

BS EN 15509:2014



BSI Standards Publication

Electronic fee collection — Interoperability application profile for DSRC

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This British Standard is the UK implementation of EN 15509:2014. It supersedes BS EN 15509:2007 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 80143 3

ICS 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2014.

Amendments issued since publication

Date	Text affected
------	---------------

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 15509

September 2014

ICS 35.240.60

Supersedes 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 - Anwendungsprofil für
DSRC Interoperabilität

This European Standard was approved by CEN on 18 July 2014.

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, 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.



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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2014 CEN All rights of exploitation in any form and by any means reserved
worldwide for CEN national Members.

Ref. No. EN 15509:2014 E

Contents

Page

Foreword.....	5
Introduction	7
1 Scope	9
2 Normative references	11
3 Terms and definitions	11
4 Symbols and abbreviations	14
5 Conformance	16
5.1 General.....	16
5.2 Base standards	16
5.3 Main contents of an EFC-DSRC-IAP	17
5.4 Conformance requirements	18
5.5 Conformation notification	18
5.6 Conformance evaluation and testing.....	18
5.7 Multiple IAPs	18
6 Requirements for EFC-DSRC-IAP 1	18
6.1 OBU requirements	18
6.1.1 General.....	18
6.1.2 DSRC requirements	18
6.1.3 DSRC L7 and EFC functions.....	19
6.1.4 Data requirements	19
6.1.5 Security requirements	21
6.1.6 Transaction requirements.....	22
6.2 RSE requirements	22
6.2.1 General.....	22
6.2.2 DSRC requirements	22
6.2.3 DSRC L7 and EFC functions.....	22
6.2.4 Data requirements	23
6.2.5 Security requirements	23
6.2.6 Transaction requirements.....	24
Annex A (normative) Data specification	25
Annex B (normative) Security calculations	29
B.1 General.....	29
B.2 Attribute authenticator	29
B.2.1 General.....	29
B.2.2 Authenticator using the attribute Payment Means.....	30
B.3 Access Credentials.....	32
B.3.1 General.....	32
B.3.2 The principle of Access Credentials.....	32
B.3.3 Calculation of Access Credentials	33
B.4 Key derivation	34
B.4.1 General.....	34

B.4.2	Calculation of derived Authentication Key	34
B.4.3	Calculation of the Access Key	34
B.5	Transaction Counter	35
Annex C	(normative) Implementation conformance statement proforma	36
C.1	General	36
C.2	Guidance for completing the ICS proforma	36
C.2.1	Purposes and structure	36
C.2.2	Abbreviations and conventions	36
C.3	Instructions for completing the ICS proforma	38
C.4	ICS proforma for OBU	38
C.4.1	Identification implementation	38
C.4.2	Identification of the standard	39
C.4.3	Global statement of conformance	39
C.4.4	ICS proforma for OBU	39
C.4.5	Profile requirements list for OBU	41
C.5	ICS proforma for RSE	45
C.5.1	Identification implementation	45
C.5.2	Identification of the standard	45
C.5.3	Global statement of conformance	45
C.5.4	ICS proforma for RSE	45
C.5.5	Profile requirements list for RSE	48
Annex D	(informative) IAP taxonomy and numbering	52
D.1	General	52
D.2	Contents of an Interoperable Application Profile (IAP)	52
D.3	IAP referencing and numbering	53
D.3.1	IAP numbering	53
D.3.2	Security levels numbering	53
D.3.3	Numbering and referencing examples	53
Annex E	(informative) Security computation examples	54
E.1	General	54
E.2	Computation of Attribute Authenticator	54
E.3	Computation of Access Credentials	55
E.4	Key derivation	55
E.4.1	Authenticator Key	55
E.4.2	Access Credentials Key	56
Annex F	(informative) Security Considerations	57
Annex G	(informative) Interlayer management	58
G.1	General	58

