BS EN 15509:2014

BSI Standards Publication

Electronic fee collection — Interoperability application profile for DSRC

bsi.

...making excellence a habit.™

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 It supersedes BS EN 15509:2007 which is withdrawn.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.

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

Contents

Page

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.

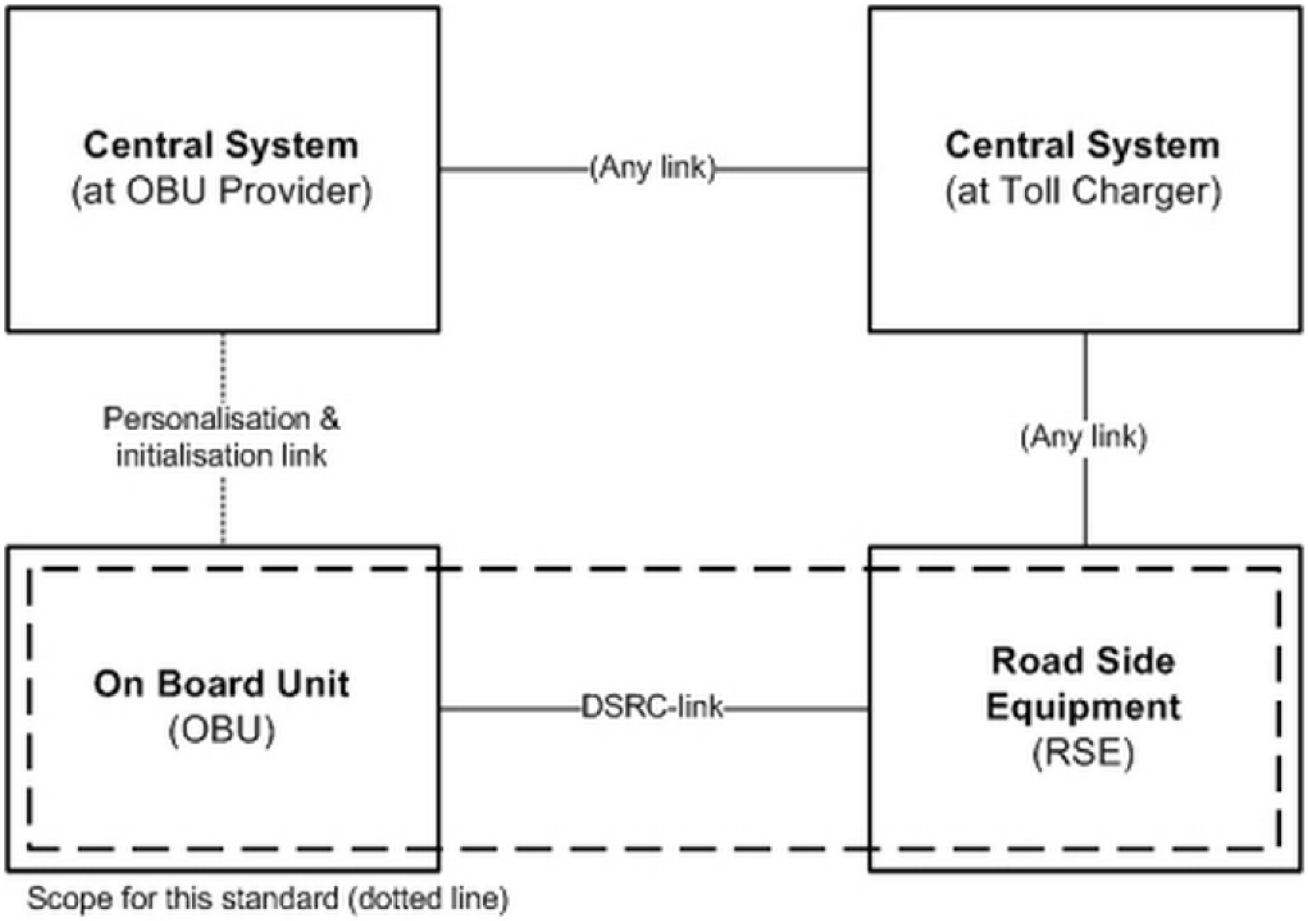

Figure 1 — Scope for this European Standard (within the box delimited with a dotted line)

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.

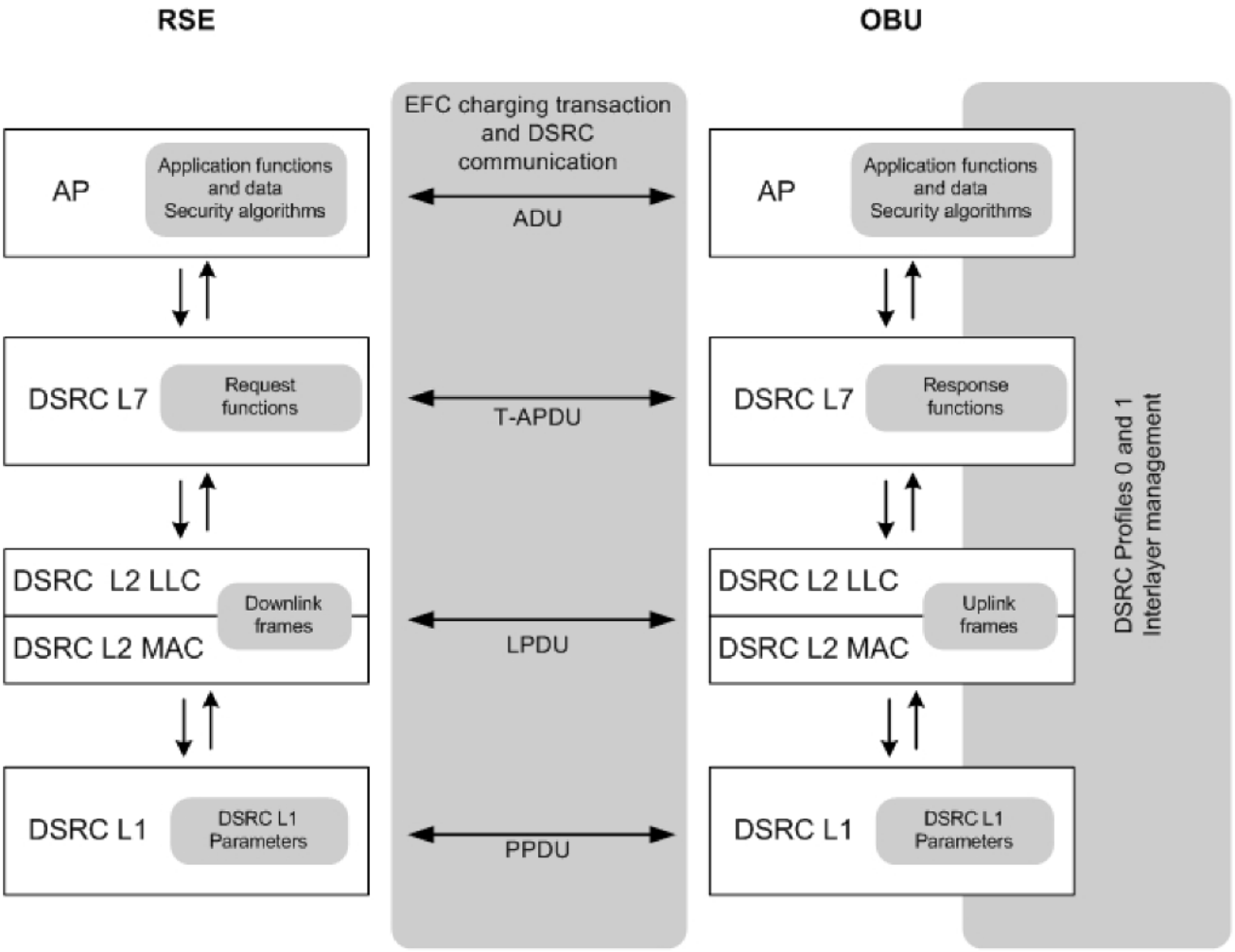

Figure 2 — Relationship between this European Standard and DSRC-stack elements

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.

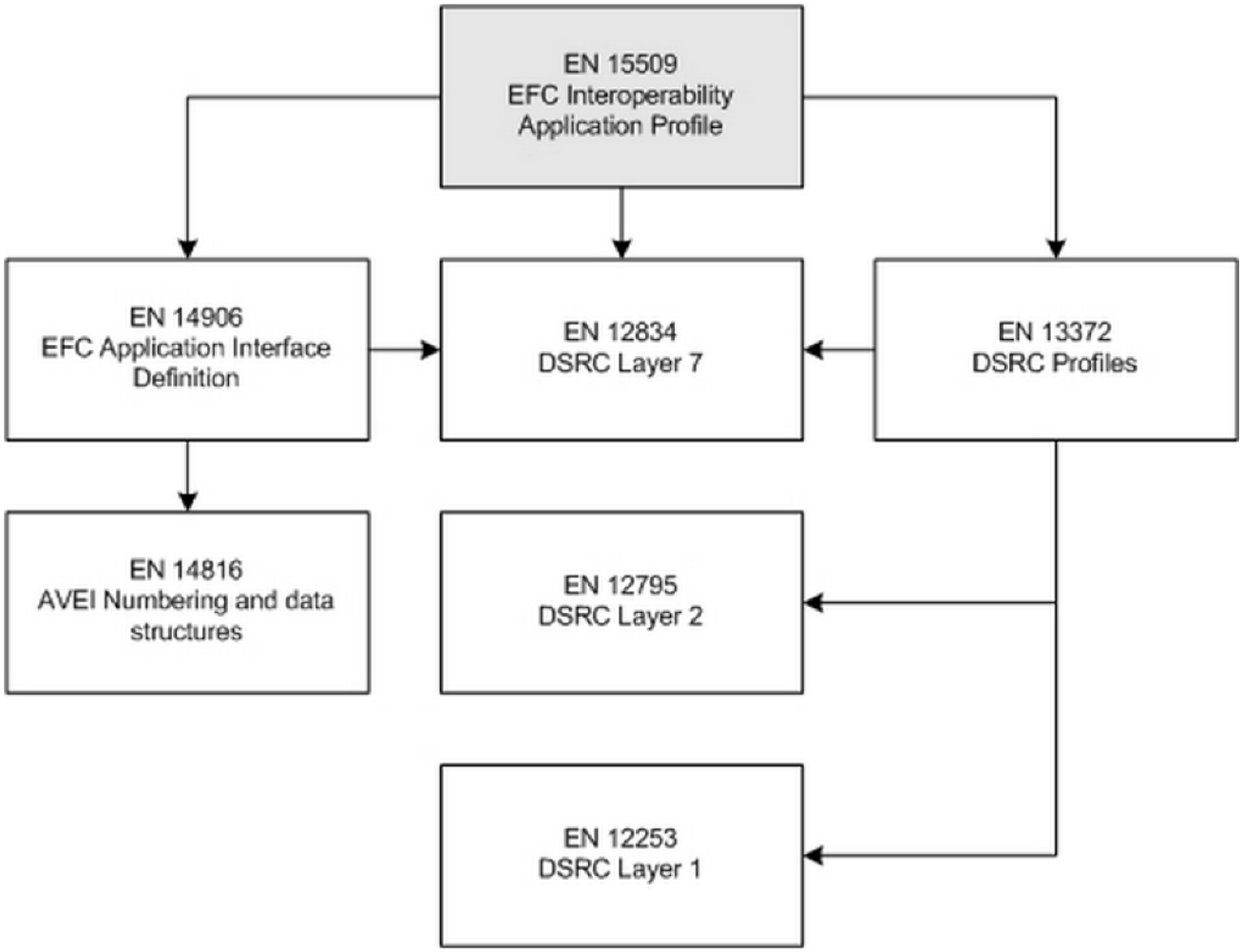

Figure 3 — Relationship and references between base standards and EN 15509

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)	Attrld	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 EFCContextMark. 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.

NOTE The OBU also supports (through the data stored in the OBU) other security features such as the TransactionCounter (see B.5) and signed receipt that are performed at the RSE or in the central system.

6.1.5.3 Security level 1 requirements

The OBU shall support the security level 0 requirements as defined in 6.1.5.2.

The OBU shall support calculation of Access Credentials for protection of user related data on the OBU. These calculations shall be performed according to B.3.

This requires the additional security data elements, in Table 4, to be implemented in the OBU.

Table 4 — OBU security related data for handling of Access Credentials

Name	**Length** (in	**Remarks**
AccessKey	**8**	Private.
AC_CR	**4**	Access credentials calculated by the RSE and the OBU using RndOBU and the Access Key AC_CRKey.
AC_CR-KeyReference	**2**	Reference to the key generation and the Diversifier for the computation of AC_CRKey.
RndOBU	**4**	Random number (nonce) used together with AccessKey (referenced through AC_CR-KeyReference) to calculate the Access credentials.

NOTE An RSE that has only implemented the security requirements associated with level 0 in this European Standard (as in 6.2.5.2) is not able to access OBU data protected by means of access credentials.

6.1.6 Transaction requirements

An OBU compliant with this European Standard shall be able to perform an EFC transaction model as defined in Clause 6 in EN ISO 14906:2011.

