INTERNATIONAL STANDARD

ISO 12813

First edition
2015-12-01

Electronic fee collection — Compliance check communication for autonomous systems

Perception du télépéage — Communication de contrôle de conformité pour systèmes autonomes

Reference number
ISO 12813:2015(E)

International Organization for Standardization

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 204, *Intelligent transport systems*.

This first edition replaces the Technical Specification ISO/TS 12813:2009, which has been technically revised. This first edition incorporates the following main modifications compared to the Technical Specification:

- conversion from a Technical Specification to an International Standard;
- new attributes added (TrailerCharacteristics, AttributeUpdateInterval, VehicleCurrentMaxTrainWeight, VehicleWeightHistory, ExtendedOBEStatusHistory, ExtendedVehicleAxlesHistory and LocalVehicleClassId);
- amendment of terms, in order to reflect harmonization of terms across electronic fee collection (EFC) standards;
- amendments to reflect changes to the underlying base standards, in particular ISO 14906 and EN 15509;
- addition of a new informative annex (i.e. Annex H) on how to use this International Standard for the European electronic toll service;
- editorial and formal corrections as well as changes to improve readability.

Introduction

On-board equipment (OBE) that uses satellite-based positioning technology to collect data required for charging for the use of roads operates in an autonomous way (i.e. without relying on dedicated road side infrastructure). The OBE will record the amount of road usage in all toll charging systems it passes through.

This International Standard defines requirements for dedicated short-range communication (DSRC) between OBE and an interrogator for the purpose of checking compliance of road use with a local toll regime. It assumes an electronic fee collection (EFC) services architecture according to ISO 17573. See Figure 1.

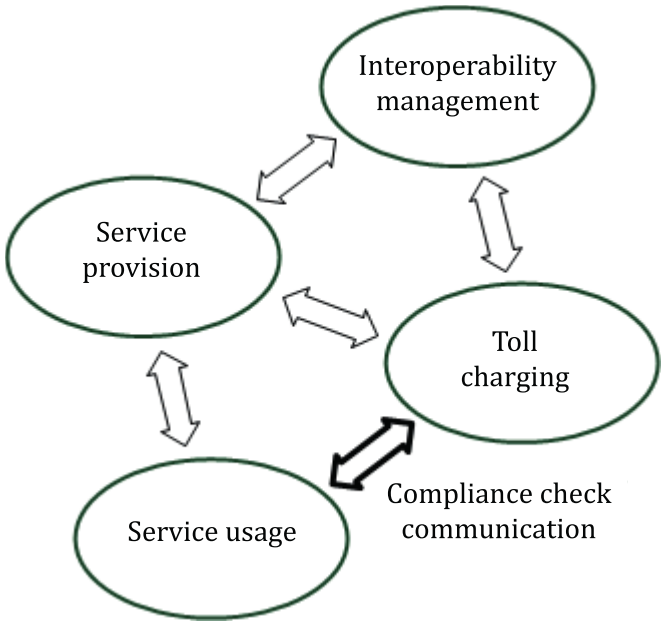

Figure 1 — Compliance check communication in EFC architecture as per ISO 17573

Toll chargers have the need to check whether the road is used in compliance with the rules in the local toll regime. One way of checking compliance is to observe a passing vehicle and to interrogate the OBE. This interrogation happens under control of an entity responsible for toll charging (see Figure 1), accomplished via short-range communication between an interrogator at road-side or in another vehicle (operated by a competent enforcement agency) and the OBE. In an interoperable environment, it is essential that this interrogation communication be standardized such that every operator of compliance checking equipment can check all passing OBE. For that purpose, this International Standard defines attributes required on all OBE for reading by an interrogator.

This International Standard has been prepared considering the prerequisites listed below in a) to e).

a) Collected evidence must be court proof. Data must be indisputable and secured such that the operator of the compliance checking interrogator can prove the integrity and authenticity of the data in case of dispute.

b) The data required for compliance checking must be read only, since the operator of the interrogator must not interfere with the working of the OBE.

c) All attributes, standardised at the time of personalisation of the OBE, should be present in the OBE such that an operator of an interrogator essentially can read the same data from all OBE independent of type and make. In case an attribute does not make sense in a certain OBE implementation, a value assignment for “not applicable” or “not defined” is provided in each case. An OBE compliant to the first edition will not answer with such a response for new attributes introduced in the current edition of this International Standard.

d) The attributes, derived from the individual toll regime, must be of general importance for all toll system types (motorway tolling, area tolling, tolls for ferries, bridges, tunnels, cordon pricing, etc.).

e) The attributes must apply to all OBE architectures, and especially to both thin (edge-light) and fat (edge heavy) client architectures. The interrogator must be able to receive essentially the same information irrespective of OBE implementation decisions.

It is assumed that the prime objective of the operator of the compliance checking interrogator is to check whether the user has fulfilled his obligations, especially:

— whether the OBE is mounted in the correct vehicle;

— whether the classification data transmitted by the OBE are correct; and

— whether the OBE is in working condition, both in a technical and a contractual sense.

Regarding the last point of the above list, on the operational status of OBE, the following model is assumed.

As long as the OBE signals to the user correct operational status ("green"), the service provider takes full responsibility for the correct working of the OBE and for the payment by the user. Hence, as long as the OBE signals "green" and the user fulfils his other obligations (such as entering correct classification data and not tampering with the OBE), the user can expect the OBE to serve as a valid payment means. As soon as the OBE signals an invalid operational status ("red") — either set by the central system of the service provider (e.g. because the user account is negative), by internal mechanisms of the OBE itself (e.g. because of a detected defect or an outdated data set) or a user manipulation with such result — the user knows that the OBE is no longer a valid payment means. The user then has to use alternative means of toll declaration or payment until the problem is remedied and the OBE is "green" again[1)].

Ultimately, the policy of when to signal "green" or "red" is defined by the service provider in accordance with the requirements defined by the toll charger(s).

In the case where the OBE status turns "red", the user has to take action, declare road usage subject to fees or pay by some alternative means as quickly as possible. Until he does, the user is in a potentially non-compliant situation. In order to allow a judgment to be made as to whether or not a user has taken the appropriate action within an acceptable period of time, information is provided by this International Standard not only on the "green/red" operational status but also on the length of time that the OBE has been in its current status.

Different toll contexts can overlap geographically. A user could be liable in several toll contexts at once, e.g. for a nation-wide distance-dependent road tax and a local city access pricing scheme — a fact of which the user might not in all cases be aware. This International Standard builds on the concept that regarding compliance, there is no notion of toll context (see especially 5.4). It is within the responsibility of the service provider to resolve issues with overlapping toll contexts and to distil all information into a binary "red/green" message to the user.

A secondary objective of the operator of the compliance checking interrogator might be to collect data on the performance of the OBE, e.g. in order to check for the correct technical functioning. Since different OBE can work according to quite different principles, the possibilities for doing this in a standardised way are quite limited. This International Standard contains some provisions for this task (e.g. the attributes CommunicationStatus, GnssStatus, DistanceRecordingStatus), but otherwise assumes that toll chargers monitor correct recording by comparing observed traffic (e.g. with cameras) with usage data received from service providers.

This International Standard has been prepared with the intention to be "minimalist" in the sense that it covers what is required by operational systems and systems planned in the foreseeable future.

---

1) Here, "red" and "green" are used in the abstract, symbolic sense, and do not imply any physical implementation. The design of the user interface of the OBE is implementation-dependent, and several methods for signalling "red" or "green" are conceivable.

A test suite for checking an OBE or RSE implementation for compliance with the first edition of this International Standard is defined in the corresponding edition of ISO/TS 13143-1 and ISO/TS 13143-2. This test suite is currently being updated to reflect the changes incorporated into this first edition of ISO 12813.

Electronic fee collection — Compliance check communication for autonomous systems

1 Scope

This International Standard defines requirements for short-range communication for the purposes of compliance checking in autonomous electronic fee-collecting systems. Compliance checking communication (CCC) takes place between a road vehicle's on-board equipment (OBE) and an outside interrogator (road-side mounted equipment, mobile device or hand-held unit), and serves to establish whether the data that are delivered by the OBE correctly reflect the road usage of the corresponding vehicle according to the rules of the pertinent toll regime.

The operator of the compliance checking interrogator is assumed to be part of the toll charging role as defined in ISO 17573. The CCC permits identification of the OBE, vehicle and contract, and verification of whether the driver has fulfilled his obligations and the checking status and performance of the OBE. The CCC reads, but does not write, OBE data.

This International Standard is applicable to OBE in an autonomous mode of operation; it is not applicable to compliance checking in dedicated short-range communication (DSRC)-based charging systems.

It defines data syntax and semantics, but does not define a communication sequence. All the attributes defined herein are required in any OBE claimed to be compliant with this International Standard, even if some values are set to "not defined" in cases where certain functionality is not present in an OBE. The interrogator is free to choose which attributes are read, as well as the sequence in which they are read. In order to achieve compatibility with existing systems, the communication makes use of the attributes defined in ISO 14906 wherever useful.