G.2	RSE Inter Layer Management guidelines	58
G.3	OBU Inter Layer Management guidelines	58
G.4	State Transition Tables	58
Annex H (informative)	Mounting guidelines for the OBU	64
H.1	General.....	64
H.2	OBU mounting position	64
Annex I (informative)	Use of this standard for the EETS	67
I.1	General.....	67
I.2	Overall relationship between European standardization and the EETS.....	67
I.3	European standardisation work supporting the EETS	67
I.4	Correspondence between this standard and the EETS.....	68
Bibliography		69

Foreword

This document (EN 15509:2014) has been prepared by Technical Committee CEN/TC 278 "Intelligent transport systems", 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 March 2015 and conflicting national standards shall be withdrawn at the latest by March 2015.

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 15509:2007.

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

This second edition of EN 15509 incorporates the following main modifications compared to the previous one:

- amendment of terms, in order to reflect harmonization of terms across electronic fee collection (EFC) standards;
- addition of a new clause (i.e. Clause 5) on conformance;
- amendment of the definition of vehicle licence plate number (size constraints and clarification that only Latin alphabet coding is supported)
- revision of the informative annex on security considerations (i.e. Annex F), and reference to CEN/TS 16439 on Electronic fee collection – Security framework;
- addition of a new informative annex (i.e. Annex I) on how to use this standard for the European electronic toll service;
- deletion of informative Annex H, part of the first edition, on Vehicle classification data, as it was deemed obsolete in view of EN ISO 14906:2011;
- deletion of informative Annex I, part of the first edition, on Using this European Standard for other DSRC-based transactions, as it was deemed obsolete in view of CEN ISO/TS 12813 and CEN ISO/TS 13141;
- amendments to reflect changes to the underlying base standards, with emphasis on backward compatibility with the first edition of this standard.

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

- take into account the evolution of some of the underlying standards and technical specifications, i.e. EN ISO 14906:2011, CEN/TS 16439, ISO/IEC 9797-1;
- maintain compatibility with the previous edition of this European Standard.

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, 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 the United Kingdom.

Introduction

CEN/TC 278 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 between DSRC-EFC-systems. This European Standard provides for a coherent set of requirements of the EFC-application and that is intended to 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 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 harmonization 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 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. After publication of EN 15509:2007 an EC-decision (2009/750/EC) on the EETS was adopted, that notes the first edition of this standard (EN 15509:2007) as a mandatory technical reference for the EETS. This has been fully maintained in this second edition of EN 15509.

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 European Directive (2004/52/EC), the European Commission Decision (2009/750/EC of 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 summarized 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 avoid 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 general requirements of the Interoperable Application Profile are set out in Clause 5, whilst the specific conformance requirements are given in Clause 6. To facilitate easy referencing, testing and look-up, these specific requirements are divided into two parts; On-Board Unit (OBU) requirements and Roadside Equipment (RSE) requirements.

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 the revision introduced in this base standard.

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

EN 15876 defines 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.

NOTE EN 15786-1 and EN 15786-2 will be subject to revision to accommodate the changes introduced in this second edition of EN 15509.

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.

