BS EN 16312:2013

BSI Standards Publication

Intelligent transport systems — Automatic Vehicle and Equipment Registration (AVI/AEI) — Interoperable application profile for AVI/AEI and Electronic Register Identification using dedicated short range communication

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 16312:2013.

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

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 75589 7

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 28 February 2013.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16312

January 2013

ICS 35.240.60

English Version

Intelligent transport systems - Automatic Vehicle and Equipment Registration (AVI/AEI) - Interoperable application profile for AVI/AEI and Electronic Register Identification using dedicated short range communication

Systèmes de transport intelligents - Identification automatique des véhicules et des équipements (AVI/AEI) - Profil d'application d'interopérabilité pour AVI/AEI et identification d'enregistrement électronique en utilisant des systèmes de communication dédiés à courte portée

Intelligente Transportsysteme - Automatische Fahrzeug und Ausstattungsregistrierung (AVI/AEI) - Interoperables Anwendungsprofil für AVI/AEI und elektronische Registrierungsidentifikation unter Verwendung von dedizierter Nahbereichskommunikation

This European Standard was approved by CEN on 27 October 2012.

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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 16312:2013: E

Contents

Page

Foreword 4
Introduction 5
1 Scope 7
2 Normative references 9
3 Terms and definitions 10
4 Abbreviations 12
5 Conformance 13
5.1 ERT requirements 13
5.1.1 General 13
5.1.2 DSRC requirements 13
5.1.3 DSRC L7 and ERI functions 13
5.1.4 Data requirements 14
5.1.5 Security requirements 14
5.1.6 ERI session requirements 15
5.2 ERR requirements 15
5.2.1 General 15
5.2.2 DSRC requirements 15
5.2.3 DSRC L7 and ERI functions 16
5.2.4 Data requirements 16
5.2.5 Security requirements 16
5.2.6 ERI session requirements 17
Annex A (normative) **Data specification** 18
A.1 General 18
A.2 Data tables 18
Annex B (normative) **ICS proforma** 23
B.1 General 23
B.2 Guidance for completing the ICS proforma 23
B.2.1 Purposes and structure 23
B.2.2 Abbreviations and conventions 23
B.3 Instructions for completing the ICS proforma 25
B.4 ICS proforma for ERT 26
B.4.1 Identification implementation 26
B.4.2 Identification of the standard 26
B.4.3 Global statement of conformance 26
B.4.4 ICS proforma for ERT 27
B.4.5 Profile requirement list for ERT 28
B.5 ICS proforma for ERR 32
B.5.1 Identification implementation 32
B.5.2 Identification of the standard 32
B.5.3 Global statement of conformance 32
B.5.4 ICS proforma for ERR 33
B.5.5 Profile requirement list for ERR 34
Annex C (normative) **IAP taxonomy and numbering for AVI/AEI** 38
C.1 General 38
C.2 Contents of an Interoperable Application Profile (IAP) 38
C.3 IAP referencing and numbering 39
C.3.1 IAP numbering 39

C.3.2 Security levels numbering **39**
C.3.3 Numbering and referencing examples **39**

Annex D (informative) **Security computation examples** **40**
D.1 General **40**
D.2 Computation of Attribute Authenticator **40**
D.3 Computation of Access Credentials **41**
D.4 Key derivation **42**
D.4.1 Authenticator Key **42**
D.4.2 Access Key **42**

Annex E (informative) **Security considerations** **43**
E.1 General **43**
E.2 Specific security recommendations **43**

Annex F (informative) **Using this European Standard for other DSRC-based transactions** **45**
F.1 General **45**
F.2 Specific purposes for data attributes and the transactions **45**
F.2.1 Access control applications **45**
F.2.2 Private freight management applications **45**
F.2.3 Simple traffic management applications **45**
F.2.4 Dangerous good tracking application **45**

Bibliography **46**

Foreword

This document (EN 16312:2013) has been prepared by Technical Committee CEN/TC 278 “Road transport and traffic telematics”, the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by July 2013, and conflicting national standards shall be withdrawn at the latest by July 2013.

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 draft 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 AVI/AEI DSRC-based systems. 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 organisations 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 automatic vehicle identification and automatic equipment identification using dedicated short-range communication (DSRC)-based systems (e.g. EN ISO 17264:2009, a “toolbox” for defining automatic vehicle identification and automatic equipment identification (AVI/AEI)-application transactions). However, these standards are necessary but not sufficient to ensure technical interoperability. This European Standard provides for a coherent set of requirements of the AVI/AEI-application intended to serve as a common technical platform for AVI/AEI-interoperability.

This European Standard defines an Interoperable Application Profile for AVI/AEI and electronic registration identification (ERI) using CEN DSRC-. The main objective is to support technical interoperability between ERI systems within the scope of the standard (as defined in Clause 1 below). This includes equipment compatibility between equipment suppliers and technical compatibility between different AVI/AEI systems compliant with this standard. This Standard is based on AVI/AEI standards such as ISO 14816, ISO 17264 and ISO 24534. Therefore, this Interoperable Application Profile enables other AVI/AEI application implementations to use the elements of this Standard as a basis for technical interoperability.

In order to enable multipurpose equipment where AVI/AEI applications share resources with other applications such as EFC, this standard is patterned on EN 15509:2007, which is the interoperability application profile for EFC over CEN DSRC. This ensures that the AVI/AEI application implementations feature equivalent services as EFC.

This European Standard only defines a basic level of technical interoperability for ERI equipment, i.e. Electronic Registration Tag (ERT) and ERI Reader/Writer (ERR) 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.

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

— defines the necessary and sufficient -DSRC requirements to support technical interoperability;

— enables multi-application equipment;

— fulfils the necessary additional DSRC-requirements;

— provides a choice of data elements including vehicle data;

— gives an extended definition of the use of some data elements, including semantics and coding;

— lays down clear choices for security implementation;

— facilitates a complementing test specification (with clear relations between the conformance requirements; and evaluation tests);

— provides 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 AVI/AEI, where a set of toolbox base standards allows for different choices that are not interoperable.

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

— an ISP shall make references only to base standards or other ISPs;

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

— the ISP shall not copy content of the base standards (in order to void consistency problems with the base standards);

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

— the profile may contain conformance requirements that are more specific and limited in scope than those of the base standards;

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

On this background, this Standard uses the structure and approach of existing IAP definitions, such as EN 15509:2007, made by other ITS application working groups.

The Interoperable Application Profile is defined in terms of conformance requirements as given in Clause 5. To facilitate easy referencing, testing and look-up, these requirements are divided into two parts; Electronic Registration Tag (ERT) requirements (5.1) and ERI Reader/Writer (ERR) requirements (5.2).

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

This European Standard is complemented by a set of standards defining Conformity Evaluation of the Conformance Requirements for Layer 1, Layer 2 and Layer 7 of the CEN DSRC Stack and elements of the application definition in this European Standard, patterned on EN 15509:2007.