The CCC is suitable for a range of short-range communication media. Specific definitions are given for the CEN-DSRC as specified in EN 15509, as well as for the use of ISO CALM IR, the Italian DSRC as specified in ETSI ES 200 674-1 and ARIB DSRC as alternatives to the CEN-DSRC. The attributes and functions defined are for compliance checking by means of the DSRC communication services provided by DSRC layer 7, with the CCC attributes and functions made available to the CCC applications at the road-side equipment (RSE) and OBE. The attributes and functions are defined on the level of application data units (ADU).

The definition of the CCC includes:

— the application interface between OBE and RSE (as depicted in Figure 2),

— use of the generic DSRC application layer as specified in ISO 15628 and EN 12834,

— use of the CEN-DSRC stack as specified in EN 15509, or other equivalent DSRC stacks as described in Annexes C, D and E, and

— security services for mutual authentication of the communication partners and for signing of data (see Annex G).

CCC data type specifications are given in Annex A, protocol implementation conformance statement (PICS) proforma in Annex B. An example CCC transaction is presented in Annex F. The informative Annex H highlights how to use this International Standard for the European electronic toll service (as defined in Commission Decision 2009/750/EC).

Test specifications are not within the scope of this International Standard.

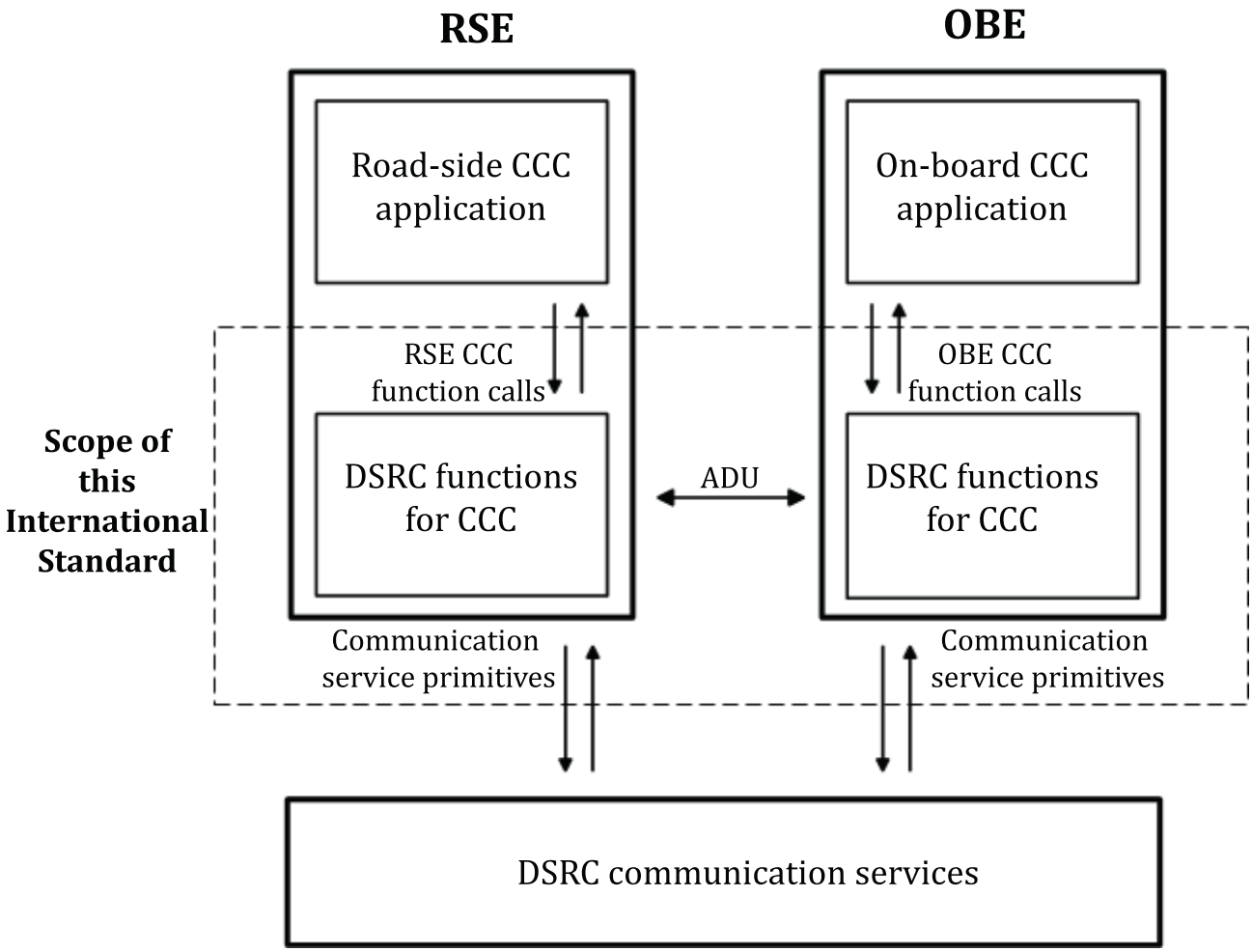

Figure 2 — CCC application interface

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.

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

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

ISO 14906:2011/Amd1:2005, *Electronic fee collection — Application interface definition for dedicated short-range communication*

ISO 15628:2013, *Intelligent transport systems — Dedicated short range communication (DSRC) — DSRC application layer*

EN 12834:2003, *Road transport and traffic telematics — Dedicated Short Range Communication (DSRC) — DSRC application layer*

EN 15509:2014, *Electronic fee collection — Interoperability application profile for DSRC*

NIMA Technical Report TR8350.2 version 3 — *Department of Defense World Geodetic System 1984, Its Definition and Relationships With Local Geodetic Systems*

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

[SOURCE: EN 15509:2014, 3.1]

3.2
attribute
addressable package of data consisting of a single data element or structured sequences of data elements

3.3
authentication
security mechanism allowing verification of the provided identity

[SOURCE: EN 301 175]

3.4
authenticator
data, possibly encrypted, that is used for authentication

[SOURCE: ISO/TS 19299:2015, 3.5]

3.5
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO/TS 19299:2015, 3.28]

3.6
fixed roadside equipment
roadside equipment located at a fixed position

3.7
mobile roadside equipment
equipment mounted on a mobile unit or handheld equipment to be used along the road

3.8
on-board equipment
OBE
all required equipment on-board a vehicle for performing required EFC functions and communication services

3.9
roadside equipment
RSE
equipment located along the road, either fixed or mobile

3.10
toll service provider
TSP
entity providing toll services in one or more toll domains

[SOURCE: ISO 17573:2010]

3.11
service primitive
elementary communication service provided by the application layer protocol to the application processes

[SOURCE: ISO 14906:2011, 3.18 modified]

3.12
toll context
logical view as defined by attributes and functions of the basic elements of a toll scheme consisting of a single basic tolling principle, a spatial distribution of the charge objects and a single behaviour of the related Front End

3.13
toll regime
set of rules, including enforcement rules, governing the collection of a toll in a toll domain

[SOURCE: ISO 17573:2010, 3.20]

3.14
transaction
whole of the exchange of information between two physically separated communication facilities

4 Abbreviated terms

For the purpose of this document, the following abbreviations apply.

AC_CR	access credentials
ADU	application data unit (ISO 14906)
ASN.1	abstract syntax notation one (ISO/IEC 8824-2)
BST	beacon service table (ISO 14906)
CCC	compliance check communication
DSRC	dedicated short-range communication (ISO 14906)
EID	element identifier (ISO 15628 and EN 12834)
EFC	electronic fee collection
GNSS/CN	global navigation satellite systems/cellular network
MAC	media access control (EN 12795) or message authentication code (ISO 14906)
OBE	on-board equipment (ISO 14906)
PICS	protocol implementation conformance statement
RSE	roadside equipment (ISO 14906)
TSP	toll service provider
VST	vehicle service table (ISO 14906)
WGS84	World Geodetic System 1984

5 Application interface architecture

5.1 General

This clause gives an insight into the CCC architecture. It identifies the services provided to CCC applications and the functions that implement these services. It also defines principles regarding attributes and the use of DSRC communication primitives. A detailed description of the functions is given in Clause 6, whilst the detailed list of the attributes is given in Clause 7.

The CCC application interface has been designed to make use of the CEN-DSRC communication stack, via the application layer specified in ISO 15628 and EN 12834. For other identified DSRC communication media, detailed mappings to corresponding services are given in annexes.

From a general addressing viewpoint, it should be noted that only one CCC context is used, as compliance checking attributes are independent of context.

5.2 Services provided

The CCC application interface offers the following services to CCC applications:

— retrieval of compliance significant attributes, in order for RSE to assess OBE compliance,

— mutual authentication of RSE and OBE by means of exchange of credentials, and

— a command to the OBE to signal to the user the result of the compliance check

NOTE 1 The policy of whether or not the result of the compliance check or the fact that a transaction has taken place is signalled to the user is decided by the entity operating the CCC interrogator and is outside the scope of this International Standard.