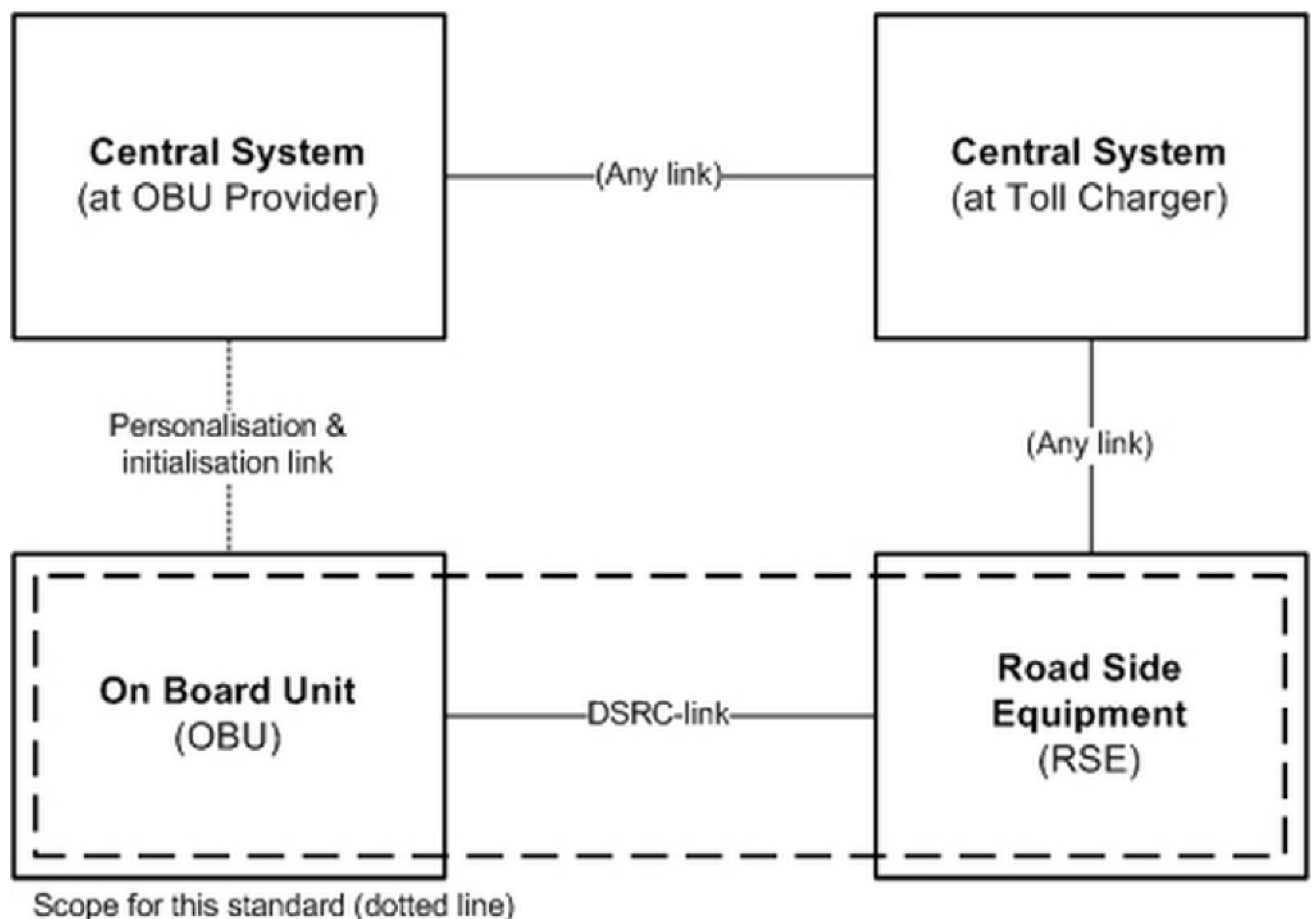


Figure 1 — Scope for this European Standard (within the box delimited with a dotted line)

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 organizations (e.g. toll charger, toll service provider, 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;
- non-EFC transactions over the DSRC interface (e.g. CCC and LAC communication, which is defined in other standards);
- other interfaces or functions in EFC-systems than those specified above (i.e. information flows and data exchange between operators or personalization, initialization and customization 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.