Annex B in EN ISO 14906:2011 provides an informative example of a transaction by specifying the CARDME transaction.

6.2 RSE requirements

6.2.1 General

6.2 contains the normative conformance requirements on the RSE for profile number 1; EFC-DSRC-IAP 1.

6.2.2 DSRC requirements

The RSE shall support any OBU complying with 6.1.2.

NOTE 1 This implies indirect references to and RSE's compliance with the DSRC-standards for Profiles, L1, L2 and L7 [EN 13372, EN 12253, EN 12795 and EN 12834].

NOTE 2 This implies indirect references to and mobile RSE's compliance with the DSRC-standards for Profiles, L1, L2 and L7 [EN 13372, EN 12253, EN 12795 and EN 12834], excepting Downlink Parameter D4a (not applicable to mobile RSE).

6.2.3 DSRC L7 and EFC functions

The RSE shall support the DSRC Layer 7 services and EFC functions, defined in EN 12834 and EN ISO 14906:2011, 7.2, in Table 5.

Table 5 — 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

6.2.4 Data requirements

The RSE shall support any OBU complying with 6.1.4.

There are no specific data requirements for the RSE, other than the possibility to retrieve read and write (including decoding and encoding, respectively) data as defined in 6.1.4.

6.2.5 Security requirements

6.2.5.1 General

A framework and toolbox for security is given in CEN/TS 16439. This European Standard defines security features and mechanisms based on this framework.

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. The associated security related data elements that are used for data exchanges over the EFC-DSRC interface are defined in 6.1.5.

NOTE See Annex D for further details and explanation.

6.2.5.2 Security level 0 requirements

The RSE shall be able to calculate Authenticators to validate data integrity and origin of the application data. These calculations shall be performed according to B.2.

The RSE shall update the TransactionCounter according to B.5.

NOTE An RSE that has only implemented the security requirements associated with level 0 in this European Standard is not able to access OBU data protected by means of access credentials according to security level 1 (see 6.1.5.3).

6.2.5.3 Security level 1 requirements

The RSE shall support the security level 0 requirements as defined in 6.2.5.2.

The RSE shall be able to calculate Access Credentials for access to protected user related data on the OBU. These calculations shall be performed according to B.3.

6.2.6 Transaction requirements

The EFC transaction model shall comply with EN ISO 14906:2011, Clause 6.

There are no additional specific normative requirements on the transaction in this European Standard. This means that the RSE may perform the transaction in any way suitable as long as the other requirements in this European Standard (and base standards) are met.

An informative example of a transaction can be found in EN ISO 14906:2011, Annex B.

Annex A
(normative)

Data specification

The specification and use of data elements is defined in EN ISO 14906 and in EN 12834. Annex A includes EFC attribute and security related data requirements that restrict choices of or which are more specific and limited in scope than those of the base standards.

NOTE The length column in the tables below includes the length determinant as defined in ISO/IEC 8825-2 (unaligned packed encoding rules for ASN.1 is used in EN ISO 14906).

Table A.1 — Application related data (defined in EN 12834)

Name / Data element	Definition and remarks	Usage	Length in octets
ApplicationContextMark	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 EFCContextMark. The Toll Service Provider shall ensure that the value of the EFCContextMark corresponds to one unique dated version of EN 15509 through a reference table, which is made available to the Toll Charger, allowing it to identify to which specific version of the EN 15509 application profile the OBU complies.	Data content for security level 0: EFCContextMark EXAMPLE: ‘A4 00 02 00 00 00’H	**6**
		Data content for security level 1: EFCContextMark, AC_CR_Keyreference, RndOBU The AC_CR_Keyreference and RndOBU data elements are defined as octet strings with a container Choice = 2 and a length indicator. EXAMPLE: ‘A4 00 02 00 00 00 02 02 00 AA 02 04 12 34 56 78’H where: - EFCCOntextMark: ‘A4 00 02 00 00 00’H - AC_CR_Keyreference: ’00 AA’H - RndOBU: ’12 34 56 78’H	**16**

Table A.2 — Vehicle data (defined in EN ISO 14906)

Attribute Id / Name Data element	Definition and remarks	Usage	Length in octets
VEHICLE	Information pertaining to the identification and characteristics of the vehicle		
16 / Vehicle Licence Plate Number VehicleLicence PlateNumber	Claimed licence plate of the vehicle Only letters and numbers are allowed for the definition of the LPN. Only Latin alphabet is used for the coding of the Licence plate. latinAlphabetNo1 (1), -- encoded as 00 00 00'B	The usage is according to EN ISO 14906 but more specific and limited in its scope. Claimed licence plate of the vehicle, the length of the padded LPN should be between 10 octets to 14 octets (i.e. 13 octets to 17 octets including the country code, alphabet indicator, length determinant and the LPN). A LPN, which is shorter than 10 characters, is padded with NUL characters so as to achieve a total of 10 characters to 14 characters. EXAMPLE : SE, LatinAlphabethNo1, OCD560 Country code = SE = 1010010000'B Alphabet indicator = LatinAlphabethNo1 = 000000'B Length determinant = 14 octets = 00001110'B LPN = OCD560 = 4F 43 44 35 36 30 00 00 00 00 00 00 00 00'H	**17**
17 / Vehicle Class Vehicle Class	Service provider specific information pertaining to the vehicle**.**	The usage is according to EN ISO 14906 but more specific and limited in its scope. Vehicle class' substructure TCCC LLLL, where T (trailer indicator) : 0'B = no trailer, also used the default value 1'B = trailer present CCC : 000'B = No entry 001'B = Group 1 - Small passenger vehicles (UNECE class M 1) 010'B = Group 2 - Light Goods Vehicles (UNECE class N 1) 011'B = Group 3 - Large passenger vehicles (UNECE class M 2, M 3) 100'B = Group 4 - Heavy Goods Vehicles up to 12 t (UNECE class N 2) 101'B = Group 5 - Heavy Goods Vehicles over 12 t (UNECE class N 3) 110'B = Group 6 - Motorcycles (UNECE class L) 111'B = Group 7 - Other vehicles including vehicles above 3,5 t not included in previous groups LLLL (Local vehicle classes): value assignments according to a local scheme. If the Local Class isn't used for the contract between the user and the service provider, the value for the Local class should be 0.	**1**

Table A.3 — Equipment data (defined in EN ISO 14906)

Attribute Id / Name ata element	Definition and remarks	Usage	Length in octets
EQUIPMENT	Information pertaining to the OBU.		
26 / EquipmentStatus EquipmentStatus	Toll Charger-specific EFC application-related information pertaining to the status of the equipment. Boolean information to support an Toll Charger's handling of an OBU on application level. (E.g. 'next suitably equipped gantry should take an enforcement picture')	The usage is according to EN ISO 14906 but more specific and limited in its scope. LLLL CCCC CCCC CCCC, where LLLL'B : Local use (4 bits), coding and use at the discretion of the Toll Charger. CCCC CCCC CCCC'B : sequential transaction counter (12 bits), upon personalization. It is updated by the roadside equipment according to B.5	**2**

Table A.4 —Authentication keys, access keys and security related data

Data element	Definition and remarks	Usage	Length in octets
AuthenticationKey1	Private	A key used to compute authenticators for security levels 0 and 1 of EFC-DSRC-IAP 1 (see B.4.2).	**8**
AuthenticationKey2	Private	Idem	**8**
AuthenticationKey3	Private	Idem	**8**
AuthenticationKey4	Private	Idem	**8**
AuthenticationKey5	Private	Idem	**8**
AuthenticationKey6	Private	Idem	**8**
AuthenticationKey7	Private	Idem	**8**
AuthenticationKey8	Private	Idem	**8**
AccessKeys	Private.	The access key is the key used to compute Access credentialsfor security level 1 (see B.3).	**8**
AC_CR	Access credentials calculated by the RSE and the OBU using RndOBU and the Access Key AC_CRKey. When the security level to be applied for an Element is requiring an AC-CR, the data of the VST regarding this Element has to include a Random Number.	Integer (0..4'294'967'295). AC_CR = DES. Compute AC_CR(k) according to the DES algorithm [DEA], see also Annex E.	**1+4**
AC_CR-KeyReference	Reference to the key generation and the Diversifier for the computation of AC_CRKey.	Key reference (k): Integer (0..255) (8 bits) Diversifier: Integer (0..255). (8 bits) EXAMPLE : Key reference (# 1) and Diversifier # 2 : 0000 0001’B (Key reference (1)): 0000 0010’B (Diversifier(2)).	**2**
KeyRef	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).	Integer (0..255). EXAMPLE: AuthenticationKey1 reference (=111_{10})	**1**
RndOBU	Random number (nonce) used together with AccessKey (referenced through AC_CR-KeyReference) to calculate the Access credentials.	Integer (0..4’294’967’295)	**5 = 1+4**
RndRSE	Random number, containing SessionTime, from RSE used for the computation of Authenticator.	See ReceiptData1.SessionTime in Clause 8 and Annex A in EN ISO 14906.	**5 = 1+4**

Annex B
(normative)

Security calculations

B.1 General

Annex B contains detailed definitions of required the security features and calculations. Annex E illustrates the defined cryptographic mechanisms by means of a few numerical examples.

B.2 Attribute authenticator

B.2.1 General

For authentication of attributes requested by the GET_STAMPED.request function, the OBU shall use the algorithm described below, i.e. Message Authentication Code calculation in Chained Block Cipher mode according to ISO/IEC 9797-1:2011, MAC Algorithm 1 using the DEA algorithm according to ISO/IEC 18033-3.

a) Let AuK be the OBU's Authentication Key of a given generation k, referenced by the KeyRef in the GET_STAMPED.request.

b) Let M be the Attributelist in the GET_STAMPED.response concatenated by the octet string containing the RndRSE sent in the GET_STAMPED.request. The RndRSE shall contain of the Session Time. (see example in Table B.1).

c) Split M into 8-octet blocks D_1 (octets 1 to 8), D_2 (octets 9 to 16),...., D_{n-1} (octets 8(n-1)+1 to 8n).

d) According to ISO/IEC 9797-1:2011, MAC Algorithm 1 the remaining bits shall be left justified. To the right of these shall be appended zero value bits, so that a final 8-octet block results D_n.

e) First Step: the first block $I_1=D_1$ shall be encrypted with AuK:

f) $O_1= e[AuK](I_1)$

g) The output O_1 shall be XORed with D_2 and this result shall be the input I_2 of the next step:

h) $I_2= [O_1]$ XOR $[D_2]$

i) Second Step: I_2 shall be encrypted with AuK:

j) $O_2= e[AuK](I_2)$

k) The output O_2 shall be XORed with D_3 and this result shall be the input I_3 of the next step:

l) $I_3= [O_2]$ XOR $[D_3]$

m) This process shall continue with further 8-octet blocks D_x until the ultimate step D_n.

n) Finally the input I_n shall be encrypted with e[AuK]:

o) $O_n= e[AuK](I_n)$

p) The output O_n shall be truncated: The four leftmost octets shall form the AttributeAuthenticator in the EFC function GET_STAMPED.response.

An illustration of the calculation of an authenticator is given in Figure B.1 below.

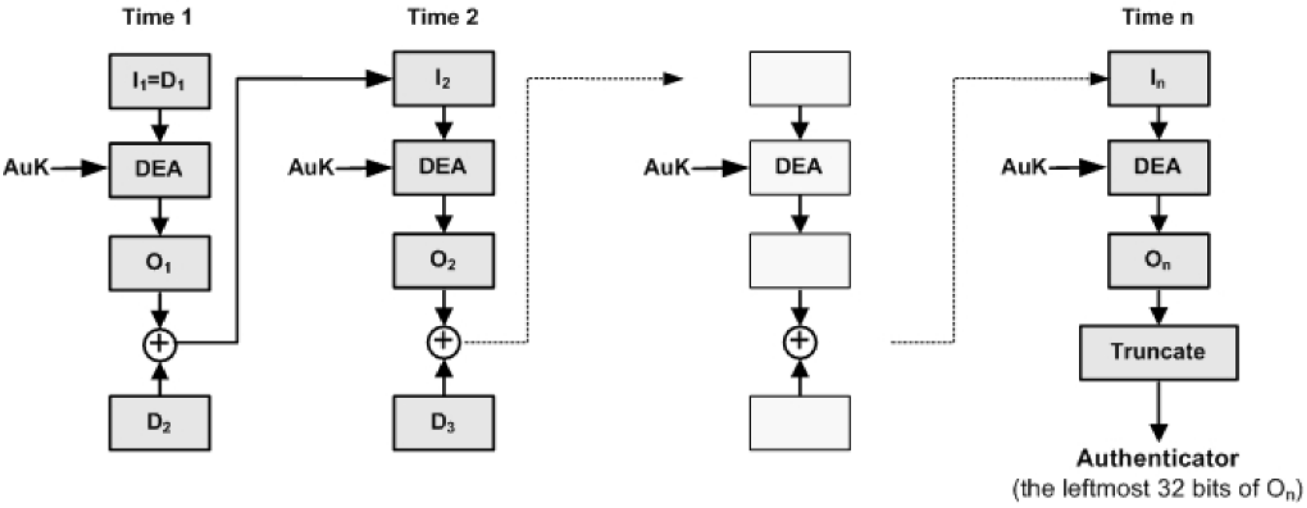

Figure B.1 — Illustration of calculation of an authenticator, where ⊕ denotes the XOR operation

B.2.2 Authenticator using the attribute Payment Means

The authenticator when the Attributelist in the GET_STAMPED.response only contains the attribute Payment Means is calculated as follows.

a) Let M be the Attributelist in the GET_STAMPED.response containing the single attribute PaymentMeans concatenated by the octet string containing the RndRSE sent in the GET_STAMPED.request. M will have the content as in Table B.1.

b) Split M into 8-octet blocks D_1, (octets 1 to 8), D_2 (octets 9 to 16) and D_3 (octets 17 to 24).

c) Calculate the algorithm as in B.2.1 using 3 iterations (see Figure B.2).