The above services are realized by means of protocol exchanges performed by means of communication services and transactions as described in Clause 8.

The services are provided by the following functions:

— the “initialise communication” function, which shall be used to establish the CCC communication link between RSE and OBE;

— the “data retrieval” function, which shall be used to retrieve CCC attributes;

— the “authenticated data retrieval” function, which shall be used to retrieve data with an authenticator from the OBE;

— the “driver notification” function, which shall be used to invoke a human-machine-interface (HMI) function (e.g. signal “OK” via a buzzer sound);

— the “terminate communication” function, which shall be used to terminate the CCC communication;

— the “test communication” function, which shall be used for testing and localizing the OBE.

NOTE 2 A “write” service is not provided, since the writing of data into the OBE is not foreseen.

5.3 Attributes

The attributes available on the OBE side for a CCC application at road-side for checking the compliance of a vehicle are given in detail in Clause 7.

All attributes defined in this International Standard shall be available on the OBE side.

The RSE is free to decide to read any combination of attributes from the OBE. The attributes shall be identified and retrieved using the mechanisms defined in ISO 14906. More specifically, the addressing

of the CCC application data implemented by the OBE and RSE shall conform to the rules defined in ISO 14906:2011, 5.3.

Multiple instances of attributes are not supported.

5.4 Toll context

An OBE may be in several tolling contexts at once. This can occur, e.g. in situations where a motorway toll geographically overlaps with an area charging system. In these different tolling contexts, the OBE might run different charging applications or several instances of one charging application in parallel.

This International Standard builds on the concept that for compliance checking, there is no need to distinguish between tolling contexts. The data relevant for checking compliance, e.g. the identity of the vehicle, classification parameters and operational status of the OBE ("red" or "green"), are independent of the tolling context. Also, for legal reasons, a user must know whether or not he is acting in a compliant way without understanding technical detail, such as how many overlapping tolling contexts there are at a given moment.

Hence, there is only one CCC context, and context-related concepts known from DSRC charging — such as identification of the toll context via the EFC context mark or addressing a specific context via a corresponding EID — are not required. Therefore, the OBE shall hold only one CCC context, identified by a single EID value.

5.5 Use of lower layers

5.5.1 Supported DSRC communication stacks

The CCC application interface makes use of the CEN-DSRC communication stack as described in Table 1. Other communication media can be used as listed in Table 1 if an equivalent mapping to corresponding services is provided. Detailed examples are provided in informative annexes.

Table 1 — Supported short-range communication stacks

Medium	Application layer	Lower layers	Detailed specifications
CEN-DSRC	ISO 15628 EN 12834	EN 12795 EN 12253	Specification in 5.5.2
Italian DSRC	ETSI/ES 200 674–1 (Clause 11 and Annex D)	ETSI/ES 200 674–1 (Clauses 7 to 10 and Annex D)	Implementation example in Annex C
ISO CALM IR	ISO 15628 EN 12834	ISO 21214	Implementation example in Annex D
ARIB DSRC	ARIB STD-T75 ISO 15628	ARIB STD-T75 ITU-R.M1453–2	Implementation example in Annex E
NOTE 1:EN 12795 and EN 12253 have been adopted in ITU-R.M 1453–2.			

If more than one communication medium is implemented in an OBE, then the OBE shall respond to RSE interrogations on the same medium that the RSE has initiated the CCC interrogation.

5.5.2 Use of the CEN-DSRC stack

The following requirements apply to the CCC application when used with the CEN-DSRC communication stack.

The OBE shall comply with EN 15509:2014, 6.1.2.

Fixed RSE shall comply with EN 15509:2014, 6.2.2.

Mobile RSE shall comply with EN 15509:2014, 6.2.2, except for *Downlink Parameter D4a* (not applicable to mobile RSE).

NOTE EN 15509 defines the CEN-DSRC communication stack for fixed RSE only.

6 Functions

6.1 Functions in detail

6.1.1 General

All functions defined in 6.1 shall be available on the OBE side.

For CEN-DSRC, the OBE shall provide the following functions:

— INITIALISATION, GET, and RELEASE application layer services according to ISO 15628 and EN 12834;

— GET_STAMPED, SET_MMI, and ECHO EFC functions according to ISO 14906.

Subclauses 6.1.2 to 6.1.7 define the functions for CEN-DSRC only. For other supported media, according to 5.5.1, equivalent functionality should be provided. See Annex C for ETSI/ES 200 674-1 5.8 GHz microwave DSRC, Annex D for CALM Infrared DSRC, and Annex E for ARIB microwave DSRC.

6.1.2 Initialise communication

Initialisation of the communication between the RSE and the OBE shall be initiated by the RSE, by means of the invocation of an initialisation request by the RSE. After successful initialisation, the function “Initialise communication” shall notify the applications on the RSE and OBE sides.

The initialisation notification on the OBE side shall carry at least the identity of the beacon (e.g. beacon serial number) and absolute time.

The initialisation notification on the RSE side shall carry the CCC application identity and shall also carry data required for the security services (e.g. nonce value, key identifier).

The function “Initialise communication” shall be provided by the application layer INITIALISATION services as specified in ISO 15628 and EN 12834. It is defined in Annex A: refer to CCC-InitialiseComm-Request and CCC-InitialiseComm-Response.

6.1.3 Data retrieval

The function “Data retrieval” shall be provided by the application layer GET service as specified in ISO 15628 and EN 12834. It is defined in Annex A: refer to CCC-DataRetrieval-Request and CCC-DataRetrieval-Response.

In the GET service primitives, iid shall not be used.

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

GET shall always carry access credentials.

6.1.4 Authenticated data retrieval

The function “Authenticated data retrieval” shall be implemented by the EFC function GET_STAMPED as specified in ISO 14906. It is defined in Annex A: refer to CCC-AuthDataRetrieval-Request and CCC-AuthDataRetrieval-Response.

GET_STAMPED shall always carry access credentials.

NOTE Access credentials carry information needed to fulfil access conditions in order to perform the operation on the addressed element in the OBE. Access credentials can carry passwords as well as cryptography-based information such as authenticators

6.1.5 Driver notification

The function "Driver notification" shall be implemented by the EFC function SET_MMI as specified in ISO 14906. It is defined in Annex A: refer to CCC-Notification-Request and CCC-Notification-Response.

NOTE According to ISO 14906, SET_MMI.request uses EID = 0 and does not carry access credentials.

6.1.6 Terminate communication

The RSE may terminate the communication on application level with the OBE with the function "Terminate communication", by means of the invocation of a release request by the RSE.

NOTE 1 A termination of the communication on link level is outside of the scope of this International Standard.

The function "Terminate communication" shall be provided by the application layer service EVENT-REPORT as specified in ISO 15628 and EN 12834. It is defined in Annex A: refer to CCC-TerminateComm.

NOTE 2 According to ISO 15628 and EN 12834, EVENT-REPORT (Release) uses EID = 0 and does not carry access credentials.

6.1.7 Test communication

The function "Test communication" shall be implemented by the EFC function ECHO of ISO 14906, and is defined in Annex A: refer to CCC-TestComm-Request and CCC-TestComm-Response.

NOTE According to ISO 14906, ECHO uses EID = 0 and does not carry access credentials.

6.2 Security

6.2.1 General

Security is an essential part of CCC applications. This International Standard provides for generic security services. The detailed implementations are media-specific.

This International Standard provides for an authentication service that may serve to prove the identity of the data source, the integrity of the data and/or to provide for non-repudiation. It contains a mechanism for control of access to the OBE data by means of access credentials. Access protection is also used for protection of user privacy.

It does not provide for an encryption service on the assumption that privacy protection requirements are covered by the access credentials mechanism.

NOTE 1 Transaction counter according to EN 15509:2014 is not supported by the CCC application.

NOTE 2 The security measures defined in the following subclauses are fulfilling the CCC interface security countermeasures defined in ISO/TS 19299:2015, 7.3.3.

6.2.2 Authentication/non-repudiation

Authenticated reading of data are provided by the function "Authenticated data retrieval". Authenticators are defined as being of ASN.1 type OCTET STRING. This only pertains to the ASN.1 syntax; the semantics are media dependent.

When using the CEN-DSRC communication stack:

— the OBE shall be able to calculate authenticators according to security level 0 as defined in EN 15509:2014, 6.1.5.2;

— the RSE shall able to calculate authenticators to security level 0 as defined in EN 15509:2014, 6.2.5.2;

— the RSE shall request a message authentication code (MAC) by addressing at least the PaymentMeans attribute.

When using one of the other communication stacks described in Annexes C, D or E, algorithms and the use of lower communication layer services shall be as specified in the corresponding annex.

Authenticators shall primarily pertain to values and prove the source, the integrity of the data unit, protect against forgery and/or provide non-repudiation. Authenticators shall be transmitted from the OBE to the RSE.

NOTE The MasterAuthentication keys can be CCC-specific.

6.2.3 Access credentials

Access credentials shall be used to manage access to attributes. Access credentials are mandatory for all attributes defined in this International Standard. The “Data retrieval” and “Authenticated data retrieval” functions shall always carry access credentials.