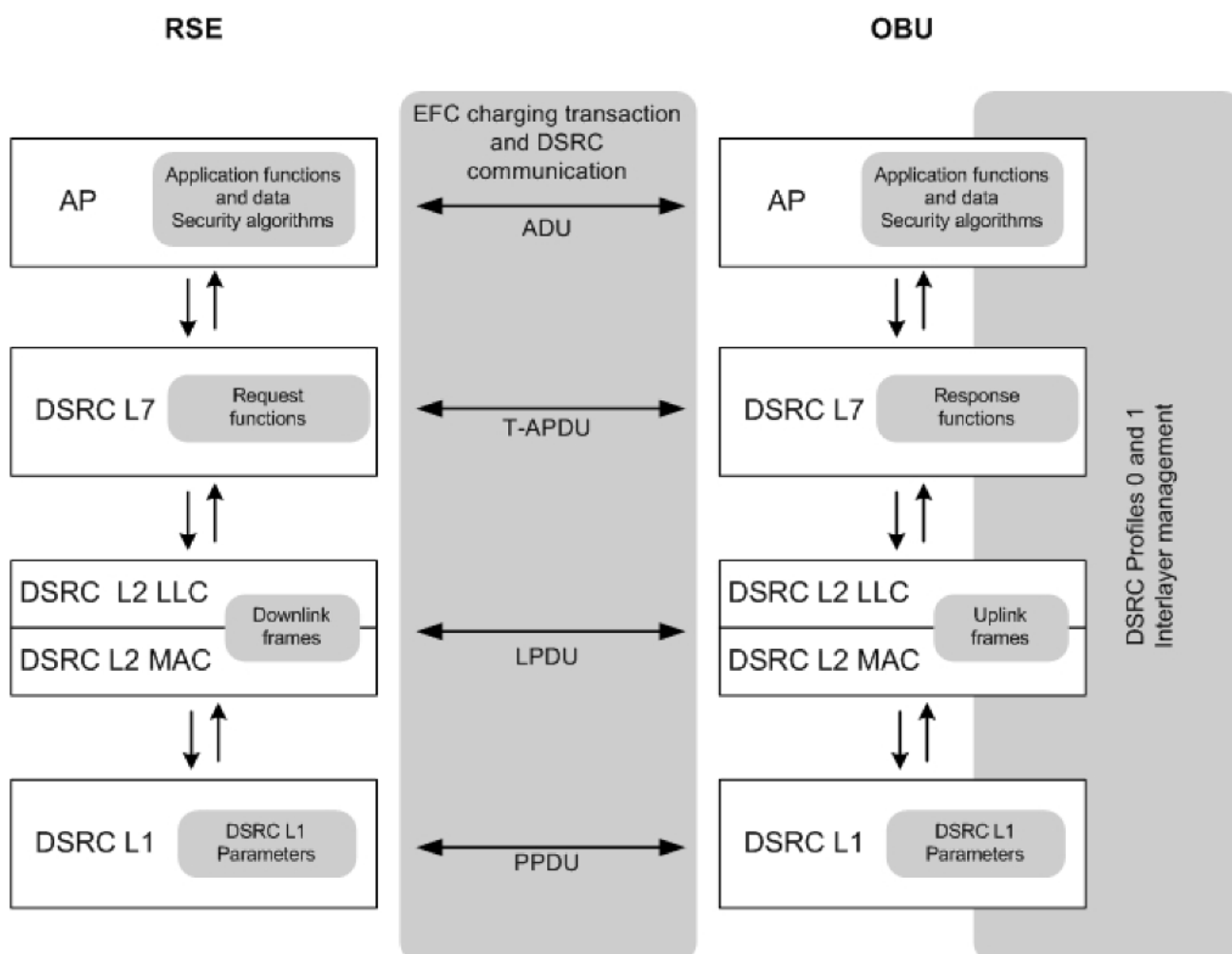


Figure 2 — Relationship between this European Standard and DSRC-stack elements

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.

EN 12834:2003, *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 V1.2.1 (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*

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

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

ISO/IEC 18033-3:2010, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

access credentials

trusted attestation or secure module that establishes the claimed identity of an object or application

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

attribute

addressable package of data consisting of a single data element or structured sequences of data elements

3.3

authenticator

data, possibly encrypted, that is used for authentication

3.4

base standard

approved international standard or ITU-T Recommendation

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

3.5

channel

information transfer path

[SOURCE: ISO 7498-2, 3.3.13]

3.6

cryptography

principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorized use

[SOURCE: ISO 7498-2:1989, modified]