Table B.1 — Content of M used as input to generate the authenticator of the PaymentMeans attribute

Block#	Octet #	Attribute / Field	Bits in Octet b_7 b_0	Description
D_1	1	AttributeList SEQUENCE (0..127,...) OF {	**0**000 0001	No extension, number of attributes: 1
	2	Attributes SEQUENCE { AttributeId	**0**010 0000	PaymentMeans = 32_{10}
	3	AttributeValue CONTAINER {	**0**100 0000	Container Choice: 64_{10} = PaymentMeans
	4	PaymentMeans	xxxx xxxx	PaymentMeans
	5		xxxx xxxx	
	6		xxxx xxxx	
	7		xxxx xxxx	
	8		xxxx xxxx	
D_2	9		xxxx xxxx	
	10		xxxx xxxx	
	11		xxxx xxxx	
	12		xxxx xxxx	
	13		xxxx xxxx	
	14	PaymentMeansExpiryDate	dddd dddd	DateCompact
	15		dddd dddd	
	16	PaymentMeansUsageControl	cccc cccc	
	17	}	cccc cccc	
D_3	18	Nonce OCTET STRING {	**0**000 0100	No extension, octet string length = 4_{10}
	19	RndRSE	rrrr rrrr	Random number from RSE, containing the SessionTime
	20		rrrr rrrr	
	21		rrrr rrrr	
	22	}	rrrr rrrr	
	23	Padding	**0**000 0000	Padding to obtain a multiple of 8-octet blocks
	24		**0**000 0000	

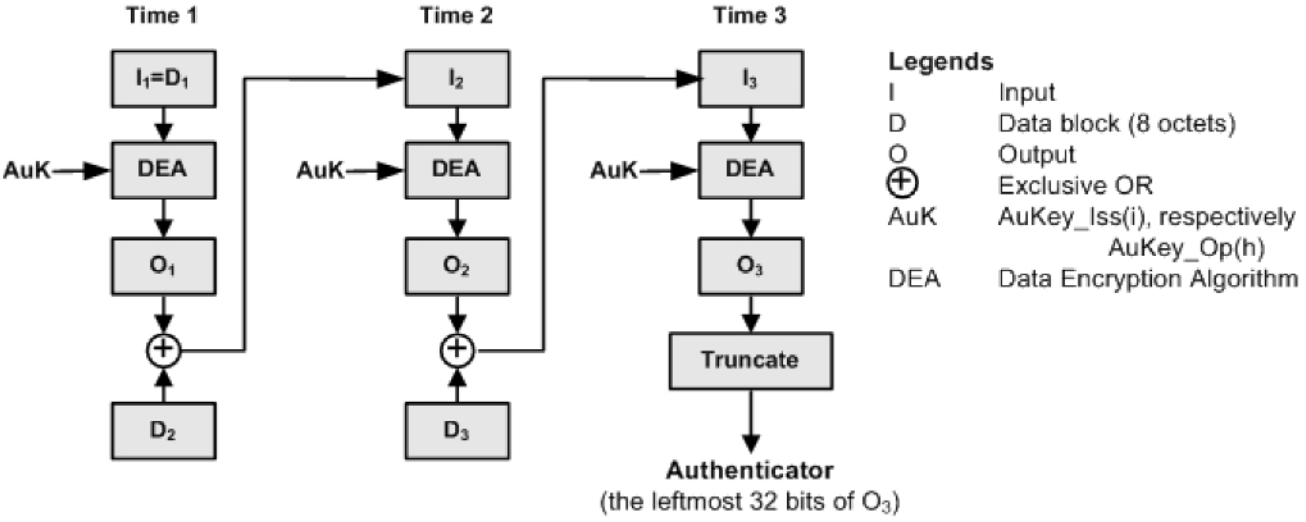

Figure B.2 — Computation of the PaymentMeans authenticator where ⊕ denotes the XOR operation

B.3 Access Credentials

B.3.1 General

NOTE B.3 only applies for implementation of EFC-DSRC-IAP 1 Security Level 1 according to 6.1.5 and 6.2.5.

B.3.2 The principle of Access Credentials

Access credentials are used in transactions, in order to protect against non-authorized access to sensitive user data and against (commercial) use of the OBU by non-authorized Toll Chargers.

The principle of access control to the OBU information is shown below (see Figure B.3). When an OBU, having entered the communication zone, responds to a polling message (BST) from the RSE, it returns a VST that for each available Contract contains information about an Access Credential Reference (AC_CR-KeyReference) and a random number (RndOBU). Access Credential Reference contains the diversifier and a reference to a secret master key (MAcK) that shall be used for the computation of the secret key (AcK). This key shall be used for the computation of the Access Credentials (AC_CR) using the RndOBU number as input. The RSE returns the access credential calculated and the OBU compares the access credential with its own calculation. In case they are equal the OBU accepts the RSE as a genuine RSE and reading data from the OBU is allowed.

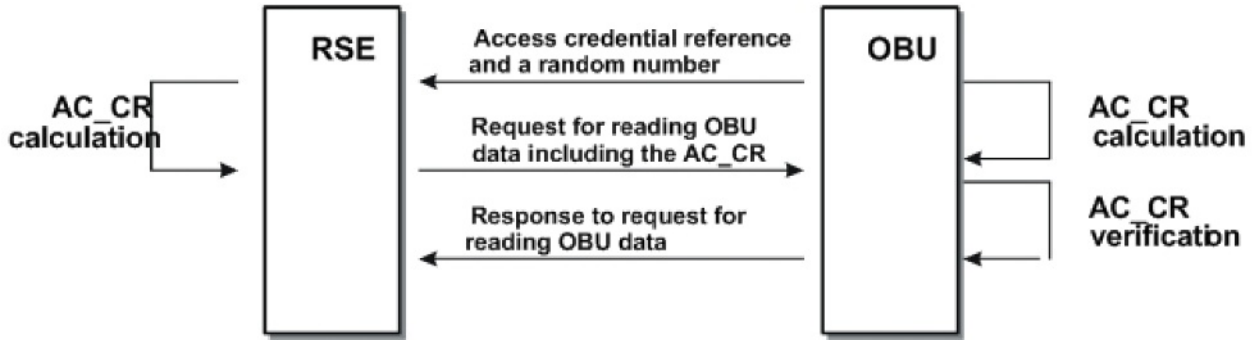

Figure B.3 — The principle of access control to the OBU data

B.3.3 Calculation of Access Credentials

When access to an Element, which is protected in the OBU, is requested by an RSE, the processing of any command addressed to that Element shall require AccessCredentials as a cryptographic value. The same AccessCredentials shall be used for the protection of all attributes belonging to the same EFC-Element.

The access of an attribute that belongs to an Element shall be granted only to RSEs presenting the correct access credentials. Therefore, the access credentials shall be calculated at both the RSE, in order to present them to the OBU when requesting access to protected data, and the OBU, in order to verify the correctness of the credentials presented by the RSE.

For calculation of the Access Credentials, the algorithm described below shall be used (see Figure B.4). The encryption shall be performed using the DEA algorithm in ISO/IEC 18033-3:

a) the 4-octet RndOBU is sent from the OBU to the RSE in the VST. These 4-octet RndOBU shall be left aligned;

b) let AcK be the derived Access Key;

   The generation k of the AcK is defined at the moment of personalization and should be associated to the OBU (e.g. through information in the ContextVersion). How this is done is outside the scope of this European Standard.

c) To the right 4 zero octets shall be appended. The result shall be an 8-octet string:

d) I = ‘RndOBU’ || ‘00 00 00 00’Hex;

e) The resulting 8-octet string I shall be encrypted as follows:

f) O = e [AcK] (I);

g) The access credentials AC_CR shall be obtained by truncating the 8-octet string output O and keeping the four left-most octets.

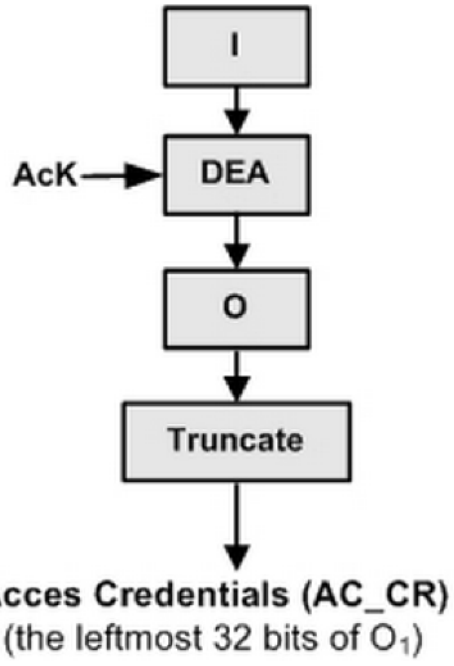

Figure B.4 — Calculation of Access Credentials

B.4 Key derivation

B.4.1 General

In order to avoid disclosure of the secret keys stored in the OBU and consequent possibility of replication of the OBU keys, the OBU shall only carry specific diversified keys. These keys are derived from Master keys (or key generations) using OBU specific data:

— every OBU key can be derived from the Masterkey;

— every OBU key is bound to that specific OBU;

— the Masterkey cannot be recalculated from the OBU Key.

B.4.2 Calculation of derived Authentication Key

The Authentication Key of a Key Generation k shall have a length of 8-octets and shall be derived from the 16 octet Master Authentication Key as described below:

a) let the Master Authentication Key for a given generation k be: MAuK(k);

b) let the derived Authentication Key be: AuK(k);

c) compute the Compact_PersonalAccountNumber by truncating the first 64 bits in the PaymentMeans attribute to 32 bits with the following algorithm:

d) Compact_PersonalAccountNumber = [HighDWord32(PAN)] XOR [LowDWord32(PAN)];

e) compute the 8 octet value VAL concatenating the Compact_PersonalAccountNumber with ContractProvider and padding it with ‘00’:

f) VAL = ‘Compact_PersonalAccountNumber || ContractProvider || 00’;

g) compute the AuK(k) for a given generation k as follows:

AuK(k) = ede [MAuK(k)] (VAL).

B.4.3 Calculation of the Access Key

NOTE B.4.3 only applies for implementation of EFC-DSRC-IAP 1 Security Level 1 according to 6.1.5 and 6.2.5.

The Access Key of a Key Generation k shall have a length of 8 octets and shall be derived from the 16 octet Master Access Key using the AC_CR_KeyRef as described below:

a) let the Master Access Key for a given generation k be: MAcK(k);

b) let the derived Access Key be: AcK(k);

c) make the concatenation of AC_CR-KeyReference || AC_CR-KeyReference || AC_CR-KeyReference || AC_CR-KeyReference to obtain an 8 octets value VAL:

d) VAL = ‘AC_CR_KeyReference || AC_CR-KeyReference || AC_CR-KeyReference || AC_CR-KeyReference ’;

e) Compute the AC_CRKey(k) as follows:

AcK(k) = ede[MAcK (k)] (VAL).

B.5 Transaction Counter

Use the following procedure for the RSE computation of the Transaction Counter:

a) get the EFC attribute EquipmentStatus (sent by the OBU in the Presentation Phase);

b) let the Transaction Counter be the value of the last 12 bits in EquipmentStatus (0...4095);

c) increase the Transaction Counter by 1;

d) insert the changed Transaction Counter into the last 12 bits of EquipmentStatus.

The updated EquipmentStatus is sent to the OBU in the Receipt Phase (SET.Request).

NOTE See the CARDME-4 concept or B.3.5 in EN ISO 14906:2011 for further explanation of the context and use of the Transaction Counter.

Annex C
(normative)

Implementation conformance statement proforma

C.1 General

To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented. Such a statement is called an implementation conformance statement (ICS). Annex C provides proforma ICS templates, to be filled in by equipment suppliers.

The actual ICS proforma to be filled in by a supplier, claiming conformity for a product to this European Standard, shall be technically equivalent to the text of the ICS proforma given in Annex C, and shall preserve the numbering, naming and ordering of the proforma items.

The forms in Annex C shall be completed by the supplier of the item under test (IUT, i.e. the OBU or RSE).