The OBE shall support calculation of access credentials to security level 1 as defined in EN 15509:2014, 6.1.5.3.

The RSE shall be able to calculate access credentials to security level 1 as defined in EN 15509:2014, 6.2.5.3.

Access credentials are defined as being of ASN.1 type OCTET STRING. This only pertains to the ASN.1 syntax; the semantics are media-dependent.

7 Attributes

7.1 General

Within the context of CCC, all of the attributes given in Tables 2 and 3 shall be available on the OBE side.

Table 2 — CCC attributes as defined in EN 15509

AttributeID	Attribute	Length (octets)[a]	Data set
0	CCC-ContextMark	6[b]	Identification
24	EquipmentOBUId	5 (1+4)[c]	
32	PaymentMeans	14 [c]	
16	VehicleLicencePlateNumber	17 [c]	Vehicle
17	VehicleClass	1 [c]	
18	VehicleDimensions	3 [c]	
19	VehicleAxles	2 [c]	
20	VehicleWeightLimits	6 [c]	
22	VehicleSpecificCharacteristics	4 [c]	
46	TrailerCharacteristics	5	

[a] For information only.

[b] According to ISO 14906.

[c] According to EN 15509.

Table 3 — CCC specific attributes

AttributeID	Attribute	Length (octets)[a]	Data set
48	VehicleAxlesHistory	6	Vehicle
49	CommunicationStatus	8	Status
50	GnssStatus	25	
51	DistanceRecordingStatus	6	
52	ActiveContexts	Variable 1+(x *4)	
53	OBEStatusHistory	13	
64	AttributeUpdateInterval	1	
55	VehicleCurrentMaxTrainWeight	2	Vehicle
60	VehicleWeightHistory	12	
61	ExtendedOBEStatusHistory	18	
62	ExtendedVehicleAxlesHistory	10	
63	LocalVehicleClassId	2	

[a] For information only.

In this clause, CCC attributes are specified in terms of

— the name of a data attribute,

— the names of the data elements forming the CCC attribute (there are no optional data elements within any one CCC attribute),

— the semantic definition of the data element, and

— informative remarks, including references to other standards.

The specification of the corresponding data types in ASN.1 is provided in Annex A.

7.2 Data regarding identification

This data set (see Table 4) helps answer the question: Is the passing vehicle equipped with an authentic and activated OBE assigned to a certified toll service provider?

Table 4 — Data regarding identification

EFC attribute	Data element	Definition of semantics	Informative remarks
CCC-ContextMark	Same as EFC-ContextMark in ISO 14906	See ISO 14906	Contains the contract provider, type of contract and context version transmitted as part of the VST (vehicle service table).
EquipmentOBUId	Same as in EN 15509	See EN 15509	—
PaymentMeans	Same as in ISO 14906	See ISO 14906	Contains personal account number, the payment means' expiry date and usage control (restrictions on the geographic usage and services).

7.3 Data regarding status

This data set (see Table 5) helps answer the question: Does the OBE indicate correct (GO) operational status to the user and does it operate properly regarding core technical functionality?

Table 5 — Data regarding status (1 of 3)

EFC attribute	Data element	Definition of semantics	Informative remarks
ActiveContexts	tollContext	Identification of the toll context(s) the OBE has currently loaded. The coding all zero indicates that a generic context is active (e.g. thin clients). If more than one toll context is listed then the first entry shall correspond with the EFC context where the last charge object was recognized as being used. The identification type and value of a toll context is the same as for identifying the toll charger of the context.	Can be used to check if the current context(s) are active in the OBE.
	contextVersion	Version number of the active context. Shall correspond with the identifier of the VersionID as specified in ISO 17575-1 (to be published)	Can include versions of context parameters and maps (if required in that context).

Table 5 — (2 of 3)

EFC attribute	Data element	Definition of semantics	Informative remarks
OBEStatusHistory	statusIndicator	Set to the same value as a go/no-go user indicator. If the OBE indicates operating in a compliant status the value is: - go (1) Non-compliant status values are: - noGo (0): OBE no-go due to technical reasons. - noGoContractual (2): OBE no-go due to contractual aspects. - noGoUserSwitchedOff (3): OBE toll collection function switched off by the user.	Can be used to check if the user complies with his obligation to cooperate, and drives with an OBE with GO-status.
	timeWhenChanged	Time when GO/NO-GO status was changed to current status.	
	timeWhenActivated	Time when OBE was activated by the driver.	Used to prevent fraud by incorrect deactivation while in transit. May be same as TimeWhenObePowered.
	timeWhenObePowered	Time the OBE was connected to vehicle power.	
ExtendedOBEStatusHistory	statusIndicator timeWhenChanged	same as in OBEStatusHistory	
	previousStatusIndicator	same Format as StatusIndicator but related to the previous settings	may be used to detect fraud by manipulation of the OBE status claiming the excuse that it happened recently
	timeWhenChangedToPrevious	same as in OBEStatusHistory	
	timeWhenActivated timeWhenOBEPowered	same as in OBEStatusHistory	
Communication Status	timeOfLastTransmission	Date and time of the end of the last successful data transmission between OBE and the central system.	Can be used to check if the communication is operational (not tampered with). Such a check done by the RSE depends on the OBE communication possibilities and the details has to be agreed between TC and TSP.
	pendingSince	Date and time when the last transmission request of the application became pending. Shall be set to "0" when no transmission is pending.	
GnssStatus [1)]	lastGnssFixLon	Latest geographic longitudinal coordinate the GNSS sensor of the OBE has determined. Value in microdegrees[1)]. Values > 0 = east, < 0 = west, absolute value shall not exceed 180 degrees.	Can be used to check if GNSS reception is operational (not tampered with). Such a check done by the RSE depends on the OBE GNSS implementation and the details has to be agreed between TC and TSP.
	lastGnssFixLat	Latest geographic latitudinal coordinate the GNSS sensor of the OBE has determined. Value in microdegrees[1)]. Values > 0 = north, < 0 = south, absolute value shall not exceed 90 degrees.	
	lastGnssFixAlt	Latest altitude of the centre of the road surface (according to definition of the chosen geodetic model) the GNSS sensor of the OBE has determined, Value unit is 0,25 m.	

Table 5 — (3 of 3)

EFC attribute	Data element	Definition of semantics	Informative remarks
	lastGnssFixTime	Date and time associated to the LastGnssFixLat and LastGnssFixLon.	
	currentHDOP	Horizontal Geometric Dilution of Precision of the current used satellite constellation according to NATO STANAG 4294; Number of received satellites.	
	lastLAC	Date and time when the last localization augmentation message was received (timeOfLAC); identification of the operator of the localization augmentation communication (lACOperator); identifier of the operator's RSE (rSEId).	Can be used to check if the localization augmentation communication is operational (not tampered with).
DistanceRecording Status	distRecordingStatus	Indicates the status of an interface to the vehicle distance measurement (e.g. odometer) and correct reception of a signal	Value range: Distance recording - not present - present and active - present and inactive
	accumulatedTravelled Distance	Accumulated travelled distance of the vehicle since OBE installation. Value not relevant if no distance recording present.	Can be used, for example, to check distance recording accuracy using two successive beacons.
	deviationFromGnss	Average deviation over one hour between speed measured by GNSS and speed measured by odometer in 0,1 % steps. Positive value means that the GNSS measured larger distance. Value not relevant if equal to –12,8 % (–128).	Can be used to check quality of distance recording.
AttributeUpdate Interval	attributeUpdate Interval	Maximum time between two updates of the CCC attributes stored in the DSRC communication unit in seconds for corresponding attributes that have been changed in the OBE. A zero value indicates that the values are updated during CCC transaction. The maximum value 255 is used also for longer periods than 255 s.	Maximum update delay (age) in seconds of information in attributes in the DSRC communication unit of a changed attribute value in the OBE. If the interval exceeds the maximum time of the attribute, then the value shall be 255.
1) To translate **lastGnssFixLon** (the longitude), **lastGnssFixLat** (the latitude) and **lastGnssFixAlt** (the altitude) coordinates to the corresponding real position on earth or vice-versa the geodetic datum shall be WGS84(G1150), according to NIMA TR8350.2 version 3, per default unless another earth-centred earth-fixed polar coordinate geodetic datum is agreed mutually by the TC and TSP.			

Furthermore, by default any earth-centred earth-fixed polar coordinate geodetic datum can be used, as long as the maximum datum displacement relative to the geodetic datum prescribed is acceptable to the toll charger of the related toll domain.

The maximum tolerated datum displacement, also called datum shift, should not exceed 0,4 m.

NOTE The recommended maximum tolerated displacement allows, for example, for using one of the International Terrestrial Reference Frames (ITRF), the Russian PZ90.2 or one of the European Terrestrial Reference Frames (ETRF) as geodetic datums alternative to the WGS84.

The calculated datum displacement should be determined according to the definitions in ASME Y14.5 – 2009 "Dimensioning and Tolerancing".