1 Scope

The scope for this European Standard is limited to:

— physical systems: ERT, ERR and the DSRC interface between them (all functions and information flows related to these parts);

— DSRC-link requirements;

— ERI session over the DSRC interface;

— data elements to be used by ERT and ERR used in ERI session;

— security mechanisms for ERT and ERR used in ERI session.

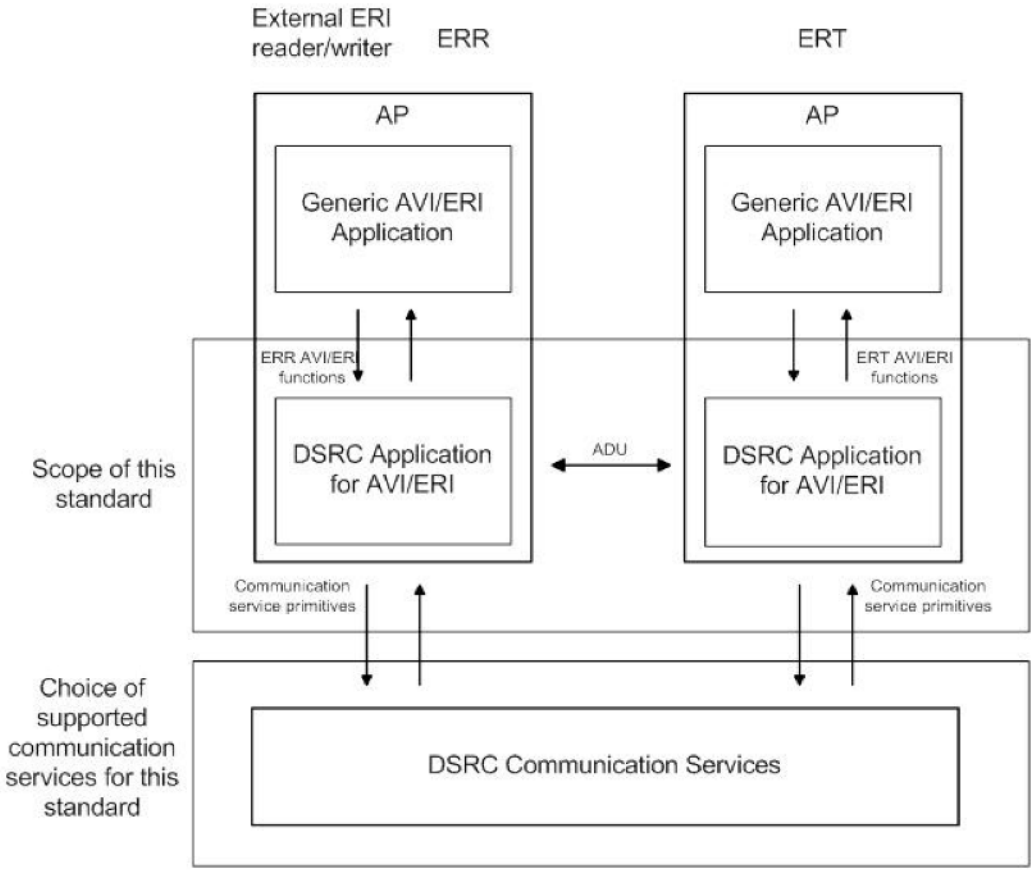

Figure 1 — Scope for this European Standard

It is outside the scope of this European Standard to define:

— contractual and procedural interoperability requirements;

— provisions for electronic payments such as EFC;

— conformance procedures and test specification;

— setting-up of operating organisations (e.g. application service provider, issuing, trusted third party etc.);

— legal issues;

— use of other communication technologies (e.g. RFID such as ISO 18000 series); and

— other interfaces or functions in ERI-systems than those specified above (i.e. information flows and data exchange between ERI Application providers or personalisation, initialisation and customisation of the OBU).

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

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

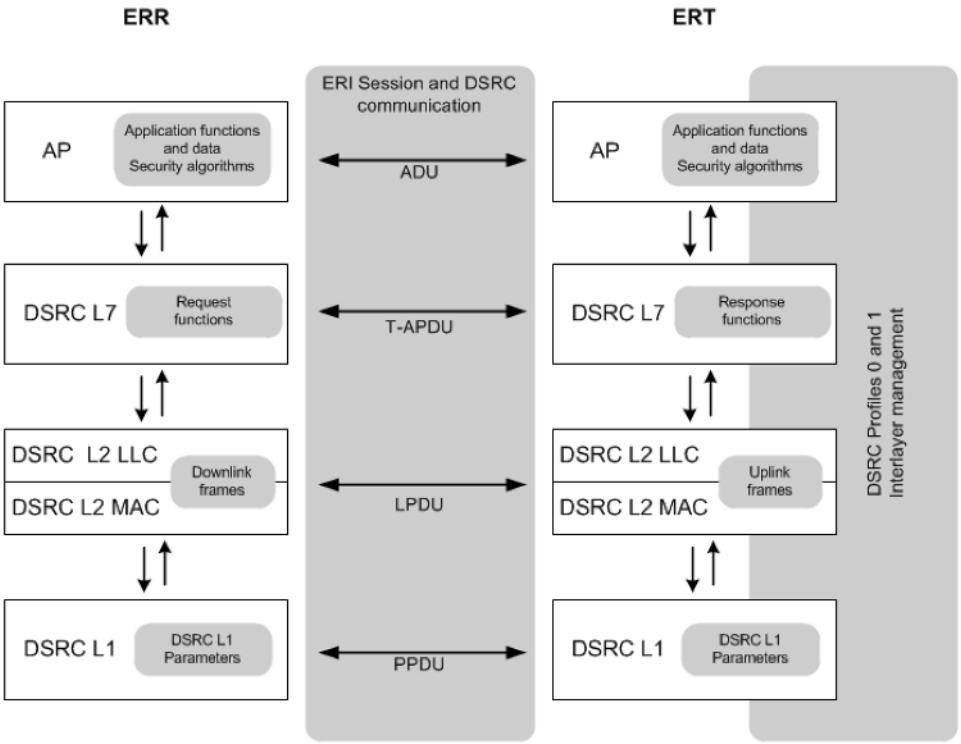

Figure 2 — Relations between this European Standard and DSRC-stack elements

NOTE For interlayer management, see EN 15509:2007, Annex G.

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

— EN ISO 14906:2011 and ISO 17264:2009 on ERI 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);

— EN 15509:2007: Interoperable Application Profile for EFC using CEN DSRC;

— ISO 24534 on ERI application.