C.2 Guidance for completing the ICS proforma

C.2.1 Purposes and structure

The purpose of this ICS proforma is to provide a mechanism whereby a supplier of an implementation of the requirements defined in this European Standard may provide information about the implementation in a standardized manner.

The ICS proforma is subdivided into clauses for the following categories of information:

— guidance for completing the ICS proforma;

— identification of the implementation;

— identification of the protocol;

— global statement of conformance;

— ICS proforma tables.

C.2.2 Abbreviations and conventions

C.2.2.1 General

The ICS proforma contained in Annex C is comprised of information in tabular form in accordance with the guidelines presented in ISO/IEC 9646-7.

C.2.2.2 Item column

The item column contains a number which identifies the item in the table.

C.2.2.3 Item description column

The item description column describes in free text each respective item (e.g. parameters, timers). It implicitly means "is <item description> supported by the implementation?".

C.2.2.4 Status column

The following notations, defined in ISO/IEC 9646-7, shall be used for the status column:

m mandatory - the capability is required to be supported;

o optional - the capability may be supported or not;

n/a not applicable - in the given context, it is impossible to use the capability;

x prohibited (excluded) - there is a requirement not to use this capability in the given context;

o.i qualified optional - for mutually exclusive or selectable options from a set. "i" is an integer which identifies a unique group of related optional items and the logic of their selection which is defined immediately following the table;

ci conditional - the requirement on the capability ("m", "o", "x" or "n/a") depends on the support of other optional or conditional items. "i" is an integer identifying a unique conditional status expression which is defined immediately following the table.

C.2.2.5 Reference column

The reference column makes reference to this European Standard, except where explicitly stated otherwise.

C.2.2.6 Support column

The support column shall be filled in by the supplier of the implementation. The following common notations, defined in ISO/IEC 9646-7, shall be used for the support column:

Y or y	supported by the implementation;
N or n	not supported by the implementation;
N/A, n/a or -	no answer required (allowed only if the status is n/a, directly or after evaluation of a conditional status).

NOTE As stated in ISO/IEC 9646-7, support for a received PDU requires the ability to parse all valid parameters of that PDU. Supporting a PDU while having no ability to parse a valid parameter is non-conformant. Support for a parameter on a PDU means that the semantics of that parameter are supported.

C.2.2.7 Values allowed column

The values allowed column contains the type, the list, the range, or the length of values allowed. The following notations are used:

— range of values: <min value> .. <max value>

EXAMPLE 1 5 .. 20

— list of values: <value1>, <value2>, ..., <valueN>

EXAMPLE 2 2 ,4 ,6 ,8, 9

EXAMPLE 3 '1101'B, '1011'B, '1111'B

EXAMPLE 4 '0A'H, '34'H, '2F'H

— list of named values: <name1>(<val1>), <name2>(<val2>), ..., <nameN>(<valN>)

EXAMPLE 5 reject(1), accept(2)

— length: size (<min size> .. <max size>)

EXAMPLE 6 size (1 .. 8)

C.2.2.8 Values supported column

The values supported column shall be filled in by the supplier of the implementation. In this column, the values or the ranges of values supported by the implementation shall be indicated.

C.2.2.9 References to items

For each possible item answer (answer in the support column) within the ICS proforma a unique reference exists, used, for example, in the conditional expressions. It is defined as the table identifier, followed by a solidus character "/", followed by the item number in the table. If there is more than one support column in a table, the columns are discriminated by letters (a, b, etc.), respectively.

EXAMPLE 1 C.5/4 is the reference to the answer of item 4 in Table C.5.

EXAMPLE 2 C.6/3b is the reference to the second answer (i.e. in the second support column) of item 3 in Table C.6.

C.2.2.10 Prerequisite line

A prerequisite line takes the form: Prerequisite: <predicate>.

A prerequisite line after a clause or table title indicates that the whole clause or the whole table is not required to be completed if the predicate is FALSE.

C.3 Instructions for completing the ICS proforma

The supplier of the implementation shall complete the ICS proforma in each of the spaces provided. In particular, an explicit answer shall be entered, in each of the support or supported column boxes provided, using the notation described in C.2.2.

If necessary, the supplier may provide additional comments in space at the bottom of the tables or separately.

A separate ICS shall be provided by the supplier for each supported IAP.

C.4 ICS proforma for OBU

C.4.1 Identification implementation

C.4.1.1 Identification of OBU supplier

Table C.1 — Identification of OBU supplier form

Company	
Postal address	
Telephone	
Contact person	
E-mail address	

C.4.1.2 Identification of OBU

Table C.2 — Identification of OBU form

Brand	
Type, Version	
ManufacturerID	
EquipmentClass	
Serial numbers of supplied units	

C.4.2 Identification of the standard

This ICS proforma applies to the following standard:

EN 15509 (this document)

This ICS proforma applies only for OBUs.

C.4.3 Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No) ……

NOTE 1 Answering "No" to this question indicates non-conformance to the specification. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming, on pages attached to the ICS proforma.

Which security level is implemented (0/1) ……

NOTE 2 See 6.1.5 and Annex D for definition of the security levels.

C.4.4 ICS proforma for OBU

Table C.3 — Security level

Item		Reference	Status	Support
1	Security level 0	6.1.5.2	m	
2	Security level 1	6.1.5.3	o	

Table C.4 — DSRC requirements

Item		Reference	Status	Support
1	Profile P0/P1 set L1-B	6.1.2/0	o.1	
2	Profile P0/P1 set L1-A	6.1.2/0	o.1	
3	Conversion gain limit	6.1.2/0	c.1	
4	Cut-off power level minimum	6.1.2/0	c.1	
5	Concatenation with chaining	6.1.2/0	m	
6	Concatenation without chaining	6.1.2/0	m	
7	Fragmentation header of 1 octet	6.1.2/0	m	
8	Fill bits	6.1.2/0	m	

o.1: It is mandatory to support at least one of these items

c.1: IF C.4/2 – “Profile P0/P1 set L1-A” supported THEN ‘m’ ELSE ‘n/a’

If item 1 or 2 supported, this implies that ETSI tests for L1, L2 and L7 shall be performed.

Table C.5 — DSRC L7 and EFC functions

Item		Reference	Status	Support
1	INITIALIZATION	6.1.3/0	m	
2	ACTION – GetStamped	6.1.3/0	m	
3	GET	6.1.3/0	m	
4	SET	6.1.3/0	m	
5	ACTION – SetMMI	6.1.3/0	m	
6	ACTION – Echo	6.1.3/0	m	
7	EVENT-REPORT – Release	6.1.3/0	m	
8	AC_CR support	6.1.3/0	c.1	

c.1: IF C.3/2 – “Security Level 1” supported THEN ‘m’ ELSE ‘n/a’

Table C.6 — Data requirements

Item		Reference	Status	Support read protection	Support write protection	Support length and coding
1	Addressing of EFC system and application data	6.1.4/0	m			
2	ApplicationContextMark	6.1.4/0	m			
3	EFC Context Mark	6.1.4/0	m			
4	PaymentMeans	6.1.4/0	m			
5	VehicleLicencePlateNumber	6.1.4/0	m			
6	VehicleClass	6.1.4/0	m			
7	VehicleDimensions	6.1.4/0	m			
8	VehicleAxles	6.1.4/0	m			
9	VehicleWeightLimits	6.1.4/0	m			
10	VehicleSpecificCharacteristics	6.1.4/0	m			
11	EquipmentOBUId	6.1.4/0	m			
12	EquipmentStatus	6.1.4/0	m			
13	ReceiptData1	6.1.4/0	m			
14	ReceiptData2	6.1.4/0	m			

Table C.7 – Security requirements

Item		Reference	Status	Support read protection	Support write protection	Support length and coding
1	AuthenticationKey1	6.1.5.2/0	m			
2	AuthenticationKey2	6.1.5.2/0	m			
3	AuthenticationKey3	6.1.5.2/0	m			
4	AuthenticationKey4	6.1.5.2/0	m			
5	AuthenticationKey5	6.1.5.2/0	m			
6	AuthenticationKey6	6.1.5.2/0	m			
7	AuthenticationKey7	6.1.5.2/0	m			
8	AuthenticationKey8	6.1.5.2/0	m			
9	KeyRef	6.1.5.2/0	m			
10	RndRSE	6.1.5.2/0	m			
11	AccessKeys	6.1.5.3/0	c.1			
12	AC_CR	6.1.5.3/0	c.1			
13	AC_CR-KeyReference	6.1.5.3/0	c.1			
14	RndOBU	6.1.5.3/0	c.1			

c.1: IF C.3/2 – “Security Level 1” supported THEN ‘m’ ELSE ‘n/a’

Table C.8 – Security requirements

Item		Reference	Status	Support
1	Authenticator (calculation on an attribute list)	6.1.5/0	m	
2	TransactionCounter	6.1.5/0	m	
3	AccessCredentials calculation	6.1.5.3/0	c.1	

c.1: IF C.3/2 – “Security Level 1” supported THEN ‘m’ ELSE ‘n/a’

Table C.9 – Transaction requirements

Item		Reference	Status	Support
1	EFC transaction model	6.1.6/0	m	

C.4.5 Profile requirements list for OBU

C.4.5.1 General

The purpose of this requirement list is to specify the modifications that apply to the status of the items affected in the ICS proforma of each base specification.

The supplier of a protocol implementation which is claimed to conform to the OBU specific requirements of this European Standard (EN 15509) shall verify that his particular application layer protocol implementation

meets the profile requirements list (RL) for this layer. For this, he shall complete a copy of the corresponding layer PICS proforma contained in Annex A of ETSI/TS 102 486-1-1 V1.1.1 (2006-03), Annex A (data link layer) and ETSI/TS 102 486-2-1 V1.2.1 (2008-10) (application layer), updated with the requirements from this annex.

C.4.5.2 Profile requirements list (profile RL)

The profile Requirements List (profile RL) for the application layer as defined in this annex is based on Annex A of ETSI/TS 102 486-1-1 V1.1.1 (2006-03) (data link layer) and ETSI/TS 102 486-2-1 V1.2.1 (2008-10) (application layer). For every capability listed in Annex A, the profile requirements are expressed by restriction upon allowed support answers in Annex A of ETSI/TS 102 486-1-1 V1.1.1 (2006-03). The profile RL is produced by copying selected tables from Annex A of ETSI/TS 102 486-1-1 V1.1.1 (2006-03), removing the column(s) to be completed by the supplier, and adding a new set of columns giving the new profile requirements, both in terms of the status and allowed values. The tables are referenced by their numbering in Annex A of ETSI/TS 102 486-1-1 V1.1.1 (2006-03).

C.4.5.3 Reference column:

The reference column gives reference to ETSI/TS 102 486-1-1 V1.1.1 (2006-03) (data link layer) and ETSI/TS 102 486-2-1 V1.2.1 (2008-10) (application layer), except where explicitly stated otherwise.

C.4.5.4 Data link layer

Table C.10 — LLC Service Modes

Item	Service mode implemented	Reference	Status
2	LLC Acknowledged connectionless mode	8.1	m

Table C.11 — ACn command functionality

Item	Parameter	Reference	Status
3	Exchanging Data	8.4.3.2	m

Table C.12 — MAC Control field values

Item	Field implemented	Reference	Status	Values
				Allowed
3	MAC control field transmitted	6.4.2	m	'D0'H
8	MAC control field received	6.4.2	m	'A8'H

Table C.13 — ACn protocol procedures

Item	Procedure	Reference	Status
1	Late response procedure I	7.2.2	m

C.4.5.5 Application layer

Table C.14 — T-Kernel Procedures

Item	Procedures supported	Reference	Status
4	Application capable of creating T-APDUs which cause max length of LLC frame to be exceeded	6.3.10	x
5	Fragmentation and Defragmentation	6.3.3, 6.3.10	x
8	Concatenation	6.3.7	m
9	Concatenation with Chaining	6.3.8	m

Table C.15 — T-Kernel PDUs

Item	PDUs implemented	Sending		Receiving	
		Reference	Status	Reference	Status
1	Get-Request	6.3.2, 6.4.2	x	6.3.2, 6.4.2	m
2	Get-Response	6.3.2, 6.4.2	m	6.3.2, 6.4.2	n/a
3	Set-Request	6.3.2, 6.4.2	x	6.3.2, 6.4.2	m
4	Set-Response	6.3.2, 6.4.2	m	6.3.2, 6.4.2	n/a
5	Action-Request	6.3.2, 6.4.2	x	6.3.2, 6.4.2	m
6	Action-Response	6.3.2, 6.4.2	m	6.3.2, 6.4.2	n/a

Table C.16 — Received Get-Request Parameters

Item	Parameter	Reference	Status
3	accessCredentials	A	m
4	iid	A	x
5	attrIdList	A	m

Table C.17 — Transmitted Get-Response Parameters

Item	Parameter	Reference	Status
3	iid	A	x
4	Attributelist	A	m
5	ret	A	m

Table C.18 — Received Set-Request Parameters

Item	Parameter	Reference	Status
4	accessCredentials	A	m
6	iid	A	x

Table C.19 — Transmitted Set-Response Parameters

Item	Parameter	Reference	Status
3	iid	A	x
4	ret	A	m

Table C.20 — Received Action-Request Parameters

Item	Parameter	Reference	Status
4	accessCredentials	A	m
5	actionParameter	A	m
6	iid	A	x

Table C.21 — Transmitted Action-Response Parameters

Item	Parameter	Reference	Status
3	iid	A	x
4	responseParameter	A	m
5	ret	A	m

Table C.22 — Received Event-Report-Request Parameters

Item	Parameter	Reference	Status
4	accessCredentials	A	x
5	eventParameter	A	x
6	iid	A	x

Table C.23 — Valid frames

Item	Frame type	Reference	Status
11	Private LID, ACn command GET.request	6.4.2	m
12	Private LID, ACn command SET.request, mode=1	6.4.2	m
13	Private LID, ACn command ACTION.request, mode=1	6.4.2	m

Table C.24 — Allowed frames

Item	Frame type	Reference	Status
9	Private LID, ACn response GET.response, f=1	6.4.2	m
10	Private LID, ACn response SET.response, f=1	6.4.2	m
11	Private LID, ACn response ACTION.response, f=1	6.4.2	m

C.5 ICS proforma for RSE

C.5.1 Identification implementation

C.5.1.1 Identification of RSE supplier

Table C.25 — Identification of RSE supplier form

Company	
Postal address	
Telephone	
Contact person	
E-mail address	

C.5.1.2 Identification of RSE

Table C.26 — Identification of RSE form

Brand	
Type, Version	
ManufacturerID	
EquipmentClass	
Serial numbers of supplied units	

C.5.2 Identification of the standard

This ICS proforma applies to the following standard:

EN 15509 (this document)

This ICS proforma applies only for RSEs.