3.7

data group

class of closely related attributes

3.8

EFC service

service for electronic payment offered by a payment service provider

3.9

Element

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

[SOURCE: EN ISO 14906:2011, 3.11]

3.10

International Standardised Profile

ISP

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

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

3.11

integrity

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

[SOURCE: ISO/TS 17574:2009]

3.12

interoperability

ability of 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]

3.13

mobile roadside equipment

equipment mounted on a mobile unit or handheld equipment to be used along the road

3.14

on-board equipment

OBE

equipment located on-board a vehicle including nomadic devices with the function of exchanging information with external systems

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

[SOURCE: EN ISO 14906:2011, 3.13]

3.15

on-board unit

OBU

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]

3.16

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]

3.17

roadside equipment

RSE

equipment located along the road, either fixed or mobile

3.18

service primitive

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.

3.19

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]

3.20

toll charger

entity which levies toll for the use of vehicles in a toll domain

[SOURCE: ISO 17573:2010]

3.21

toll service provider

entity providing toll services in one or more toll domains

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: ISO 17573:2010]

3.22

transaction

whole of the exchange of information between two physically separated communication facilities

[SOURCE: EN ISO 14906:2011, 3.24, modified]

3.23

transaction counter

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

3.24

transaction model

functional model describing the structure of electronic payment transactions

[SOURCE: EN ISO 14906:2011, 3.25]

3.25

transport service

a transport infrastructure related service which is offered to the user

4 Symbols and abbreviations

For the purposes of this document, the following symbols and abbreviations apply.

AC_CR	Access Credentials
ADU	Application Data Unit
APDU	Application Protocol Data Unit
AP	Application Process
ASN.1	Abstract Syntax Notation One
AuK	AuKEY
BST	Beacon Service Table
CCC	Compliance check communication for autonomous systems

DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DSRC	Dedicated Short-Range Communication
EETS	European Electronic Toll Service
e [key] (value)	encryption of the value using the key
ede [key] (value)	chained encryption, decryption and encryption of the value using the key
EID	Element Identifier
EFC	Electronic Fee Collection
GNSS	Global Navigation Satellite Systems
IAP	Interoperable Application Profile
ICS	Implementation Conformance Statement
ISP	International Standardised Profile
IUT	Implementaton Under Test
L1	Layer 1 of DSRC (Physical Layer)
L2	Layer 2 of DSRC (Physical Layer)
L7	Layer 7 of DSRC (Application Layer Core of DSRC)
LAC	Localization augmentation communication for autonomous systems
LLC	Logical Link Control
LID	Logical Link Control identifier
LSDU	Link Service Data Unit
MAC	Media Access Control
MMI	Man-Machine Interface
OBU	On-board Unit
RL	Requirements List
RSE	Roadside Equipment

T-APDU Transfer-Application Protocol Data Unit

VST Vehicle Service Table

5 Conformance

5.1 General

This clause describes in general terms what it means to be conformant with (the profile in) EN 15509.

5.2 Base standards

This European Standard defines one Application Profile based on the ISP-concept. The base standards that this Application Profiles 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.