7.4 Data regarding vehicle

This data set (see Table 6) helps answer the question: What are the tariff-relevant vehicle parameters currently claimed by the user?

Table 6 — Data regarding the vehicle

EFC Attribute	Data element	Definition of semantics	Informative remarks
VehicleLicensePlateNumber	Same as in EN 15509	See EN 15509:2014 Table A.2.	
VehicleClass	Same as in EN 15509	See EN 15509[1)]. Shall correspond with the first entry of ActiveContexts	Service provider specific information pertaining to the vehicle. Includes trailer attached, the basic vehicle class and the local vehicle class
LocalVehicleClassId	Same as in ISO 17575-3 [a]	See ISO 17575-3 Shall correspond with the first entry of ActiveContexts	Toll Charger specific definition determined in the Front End when evaluating the context data attribute LocalVehicleClass-Definition as specified in ISO 17575-3
VehicleDimensions	Same as in ISO 14906.	See ISO 14906	Includes vehicle length overall, vehicle height overall and vehicle width overall according to ISO 612
VehicleAxles	Same as in ISO 14906.	See ISO 14906	Includes vehicle first axle height and vehicle axle number
VehicleAxlesHistory	timeWhenChanged	Date and time of the last change of the value of the attribute VehicleAxles	Can be used to check if a change of the declared number of axles occurred during the trip, e.g. just before a CCC
	previousVehicleAxles	Value of the attribute VehicleAxles before last change	
ExtendedVehicle AxlesHistory	timeWhenChanged previousVehicleAxles	Same as in VehicleAxlesHistory	
	timeWhenChangedTo Previous	Same as in TimeWhenChanged but related to the previous settings	may be used to detect fraud by shortly correcting the VehicleAxles
VehicleWeightLimits	Same as in ISO 14906	See EN 15509	Includes vehicle max laden weight, vehicle train max weight and vehicle weight unladen
VehicleCurrentMax TrainWeight	Same as in ISO 14906	See EN 14906	This weight may be lower than VehicleTrainMaximumWeight as it represents the current maximum train weight and not the maximum design mass
VehicleWeightHistory	timeWhenChangedTo Current Value	indicates the time when the driver has changed to the reported value	may be used to detect fraud by using normally a too low value of vehicleWeightLimits and changing it just before passing an enforcement RSE
	previousVehicleWeight	Indicates the settings of the vehicle weight before the last change. The data element shall be set 0 if no previous weight is available	
	previousLocalVehicle ClassID	Indicates the settings of local vehicle class ID before the last change. The data element shall be set 0 if no previous local vehicle class ID is available	
	timeWhenChangedTo Previous	Indicates the time when the previous settings were set	
VehicleSpecific Characteristics	Same as in ISO 14906	See ISO 14906	Includes information on engine fuel type, EURO emission class and CO_2 emission rating
TrailerCharacteristics	Same as in ISO 14906	See ISO 14906	includes information on trailers such if present, general type and allowed weight

1) The LLLL element within the VehicleClass shall contain the LocalVehicleClassId In case its value is greater than 15 the LLLL element shall be set to 0000'B.

[a] To be published.

NOTE Depending on the layout of an EFC cluster the actual **VehicleClass** and the **LocalVehicleClassId** may exist in a Front End in more than one instance. This will happen if the vehicle is present in more than one of overlapping EFC domains and when different EFC domains are using different definitions of local vehicle class identifiers.

8 Transaction model

8.1 General

The transaction model related to the CCC application interface for DSRC shall comply with ISO 14906:2011, Clause 6, with the restrictions and amendments defined below for implementations using the CEN-DSRC communication stack. Details on the transaction model and addressing for other communication media are given in the relevant annexes.

The transaction model comprises two phases: initialisation and transaction.

8.2 Initialisation phase

8.2.1 Initialisation request

Initialisation of the communication shall be initiated by the RSE by means of the function "Initialise Communication". The OBE evaluates the initialisation request in order to decide whether the CCC application is supported. If the OBE does not support the CCC application, it shall not respond to the initialisation request. If the OBE supports the CCC application, it shall respond to the initialisation request.

8.2.2 CCC application-specific contents of BST

AID = 20 shall be used for the CCC application.

The RSE shall initialise only one instance of the CCC application; this means that there shall be only one instance of AID = 20 in the beacon service table (BST).

NOTE This does not exclude the BST from carrying information related to other applications which could be active at the RSE.

The CCC application shall be qualified as a mandatory application. EID shall not be transmitted in the BST related to the CCC application. No parameter shall be transmitted in the BST related to the CCC application.

8.2.3 CCC application-specific contents of VST

There shall be only one instance of AID = 20 in the ApplicationList in the VST. This instance shall contain the parameter CCC-ContextMark, which shall be equal to the ApplicationContextMark as defined in EN 15509:2014, Annex A, corresponding to security level 1.

The Service Provider shall make use of the data element contextVersion to ensure that the value of the CCC-ContextMark corresponds to one unique dated version of ISO 12813 through a reference table, which is made available to the Toll Charger, allowing it to identify to which specific version of the CCC application interface definition the OBE complies.

8.3 Transaction phase

After completion of the initialisation phase, the RSE application shall be notified.

There are no requirements specific to the transaction phase. The RSE may perform a transaction by using the functions in any sequence as long as the requirements of this International Standard are met. The OBE shall respond to the functions invoked by the RSE, and shall not initiate any functions on its side.

Annex A
(normative)

CCC data type specifications

This Annex presents the abstract syntax notation one (ASN.1) definition of

— the data types related to the CCC functions specified in Clause 6,

— the data types related to the CCC attributes specified in Clause 7, and

— the ASN.1 container types for ISO Layer 7,

in accordance with the ASN.1 technique specified in ISO/IEC 8824-1. The packed encoding rules given in ISO/IEC 8825-2 with the restrictions defined in ISO 15628:2013, 6.2.7, apply.

The actual ASN.1 module is contained in the attached file “ISO 12813 (2015)EfcCccV2.asn”.’

NOTE The ASN.1 module is also stored at: http://standards.iso.org/iso/12813/

Annex B
(normative)

PICS proforma for the attributes

B.1 General

In order to evaluate the conformance of a particular implementation, it is necessary to have a statement of those capabilities and options that have been implemented. This is called an implementation conformance statement (ICS) or, more specifically when it covers transactions, a protocol implementation conformance statement (PICS).

This Annex presents the (PICS) proforma to be used for the attributes defined in Clause 7 and Annex A, with PICS templates that are to be filled in by equipment suppliers.

B.2 Purpose and structure

The purpose of this PICS proforma is to provide a mechanism whereby a supplier of an implementation of the CCC defined in this International Standard can provide information about the implementation in a standardised manner.

The PICS proforma is subdivided as follows corresponding to categories of information:

— identification of the implementation;

— identification of the protocol;

— global statement of conformance;

— PICS proforma tables.

B.3 Instruction for completing PICS proforma

B.3.1 Definition of support

A capability is said to be supported if the implementation under test (IUT) can

— generate the corresponding operation parameters (either automatically or because the end user requires that capability explicitly), and

— interpret, handle and, when required, make available to the end user the corresponding error or result.

A protocol element is said to be supported for a sending implementation if it is able to generate it under certain circumstances (either automatically or because the end user requires relevant services explicitly).

A protocol element is said to be supported for a receiving implementation if it is correctly interpreted and handled and also, when appropriate, made available to the end user.

B.3.2 Status column

This column (see Tables B.1 to B.14) indicates the level of support required for conformance. The values are as follows:

m	mandatory support is required;
o	optional support is permitted for conformance to the standard. If implemented it must conform to the specifications and restrictions contained in the standard. These restrictions may affect the optionality of other items;
c	the item is conditional (support of the capability is subject to a predicate);
c: m	the item is mandatory if the predicate is true, optional otherwise;
-	the item is not applicable;
i	the item is outside the scope of this PICS.

In the PICS proforma tables, every leading item marked “m” shall be supported by the IUT. Sub-items marked “m” shall be supported if the corresponding leading item is supported by the IUT.

B.3.3 Support column

This column (see Tables B.6 to B.22) shall be completed by the supplier or implementer to indicate the level of implementation of each item. The proforma has been designed such that values required are the following:

Y	Yes, the item has been implemented;
N	No, the item has not been implemented;
-	the item is not applicable.

All entries within the PICS proforma shall be made in ink. Alterations to such entries shall be made by crossing out, neither erasing nor making the original entry illegible, and by writing the new entry alongside. All such alterations to records shall be initialised by the person who made them.

B.3.4 Item reference numbers

Each line within the PICS proforma which requires that implementation details be entered is numbered at the left hand edge of the line. This numbering is included as a mean of uniquely identifying all possible implementation details within the PICS proforma. This referencing is used both inside the PICS proforma, and for references from other test specification documents.

The means of referencing individual responses is done in the following sequence:

a) a reference to the smallest individual response enclosing the relevant item;

b) a solidus character (“/”);

c) the reference number of the row in which the response appears;

d) if — and only if — more than one response occurs in the row identified by the reference number, implicit labelling of each possible entry as “a”, “b”, “c”, etc., from left to right, with this letter appended to the sequence.