C.5.3 Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No) ……

NOTE 1 Answering "No" to this question indicates non-conformance to the specification. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming, on pages attached to the ICS proforma.

Which security level is implemented (0/1) ……

NOTE 2 See 6.1.5 and Annex D for definition of the security levels.

C.5.4 ICS proforma for RSE

Table C.27 — Security level

Item		Reference	Status	Support
1	Security level 0	6.2.5.3	m	
2	Security level 1	6.2.5.3	o	

Table C.28 — DSRC requirements

Item		Reference	Status	Support
1	Profile P0/P1 set L1-B	6.2.2/0	o.1	
2	Profile P0/P1 set L1-A	6.2.2/0	o.1	
3	Conversion gain limit	6.2.2/0	c.1	
4	Cut-off power level minimum	6.2.2/0	c.1	
5	Concatenation with chaining	6.2.2/0	m	
6	Concatenation without chaining	6.2.2/0	m	
7	Fragmentation header of 1 octet	6.2.2/0	m	
8	Fill bits	6.2.2/0	m	
9	Parameter D4a	6.2.2/0	c.2	

o.1: It is mandatory to support at least one of these items

c.1: IF C.28/2 – “Profile P0/P1 set L1-A” supported THEN ‘m’ ELSE ‘n/a’

c.2: Mandatory (‘m’) if RSE-type = fixed; Not applicable (‘n/a’) if RSE-type = other

If item 1 or 2 supported, this implies that ETSI tests for L1, L2 and L7 shall be performed.

Table C.29 — L7 and EFC functions

Item		Reference	Status	Support
1	INITIALIZATION	6.2.3/0	o	
2	ACTION – GetStamped	6.2.3/0	o	
3	GET	6.2.3/0	o	
4	SET	6.2.3/0	o	
5	ACTION – SetMMI	6.2.3/0	o	
6	ACTION – Echo	6.2.3/0	o	
7	EVENT-REPORT – Release	6.2.3/0	o	
8	AC_CR support	6.2.3/0	c.1	

c.1: IF C.27/2 – “Security Level 1” supported THEN ‘m’ ELSE ‘n/a’

Table C.30 — Data requirements

Item		Reference	Status	Support read protection	Support write protection	Support length and coding
1	EFC Context Mark	6.2.4/0	o			
2	PaymentMeans	6.2.4/0	o			
3	VehicleLicencePlateNumber	6.2.4/0	o			
4	VehicleClass	6.2.4/0	o			
5	VehicleDimensions	6.2.4/0	o			
6	VehicleAxles	6.2.4/0	o			
7	VehicleWeightLimits	6.2.4/0	o			
8	VehicleSpecificCharacteristics	6.2.4/0	o			
9	VehicleAuthenticator	6.2.4/0	o			
10	VehicleSuspensionType	6.2.4/0	o			
11	EquipmentOBUId	6.2.4/0	o			
12	EquipmentStatus	6.2.4/0	o			
13	ReceiptData1	6.2.4/0	o			
14	ReceiptData2	6.2.4/0	o			

Table C.31 — Security requirements

Item		Reference	Status	Supprt read protection	Support write protection	Support length and coding
1	AuthenticationKey1	6.2.5.2/0	m			
2	AuthenticationKey2	6.2.5.2/0	m			
3	AuthenticationKey3	6.2.5.2/0	m			
4	AuthenticationKey4	6.2.5.2/0	m			
5	AuthenticationKey5	6.2.5.2/0	m			
6	AuthenticationKey6	6.2.5.2/0	m			
7	AuthenticationKey7	6.2.5.2/0	m			
8	AuthenticationKey8	6.2.5.2/0	m			
9	KeyRef	6.2.5.2/0	m			
10	RndRSE	6.2.5.2/0	m			
11	AccessKeys	6.2.5.3/0	c.1			
12	AC_CR	6.2.5.3/0	c.1			
13	AC_CR-KeyReference	6.2.5.3/0	c.1			
14	RndOBU	6.2.5.3/0	c.1			

c.1: IF C.3/2 – “Security Level 1” supported THEN ‘m’ ELSE ‘n/a’

Table C.32 — Security requirements

Item		Reference	Status	Support
1	Authenticator calculation on an attribute list	6.2.5/0	m	
2	TransactionCounter update	6.2.5/0	m	
3	AccessCredentials calculation	6.2.5.3/0	c.1	

c.1: IF C.27/2 – “Security Level 1” supported THEN ‘m’ ELSE ‘n/a’

Table C.33 — Transaction requirements

Item		Reference	Status	Support
1	EFC transaction model	6.2.6/0	m	

C.5.5 Profile requirements list for RSE

C.5.5.1 General

The purpose of this requirement list is to specify the modifications that apply to the status of the items affected in the ICS proforma of each base specification.

The supplier of a protocol implementation which is claimed to conform to the OBU specific requirements of EN 15509 shall verify that his particular application layer protocol implementation meets the profile RL for this layer. For this, he shall complete a copy of the corresponding layer PICS proforma contained in Annex B of ETSI/TS 102 486-1-1 V1.1.1 (2006-03) (data link layer) and ETSI/TS 102 486-2-1 V1.2.1 (2008-10) (application layer), updated with the requirements from this annex.

C.5.5.2 Profile requirements list (profile RL)

The profile requirements list (profile RL) for the application layer as defined in this annex is based on Annex B of ETSI/TS 102 486-1-1 V1.1.1 (2006-03) (data link layer) and ETSI/TS 102 486-2-1 V1.2.1 (2008-10) (application layer). For every capability listed in Annex B of ETSI/TS 102 486-1-1 V1.1.1 (2006-03), the profile requirements are expressed by restriction upon allowed support answers in Annex B of ETSI/TS 102 486-1-1 V1.1.1 (2006-03). The profile RL is produced by copying selected tables from Annex B of ETSI/TS 102 486-1-1 V1.1.1 (2006-03), removing the column(s) to be completed by the supplier, and adding a new set of columns giving the new profile requirements, both in terms of the status and allowed values. The tables are referenced by their numbering in Annex B of ETSI/TS 102 486-1-1 V1.1.1 (2006-03).

C.5.5.3 Reference column

The reference column gives reference to ETSI/TS 102 486-1-1 V1.1.1 (2006-03) (data link layer) and ETSI/TS 102 486-2-1 V1.2.1 (2008-10) (application layer), except where explicitly stated otherwise.

C.5.5.4 Data link layer

Table C.34 — LLC Service Modes

Item	Service mode implemented	Reference	Status
2	LLC Acknowledged connectionless mode	8.1	m

Table C.35 — ACn command functionality

Item	Parameter	Reference	Status
3	Exchanging Data	8.4.3.2	m

Table C.36 — MAC Control field values

Item	Field implemented	Reference	Status	Values
				Allowed
3	MAC control field received	6.4.2	m	'D0'H
8	MAC control field transmitted	6.4.2	m	'A8'H

Table C.37 — ACn protocol procedures

Item	Procedure	Reference	Status
1	Late response procedure I	7.2.2	m

C.5.5.5 Application layer

Table C.38 — T-Kernel Procedures

Item	Procedures supported	Reference	Status
4	Application capable of creating T-APDUs which cause max length of LLC frame to be exceeded	6.3.10	x
5	Fragmentation and Defragmentation	6.3.3, 6.3.10	x
8	Concatenation	6.3.7	m
9	Concatenation with Chaining	6.3.8	m

Table C.39 — T-Kernel PDUs

Item	PDUs implemented	Sending		Receiving	
		Reference	**Status**	**Reference**	**Status**
1	Get-Request	6.3.2, 6.4.2	m	6.3.2, 6.4.2	n/a
2	Get-Response	6.3.2, 6.4.2	x	6.3.2, 6.4.2	m
3	Set-Request	6.3.2, 6.4.2	m	6.3.2, 6.4.2	n/a
4	Set-Response	6.3.2, 6.4.2	x	6.3.2, 6.4.2	m
5	Action-Request	6.3.2, 6.4.2	m	6.3.2, 6.4.2	n/a
6	Action-Response	6.3.2, 6.4.2	x	6.3.2, 6.4.2	m

Table C.40 — Transmitted Get-Request Parameters

Item	Parameter	Reference	Status
3	accessCredentials	A	m
4	iid	A	x
5	attrIdList	A	m

Table C.41 — Received Get-Response Parameters

Item	Parameter	Reference	Status
3	iid	A	x
4	Attributelist	A	m
5	ret	A	m

Table C.42 — Transmitted Set-Request Parameters

Item	Parameter	Reference	Status
4	accessCredentials	A	m
6	iid	A	x

Table C.43 — Received Set-Response Parameters

Item	Parameter	Reference	Status
3	iid	A	x
4	ret	A	m

Table C.44 — Transmitted Action-Request Parameters

Item	Parameter	Reference	Status
4	accessCredentials	A	m
5	actionParameter	A	m
6	iid	A	x

Table C.45 — Received Action-Response Parameters

Item	Parameter	Reference	Status
3	iid	A	x
4	responseParameter	A	m
5	ret	A	m

Table C.46 — Transmitted Event-Report-Request Parameters

Item	Parameter	Reference	Status
4	accessCredentials	A	x
5	eventParameter	A	x
6	iid	A	x

Table C.47 — Allowed frames

Item	Frame type	Reference	Status
11	Private LID, ACn command GET.request	6.4.2	m
12	Private LID, ACn command SET.request, mode=1	6.4.2	m
13	Private LID, ACn command ACTION.request, mode=1	6.4.2	m

Table C.48 — Valid frames

Item	Frame type	Reference	Status
9	Private LID, ACn response GET.response, f=1	6.4.2	m
10	Private LID, ACn response SET.response, f=1	6.4.2	m
11	Private LID, ACn response ACTION.response, f=1	6.4.2	m

Annex D
(informative)

IAP taxonomy and numbering

D.1 General

The intentions of application profiling for EFC-DSRC are outlined in Annex D together with a basic taxonomy and numbering of IAPs within the framework of this standard. Annex D may be used for referencing, e.g. when stating conformance to this European Standard, or when preparing future editions of this European Standard or IAP standards.

D.2 Contents of an Interoperable Application Profile (IAP)

Whereas this edition of EN 15509 only defines one IAP, D.2 outlines the principles of creating an IAP in case subsequent editions (or other standards) will do so. It should be noted that the purpose of an IAP is to ensure technical interoperability between different EFC-systems in Europe (i.e. it should not merely describe a local or national EFC-system).

The scope for an IAP is defined in Clause 1 and the general provisions for conformance in Clause 5. An IAP is a coherent set of choices and parameter values within the following base standards*:*

— EN ISO 14906:— EFC application interface definition for DSRC (this implies indirect references to; EN ISO 14816:— Numbering and data structures);

— EN 12834 — DSRC application layer (L7);

— EN 13372 — DSRC Profiles (this implies indirect references to the DSRC L1, L2 and L7 standards: EN 12253, EN 12795 and EN 12834).

An IAP is defined by stating a set of conformance requirements (as done in Clause 6 above). This is done according to the ISP-principles as in ISO/IEC/TR 10000-1 (summarized in the Introduction above). The resulting set of requirements shall define one single IAP in terms of chosen classes, subsets, options and parameter values within the limits of the base standards.

The conformance requirements for EFC-DSRC-IAPs shall include the following parts (divided into separate sets of requirements for OBU and RSE):

— DSRC requirements;

— DSRC L7 and EFC functions;

— data requirements;

— security requirements;

— transaction requirements.