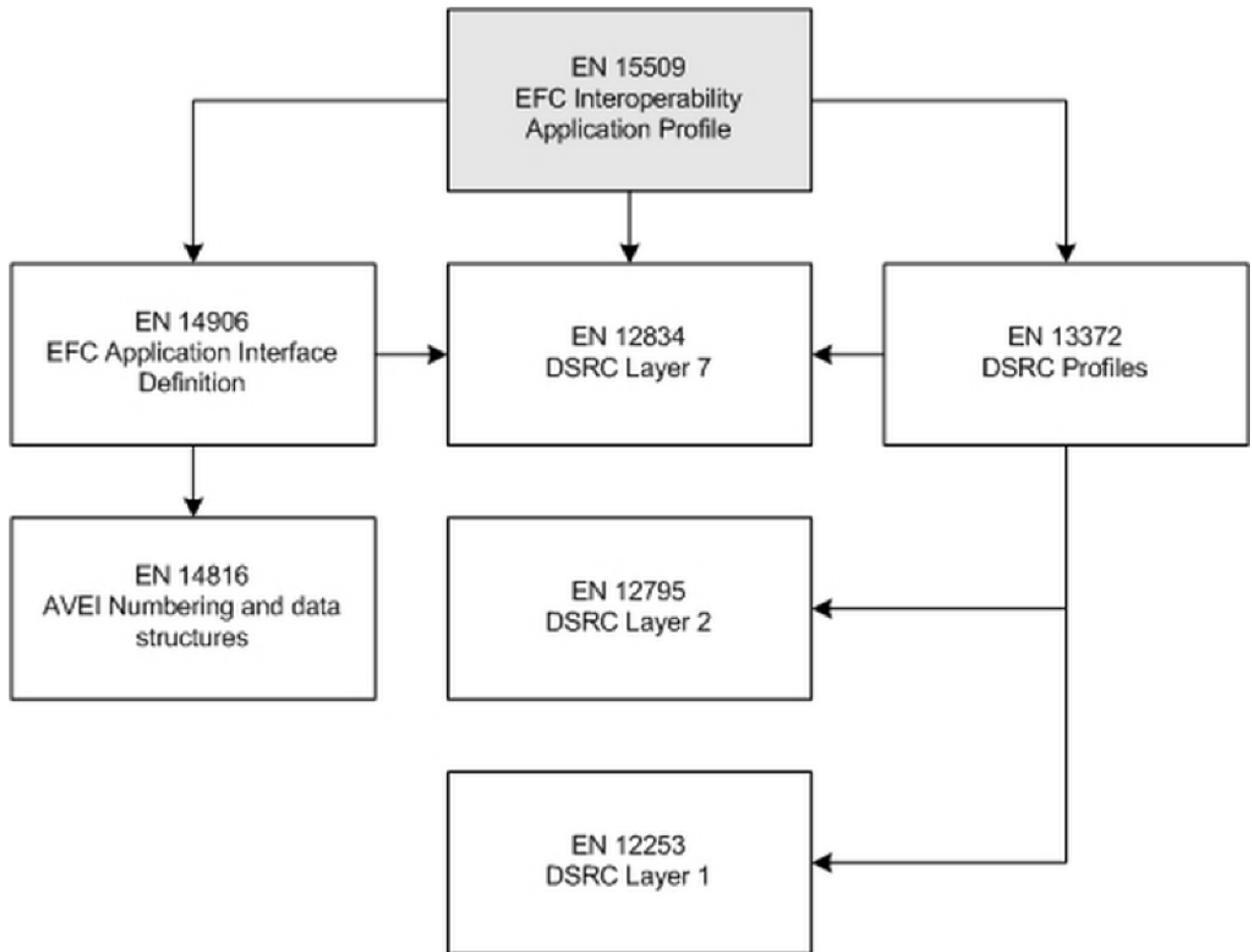


Figure 3 — Relationship and references between base standards and EN 15509

All requirements defined in this standard are either choices made from these base standards or more specific and limited requirement based on the general provisions of these standards.

5.3 Main contents of an EFC-DSRC-IAP

The conformance requirements of an IAP are divided between requirements for the On-Board Unit (OBU) and the Road-Side Equipment (RSE). The requirements are listed separately for OBU and RSE. This applies for all parts; requirements, PICS and conformance testing.

The conformance requirements of an IAP according to this standard shall include the following parts (divided into separate requirements for OBU and RSE):

- DSRC requirements;
- DSRC L7 and EFC functions;
- data requirements;
- security requirements;
- transaction requirements.

5.4 Conformance requirements

Conformance requirements are listed and defined in Clause 6 supported by Annexes A and B.

NOTE Conformance requirements are deliberately expressed concisely, in order to achieve clarity of the requirements. For motivations, explanations, etc., see the supporting parts of this European Standard (Foreword, Introduction, Annex E to Annex I).