B.4 PICS proforma for OBE

B.4.1 Identification of the implementation

The following proforma are to be used to identify the implementation on the OBE side.

Table B.1 — Identification of PICS

Item no.	Question	Response
1	Date of statement (DD/MM/YY)	
2	PICS serial number	
3	System conformance statement cross reference	

Table B.2 — Identification of the implementation and/or system

Item no.	Question	Response
1	Service provider or EFC context name	
2	Version number	
3	Other information	

Table B.3 — Identification of the OBE supplier

Item No.	Question	Response
1	Organization name	
2	Contact name(s)	
3	Address	
4	Telephone number	
5	e-mail address	
6	Other information	

Table B.4 — Identification of the OBE

Item No.	Question	Response
1	Brand name	
2	Type, version	
3	Manufacturer ID	
4	Equipment class	
5	Serial numbers of supplied units	
6	Other information	

Table B.5 — Identification of ISO 12813

Item No.	Question	Response
1	Title, reference no., publication date	
2	ISO 12813 version (edition) no.	
3	Implemented addenda	
4	Implementer's guide version no.	
5	Implementation defect reports (ref. no.)	
6	Other information	

B.4.2 Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No)[2] .....

Which security level is implemented? (0/1) .....

NOTE See 6.2 for a definition of security levels.

B.4.3 PICS proforma tables

This part of the PICS proforma identifies the supported application context, communication services and attributes (ADU) for the OBE side.

Table B.6 — Security requirements

Item no.	Element	Reference	Status	Support
1	Security level 1	EN 15509:2014, 6.1.5.3	m	
2	Authenticator calculation	6.2.2	m	
3	AccessCredentials calculation	6.2.3	m	

Table B.7 — Required layer 7 functions

Item no.	Element	Reference	Status	Support
1	INITIALISATION	6.1.2	m	
2	GET	6.1.3	m	
3	GET_STAMPED	6.1.4	m	
4	SET_MMI	6.1.5	m	
5	EVENT_REPORT	6.1.6	m	
6	ECHO	6.1.7	m	

Table B.8 — Implemented DSRC stacks

Item no.	Element	Reference	Status [a]	Support
1	CEN-DSRC	5.5.2	o.	
2	Italian DSRC according to ETSI/ES 200 674–1	Annex C	o.	
3	CALM IR	Annex D	o.	
4	ARIB DSRC	Annex E	o.	

[a] One or more DSRC stacks shall be implemented.

Table B.9 — Data requirements regarding identification

Item no.	Element	Reference	Status	Support read protection	Support write protection	Support coding
1	CCC-ContextMark	7.2	m			
2	EquipmentOBUId	7.2	m			
3	PaymentMeans	7.2	m			

2) Answering “No” to this question indicates non-conformance with 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.

Table B.10 — Data requirements regarding status

Item no.	Element	Reference	Status	Support read protection	Support write protection	Support coding
1	ActiveContexts	7.3	m			
2	OBEStatusHistory	7.3	m			
3	ExtendedOBEStatusHistory	7.3	m			
4	CommunicationStatus	7.3	m			
5	GnssStatus	7.3	m			
6	DistanceRecording Status	7.3	m			
7	AttributeUpdateInterval	7.3	m			

Table B.11 — Data requirements regarding the vehicle

Item no.	Element	Reference	Status	Support read protection	Support write protection	Support coding
1	VehicleLicensePlate number	7.4	m			
2	VehicleClass	7.4	m			
3	LocalVehicleClassId	7.4	m			
4	VehicleDimensions	7.4	m			
5	VehicleAxles	7.4	m			
6	VehicleAxlesHistory	7.4	m			
7	ExtendedVehicleAxlesHistory	7.4	m			
8	VehicleWeightLimits	7.4	m			
9	VehicleCurrentMaxTrain Weight	7.4	m			
10	VehicleWeightHistory	7.4	m			
11	VehicleSpecific Characteristics	7.4	m			
12	TrailerCharacteristics	7.4	m			

B.5 PICS proforma for RSE

B.5.1 Identification of the implementation

The following proforma are to be used to identify implementation on the RSE side.

Table B.12 — Identification of PICS

Item no.	Question	Response
1	Date of statement (DD/MM/YY)	
2	PICS serial number	
3	System conformance statement cross reference	

Table B.13 — Identification of the implementation and/or system

Item no.	Question	Response
1	Service provider or EFC context name	
2	Version number	
3	Other information	

Table B.14 — Identification of the RSE supplier

Item no.	Question	Response
1	Organization name	
2	Contact name(s)	
3	Address	
4	Telephone number	
5	e-mail address	
6	Other information	

Table B.15 — Identification of the RSE

Item no.	Question	Response
1	Brand name	
2	Type, version	
3	Manufacturer ID	
4	Serial numbers of supplied units	
5	Other information	

Table B.16 — Identification of ISO 12813

Item No.	Question	Response
1	Title, reference no., publication date	
2	ISO 12813 version (edition) no.	
3	Implemented addenda	
4	Implementer's guide version no.	
5	Implementation defect reports (ref. no.)	
6	Other information	

B.5.2 Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No) [3)]……

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

NOTE See 6.2 and Annex G for a definition of security levels.

B.5.3 PICS proforma tables

This part of the PICS proforma identifies the supported application context, communication services and attributes (ADU) for the RSE side.

3) Answering "No" to this question indicates non-conformance with 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.

Table B.17 — Security requirements

Item No.	Element	Reference	Status	Support
1	Security level 1	EN 15509:2014, 6.1.5.3	m	
2	Authenticator calculation	6.2.2	m	
3	AccessCredentials calculation	6.2.3	m	

Table B.18 — Required layer 7 functions

Item No.	Element	Reference	Status	Support
1	INITIALISATION	6.1.2	m	
2	GET	6.1.3	m	
3	GET_STAMPED	6.1.4	m	
4	SET_MMI	6.1.5	m	
5	EVENT_REPORT	6.1.6	m	
6	ECHO	6.1.7	m	

Table B.19 — Implemented DSRC stacks

Item No.	Element	Reference	Status[a]	Support
1	CEN-DSRC	5.5.2	o	
2	Italian DSRC according to ETSI/ES 200 674–1	Annex C	o	
3	CALM IR	Annex D	o	
4	ARIB DSRC	Annex E	o	

[a] One or more DSRC stacks shall be implemented.

Table B.20 — Data requirements regarding identification

Item No.	Element	Reference	Status	Support read protection	Support write protection	Support coding
1	CCC-ContextMark	7.2	m			
2	EquipmentOBUId	7.2	m			
3	PaymentMeans	7.2	m			

Table B.21 — Data requirements regarding status

Item No.	Element	Reference	Status	Support read protection	Support write protection	Support coding
1	ActiveContexts	7.3	m			
2	OBEStatusHistory	7.3	m			
3	ExtendedOBEStatusHistory	7.3	m			
4	CommunicationStatus	7.3	m			
5	GnssStatus	7.3	m			
6	DistanceRecording Status	7.3	m			
7	AttributeUpdateInterval	7.3	m			

Table B.22 — Data requirements regarding the vehicle

Item No.	Element	Reference	Status	Support read protection	Support write protection	Support coding
1	VehicleLicensePlateNumber	7.4	m			
2	VehicleClass	7.4	m			
3	LocalVehicleClassId	7.4	m			
4	VehicleDimensions	7.4	m			
5	VehicleAxles	7.4	m			
6	VehicleAxlesHistory	7.4	m			
7	ExtendedVehicleAxlesHistory	7.4	m			
8	VehicleWeightLimits	7.4	m			
9	VehicleCurrentMaxTrain Weight	7.4	m			
10	VehicleWeightHistory	7.4	m			
11	VehicleSpecificCharacteristics	7.4	m			
12	TrailerCharacteristics	7.4	m			

Annex C
(informative)

ETSI/ES 200 674-1 communication stack usage for CCC applications

C.1 General

This Annex lists the requirements for CCC application using the Italian DSRC communication stack defined in ETSI/ES 200 674-1 as the communications medium. It shows how CCC generalized communication functions are mapped onto ETSI/ES 200 674-1 protocol directives and specifies how CCC information types can be stored in, and information retrieved from, an ETSI/ES 200 674-1-compliant OBE.

Security algorithms and calculations, as well as the transaction model, are specified in Annex D of ETSI/ES 200 674-1.

C.2 Requirements

Using the ETSI/ES 200 674-1 communication stack for transferring CCC data means being compliant to the whole standard, including its Annex D.

C.3 Function correspondences

Table C.1 shows the correspondences between CCC functions and the directives defined in Clause 11 of ETSI/ES 200 674-1. Different directives are used to access data which are located in different memory areas.

After the first interaction to initialise the communication link, a Select-TBA-Id-Rq directive is concatenated to all other requests.

If the compliance check transaction spans a number of DSRC interactions, the RSE should repeat its authentication, as long as there is room for authentication data and primitives in that interaction.