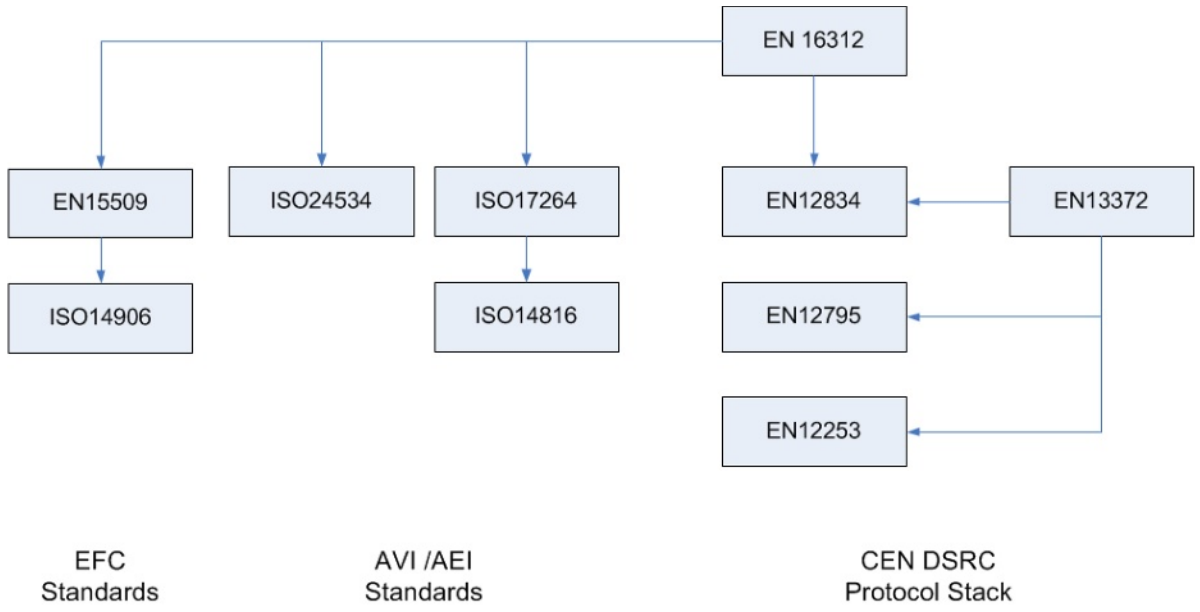

Figure 3 — Relation and references between base standards and EN 16312 (this European Standard)

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

EN 13372, *Road Transport and Traffic Telematics (RTTT) — Dedicated short-range communication — Profiles for RTTT applications*

EN 15509:2007*, Road transport and traffic telematics — Electronic fee collection — Interoperability application profile for DSRC*

EN ISO 14816, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure (ISO 14816)*

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

EN ISO 17264:2009, *Intelligent transport systems - Automatic vehicle and equipment identification — Interfaces (ISO 17264:2009)*

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

3 Terms and definitions

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

3.1
access credentials
data that is transferred to Electronic Registration Tag (ERT), in order to establish the claimed identity of a ERI Reader/Writer (ERR) application process entity

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.

[SOURCE: EN ISO 14906:2011, definition 3.1]

3.2
action
function that an application process resident at the *ERI Reader/Writer* can invoke in order to make the *on-board equipment* execute a specific operation during the *transaction*

[SOURCE: adapted from EN ISO 14906:2011, definition 3.2]

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

[SOURCE: EN ISO 14906:2011, definition 3.3]

3.4
authenticator
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and/or the integrity of the data unit and protect against forgery

[SOURCE: EN ISO 14906:2011, definition 3.4]

3.5
AVI/AEI attribute
an attribute specifically defined for the AVI/AEI application

[SOURCE: adapted from ISO 17264:2009, definition 4.3]

3.6
base standard
an approved international standard or ITU-T Recommendation

[SOURCE: ISO/IEC TR 10000:1998]

3.7
CEN DSRC profile
a set of parameters constituting a certain international standardised profile of the DSRC protocol stack (L1, L2 and L7)

[SOURCE: EN 13374]

3.8
cryptography
discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use

[SOURCE: EN ISO 14906:2011, definition 3.8]

3.9
data group
collection of closely related ERI data attributes which together describe a distinct part of an ERI transaction

[SOURCE: adapted from EN ISO 14906:2011:2011, definition 3.9]

3.10
data integrity
property that data has not been altered or destroyed in an unauthorised manner

[SOURCE: EN ISO 14906:2011, definition 3.10]

3.11
Electronic Registration Reader / Writer
ERR
device used to read/write data from or to an 'Electronic Registration Tag'

[SOURCE: ISO 24534-1:2010, definition 2.7]

3.12
ERI Operator
entity responsible for facilitating the ERR for a defined purpose

3.13
Electronic Registration Tag
ERT
onboard ERI device that contains the ERI data, including relevant secuirty promisions and one or more interfaces to access that data

[SOURCE: ISO 24534-1:2010, definition 2.8]

3.14
element
in the context of DSRC, a directory containing application information in form of *attributes*

[SOURCE: adapted from EN ISO 14906:2011, definition 3.11]

3.15
international standardised profile
an internationally agreed-to, harmonised document which describes one or more profiles

[SOURCE: ISO/IEC TR 10000:1998]

3.16
interoperability
the ability of two or more IT systems to exchange information and to make mutual use of the information that has been exchanged

[SOURCE: ISO/IEC TR 10000:1998]

3.17
ERI application provider
entity responsible for issuing the ERI application including personalisation of mandatory AVI/AEI attributes in the ERT

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

[SOURCE: ISO/IEC TR 10000:1998]

3.19
ERI session
an instance of a 'Vehicle Identification' using a harmonised air interface protocol known as 'CEN DSRC profile', using a distinct set of 'AVI/AEI attributes', retrieved by 'service primitives (communication)' and 'security mechanisms' defined in Annex B of this Standard

3.20
session counter
data value in the on-board unit that is incremented by the ERI Reader/Writer at each ERI session

3.21
user
vehicle/equipment or person carrying the OBE though the point of identification with the objective of unambiguous identification of the OBE being carried

[SOURCE: EN ISO 14814:2006, definition 3.28]

3.22
vehicle identification
action or act of establishing the identity of a vehicle

[SOURCE: EN ISO 24534-1:2010, definition 2.15]

4 Abbreviations

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

AcK	Access Key
AC_CR	Access Credentials [EN ISO 14906:2011]
ADU	Application Data Unit [EN ISO 14906:2011]
APDU	Application Protocol Data Unit [EN ISO 14906:2011]
AP	Application Process [EN ISO 14906:2011]
ASN.1	Abstract Syntax Notation One [ISO/IEC 8824-1:2008]
AuK	AuKEY
BST	Beacon Service Table [EN ISO 14906:2011]

DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DSRC	Dedicated Short-Range Communication [EN ISO 14906:2011]
e [key] (value)	encryption of the value using the key [EN 15509:2007]
ede [key] (value)	chained encryption, decryption and encryption of the value using the key [EN 15509:2007]
EID	Element Identifier [EN ISO 14906:2011]
ERI	Electronic Registration Identification [EN ISO 24534-1:2010]
IAP	Interoperable Application Profile [EN 15509:2007]
ICS	Implementation Conformance Statement [ISO/IEC TR 10000:1998]
ISP	International Standardised Profile [ISO/IEC TR 10000:1998]
IUT	Implementaton Under Test [CEN ISO/TS 14907-1:2010]
L1	Layer 1 of DSRC (Physical Layer) [EN ISO 14906:2011]
L2	Layer 2 of DSRC (Physical Layer) [EN ISO 14906:2011]
L7	Layer 7 of DSRC (Application Layer Core of DSRC) [EN ISO 14906:2011]
LLC	Logical Link Control [EN ISO 14906:2011]
LID	Logical Link Control identifier [EN ISO 14906:2011]
MAC	Media Access Control [EN ISO 14906:2011]
T-APDU	Transfer-Application Protocol Data Unit [EN ISO 14906:2011]
VST	Vehicle Service Table [EN ISO 14906:2011]

5 Conformance

5.1 ERT requirements

5.1.1 General

This clause contains the normative conformance requirements on the ERT in terms of OBU requirements from the base standards.

5.1.2 DSRC requirements

The ERT shall comply with EN 15509:2007, 5.1.2.

5.1.3 DSRC L7 and ERI functions

The ERT shall comply with EN 15509:2007, 5.1.3.

NOTE EN 15509:2007, 5.1.3 requires the implementation of the GET_STAMPED and SET_MMI commands. According to EN ISO 14906:2011, Container type 17 identifies GET_STAMPED.request and 69 identifies SET_MMI.request: those container types can be used even if reserved for future use in EN ISO 17264:2009. Container type 18 identifying GET_STAMPED.response is available for use since the AVI ContextMark defined in EN ISO 17264:2009 is not used as an attribute but only sent in the VST.

5.1.4 Data requirements

The addressing of the ERI data shall conform to the rules defined in EN ISO 14906:2011, 5.3.

The ERI attributes in Table 1 as defined in EN ISO 17264:2009 and EN ISO 14816 shall be implemented in the OBU.

Table 1 — Overview of the ERT ERI application data

ATTRIBUTES (EID>0)	AttrId	Length [a] (in	Read [b]	Write [b]	Remarks
APPLICATION CONTEXT					This attribute is defined in EN 12834.
ApplicationContextMark	N/A	16	Yes	No	Data that is sent from the ERT in the Initialisation phase (VST) that contains the identification of a specific DSRC application context. The elements carried by the ApplicationContextMark are: AVI-ContextMark CS1 AC_CR_Keyreference RndOBU
ERI Application Data					
CS2	2	6	Yes	No	RTTT Manufacturer Serial Number.
CS3	3	22	Yes	No	Validity Information.
CS4	4	17	Yes	No	License Plate Number, with fixed length
CS5	5	17	Yes	No	VIN Number with fixed length
OperatorData					
OperatorData	40	1+20	Yes	Yes	General ERI Data structure to be read and written.
Security					
SessionCounter	41	1+2	Yes	Yes	Usage see 5.2.5

[a] Including any length determinant as defined in ISO/IEC 8825-2 (packed encoding rules for ASN.1 is used in EN ISO 17264:2009 Container).
[b] The read and write columns denotes read and write operations in an ERI Vehicle Identification (not other possible situations)

5.1.5 Security requirements

5.1.5.1 General

This European Standard defines security features and mechanisms based on the general security framework defined in EN ISO 14906:2011, 7.1.4.

NOTE See Annex D for further details and explanation.

5.1.5.2 Security data requirements

The security related data elements listed in Table 2, shall be implemented in the ERT:

Table 2 — Overview of the ERT security related data

Name	Length (in octets)	Remarks
AuthenticationKey1	**8**	Private
AuthenticationKey2	**8**	Private
KeyRef	**1**	Reference to AuthenticationKey'x', 'x'=1..2 used for the computation of the Authenticators, e.g. Issuer and Operator Authenticators. KeyRef value for Authentication Key1 is 111. KeyRef value for Authentication Key2 is 112.
RndRSE	**5 = 1+4**	Random number from ERR used for the computation of Authenticator.
AccessKey	**8**	Private.
AC_CR	**5 = 1+4**	Access credentials calculated by the ERR and the ERT using RndOBU and the AccessKey
AC_CR-KeyReference	**2**	Reference to the key generation and the Diversifier for the computation of AccessKey
RndOBU	**5 = 1+4**	Random number (nonce) used together with AccessKey (referenced through AC_CR-KeyReference) to calculate the Access credentials (AC_CR).

The ERT shall be able to calculate an Authenticator (i.e. support the GET_STAMPED function operating on an attribute list considering that the response shall fit into one EN 12795 / DSRC Layer 2 frame) to validate data integrity and origin of the application data. These calculations shall be performed according to EN 15509.

NOTE The ERT also supports the SessionCounter functionality (see 5.2.5.3).

The ERT shall support calculation of Access Credentials for protection of user related data on the ERT. These calculations shall be performed according to EN 15509:2007, 5.2.5.2.

5.1.6 ERI session requirements

An ERT compliant with this European Standard shall be able to perform an ERI session as defined in ISO 17264:2009, Annex A.

The ERT shall use AVIContextMark with an aVIProfile equal to value 12 "isoEriProfileAttrPointer".

NOTE The ERT AVIContextMark – profileVersion is to be coded at the ERI application provider's discretion.

5.2 ERR requirements

5.2.1 General

This subclause contains the normative conformance requirements on the ERI Reader/Writer (ERR) in terms of requirements for RSE in EN 15509.

5.2.2 DSRC requirements

The ERR shall support any ERT complying with 5.1.2.

NOTE This implies that the ERR needs to comply with the DSRC-standards for Profiles, L1, L2 and L7 [EN 13372, EN 12253, EN 12795 and EN 12834].

5.2.3 DSRC L7 and ERI functions

The ERR shall comply with EN 15509:2007, 5.2.3.

NOTE Same note as in 5.1.3 applies.

5.2.4 Data requirements

The ERR shall support any ERT complying with 5.1.4.

There are no specific data requirements for the ERR, other than the possibility to read and write (including decoding and encoding, respectively) data as defined in 5.1.4.

5.2.5 Security requirements

5.2.5.1 General

A general framework and toolbox for security is given in EN ISO 14906:2011, 7.1.4. This European Standard defines security features and mechanisms based on this framework.

NOTE See Annex D for further details and explanation.

5.2.5.2 Mandatory Security requirements

The ERR shall be able to calculate Authenticators to validate data integrity and origin of the application data. These calculations shall be performed according to EN 15509.

The ERR shall perform key derivation of authentication keys according to the procedures defined in EN 15509. For key derivation the following diversifier value (VAL) shall be used:

Compute VAL concatenating CS2-ServiceNumber, CS1-CountryCode, CS1-IssuerIdentifier and 00H:

VAL = CS2-ServiceNumber || CS1-CountryCode || CS1-IssuerIdentifier || 00H

The ERR shall perform key derivation of access credential keys according to the procedures defined in EN 15509.