The conformance requirements shall not contain options (with the exception for security levels, which may be subject to staged implementation by EFC-scheme owners). Each IAP may have its own set of security levels. Security levels are incremental; meaning that implementation of a higher security level automatically implies implementation of all the requirements for lower levels of security.

This implies that large changes and updates in security that are not incremental (e.g. the use of completely new methods for cryptographic calculations replacing old methods) should be implemented as a new IAP.

NOTE This implies that any RSE that has only implemented the security requirements associated with level 0 in this European Standard (as in 6.2.5.3) will not access OBU data protected by means of access credentials (as it is the "security level 1 OBU" that requires verification of the RSE authenticity in order to grant access to the protected OBU data).

D.3 IAP referencing and numbering

D.3.1 IAP numbering

This European Standard defines only one Interoperable Application Profile. In case there will be more IAPs defined for the future this is to be referred to as IAP number 1. Any further IAPs are to be numbered sequentially (2, 3, etc.).

NOTE 1 The DSRC-standards EN 12834 and EN 13372 define and use an ASN.1 attribute called "Profile" for defining a fixed set of DSRC characteristics. The IAPs defined in this European Standard is not to be confused with the (DSRC) Profile defined in the DSRC-standards.

This European Standard defines different sets of conformance requirements for OBU and for RSE. Hence, conformance to EN 15509 shall be noted separately for the OBU and the RSE.

NOTE 2 The ISP-standards, ISO/IEC/TR 10000-1, ISO/IEC/TR 10000-2 and ISO/IEC/TR 10000-3, define an overall hierarchical structure for IT-taxonomy of ISP-standards. This is deemed not applicable for this European Standard (EN 15509), and is not used here.

D.3.2 Security levels numbering

This European Standard defines two security levels that may be implemented independently in OBU and RSE (i.e. with or without support for Access Credentials). These are labelled; Level 0 and Level 1. In case there will be more security levels defined for the future they are to be numbered sequentially (2, 3, etc.). Security levels are noted as a decimal index to the IAP number in case they are used for a profile (i.e. IAP-number.SecurityLevel).

As this European Standard defines different sets of conformance requirements for OBU and for RSE, security level conformance shall be noted separately for the OBU and the RSE.

D.3.3 Numbering and referencing examples

EXAMPLE 1 An RSE conformant with IAP-1 of EN 15509 without support for Access Credentials is noted: "RSE conformant with 15509 IAP 1.0"

EXAMPLE 2 An OBU conformant with IAP-1 of EN 15509 with support for Access Credentials is noted: "OBU conformant with 15509 IAP 1.1"

Annex E
(informative)

Security computation examples

E.1 General

Annex E illustrates the cryptographic mechanisms defined in the conformance clause (Clause 5) and in Annex B by means of a few numerical examples. Numeric values in the examples below are in hexadecimal.

E.2 Computation of Attribute Authenticator

EXAMPLE This example describes the calculation of an authenticator using an AttributeList containing the only attribute PaymentMeans. The following values are used, the authenticator is calculated using the following values:

PaymentMeans = '52 75 12 34 56 78 90 12 FF FF 21 21 00 00'

RndRSE: '1A 61 A9 85' (1st of March 2003, 21:12:10)

AuK = '26 BF 3D F3 BC E3 65 6B' (Derived from the MAuK according to example in B.4.2).

The message M (the input data) is then equal to:

M = ‘AttributeList (PaymentMeans) || RndRSE (octet string) || Padding’ = ‘01 20 40 52 75 12 34 56 78 90 12 FF FF 21 21 00 00 04 1A 61 A9 85 00 00’

and

$D_1 = I_1$ = Sub(M, 0, 8) = ‘01 20 40 52 75 12 34 56’

D_2 = Sub(M, 8, 8) = ‘78 90 12 FF FF 21 21 00’

D_3 = Sub(M, 16, 8) = ‘00 04 1A 61 A9 85 00 00’

With ICV : '00 00 00 00 00 00 00 00': the Input I_1 = ICV xor I_1 = D_1 = ‘01 20 40 52 75 12 34 56’

O_1 = e[AuK](I_1) = ‘45 1F F4 A9 72 9B CE 58’

and

I_2 = O_1 xor D_2 = ‘45 1F F4 A9 72 9B CE 58’ xor ‘78 90 12 FF FF 21 21 00’ = ‘3D 8F E6 56 8D BA EF 58’

Calculation of O_2 gives:

O_2 = e[AuK](I_2) = ‘4F BB E8 C6 4B 0B EF A5’

and

I_3 = O_2 xor D_3 = ‘4F BB E8 C6 4B 0B EF A5’ xor ‘00 04 1A 61 A9 85 00 00’ = ‘4F BF F2 A7 E2 8E EF A5’

Calculation of O_3 gives:

O_3 = e[AuK](I_3) = ‘BF 87 5F F0 90 AD BF E0’

The leftmost 32 bits represent the Authenticator:

Auth = Sub(O_3, 0, 4) = ‘BF 87 5F F0’

A change in the input parameters will completely change the Authenticators. To illustrate this we calculate the Authenticator for a different value of RndRSE, without changing the values for the other parameters.

With:

RndRSE: '1A 61 A9 86' (1th of March 2003, 21:12:12)

we find:

Auth = ‘23 98 AA 8D’

E.3 Computation of Access Credentials

NOTE E.3 only applies for implementation of Security Level 1 according to 6.1.5 and 6.2.5.

EXAMPLE For the computation of the Access Credentials the AcK = '9B 48 AA E0 7A 7B C0 08' derived from the MAcK according to B.4.3.

Assuming:

RndOBE = '97 86 75 64'

this gives:

VAL = ‘RndOBE || 00 00 00 00' = '97 86 75 64 00 00 00 00'.

Calculation gives:

O_1 = e[AcK](VAL) = ‘E0 55 EA 12 1F 5C 97 D7’

and hence:

AC_CR = Sub(O_1, 0, 4) = ‘E0 55 EA 12’

E.4 Key derivation

E.4.1 Authenticator Key

EXAMPLE In this example shows how the Authentication Key is calculated using the following application data and Master Key value:

PaymentMeans:

- PersonalAccountNumber, PAN: '52 75 12 34 56 78 90 12 FF FF' (16 characters PAN, padding with '1' bits)
- PaymentMeansExpiryDate: '21 21' (2006-09-01)
- PaymentMeansUsageControl: '00 00'
- ContractProvider: A4 00 01 (Country SE , Toll Service Provider #1)
- MAuK : '13 13 13 13 13 13 13 13 AB AB AB AB AB AB AB AB';

The CompactPAN is calculated as:

CompactPAN = Sub(PAN, 0, 4) xor Sub(PAN, 4, 4) = '04 0D 82 26', where:

- Sub(PAN,0,4) = HighDWord32(PAN),

- Sub(PAN, 4,4) is LowDWord32(PAN)

The input data (VAL) follow from:

VAL = ‘CompactPAN || ContractProvider || 00' = '04 0D 82 26 A4 00 01 00'

gives the following value for the Authentication Key:

AuK = ede[MAuK](VAL) = '26 BF 3D F3 BC E3 65 6B"

With a different value for the PAN the derived key will be different. As an example, with a PAN = '58 61 12 34 56 78 90 12 FF FF', and the same Contract Provider and Master Keys as above, the calculation leads to the following derived keys:

AuK = 'A7 AD C3 82 44 1C 1D 00'

E.4.2 Access Credentials Key

NOTE E.4.2 only applies for implementation of Security Level 1 according to 6.1.5 and 6.2.5.

EXAMPLE The derivation of the Access Credentials Key is quite similar to the derivation of the Authenticators keys. Instead of the PAN the AC_CR-KeyReference is used.

Using the following application data values and Master Key:

- AC_CR-KeyReference: ’12 34’

- MAcK: '57 57 57 57 57 57 57 57 EF EF EF EF EF EF EF EF'

this gives:

VAL = ‘AC_CR-KeyReference || AC_CR-KeyReference || AC_CR-KeyReference || AC_CR-KeyReference’ = '12 34 12 34 12 34 12 34'

and:

AcK = ede[MAcK](VAL) = '9B 48 AA E0 7A 7B C0 08'

Again, a different AC_CR-KeyReference or Master Key will produce a completely different Access Credentials Key.

Annex F
(informative)

Security Considerations

This annex describes how this European standard supports the security measures and implementations that according to CEN/TS 16439 on "EFC - Security Framework" are required for the DSRC-EFC interface.

CEN/TS 16439 section 7.3.2 defines the following security measures (SM) to be implemented:

SM210 – The RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for Toll Charger (MAC_TC) over at least the EN ISO 14906 attribute PaymentMeans, using a key known only to the Toll Charger and the Toll Service Provider.

SM211 – The RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for Toll Service Provider (MAC_TSP) over at least the EN ISO 14906 attribute PaymentMeans, using a key known only to the Toll Service Provider.

SM212 – The OBE shall implement an access control mechanism for EFC commands addressing its data attributes. The RSE shall implement the calculation of the corresponding access codes.

SM213 – The RSE shall read, increment and write a transaction counter to the OBE. The OBE shall support this.

To fulfil SM210, the Toll Service Provider shall have provided at least one Master Authentication Key to the Toll Charger RSE.

The SM210 is performed when the Toll Charger RSE submits the DSRC L7 – EFC function; ACTION – GET_STAMPED according to 6.2.3 to the OBE and the OBE responds to this request according to 6.1.3. In the response the OBE includes the MAC_TC (Attribute Authenticator) calculated according to B.2. This MAC_TC is checked by the RSE in order to determine the authenticity of the OBE.

The SM211 is performed when the Toll Charger RSE submits the DSRC L7 – EFC function; ACTION – GET_STAMPED according to 6.2.3 to the OBE and the OBE responds to this request according to 6.1.3. In the response the OBE includes the MAC_TSP (Attribute Authenticator) calculated according to B.2. This MAC_TSP is submitted from the Toll Charger in the payment claim to the Toll Service Provider that in this way can determine that the OBE is authentic.

To fulfil SM212 the Toll Service Provider shall have provided the Master Access Key to the Toll Charger RSE.

The SM212 is performed when the RSE, according to the security Level 1 described in 6.2.5.3, calculates Access Credentials according to B.3 and includes these in every DSRC L7 or EFC function that retrieves or writes data from/to the OBE. An OBE compliant with Level 1 according to 6.1.5.3, will check the Access Credentials and only perform the requested operation if the Access Credentials are correct.

The SM213 is performed when the RSE reads and updates the transaction counter value in the attribute EquipmentStatus according to B.5. The transaction counter value is used by the Toll Charger to verify that no transactions from a certain OBE are missing or duplicated.

Annex G
(informative)

Interlayer management

G.1 General

There are no normative requirements on Inter Layer Management (i.e. State Transition Tables etc.) in this European Standard as there are no base standards defining these issues. Therefore, this Application Profile standard cannot make requirements on Inter Layer Management using the ISP-format. Annex G provides a set of guidelines and an outline on how Inter Layer Management can be performed.

G.2 RSE Inter Layer Management guidelines

OBUs may use a sleep mode to reduce power consumption. An OBU that has gone into sleep mode during a transaction may need a BST to resume the transaction since this is needed to establish that the OBU is still at the same beacon. This forces the requirement on the RSE that BSTs should be sent interleaved in the transaction and continuously when no transaction is taking place.

In case an OBU does not support the services required by the RSE (no EFC CM mutually agreed), the RSE shall send an Event-Report Release without any other command.

The OBU shall enter in “Blocked State”, when receiving an Event Report Release

G.3 OBU Inter Layer Management guidelines

When an OBU has finished its initialization process, it should not respond to any BSTs as long as the BST contains the same BeaconId, The initialization process is finished when the OBU receives its first privately addressed command (except for PrWA).

An OBU that has been in power save mode, should, after reception of the first BST, go back to the same state as it was when it went to the power save mode. The OBU should not lose any information in the power save mode and be able to retransmit the previously sent frame.

NOTE Power save mode is optional.

If the OBU has a pending response LSDU to be sent in a Private UI command, the OBU should answer with PrWRq to all BSTs until a new privately addressed command has been received by the OBU. When a new privately addressed command has been received by the OBU, the OBU should not respond to any BSTs as long as the BST contains the same BeaconId.

G.4 State Transition Tables

Tables G.1 to G.4 below identify the events used in the transition table.