5.5 Conformation notification

A statement of conformance to a specific IAP shall all be done according to the ICS proforma requirements defined in Annex C "ICS Proforma".

5.6 Conformance evaluation and testing

Conformance evaluation and testing are done according to provisions laid down in EN 15876-1 and EN 15876-2.

NOTE The use of EN 15876 implies use of other underlying test standards for evaluation of conformance to EN 15509.

5.7 Multiple IAPs

This standard defines one profile (EFC-DSRC-IAP-1) as in the clause for conformance requirements (Clause 6). For future use it may be possible to define more IAPs using the same structure as is defined here.

A taxonomy for EFC-DSRC-IAP-profiles is contained in Annex D on "IAP taxonomy and numbering" below.

6 Requirements for EFC-DSRC-IAP 1

6.1 OBU requirements

6.1.1 General

6.1 contains the normative conformance requirements on the On-Board Unit (OBU) for profile number 1; EFC-DSRC-IAP 1.

6.1.2 DSRC requirements

The OBU shall comply with:

- DSRC Profiles P0 / P1 L1-B according to EN 13372, or
- DSRC Profiles P0 / P1 L1-A according to EN 13372 with a Conversion Gain which is limited to a maximum value of 10 dB (Parameter U12b = 10 dB) and a Cut-off power level of minimum - 60 dBm (Parameter D12 = - 60 dBm).

NOTE This implies indirect references to and OBU's compliance with the underlying DSRC-standards for L1, L2 and L7 [EN 12253, EN 12795 and EN 12834].

The following DSRC-L7 according to EN 12834 features shall be supported by the OBU:

- concatenation of multiple consecutive T-APDU fragments in one layer 2 frame (i.e. LLC-service) with and without chaining, given that the size constraint for the LLC-frames are not violated (i.e. fit into 1 L2 frame);
- fragmentation header limited to 1 octet only;

— any “fill bit” (as defined 6.3.4 in EN L7), used for octet alignment, shall be assigned the value zero.

6.1.3 DSRC L7 and EFC functions

The OBU shall support the DSRC Layer 7 services and EFC functions, defined in EN 12834 and EN ISO 14906:2011, 7.2, in Table 1.

Table 1 — Overview of DSRC L7 and EFC functions

DSRC-L7 services	EFC function	Action/Event type	Remarks
INITIALIZATION	N/A	N/A	Establishes communication, selects the application and contract
ACTION	GET_STAMPED	0	Retrieves data with an authenticator from the OBU, with or without AC-CR
GET	N/A	N/A	Retrieves data from the OBU, with or without AC-CR
SET	N/A	N/A	Writes data to the OBU, with or without AC-CR
ACTION	SET_MMI	10	Invokes an MMI function (e.g. signal "OK" via buzzer). All SetMMIRq values (i.e. 0, 1, 2 and 255) defined in Annex A of EN ISO 14906:2011 shall be supported
ACTION	ECHO	15	OBU echoes received data
EVENT-REPORT	RELEASE	0	Terminates communication

6.1.4 Data requirements

The addressing of the EFC system and application data shall conform to the rules defined in 5.3 in EN ISO 14906:2011.

The EFC attributes in Table 2 as defined in EN ISO 14906:2011 (in Clause 8 and Annex A) and in EN 12834, shall be implemented in the OBU:

Table 2 — Overview of the OBU EFC application data

ATTRIBUTES (EID>0)	Attrib d	Type	Length ^a (in octets)	Read ^b	Write ^b	Remarks
APPLICATION CONTEXT						This attribute is defined in EN 12834.
ApplicationContextMark	N/A	N/A	6 or 16	Yes	No	An octet string that is sent from the OBU in the Initialization phase (VST) that contains the identification of a specific DSRC application context. For EFC the first 6 octets always will contain the EFContextMark. Length varies between security levels (see Annex A, Table A.1 for details in particular for the length in octets).
CONTRACT						Information associated with the service rights of the toll service provider.