The ERR shall calculate Access Credentials (AC_CR) for access to protected ERI data on the ERT. These calculations shall be performed according to EN 15509.

5.2.5.3 Optional Security requirements

The ERR may update the SessionCounter according to the following procedures:

a) get the ERI attribute SessionCounter from the ERT ;

b) increase the SessionCounter by 1 Modulo 65.536;

c) insert the changed SessionCounter value into the ERI attribute;

d) send the updated SessionCounter value to the ERT (SET.Request).

NOTE The Session Counter may provide additional security to an operator, if the values are collected and checked in a back-office.

5.2.6 ERI session requirements

The ERR shall comply with EN ISO 17264:2009, Annex A.

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

Annex A
(normative)

Data specification

A.1 General

The specification and use of data elements is defined in EN ISO 17264:2009, EN ISO 14816 and in EN 12834. This annex includes ERI attribute and security related data requirements that restrict choices of or which are more specific and limited in scope than those of base standards.

A.2 Data tables

Tables with ERI attributes are included below. The tables describe the attributes in terms of name, definition, usage.

NOTE The length column in the tables below includes the length determinant as defined in ISO/IEC 8825-2 (packed encoding rules for ASN.1 is used in EN ISO 17264:2009). Consider general purpose container for read/write access.

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

Name / Data element	**Definition & remarks**	**Usage**	**Length In octets**

ApplicationContextMark	Encoded data that is sent from the ERT in the Initialisation phase (VST) that contains the identification of a specific DSRC application context. For ERI the first 3 octets always will contain the AVI-ContextMark. The formal ASN.1 definition of ApplicationContextMark is:
	
	ApplicationContextMark ::= SEQUENCE {
	aContextMark AVI-ContextMark,
	cs1 CS1, --ISO14816
	accr-key-ref AC-CR-KeyReference,
	rndOBU OCTET STRING(SIZE(4))
	}
	AC-CR-KeyReference ::= SEQUENCE {
	keyreference INTEGER (0..255),
	diversifier INTEGER (0..255)
	}
		The ApplicationContextMark is the concatenation of:
		AVI-ContextMark, CS1, AC_CR_Keyreference, RndOBU
		
		EXAMPLE ’00 12 01 01 02 03 11 22 33 44 01 02 12 34 56 78’H
		
		where:
		- AVI-ContextMark: ’00 12 01’H
		- CS1: ’01 02 03 11 22 33 44’H
		- AC_CR_Keyreference: ’01 02’H
		- RndOBU: ’12 34 56 78’H
			16

Table A.2 — ERI data (defined in EN ISO 14816)

Attribute Id / Name Data element	**Definition & remarks**	**Usage**	**Length** **In octets**
CS1	CS1 – AVI/AEI for use in RTTT application	Usage according to EN ISO 14816 but more specific and limited in scope: CountryCode and IssuerIdentifier shall indentify the ERI Application ProviderServiceNumber shall be an ERI Application Provider specific designation of rules or context applying to the ERI Data NOTE CS1 is not intended to uniquely identify an ERT	7
CS2	CS2 – RTTT Manufacturer Serial Number	Usage according to EN ISO 14816 but more specific and limited in scope: ServiceNumber shall be a BIT STRING **containing** a biunique identification number of the ERT. Therefore ServiceNumber shall be sub typed as BIT STRING (CONTAINING INTEGER (0..4294967295)). This identification number shall be available during the entire lifetime of the ERT. In case the ERT is used for multiple applications, the identification number should be harmonised across all applications.	**6**
CS3	CS3 – RTTT Validity Limitation	Usage according to EN ISO 14816 but more specific: Zero values for single data elements shall indicate that a data element is not defined.	**22**
CS4	CS4 - LicencePlate	Usage according to EN ISO 14816 but more specific and limited in scope: CS4 (WITH COMPONENTS {..., licPlateNumber (SIZE(14))}) Zero values shall indicate that the data attribute is not defined.	**17**
CS5	CS5- Vehicle Identification Number (VIN)	Usage according to EN ISO 14816 but more specific and limited in size scope: Zero values shall indicate that the data attribute is not defined.	**17**

Table A.3 — ERI Operator data

Attribute Id / Name Data element	**Definition & remarks**	**Usage**	**Length** **In octets**
OperatorData	ERI Operator specific data	ERI Operator specific application data which can be written and read-out by the ERR depending on the operator's needs	21 = 1+20

Table A.4 — Security data

Attribute Id / Name Data element	**Definition & remarks**	**Usage**	**Length** **In octets**
SessionCounter	Session Counter	Session counter, updated by the ERR according to 5.2.5.3.	3 = 1+2

Table A.5 — Authentication keys, access keys and security related data

Data element	**Definition & remarks**	**Usage**	**Length In octets**
AuthenticationKey1	Private	A key used to compute authenticators (see 5.2.5.2).	**8**
AuthenticationKey2	Private	Idem	**8**
AccessKey	Private.	The access key is the key used to compute AC_CR (see 5.2.5.2).	**8**
AC_CR	Access credentials calculated by the ERR and the ERT using RndOBU and the Access Key.	INTEGER (0..4'294'967'295). AC_CR = DES. Compute AC_CR(k) according to the DES algorithm [DEA], see also Annex E.	**5 = 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. Issuer and Operator Authenticators. The Application provider/Issuer decides which keys are kept by him and which keys are shared with other entities.	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.	OCTET STRING (SIZE4))	**4**
RndRSE	Random number, from ERR used for the computation of Authenticator.	INTEGER(0..4'294'967'295)	**5 = 1+4**

Annex B
(normative)

ICS proforma

B.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). This annex 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 this annex, and shall preserve the numbering, naming and ordering of the proforma items.

The forms in this annex shall be completed by the supplier of the item under test (IUT, i.e. the ERT or ERR).

B.2 Guidance for completing the ICS proforma

B.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 standardised 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.

B.2.2 Abbreviations and conventions

B.2.2.1 General

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

B.2.2.2 Item column

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

B.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?".

B.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.

B.2.2.5 Reference column

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

B.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.

B.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)

B.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.

B.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 .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.

B.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.

B.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 B.2.2.

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

B.4 ICS proforma for ERT

B.4.1 Identification implementation

B.4.1.1 Identification of ERT supplier

Table B.1 — Identification of ERT supplier form

Company	
Postal address	
Telephone	
Contact person	
E-mail address	

B.4.1.2 Identification of ERT

Table B.2 — Identification of ERT form

Brand	
Type, Version	
ManufacturerID	
EquipmentClass	
Serial numbers of supplied units	

B.4.2 Identification of the standard

This ICS proforma applies to the following standard:

EN 16312:2012

This ICS proforma applies only for ERTs.

B.4.3 Global statement of conformance

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

NOTE 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.