Table G.1 — Identification of downlink frames used in transition table

Identification in transition table	Identification in RTTT profiles [EN 13372:2004, Table 4]				
	no	**LID**	**MAC**	**LLC**	**APDU**
PrWA	1	Private	20/28	None	None
BST	2	Broadcast	A0	03	INIT.req
BroadcastUI	3	Broadcast	80	03	SET.req, mode = 0 ACTION.req, mode = 0
PrivateUI	4	Private	80	03	SET.req, mode = 0 ACTION.req, mode = 0
Release	5	Private	80	03	EVENT_REPORT.req, mode = 0
ACnP0	6	Private	A0/A8	67/E7	None SET.req, mode = 0 ACTION.req, mode = 0
ACnP1	7	Private	A0/A8	77/F7	GET.req, mode = 1 SET.req, mode = 1 ACTION.req, mode = 1

Table G.2 — Identification of uplink frames used in transition table

Identification in transition table	Identification in RTTT profiles [EN 13372:2004, Table 4]					
	no	**LID**	**MAC**	**LLC**	**LLC status**	**APDU**
PrWRq	1	Private	60	None	None	None
VST	2	Private	C0	03	None	INIT.rsp
UI.cmd	3	Private	C0	03	None	GET.rsp SET.rsp ACTION.rsp
NR_OK	4	Private	D0	67/E7	40	None
NE_OK	5	Private	D0	77/F7	30	None
OK_OK	6	Private	D0	77/F7	00	GET.rsp SET.rsp ACTION.rsp
---	7	Private	D0	67/E7	10	None

Table G.3 — Events not from reception of frames

WakeUp	Event occurs when the OBU wakes up [EN 12253;parameter D10]
AwakeT_expired	The awake timer has expired (recommended to time out no sooner than 100ms).
Processing finished	The processing of an LSDU with slow access is finished.

Table G.4 — State transition table

State	Event	Action(s) [d]	Next State
POWSAVE	WakeUp	(no action)	START
START	BroadcastUI	Execute UI command/s/	START
	BST new BeaconId matching Profile and App.	Create new LID Send PrWRq Initialized = FALSE	INIT_SEQ
	BST same BeaconId BST time diff. >= 255 s. matching Profile and App.	Create new LID Send PrWRq Initialized = FALSE	INIT_SEQ
	BST same BeaconId BST time diff. < 255 s. Initialized == TRUE	(no action)	MAIN
	BST same BeaconId BST time diff. < 255 s. Initialized == FALSE	Send PrWRq	INIT_SEQ
	BST new BeaconId not matching Profile or App.	(no action)	POWSAVE [a]/START
	BST same BeaconId BST time diff. >= 255 s. not matching Profile or App.	(no action)	POWSAVE [a]/START
	BST same BeaconId BST time diff. < 255 s. Initialized = FALSE	(no action)	POWSAVE [a]/START
	AwakeT_expired [b]	(no action)	POWSAVE
	(other events)	(no action)	START
INIT_SEQ	BST new BeaconId matching Profile and App.	Create new LID Send PrWRq Initialized = FALSE	INIT_SEQ
	BST new BeaconId not matching Profile or App.	(no action)	POWSAVE [a]/START
	BST same BeaconId	Send PrWRq	INIT_SEQ
	PrWA	Send VST	INIT_SEQ
	ACnP0	Execute command/s/ Send NR_OK Initialized = TRUE	MAIN
	ACnP1 fast access	Execute command/s/ Send OK_OK and response LSDU Initialized = TRUE	MAIN
	ACnP1	Execute command/s/	BUSY

State	Event	Action(s) [d]	Next State
	slow access	Send NE_OK	
	BroadcastUI	Execute UI command/s/	INIT_SEQ
	PrivateUI (not release)	Execute UI command/s/ Initialized = TRUE	MAIN
	Release	Deregister LID Initialized = FALSE	POWSAVE [a]/START
	AwakeT_expired [b]	(no action)	POWSAVE
	(other events)	(no action)	INIT_SEQ
MAIN	BST new BeaconId matching Profile and App.	Create new LID Send PrWRq Initialized = FALSE	INIT_SEQ
	BST new BeaconId not matching Profile or App.	(no action)	POWSAVE [a]/START
	BST same BeaconId	(no action)	MAIN
	PrWA	Retransmit previous frame	MAIN
	ACnP0	Execute command/s/ Send NR_OK	MAIN
	ACnP1 fast access	Execute command/s/ Send OK_OK and response LSDU	MAIN
	ACnP1 slow access	Execute command/s/ Send NE_OK	BUSY
	ACnP0 retransmission	Send NR_OK	MAIN
	ACnP1 retransmission	Send OK_OK and last response LSDU	MAIN
	BroadcastUI	Execute UI command/s/	MAIN
	PrivateUI (not release)	Execute UI command/s/	MAIN
	Release	Deregister LID Initialized = FALSE	POWSAVE [a]/START
	AwakeT_expired [b]	(no action)	POWSAVE
	(other events)	(no action)	MAIN
BUSY	Rec_PrWA	Retransmit previous frame	BUSY
	ACnP1 retransmission	Retransmit NE_OK	BUSY
	Release	Deregister LID Initialized = FALSE	POWSAVE [a]/START
	Processing Finished	Save LSDU for later transmission	SLOW_DATA_1
	(other events)	(no action)	BUSY

State	Event	Action(s) [d]	Next State
SLOW_DATA_1	BST same BeaconId	Send PrWRq	SLOW_DATA_2
	BST new BeaconId matching Profile and App.	Create new LID Send PrWRq Initialized = FALSE	INIT_SEQ
	BST new BeaconId not matching Profile or App.	(no action)	POWSAVE [a]/START
	PrWA	Send OK_OK and LSDU response	MAIN
	ACnP1 retransmission	Send OK_OK and LSDU response	MAIN
	PrivateUI (not release)	Execute UI command/s/	SLOW_DATA_1
	Release	Deregister LID Initialized = FALSE	POWSAVE [a]/START
	AwakeT_expired [b]	(no action)	POWSAVE_WAIT
	(other events)	(no action)	SLOW_DATA_1
SLOW_DATA_2	BST same BeaconId	Send PrWRq	SLOW_DATA_2
	BST new BeaconId matching Profile and App.	Create new LID Send PrWRq Initialized = FALSE	INIT_SEQ
	BST new BeaconId not matching Profile or App.	(no action)	POWSAVE [a]/START
	PrWA	Send response LSDU as a UI.cmd	SLOW_DATA_2
	ACnP1 retransmission	Send OK_OK and LSDU response	MAIN
	ACnP0	Execute command/s/ Send NR_OK	MAIN
	ACnP1 fast access	Execute command/s/ Send OK_OK and response LSDU	MAIN
	ACnP1 slow access	Execute command/s/ Send NE_OK	BUSY
	PrivateUI (not release)	Execute UI command/s/	MAIN
	Release	Deregister LID Initialized = FALSE	POWSAVE [a]/START
	AwakeT_expired [b]	(no action)	POWSAVE_WAIT
	(other events)	(no action)	SLOW_DATA_2

State	Event	Action(s) [d]	Next State
POWSAVE_WAIT [c]	BST new BeaconId matching Profile and App.	Create new LID Send PrWRq Initialized = FALSE	INIT_SEQ
	BST new BeaconId not matching Profile or App.	(no action)	POWSAVE [a]/START
	BST same BeaconId BST time diff. >= 255 s. matching Profile and App.	Create new LID Send PrWRq Initialized = FALSE	INIT_SEQ
	BST same BeaconId BST time diff. < 255 s.	Send PrWRq	SLOW_DATA_2
	BST same BeaconId BST time diff. >= 255 s. not matching Profile or App.	(no action)	POWSAVE [a]/START

[a] The OBU may be blocked for communication for some seconds to reduce power consumption since the OBU should not answer at this beacon.

[b] The event AwakeT_expired will only occur if power save mode is implemented.

[c] POWSAVE- and POWSAVE_WAIT-states are only used if power save mode is implemented.

[d] The actions specified are not complete. More actions may need to be performed to be able to handle, e.g. the state machine.

All correct received frames should reset the AwakeT timer if power saving mode is implemented.

BroadcastUI and PrivateUI are not required to be supported, but they are still in the transition table since they are not prohibited.

Annex H
(informative)

Mounting guidelines for the OBU

H.1 General

To support interoperability between equipment from different manufacturers, it is crucial that not only the transaction requirements are specified but also that the geometrical aspects of the communication are sufficiently well defined. Annex H contains guidelines for mounting, concerning position and orientation of the OBU, which will enable the RSE to be designed and installed to achieve interoperability. It is essential that all RSE have such a design that they can handle all OBU including versions that meet the minimum requirements stated below.

H.2 OBU mounting position

OBUs shall be mounted in the centre of the vehicle. The OBU should not be installed in the vision area of the windshield, as defined by international regulations (UN/ECE regulation 43).

In light vehicle, this normally means a position at the middle of the higher rim of the windscreen, generally behind the rear view mirror. The corresponding height is between 1.20 m and 1.80 m above the ground level.

In heavy commercial vehicles and bus this normally means a position at the middle of the lower rim of the windscreen, generally just above the windscreen wipers when off. The corresponding height is between 1.50 m and 2.50 m above the ground level.

NOTE Most cars with heat reflecting metal film in the windscreen has a special mounting position for OBUs. Please consult the vehicle manufacturer documentation or representative to determine the correct mounting position OBU minimum active angle.

The OBU downlink and uplink parameters stated should be met within a minimum solid angle, called the OBU active angle:

— horizontally: ± 25º with respect to the vertical plane through the longitudinal axis of the vehicle;

— vertically: $35º < \Theta < 80º$, where Θ is the angle of the bore sight with respect to the horizontal plane as defined below.

These values are the same for any type of vehicles including cars, buses and trucks. Depending on the characteristics of the OBU, to respect these requirements, it may be recommended to use:

— specific brackets for trucks with vertical windscreen,

— specific brackets for light vehicles with flat windscreen.

The following figures illustrate how these angles are defined for a car, bus and for heavy commercial vehicle. The same principles are applicable for any other vehicle.