EFC Context Mark	0	32	6	Yes	No	Contains the Contract Provider. Transmitted as part of the VST.
PAYMENT						Data associated with the Payment transaction.
PaymentMeans (including PAN)	32	64	14	Yes	No	Includes: - The Personal Account Number, including the Payment Means Issuer. - The PAN Expiry Date - The payment means Usage Control
VEHICLE						Information pertaining to the identification and characteristics of the vehicle.
VehicleLicencePlateNumber	16	47	13 to 17	Yes	No	More specific and limited in scope than in EN ISO 14906 (see Annex A, Table A.2 for details).
VehicleClass	17	49	1	Yes	No	More specific and limited in scope than in EN ISO 14906 (see Annex A, Table A.2 for details).
VehicleDimensions	18	50	3	Yes	No	
VehicleAxles	19	51	2	Yes	No	According to EN ISO 14906:2011
VehicleWeightLimits	20	52	6	Yes	No	
VehicleSpecificCharacteristics	22	54	4	Yes	No	
EQUIPMENT						Information pertaining to the OBU.
EquipmentOBUID	24	56	5 (=1+4)	Yes	No	Coded as an octet string with a length determinant = 4.
EquipmentStatus (transaction counter)	26	58	2	Yes	Yes	More specific and limited in scope than in EN ISO 14906 (see Annex A, Table A.3 for details).
RECEIPT						Information associated with a specific session, including both financial and operational data.
ReceiptData1 (last)	33	65	28	Yes	Yes	
ReceiptData2 (penultimate)	34	66	28	Yes	Yes	
^a Including the length determinant as defined in ISO/IEC 8825-2 (packed encoding rules for ASN.1 is used in EN ISO 14906). ^b The read and write columns denotes read and write operations in an EFC DSRC transaction (not other possible situations).						

EFC attribute requirements that restrict choices of or which are more specific and limited in scope than those of EN ISO 14906 can be found in Annex A.

Annex F of EN ISO 14906:2011 "Mapping table between EFC Vehicle data attribute and European registration certificate" is applicable in the context of EN 15509 for the correspondence between elements available inside the registration certificate and the data element that could use this information (coding according to EN ISO 14906).

The registration certificate is defined by the European Directive 1999/37/EC and successive amendment Directive 2003/127/EC.

The Service Providers shall provide values to the data (depending on the European Vehicle Group) before an OBU can be put in operation by a user and can be considered as "interoperable".

6.1.5 Security requirements

6.1.5.1 General

This European Standard defines security features and mechanisms based on the security framework defined in CEN/TS 16439.

EFC-DSRC-IAP 1 in this European Standard allows for implementation of two different levels of security (0,1). Support of security level 0 is mandatory whereas level 1 can be implemented on an optional basis.

NOTE See Annex F for further details and explanation.

6.1.5.2 Security level 0 requirements

The security related data elements listed in Table 3 shall be implemented in the OBU:

Table 3 — Overview of the OBU security related data

Name	Length (in)	Remarks
AuthenticationKey1	8	Private
AuthenticationKey2	8	Private
AuthenticationKey3	8	Private
AuthenticationKey4	8	Private
AuthenticationKey5	8	Private
AuthenticationKey6	8	Private
AuthenticationKey7	8	Private
AuthenticationKey8	8	Private
KeyRef	1	Reference to AuKey used for the computation of the Authenticators, e.g. Toll Service Provider and Toll Charger Authenticators. The Toll Service Provider decides which keys are shared with (MoU) Toll chargers (referenced through AuKey_Op), and which are only known by himself (referenced through AuKey_Iss).
RndRSE	4	Random number, containing SessionTime, from RSE used for the computation of Authenticator.

The OBU shall be able to calculate an Authenticator (i.e. support the GET_STAMPED function operating on one attribute list considering that the response shall fit into one Layer 2 frame) to validate data integrity and origin of the application data. These calculations shall be performed according to B.2.