B.4.4 ICS proforma for ERT

Table B.3 — DSRC requirements

Item		Reference	Status	Support
1	Profile P0/P1 set L1-B	EN 15509:2007 5.1.2	o.1	
2	Profile P0/P1 set L1-A	EN 15509:2007 5.1.2	o.1	
3	Conversion gain limit	EN 15509:2007 5.1.2	c.1	
4	Cut-off power level minimum	EN 15509:2007 5.1.2	c.1	
5	Concatenation with chaining	EN 15509:2007 5.1.2	m	
6	Concatenation without chaining	EN 15509:2007 5.1.2	m	
7	Fragmentation header of 1 octet	EN 15509:2007 5.1.2	m	
8	Fill bits	EN 15509:2007 5.1.2	m	

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

c.1: IF B.3/2 – “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 B.4 — DSRC L7 and ERI functions

Item		Reference	Status	Support
1	INITIALISATION	EN 15509:2007 5.1.3	m	
2	ACTION – GetStamped	EN 15509:2007 5.1.3	m	
3	GET	EN 15509:2007 5.1.3	m	
4	SET	EN 15509:2007 5.1.3	m	
5	ACTION – SetMMI	EN 15509:2007 5.1.3	m	
6	ACTION – Echo	EN 15509:2007 5.1.3	m	
7	EVENT-REPORT – Release	EN 15509:2007 5.1.3	m	
8	AC_CR support	EN 15509:2007 5.1.3	m	

Table B.5 — Data requirements

Item		Reference	Status	Support read protection	Support write protection	Support length and coding
1	Addressing of ERI system and application data	5.1.4	M			
2	ApplicationContextMark	5.1.4	M			
3	AVI Context Mark	5.1.4	M			
4	CS1	5.1.4	M			
5	CS2	5.1.4	M			
6	CS3	5.1.4	M			
7	CS4	5.1.4	M			
8	CS5	5.1.4	M			
9	Operatordata	5.1.4	M			
10	SessionCounter	5.1.4	M			

Table B.6 — Security requirements

Item		Reference	Status	Support read protection	Support write protection	Support length and coding
1	AuthenticationKey1	5.1.5.2	m			
2	AuthenticationKey2	5.1.5.2	m			
3	KeyRef	5.1.5.2	m			
4	RndRSE	5.1.5.2	m			
5	AccessKey	5.1.5.2	m			
6	AC_CR	5.1.5.2	m			
7	AC_CR-KeyReference	5.1.5.2	m			
8	RndOBU	5.1.5.2	m			

Table B.7 — Security requirements

Item		Reference	Status	Support
1	Authenticator (calculation on an attribute list)	5.1.5	m	
2	SessionCounter	5.2.5.3	m	
3	AccessCredentials calculation	5.1.5.3	m	

Table B.8 — Transaction requirements

Item		Reference	Status	Support
1	ERI profile	5.1.6	m	

B.4.5 Profile requirement list for ERT

B.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 ERT specific requirements of this European Standard (EN 16312:2012) 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 A of ETSI TS 102 486-1-1 (data link layer) and ETSI TS 102 486-2-1 (application layer), updated with the requirements from this annex.

B.4.5.2 Profile Requirement List (profile RL)

The profile Requirement List (profile RL) for the application layer as defined in this annex is based on Annex A of ETSI TS 102 486-1-1 (data link layer) and ETSI TS 102 486-2-1 (application layer). For every capability listed in Annex A, the profile requirements are expressed by restriction upon allowed support answers in ETSI TS 102 486-1-1, Annex A. The profile RL is produced by copying selected tables from ETSI TS 102 486-1-1, Annex A, 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 ETSI TS 102 486-1-1, Annex A.

B.4.5.3 Reference column:

The reference column gives reference to ETSI TS 102 486-1-1 (data link layer) and ETSI TS 102 486-2-1 (application layer), except where explicitly stated otherwise.

B.4.5.4 Data link layer

Table B.9 — LLC Service Modes

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

Table B.10 — ACn command functionality

Item	Parameter	Reference	Status
3	Exchanging Data	8.4.3.2	m

Table B.11 — 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 B.12 — ACn protocol procedures

Item	Procedure	Reference	Status
1	Late response procedure I	7.2.2	m

B.4.5.5 Application layer

Table B.13 — 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 B.14 — 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 B.15 — Received Get-Request Parameters

Item	Parameter	Reference	Status
3	accessCredentials	A	M
4	Iid	A	X
5	attrIdList	A	M

Table B.16 — Transmitted Get-Response Parameters

Item	Parameter	Reference	Status
3	Iid	A	x
4	Attributelist	A	m
5	Ret	A	m

Table B.17 — Received Set-Request Parameters

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

Table B.18 — Transmitted Set-Response Parameters

Item	Parameter	Reference	Status
3	Iid	A	x
4	Ret	A	m

Table B.19— Received Action-Request Parameters

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

Table B.20 — Transmitted Action-Response Parameters

Item	Parameter	Reference	Status
3	lid	A	x
4	responseParameter	A	m
5	Ret	A	m

Table B.21— Received Event-Report-Request Parameters

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

Table B.22— 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 B.23 — 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

B.5 ICS proforma for ERR

B.5.1 Identification implementation

B.5.1.1 Identification of ERR supplier

Table B.24— Identification of ERR supplier form

Company	
Postal address	
Telephone	
Contact person	
E-mail address	

B.5.1.2 Identification of ERR

Table B.25 — Identification of ERR form

Brand	
Type, Version	
ManufacturerID	
EquipmentClass	
Serial numbers of supplied units	

B.5.2 Identification of the standard

This ICS proforma applies to the following standard:

EN 16312:2012

This ICS proforma applies only for ERR s.

B.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 feature is implemented ……

NOTE 2 See 5.2.5 and Annex D for a comprehensive description of security options.

B.5.4 ICS proforma for ERR

Table B.26 — DSRC requirements

Item		Reference	Status	Support
1	Profile P0/P1 set L1-B	EN15509:2007 5.2.2	o.1	
2	Profile P0/P1 set L1-A	EN15509:2007 5.2.2	o.1	
3	Conversion gain limit	EN15509:2007 5.2.2	c.1	
4	Cut-off power level minimum	EN15509:2007 5.2.2	c.1	
5	Concatenation with chaining	EN15509:2007 5.2.2	m	
6	Concatenation without chaining	EN15509:2007 5.2.2	m	
7	Fragmentation header of 1 octet	EN15509:2007 5.2.2	m	
8	Fill bits	EN15509:2007 5.2.2	m	

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

c.1: IF B.26/2 – “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 B.27— L7 and ERI functions