The address of the CCC application (AID parameter) corresponds to the Called AP Invocation Identifier parameter in the Open-Rq directive. Table C.1 gives the correspondences between CCC functions and (sequence of concatenated) protocol directives. Refer to C.4 for the meaning of the listed directives.

Table C.1 — Functions correspondences

CCC Function	ES 200 674–1 directive
Initialise communication	Open-rq, concatenated with Get-TBA-Random-Rq, concatenated with Get-Master-Record-Rq
Data retrieval	For Master Core: Read-Master-Core-Rq For Master Record: Get-Master-Record-Rq For Application Core: Read-Appl-Core-Rq For Application Record: Read-Appl-Record-Rq
Authenticated data retrieval	Concatenation of: Set-Credential-Rq, Get-Credential-Rq, and one or more Data writing operations as above in this table
Driver notification	Set-UIF-Rq
Terminate communication	Close-Rq
Test communication	Select-TBA-Id-Rq

C.4 Data storage and addressing

The main characteristic of OBE data addressing in ETSI/ES 200 674-1 is that data are referenced by position, i.e. by specifying their location in the OBE virtual memory. There is a specific virtual memory structure for each application type. This clause describes the OBE virtual memory structure for the CCC application.

The ETSI/ES 200 674-1 virtual memory is structured for each and every application into two areas:

1) Master;

2) Application.

The Master area is common to all applications. It is read/only, and contains information that is of common use. It is divided into two subareas, which can be accessed via specific directives, as specified in the Table C.2.

Table C.2 — Master area — Subareas

Subarea	ETSI/ES 200 674–1 **directive**
Core	Read-Master-Core-Rq
Record	Get-Master-Record-Rq

The Application area is application-specific, and generally read/write. It is also divided into two subareas, that can be accessed via specific directives, as specified in Table C.3.

Table C.3 — Application area — Subareas

Subarea	ETSI/ES 200 674–1 **directive**
Core	Read-Appl-Core-Rq, Write-Appl-Core-Rq
Record	Read-Appl-Record-Rq, Write-Appl-Record-Curr-Rq

NOTE Other ETSI/ES 200 674–1 directives are available for writing and reading in the Application area, but are not used for CCC applications, and hence are not listed here.

Table C.4 shows where relevant CCC information is stored in the ES 200674-1 virtual memory.

Table C.4 — Information in virtual memory

Area	Displacement	Length	Description
Master Core	0	2	ManufacturerId
	2	2	Equipment Class
	4	10	Reserved
Master Record	0	2	EFC application. Has the value of 50F0 (Hex)
	2	2	EFC application sub-identifier. Has the value of 0002 (Hex) for the CCC application
	4	6	EFC-ContextMark (CCC Context Mark)
	10	2	AC_CR-KeyReference
Application Core	0	14	PaymentMeans
	14	17	VehicleLicencePlateNumber
	31	1	VehicleClass
	32	3	VehicleDimensions
	35	2	VehicleAxles
	37	6	VehicleWeightLimits
	43	4	VehicleSpecificCharacteristics
	47	5	TrailerCharacteristics
	52	6	VehicleAxlesHistory
	58	8	CommunicationStatus
	66	23	GnssStatus
	89	6	DistanceRecordingStatus
	95	13	OBEStatusHistory
	108	14	VehicleWeightHistory
	122	18	ExtendedOBEStatusHistory
	140	10	ExtendedVehicleAxlesHistory
	150	1	LocalVehicleClassId
Application Record	0	4	ActiveContexts

Active Contexts are to be stored in application records. There are as many Application Records as there are active contexts.

Reading or writing multiple attributes in a single DSRC interaction is possible for attributes which are stored sequentially in the same memory region. This can be accomplished by specifying a displacement corresponding to first attribute to be read or written, and a length equal to the sum of the attributes' lengths.

EXAMPLE Retrieving the EFC-ContextMark and the AC_CR-KeyReference attributes can be accomplished in one interaction by means of an operation like: Get-Master-Record-Rq, with offset = 4, and length = 8.

Annex D
(informative)

Using the IR DSRC communication stack (CALM IR) for CCC applications

D.1 General

This Annex specifies the use in CCC applications of the CALM (communications access for land mobiles) IR (infrared) stack, as defined in ISO 21214.

D.2 DSRC requirements

The DSRC requirements, in the compatibility mode, are defined in ISO 21214.

NOTE ISO 21214 defines the physical and data link layer of CALM IR.

D.3 Functions

The CCC specific functions are defined in Clause 6.

D.4 Data requirements

The addressing of the EFC system and application data implemented by the OBE and RSE conforms to the rules given in ISO 14906:2011, 5.3. For CCC application data only one context is supported. Multiple instances of attributes are not supported.

The OBE should implement the EFC attributes defined in Clause 7.

The RSE should support any OBE that is otherwise compliant.

D.5 Security requirements

The security requirements are defined in 6.2.

D.6 Transaction requirements

The transaction requirements are defined in Clause 8.

Annex E
(informative)

Using the ARIB DSRC communication stack for CCC applications

E.1 General

This Annex specifies the use of the ARIB 5.8 GHz microwave DSRC link for CCC applications.

E.2 DSRC requirements

The DSRC requirements are defined in ARIB STD-T75:2001, section 2, and the DSRC communication stack with ARIB STD-T75:2001, section 4.

E.3 CCC functions

The CCC functions are defined in ARIB-T75:2001, 4.4.2.1.2.

The SET service is not supported by the CCC application.

GET and GET_STAMPED always carry AC-CR for secure communication.

E.4 Data requirements

The addressing of the EFC system and application data implemented by the OBE and RSE should conform to the rules defined in ISO 14906:2011, 5.3. For CCC application data, EID should always be used. Multiple instances of attributes are not supported.

The OBE should implement the EFC attributes defined in Clause 7.

The RSE should support any OBE that is otherwise compliant.

E.5 Security requirements

A security mechanism could be specified independent of ARIB DSRC in the future, in the form of security protection guidelines as in ISO/TS 17574.

E.6 Transaction requirements

E.6.1 General

The EFC transaction model complies with Clause 6 in ISO 14906:2011, with the restrictions and amendments given in E.6.2 to E.6.3.

E.6.2 Initialisation phase

E.6.2.1 CCC application-specific contents of BST

AID = 20 is used for the CCC application. There is only one instance of AID = 20 in the BST.

The CCC application is qualified as a mandatory application.

E.6.2.2 CCC application-specific contents of VST

There is only one instance of AID = 20 in the ApplicationList in the VST. This instance contains the parameter ApplicationContextMark as defined in A.2 in ISO 15628:2013.

E.6.3 Transaction phase

There are no requirements specific to the transaction phase. The RSE may perform a transaction by using the CCC functions in any sequence as long as the requirements of this International Standard are met.

Annex F
(informative)

Example CCC transaction

This Annex presents an example CCC transaction reading out all data and providing signatures for OBE data integrity/authenticity and for non-repudiation.

Table F.1 shows an example of how to implement a CCC transaction in a regime where all vehicle parameters are necessary for the fee collection.

NOTE In ISO/TS 19299 the naming of the MACs of Table F.1 is different. The MAC_Authentication is called MAC_TC and MAC_NonRepudiation is called MAC_TSP, respectively, in order to indicate the recipient instead of the function of these two MACs.

Table F.1 — Example CCC transaction

Phase	Roadside Equipment		On-board equipment	Remarks
Initialisation	INITIALISATION.request (BST)	→		RSE periodically sends BST.
(BST – VST)		←	INITIALISATION.response (VST) • CCC-Context-Mark • AC_CR-KeyReference • RndOBE	A newly arrived OBE answers with VST. AC-CR-KeyReference is the reference to the access credential keys to be used by the RSE. RndOBE is a random number that the RSE uses when calculating the access credentials. The OBE will give access only when RSE provides the correct access credentials (AC_CR) in the subsequent phases.
Presentation	GET_STAMPED.request AC_CR • PaymentMeans (RndRSE, KeyRef_Auth) GET.request AC_CR • EquipmentOBUId • Static vehicle data: — VehicleDimensions — VehicleLicensePlate-Number — VehicleWeightLimits — VehicleSpecificCharacteristics	→		The OBE is asked to present itself and its static data. Authenticated retrieval of PaymentMeans from the OBE: the OBE is asked to calculate an authenticator over PaymentMeans using the authentication key (KeyRef_Auth). Retrieval of data from the OBE: remaining identification data and static vehicle data.

