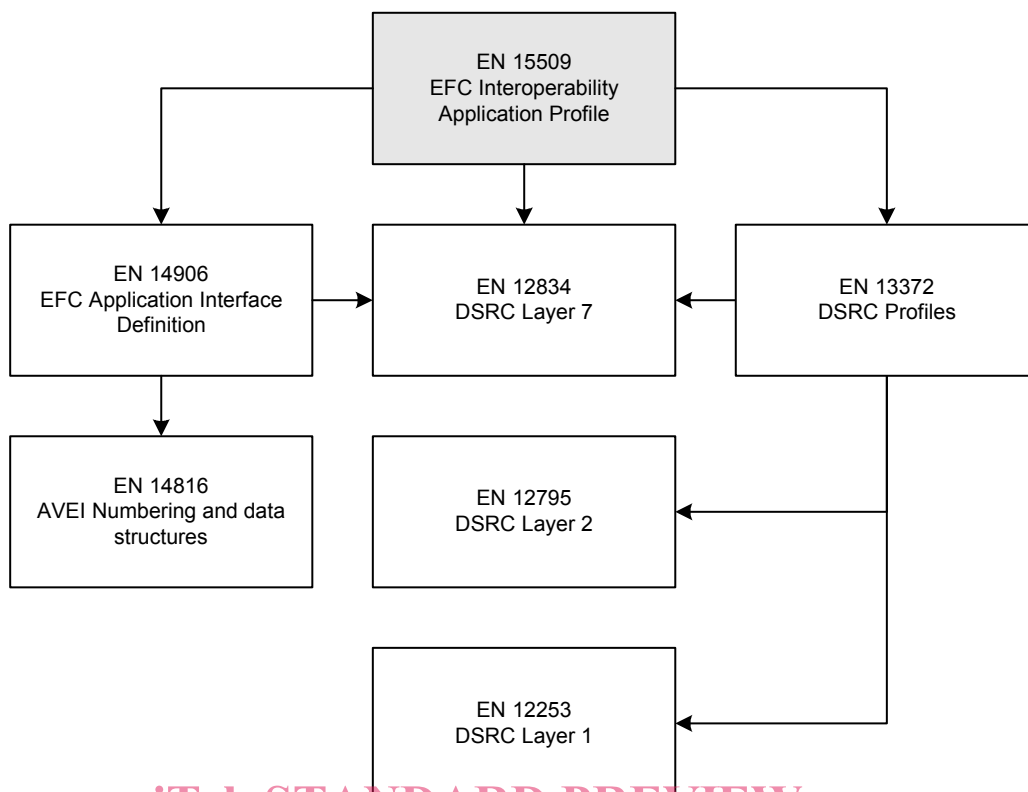


Figure 2 — Relations between this European Standard and DSRC-stack elements

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).



iTeh STANDARD PREVIEW
(standards.iteh.ai)

Figure 3 — Relation and references between base standards and EN 15509 (this European Standard)

[SIST EN 15509:2008](https://standards.iteh.ai/catalog/standards/sist/569f6cf5-0878-4d2e-ac97-55e47d883042/sist-en-15509-2008)

<https://standards.iteh.ai/catalog/standards/sist/569f6cf5-0878-4d2e-ac97-55e47d883042/sist-en-15509-2008>

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.

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

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

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

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 14906:2004, *Road transport and traffic telematics — Electronic fee collection — Application interface definition for dedicated short range communication (ISO 14609:2004)*

ETSI TS 102 486-1-1, *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 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, *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*

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

[EN ISO 14906:2004]

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* execute a specific operation during the *transaction*

[EN ISO 14906:2004]

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*

[EN ISO 14906:2004]

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

[EN ISO 14906:2004]

3.5**base standard**

an approved international standard or ITU-T Recommendation

[ISO/IEC TR 10000:1998]

3.6**channel**

information transfer path

[EN ISO/IEC 7498-2 and EN ISO 14906:2004]

3.7**component**

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

[EN ISO 14906:2004]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN 15509:2008](https://standards.iteh.ai/catalog/standards/sist/569f6cf5-0878-4d2e-ac97-55e47d883042/sist-en-15509-2008)

<https://standards.iteh.ai/catalog/standards/sist/569f6cf5-0878-4d2e-ac97-55e47d883042/sist-en-15509-2008>

3.8**contract**

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

[EN ISO 14906:2004]

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

[EN ISO 14906:2004]

3.10**data group**

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

[EN ISO 14906:2004]

3.11**data integrity**

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

[EN ISO 14906:2004]

**3.12
element**

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

[EN ISO 14906:2004]

**3.13
International Standardised Profile**

an internationally agreed-to, harmonised document which describes one or more profiles

[ISO/IEC TR 10000:1998]

**3.14
interoperability**

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

[ISO/IEC TR 10000:1998]

**3.15
issuer**

entity responsible for the payment system and responsible for issuing the Payment Means to the User

[CEN ISO/TS 17573:2003]

**3.16
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*

[EN ISO 14906:2004]

iTeh STANDARD PREVIEW

(standards.iteh.ai)

SIST EN 15509:2008

<https://standards.iteh.ai/catalog/standards/sist/569f6c5f-0878-4d2e-ac97-55e47d883042/sist-en-15509-2008>

**3.17
on-board unit**

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

[EN ISO 14906:2004]

**3.18
profile**

a 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

[ISO/IEC TR 10000:1998]

**3.19
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

[EN ISO 14906:2004]

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

[EN ISO 14906:2004]

3.21**service primitive (communication)**

elementary communication service provided by the Application layer protocol to the application processes

[EN ISO 14906:2004]

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

3.22**service provider (EFC)**

operator that accepts the user's payment means and in return provides a road-use service to the user

[EN ISO 14906:2004]

3.23**session**

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

[EN ISO 14906:2004]

3.24**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

[EN ISO 14906:2004]

3.25**transaction counter**

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

3.26**transaction model**

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

[EN ISO 14906:2004]

3.27**transport service provider**

person, company, authority or abstract entity offering a transport service to the User for which the user has to pay a fee (the fee will in some cases be zero, e.g. emergency vehicles)

[CEN ISO/TS 17573:2003]

3.28**user**

entity that uses transport services provided by the *service provider* according to the terms of a *contract*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 15509:2008

<https://standards.iteh.ai/catalog/standards/sist/5696-c5-0878-4d3e-a977-75-47d9830-12/sist-en-15509-2008>