Item		Reference	Status	Support
1	INITIALISATION	EN15509:2007 5.2.3	m	
2	ACTION – GetStamped	EN15509:2007 5.2.3	m	
3	GET	EN15509:2007 5.2.3	m	
4	SET	EN15509:2007 5.2.3	m	
5	ACTION – SetMMI	EN15509:2007 5.2.3	m	
6	ACTION – Echo	EN15509:2007 5.2.3	m	
7	EVENT-REPORT – Release	EN15509:2007 5.2.3	m	
8	AC_CR support	EN15509:2007 5.2.3	m	

Table B.28 — Data requirements

Item		Reference	Status	Support read protection	Support write protection	Support length and coding
1	AVI Context Mark	5.2.4	M			
2	CS1	5.2.4	M			
3	CS2	5.2.4	M			
4	CS3	5.2.4	M			
5	CS4	5.2.4	M			
6	CS5	5.2.4	M			
7	OperatorData	5.2.4	M			
8	SessionCounter	5.2.4	M			

Table B.29— Security requirements

Item		Reference	Status	Support read protection	Support write protection	Support length and coding
1	AuthenticationKey1	5.2.5.2	m			
2	AuthenticationKey2	5.2.5.2	m			
3	KeyRef	5.2.5.2	m			
4	RndRSE	5.2.5.2	m			
5	AccessKey	5.2.5.3	m			
6	AC_CR	5.2.5.3	m			
7	AC_CR-KeyReference	5.2.5.3	m			
8	RndOBU	5.2.5.3	m			

Table B.30 — Security requirements

Item		Reference	Status	Support
1	Authenticator calculation on an attribute list	5.2.5	m	
2	SessionCounter update	5.2.5.3	o	
3	AccessCredentials calculation	5.2.5	m	

Table B.31— ERI session requirements

Item		Reference	Status	Support
1	ERI session	5.2.6	m	

B.5.5 Profile requirement list for ERR

B.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 ERT specific requirements of this Standard 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 (data link layer) and ETSI TS 102 486-2-1 (application layer), updated with the requirements from this annex.

B.5.5.2 Profile Requirement List (profile RL)

The profile Requirement List (profile RL) for the application layer as defined in this annex is based on Annex B of ETSI TS 102 486-1-1 (data link layer) and ETSI TS 102 486-2-1 (application layer). For every capability listed in ETSI TS 102 486-1-1, Annex B, the profile requirements are expressed by restriction upon allowed support answers in ETSI TS 102 486-1-1, Annex B. The profile RL is produced by copying selected tables from ETSI TS 102 486-1-1, Annex B, 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 ETSI TS 102 486-1-1, Annex B.

B.5.5.3 Reference column

The reference column gives reference to ETSI TS 102 486-1-1 (data link layer) and ETSI TS 102 486-2-1 (application layer), except where explicitly stated otherwise.

B.5.5.4 Data link layer

Table B.32— Service Modes

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

Table B.33— ACn command functionality

Item	Parameter	Reference	Status
3	Exchanging Data	8.4.3.2	m

Table B.34 — 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 B.35— ACn protocol procedures

Item	Procedure	Reference	Status
1	Late response procedure I	7.2.2	m

B.5.5.5 Application layer

Table B.36 — 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 B.37 — 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 B.38— Transmitted Get-Request Parameters

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

Table B.39 — Received Get-Response Parameters

Item	Parameter	Reference	Status
3	Iid	A	x
4	Attributelist	A	m
5	Ret	A	m

Table B.40— Transmitted Set-Request Parameters

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

Table B.41— Received Set-Response Parameters

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

Table B.42 — Transmitted Action-Request Parameters

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

Table B.43 — Received Action-Response Parameters

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

Table B.44 — Transmitted Event-Report-Request Parameters

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

Table B.45 — 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 B.46— 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 C
(normative)

IAP taxonomy and numbering for AVI/AEI

C.1 General

The intentions of application profiling are outlined in this annex patterned on EN 15509:2007, Annex C, together with a basic taxonomy and numbering of IAPs. The annex 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.

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

Whereas this edition of the standard only defines one IAP, this sub clause outlines the principles of creating an IAP in case sub-sequent editions or other standards will do so. The purpose of an IAP is to ensure technical interoperability between different ERI-systems.

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

— EN ISO 14906:2011 - 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).

The IAP is defined by stating a set of conformance requirements (as done in Clause 5 above). This is done according to the ISP-principles as in ISO/IEC TR 10000-1 (summarised 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 base standards.

The conformance requirements include the following parts (divided into separate requirements for ERT and ERR):

— DSRC requirements;

— DSRC L7 and ERI functions;

— data requirements;

— security requirements;

— ERI profile requirements.

The conformance requirements shall not contain options except for security levels, which may be subject to staged implementation by Operators.

NOTE 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) will have to be implemented as a new IAP.

C.3 IAP referencing and numbering

C.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 IAP 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 ERT and for ERR. Hence, conformance to EN 16312:2012 shall be noted separately for the ERT and the ERR.

NOTE 2 The ISP-standards, TR 10000-1, -2 and -3, define an overall structure for IT-taxonomy of ISP-standards. This is deemed not applicable for this European Standard (EN 16312:2013), and is not used here.

C.3.2 Security levels numbering

This European Standard defines two security levels that may be implemented independently in the ERR (i.e. with or without support for SessionCounter). 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 (i.e. IAPnumber.SecurityLevel)

C.3.3 Numbering and referencing examples

EXAMPLE 1 An ERR conformant with EN XXXXX without SessionCounter is noted: "ERR conformant with XXXXX IAP 1.0 level 0"

EXAMPLE 2 An ERR conformant with EN XXXXX with SessionCounter is noted: "ERR conformant with XXXXX IAP 1.0 level 1"

Annex D
(informative)

Security computation examples

D.1 General

This annex illustrates the cryptographic mechanisms defined in Clause 5 by means of a few numerical examples. Numeric values in the examples below are in hexadecimal.

D.2 Computation of Attribute Authenticator

EXAMPLE
This example describes the calculation of an authenticator using an AttributeList containing the only attribute CS1. The authenticator is calculated using the following values:

CS1 = 'A4 00 01 00 00 00 01'

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

AuK = ’A2 4B 28 CA B6 AF C0 37’ (Derived from the MAuK according to example in **D.4.1**).

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

M = ‘AttributeList (CS1) || RndRSE (octet string) || Padding’ = ‘01 01 19 A4 00 01 00 00 00 01 04 1A 61 A9 85 00’

and

$D_1 = I_1$ = Sub(M, 0, 8) = ‘01 01 19 A4 00 01 00 00’

D_2 = Sub(M, 8, 8) = ‘00 01 04 1A 61 A9 85 00’

With ICV : '00 00 00 00 00 00 00 00': the Input I_1 = ICV xor $I_1 = D_1$ = ‘01 01 19 A4 00 01 00 00’

O_1 = e[AuK](I_1) = ‘72 67 DC CE DC AC 89 ED’

and

$I_2 = O_1$ xor D_2 = ‘72 67 DC CE DC AC 89 ED’ xor ‘00 01 04 1A 61 A9 85 00’ = ‘72 66 D8 D4 BD 05 0C ED’

Calculation of O_2 gives:

O_2 = e[AuK](I_2) = ‘C1 14 C4 18 6A 85 B3 0A’’

The leftmost 32 bits represent the Authenticator:

Auth = Sub(O_4, 0, 4) = ‘C1 14 C4 18’

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' (1^{th} of March 2003, 21:12:12)

we find:

Auth = ‘ED 70 99 75’

D.3 Computation of Access Credentials

EXAMPLE
For the computation of the Access Credentials the AccessKey = '9B 48 AA E0 7A 7B C0 08' derived from the Master Access Key according to D.4.2.