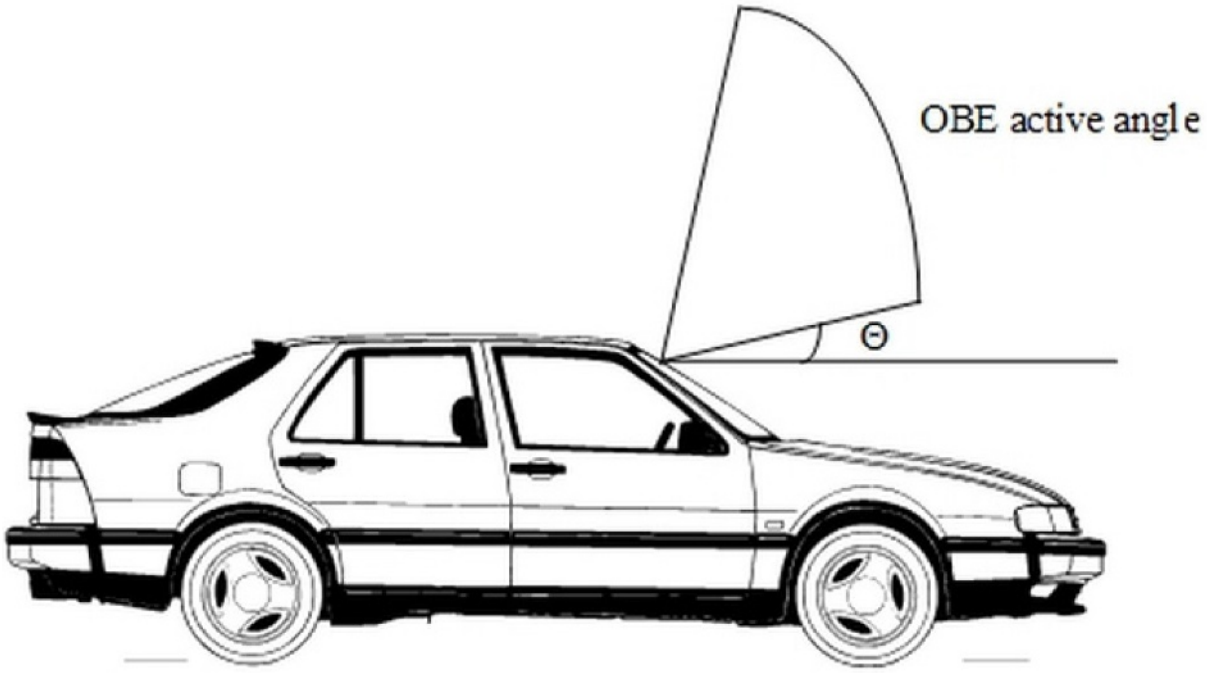

Figure H.1 — OBU active angle (vertically) for car

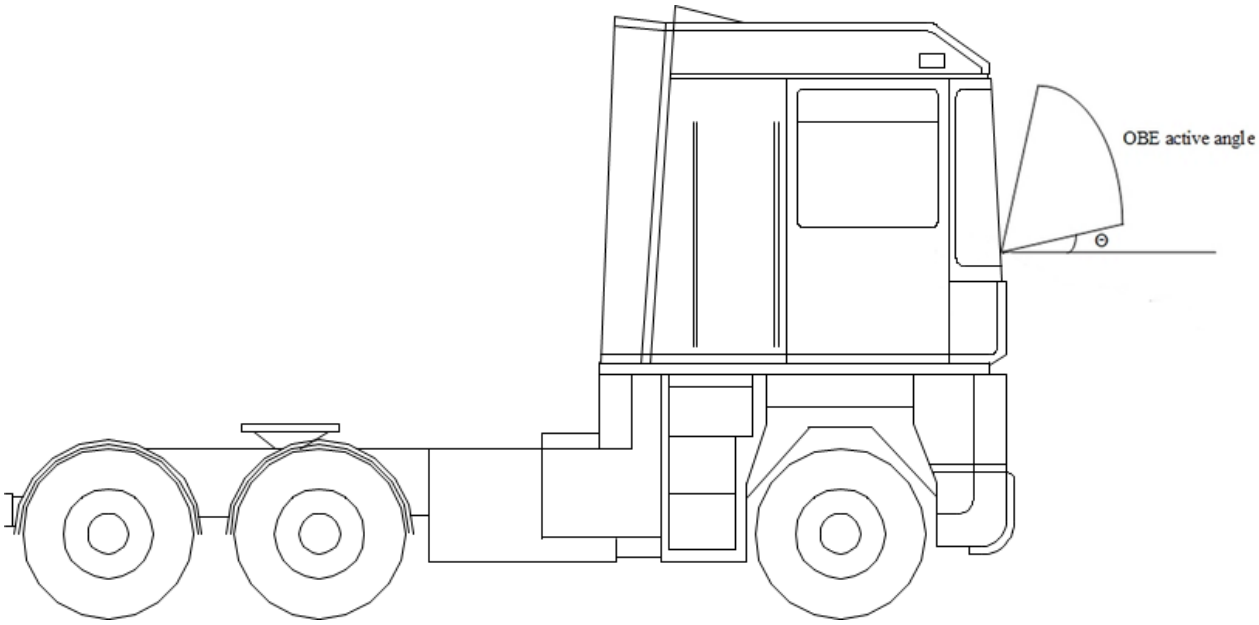

Figure H.2 — OBU active angle (vertically) for truck

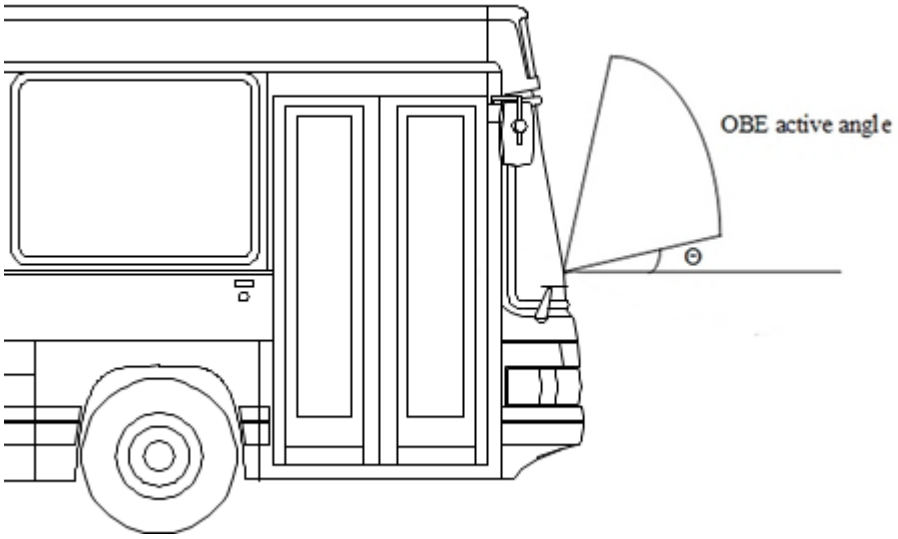

Figure H.3 — OBU active angle (vertically) for bus

Annex I
(informative)

Use of this standard for the EETS

I.1 General

In 2004, Directive 2004/52/EC of the European Parliament and of the Council "on the interoperability of electronic road toll systems in the community" was adopted. This European Directive calls for the establishment of a European Electronic Toll Service (EETS).

In 2009, EC Decision 2009/750/EC "on the definition of the European Electronic Toll Service and its technical elements" was adopted. It sets out the necessary technical specifications and requirements for that purpose, and contractual rules relating to EETS provision. The decision lays down rights and obligations on EETS Providers, Toll Chargers and EETS Users.

NOTE Other requirements and other EU Directives may also be applicable to the product(s) falling within the scope of this standard.

I.2 Overall relationship between European standardization and the EETS

Directive 2004/52/EC also triggered the establishment of a standardization mandate (M/338, "Standardisation mandate to CEN, CENELEC and ETSI in support of Interoperability of electronic road toll systems in the Community") that called for development of technical standards in support of the EETS. Activities under M/338 are supervised by the "ITS co-ordination group" (ITS-CG, previously ICTSB/ITSSG).

The M/338 does not explicitly call for the provision of harmonized standards (according to Directive 98/34/EC on the new approach to technical harmonization and standards), which means that this possibility is not available for the European standards that are developed in support of the EETS. Instead, this brief informative annex provides an outline of how this standard could be used in the context of the EETS.

EC Decisions can point out the use of specific standards, even if they are not formally harmonized. This is also done in Decision 2009/750/EC for a few standards (i.e. those that were available at the time of its approval). In case there will be more EC Decisions in support of the Directive, further European Standards could be referenced there as well.

The European Commission has also published in 2011 a "Guide for the Application of Directive on the Interoperability of Electronic Road Toll Systems" (ISBN 978-92-79-18637-0). This guide is intended to be a reference manual for all parties directly or indirectly concerned by Directive 2004/52/EC and Decision 2009/750/EC. It aims at providing help for the implementation of the EETS, including a list of standards that might be of use. The guide is only informative (e.g. the document cannot notify certain standards as "mandatory" for use in the EETS) and is intended to be updated on regular basis.

I.3 European standardisation work supporting the EETS

Many of the standards developed by CEN/TC 278 have been drafted with the EETS-requirements in mind (including the use of the results from European projects such as CARDME, PISTA, CESARE and RCI). CEN representatives have also taken part as observers in working groups, etc. initiated by the EC for the EETS. Hence, some work has been done in close cooperation between CEN working groups and the EC.

It should be noted that no CEN/ISO standards are "turnkey" solutions for the EETS. They are to be used as "building blocks" for the EETS, supporting the EETS legal framework and agreements between the parties

concerned by the EETS. A precise EETS-specification is not within the scope of CEN/ISO standards, but remains that task of the owners of the EETS-scheme.

It should also be noted that CEN/ISO standards have a wider scope than the EETS, which is a complementary service to the national services of the Members States and optional for the users, whereas CEN/ISO standards should be applicable to all EFC-services worldwide.

I.4 Correspondence between this standard and the EETS

This European standard defines requirements for interoperable EFC communication between OBU and RSE using CEN DSRC. Hence it meets the needs for definitions of one central interface in the EETS.

Decision 2009/750/EC specifically mentioned EN 15509 as a "mandatory" standard as a part of the EETS. The second edition of EN 15509 continues to support the EETS as it was referred to in the EC Decision as the defined IAP profile is being fully compliant with any implementations made based of EN 15509 edition one.

NOTE 1 EN 15509 was published after the EU Directive 2004/52/EC was adopted but before the EC Decision adopted and the Application Guide was published.

NOTE 2 The Implementers of the EETS can use IAP profile 1 as it is, but still need to decide on which security level to use.

Table I.1 shows how the requirements of IAP Profile 1 as defined in EN 15509 corresponds to essential requirements listed in Decision 2009/750/EC.

NOTE 3 The only explicit listing of essential requirements (ER) is in Annex III of 2009/750/EC. This standard also gives mention to other ERs listed below that are considered "implicit" based on the text in Directive 2004/52/EC and Decision 2009/750/EC.

Table I.1 — Correspondence between this European Standard and Decision 2009/750/EC "on the definition of the European Electronic Toll Service and its technical elements" harmonizing 2004/52/EC

Clause(s)/subclause(s) of this EN	Essential Requirements (ERs) of EC Decision 2009/750/EC	Qualifying remarks/Notes
Clause 6.1, 5.2, Annex A	Article 13.1, 14.1	Listed here as implicit ER.
Clause 6.1, 5.2, Annex A	Annex II.3(a)	Listed here as implicit ER.
Clause 6.1, 5.2, Annex A	Annex III.1.4	
Clause 6.1, 5.2, Annex B	Annex III.1.5	
Clause 6.1, 5.2, Annex A	Annex III.2.1.1	
Clause 6.1, 5.2, Annex A	Annex III.2.1.2	NOTE This standard does not cater for the requirements defined in Annex III.2.1.2 regarding the High Data Rate DSRC system as defined in ETSI ES 200674-1 and UNI 10607.

NOTE 4 Other requirements and other EU Directives may be applicable to the product(s) falling within the scope of this standard.

Bibliography

[1] INCITS 92-1981(R1998), *Data Encryption Algorithm*

[2] EN 12253, *Road transport and traffic telematics - Dedicated short-range communication - Physical layer using microwave at 5,8 GHz*

[3] EN 12795, *Road transport and traffic telematics - Dedicated Short Range Communication (DSRC) - DSRC data link layer: medium access and logical link control*

[4] EN 15876-1, *Electronic fee collection — Evaluation of on-board unit and roadside equipment for conformity to EN 15509 — Part 1: Test suite structure and test purposes*

[5] EN 15876-2, *Electronic fee collection - Evaluation of on-board and roadside equipment for conformity to EN 15509 - Part 2: Abstract test suite*

[6] CEN/TS 16439:2013[1]), *Electronic fee collection - Security framework*

[7] CEN ISO/TS 14907-1:2010, *Electronic fee collection - Test procedures for user and fixed equipment - Part 1: Description of test procedures (ISO/TS 14907-1:2010)*

[8] EN ISO 14816:2005, *Road transport and traffic telematics - Automatic vehicle and equipment identification - Numbering and data structure (ISO 14816:2005)*

[9] ETSI/TS 102 486-1-2, *Intelligent Transport Systems (ITS); 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 2: Test Suite Structure and Test Purposes (TSS&TP)*

[10] ETSI/TS 102 486-2-2, *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 2: Test Suite Structure and Test Purposes (TSS&TP)*

[11] ETSI/TS 102 486-1-3, *Intelligent Transport Systems (ITS); 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 3: Abstract Test Suite (ATS) and partial PIXIT proforma*

[12] ETSI/TS 102 486-2-3, *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 3: Abstract Test Suite (ATS) and partial PIXIT proforma*

[13] ISO 612, *Road vehicles — Dimensions of motor vehicles and towed vehicles — Terms and definitions*

[14] ISO 1176, *Road vehicles — Masses — Vocabulary and codes*

[15] ISO 16609:2012, *Financial services — Requirements for message authentication using symmetric techniques*

---

[1]) CEN/TS 16439:2013 is currently under revision and accepted as a CEN/ISO work item. The next edition will be assigned the reference CEN ISO/TS 19299.

[16] ISO 17573:2010, *Electronic fee collection — Systems architecture for vehicle-related tolling*

[17] ISO/IEC 7812-1:2006, *Identification cards — Identification of issuers — Part 1: Numbering system*

[18] ISO/IEC 8824-1:2008, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

[19] ISO/IEC 8825-2:2008, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) — Part 2*

[20] ISO/IEC/TR 10000-1:1998, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*

[21] ISO/IEC/TR 10000-2:1998, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 2: Principles and Taxonomy for OSI Profiles*

[22] ISO/IEC/TR 10000-3:1998, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 3: Principles and Taxonomy for Open System Environment Profiles*

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

[24] *Directive (2004/52/EC) of the European Parliament and of the Council of 29 April 2004 on the interoperability of electronic road toll systems in the Community*, OJ L 166, 30.4.2004, p. 124–143

[25] *2009/750/EC: Commission Decision of 6 October 2009 on the definition of the European Electronic Toll Service and its technical elements* (notified under document C(2009) 7547), OJ L 268, 13.10.2009, p.11-29

[26] *Guide for the application of the directive on the interoperability of electronic road toll systems,* ISBN 978-92-18637-0 (EC - DG for mobility and transport, ISBN 978-92-79-18637-0, 2011-06-16)

[27] *Recommendations on microwave DSRC technologies at 5.8 GHz to be used for the European electronic toll service*. Expert Group 1: Microwave technologies, 2005-03-14.

[28] *Recommendations on parameters to be stored in on-board equipment designed for use with the European Electronic Toll Service*, Expert Group 2: Vehicle Classification, v2, 2005-01-03.

[29] *Definition of the EFC Application for the EETS Based on Microwave Technologies*. Expert Group 11: EFC-DSRC Application, v6, 2006-02-06.

[30] *CARDME-4 — The CARDME concept*. Final. 2002-06-01. (ITS-1999-29053, deliverable 4.1)

[31] *CESARE-2 — Detailed CESARE Technical Specification*, D.032.1, 2002-02-27.

[32] *PISTA — Transaction Model*, D3.4 v6, 2002-11-11.

[33] *CESARE-3 project — Revised Cesare Model*, D1.2, Final.doc, 2006-10-09.

[34] *CESARE-3 project — Detailed Service Definition*, D2.1, Final.doc, 2006-10-09.

[35] UN/ECE Regulation No. 43 — *Uniform provisions concerning the approval of safety glazing materials and their installation on vehicles*.

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™