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’

D.4 Key derivation

D.4.1 Authenticator Key

EXAMPLE
This example shows how the Authentication Key is calculated using the following application data and Master Authentication Key (MAuK) value:

The input data (VAL) follow from:

VAL = CS2-ServiceNumber || CS1-CountryCode || CS1-IssuerIdentifier || 00H = '00 00 00 01 A4 00 01 00';

VAL structure:

— 00 00 00 01 (CS2-ServiceNumber =1)

— A4 00 01 (Country Code=SE || CS1- IssuerIdentifier = 1)

— 00H (padding)

Master authentication key (MAuK)

— '3b 38 98 37 15 20 f7 5e 92 2f b5 10 c7 1f 43 6e‘ ;

This gives the following value for the Authentication Key:

AuK = ede[MAuK](VAL) = ‘A2 4B 28 CA B6 AF C0 37’

With a different value for the CS2-ServiceNumber the derived key will be different. As an example, with a VAL = ‘00 00 00 02 A4 00 01 00', and the same Master Authentication Key as above, the calculation leads to the following authentication key:

AuK = ‘01 21 0C 8F A8 CA A0 0C’

D.4.2 Access Key

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

Using the following application data values and Master Access Key:

— AC_CR-KeyReference: ’12 34’

— Master Access Key - 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:

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

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

Annex E
(informative)

Security considerations

E.1 General

This annex gives a background and motivation to the security features defined in this European Standard.

The application of ERI involves:

— the user and his ERT;

— the ERI Operator;

The following security themes are here analysed with regard to:

— Data Integrity, with regard to the data stored in the ERT;

— data origin authentication, with regard to sensitive data in all transferred charging data;

— data access protection, with regard to the data stored in the ERT.

The data integrity and data access protection with regards to the data exchange networks and all processing of data are not part of this European Standard.

E.2 Specific security recommendations

In particular, the following security recommendations may apply to the contractual architecture and to its members:

a) the ERI Operators:

— ERT (data) origin authentication: The ERI Operators should be protected against counterfeit transactions by the user/customer (by means of a counterfeit ERT). It should be assured that the ERT that performed the transaction (and the data it contains) is a genuine ERT, issued by a through Contract Issuer;

b) the user and the ERT:

— the user should be protected against any identification by unauthentic ERI Operators. Only authenticated ERI Operators have be able to access the ERI Data and use it for their applications

— the user should be protected against infringement of his privacy. Sensible data in his ERT should be protected;

— non-authorised using of the ERT (by other ERI operators) should be avoided. Other operators should not be allowed to read data from the ERT (e.g. in order to estimate traffic flow);

c) all

— the ERT data's (vehicle data) integrity should be protected. Sensible data contained in the ERT should be protected against modification.

— cloning of an ERT. Producing an exact copy of a user's ERT, if possible from a technical and security point of view would mean benefiting of ERI services.

The measures to fulfil the above security recommendations are supported by this European Standard. They are summarised and briefly explained in Table E.1.

Table E.1 — Security measures related to security recommendations

Recommendation	Measure
a) ERI Operator	
Protect the ERI Operator against counterfeit ERI Session Data by its users	ERT Authentication to the ERR (Stamping) Transaction Counter
b) User and its ERT	
Protect the user/customer against infringement of his privacy	Data access protection
Avoid not-authorised using of the ERT (by other ERI operators)	Data access protection
c) All	
Protect ERT data integrity	Data access protection / Data authentication

Annex F
(informative)

Using this European Standard for other DSRC-based transactions

F.1 General

This European Standard defines an Application Profile for interoperable ERI transactions but does not define for which purposes those transactions can be used. This annex gives information on how the data attributes and the transactions can be used for specific purposes.

F.2 Specific purposes for data attributes and the transactions

F.2.1 Access control applications

Access control can be used for areas with user-restricted access such authorised parking areas (without payment), limited access zones and areas subject to specific access conditions (like registration), or vehicle-restricted areas such as areas which special access conditions on vehicles.

CS1 (sent in the VST) can be used as an identifier of the ERI application class, i.e. if the ERT is meant for the application supported by the ERI Operator. Definition of the ERT application class is at the discretion of the ERI Application Provider.

CS2 can be used to identify blacklisted ERTs

CS3 can be used to limit the validity of the ERT

CS4 can be used to identify the vehicle.

OperatorData can be used by the operator to carry system specific entry information into the area (entry ticket)

F.2.2 Private freight management applications

The attribute OperatorData can be used as an identification of the cargo containing e.g. Date&Time of cargo loading, Source Facility ID where the cargo was loaded, Destination Facility ID where cargo is shipped to; Cargo content code; dangerous goods code; authenticator.

F.2.3 Simple traffic management applications

CS1 can be used to identify specific type of authorisation, e.g. allowed to open barrier, request for green traffic sign.

F.2.4 Dangerous good tracking application

Operator data can be used by the operator to carry information about dangerous goods.

Bibliography

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

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

[3] CEN ISO/TS 14907-1:2010, *Road transport and traffic telematics — Electronic fee collection — Test procedures for user and fixed equipment — Part 1: Description of test procedures (ISO/TS 14907-1:2005)*

[4] ISO/IEC 8825-2:1998, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*

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

[6] ISO/IEC TR 10000:1998 (all parts), *Information Technology — Framework and taxonomy of International Standardized Profiles*

[7] ETSI TS 102 486-1-2, *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 2: Test Suite Structure and Test Purposes (TSS&TP)*

[8] ETSI TS 102 486-2-2, *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 2: DSRC application layer; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)*

[9] ETSI TS 102 486-1-3, *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 3: Abstract Test Suite (ATS) and partial PIXIT proforma*

[10] ETSI TS 102 486-2-3, *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 2: DSRC application layer; Sub-Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma*

[11] ANSI X9.52:1998, *Triple Data Encryption Algorithm, Modes of Operation*

[12] EN15876, *Road Transport and Traffic Telematics (RTTT); Electronic Fee Collection (EFC); Conformity Evaluation of On Board and Roadside Equipment to EN15509:2007.*

[13] EN ISO 24534-1:2010, Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles — Part 1: Architecture (ISO 24534-1:2010)

[14] EN ISO 14814:2006, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Reference architecture and terminology (ISO 14814:2006)*

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.™