Table F.1 *(continued)*

Phase	Roadside Equipment		On-board equipment	Remarks
		←	GET_STAMPED.response • MAC_Authentication GET.response	OBE responds with PaymentMeans, which points to the user contract/account at the service provider plus an authenticator (MAC_TC), providing authentication of the OBE and its data (data integrity and data origin authentication). MAC_Authentication can be directly checked by the toll charger to establish whether the OBE is authentic. OBE responds with the additional requested data.
Status	GET_STAMPED.request AC_CR • PaymentMeans • Dynamic vehicle data: — VehicleAxles — VehicleAxlesHistory — VehicleClass • Status Data: — ActiveContexts — OBEStatusHistory — CommunicationStatus — GnssStatus — DistanceRecordingStatus (RndRSE, KeyRef_NonRep)	→		The OBE is asked to present its dynamic status. Authenticated retrieval of a complete data package containing: PaymentMeans, VehicleAxles, VehicleClass and all Status data. The OBE is asked to calculate a signature that provides non-repudiation characteristics for the whole package using the non repudiation key (KeyRef_NonRep). MAC_NonRepudiation is stored together with the CCC data and can be used by the toll charger in the event of a dispute with the user.
		←	GET_STAMPED.response • MAC_NonRepudiation	OBE responds with the requested data, plus an authenticator (MAC_TSP), providing for non-repudiation characteristics.
Tracking	ECHO.request	→		Track OBE by exchanging dummy information.
And		←	ECHO.response	The usage of Echo is optional, at the discretion of the RSE, and may be repeated.
Closing	EVENT_REPORT.request (Release)	→		RSE closes transaction and releases OBE.

Annex G
(informative)

Security considerations

G.1 General

This Annex gives background and motivation for, and an example of the use of, the security-related functionalities of the CCC provided by this International Standard.

The security requirements of the CCC are derived from the following main requirements of the toll charger:

— the toll charger wishes to enforce their obligations on users who do not comply with their *obligation-to-cooperate* (e.g. by declaring the correct class and supervising the status of the OBE);

— the toll charger wishes to enforce their obligations on users who intentionally manipulate the charging process in the OBE;

— the toll charger might optionally wish to use the enforcement station to spot-check the service provider's usage data, verifying its correctness, i.e. comparing the usage data with the detected event at the enforcement station.

NOTE ISO/TS 19299 contains a detailed threat analysis and the resulting security requirements. The main requirements in the list above are a comprehensive summary of the ISO/TS 19299 security requirements from the toll chargers' perspective.

G.2 Security requirements

CCC is a means of checking the status of the GNSS/CN-based electronic fee collection process in the liable vehicle, i.e. checking the functionality of the OBE and the cooperation of the user. The retrieved data can be used, for example:

— to enforce obligations on a non-compliant vehicle, based on the user's *obligation-to-cooperate* (within the scope of this International Standard);

— to countercheck the usage data obtained from the service provider, spot-checking its correctness ["claim of incorrectness of the usage data" (not within the scope of this International Standard)].

The following security requirements are hereby considered as being relevant for a system of compliance checking (often called an *enforcement* system):

— data integrity, with regards to the data stored in the OBE, and data origin authentication, with regards to sensitive data transferred from the OBE to the compliance checking system (see G.3.1);

— repudiation or non-repudiation of data, with regards to sensitive data transferred from the OBE to the compliance checking system (see G.3.2);

— data access protection, with regards to the data stored in the OBE (see G.3.3).

These requirements relate to each entity in the EFC system as follows.

a) **Toll charger**

   1) **OBE (data) origin authentication and integrity**

The toll charger has to be protected against counterfeit transactions by the user (by means of a counterfeit OBE). It has to be ensured that the OBE that performed the transaction (and the data it contains) is a genuine OBE, issued by a true service provider.

2) **Non-repudiation of data by the user**

When issuing an enforcement claim, the toll charger has to be protected against a repudiation of the claim by the user that denies the correctness of the data retrieved from the OBE as, for example, being counterfeited by the toll charger.

3) **Non-repudiation of data by the service provider** [4)]

When the usage data provided by the service provider is counterchecked and a discrepancy between the usage data and the spot-check found, the toll charger has to be protected against repudiation of any claim of their incorrectness.

b) **Service provider**

1) **Protection against false claims by the toll charger**

The service provider has to be protected against any false claim of incorrectness of usage data made by the toll charger (when the usage data are genuine).

c) **User/Customer and OBE**

1) **Protection against false claims by the toll charger**

The user has to be protected against false enforcement claims by a toll charger.

2) **Privacy**

The user has to be protected against infringement of his privacy. Sensible data in his OBE has to be protected (licence plate number, history of last positions, etc.).

3) **Non-authorized usage of the OBE by other EFC operators**

Access to the OBE by another toll charger has to be avoided.

See Tables G.1 and G.2.

Table G.1 — Security risks for each entity in relation to other entities

	User	Service provider	Toll charger
User	—	—	False claim by an operator stating “non-compliance”. Infringement of privacy. Non-authorized usage of the OBE.
Service provider	—	—	False claim of incorrectness of usage data.
Toll charger	Counterfeit OBE Repudiation of a claim of “non-compliance” (enforcement claim).	Repudiation of a claim of incorrectness of usage data.	—

4) Optional and not strictly needed for compliance checking.

Table G.2 — Security requirements for each entity in relation to other entities

	User	Service provider	Toll charger
User	—	—	Protection against false claims of "non-compliance". Data access protection.
Service provider	—	—	Protection against false claims of incorrectness of usage data (optional).
Toll charger	OBE and data authentication and integrity. Non-repudiation of claims of "non-compliance"	Non-repudiation of a claim of incorrectness of usage data (optional).	—

G.3 Security concept based on symmetric cryptography

G.3.1 Data integrity and origin authentication

A solution to fulfilling the security requirements for data integrity and origin authentication using symmetric cryptography is based on authentication of the OBE to the toll charger (RSE) and to the service provider by means of a message authentication code (MAC). The OBE (data) origin authentication and integrity is provided by the use of a so-called symmetric "authentication" master key, shared between the toll charger and the service provider and which stores the derived key in the OBE. This key has the following characteristics:

— it is available to both the service provider and the toll charger;

— it is generally protected from disclosure but the value can be known to both the service provider and the toll charger;

— a derived version of the key is stored in the OBE and used to create message authentication codes for application layer data sent to the RSE;

— it can be used by the toll charger to verify the message authentication codes.

The MAC from the OBE calculated using the authentication key provides the (data) origin authentication and integrity characteristics to the CCC.

The toll charger can choose to check the MAC at the RSE or in his central equipment. In the first case, the key has to be distributed to the RSE in a secure way.

G.3.2 Non-repudiation

A solution for fulfilling the security requirement of non-repudiation by using symmetric cryptography is similar to that described in G.3.1, but based on the usage of a non-repudiation master key having the following characteristics:

— its value is unknown to the receiver of the compliance check message, i.e. to the toll charger, this being achieved, for example, simply by not distributing the key to the toll charger or by distributing the key inside a special secure storage area;

— a derived version of the key is stored in the OBE and used to create MAC in order to sign application layer data send to the RSE;

— it can be used by the service provider and optionally by the toll charger to verify the message authentication code(s) received from the OBE;

— if distributed to the toll charger, it is protected by a secure storage area, e.g. the key is stored in a secure application module (SAM), which provides mechanisms for verifying MAC without disclosing the key value and hence permitting the toll charger to verify a MAC but not create it himself.

The MAC from the OBE calculated using the non-repudiation key provides the non-repudiation characteristics to the CCC, because the key is unknown to the receiver of the message and hence the receiver cannot suffer from a repudiation attack, stating that "the receiver generated the message on his own". Hence the receiver (the toll charger) can use the compliance check communication message to claim the user or the service provider.

G.3.3 Data access protection

A solution for fulfilling the security requirement for data access protection by using symmetric cryptography is given by the use of access credentials, as follows.

— The value of the shared access credential master key is known to both the service provider and the toll charger.

— The RSE stores the master access credentials key.

— The OBE stores a derived access credentials key.

— Both the OBE and the RSE calculate a MAC using the key and a random number generated by the OBE and send to the RSE (challenge). The RSE sends a MAC in the form of the so-called "access credentials" as part of its request to the OBE (response). The OBE compares its own calculated access credentials with the RSE's response. If these are equal, access is allowed. Otherwise, an error message is returned to the RSE.

An overview of the security measures in relation to the security requirements is given in Table G.3.

Table G.3 — Security measures in relation to the requirements

Requirement	Measure
Toll charger (enforcement operator)	
Protect the toll charger against counterfeit OBEs	OBE authentication to the RSE (stamping) using the authentication or non-repudiation key
Protect the toll charger against repudiation of a claim of incorrectness of the usage data by the service provider	OBE authentication to the RSE (stamping) using the non-repudiation key
Protect the toll charger against repudiation of the enforcement claims by the user	OBE authentication to the RSE (stamping) using the non-repudiation key
Service provider	
Protect the service provider against false claims of incorrectness of the usage data by toll charger	OBE authentication to the RSE (stamping) using the non-repudiation key
User/Customer and its OBE	
Protect the user against false enforcement claims	OBE authentication to the RSE (stamping) using the non-repudiation key
Protect the user/customer against infringement of his privacy	Access credentials
Avoid non-authorized use of the OBE (by other toll chargers)	Access credentials
All	
Protect OBE data (vehicle and contract data) integrity	Access credentials

G.3.4 Example usage of symmetric security measures during CCC

The access credentials key is used by the RSE during the CCC to calculate and present the correct access credentials in its layer 7 requests to the OBE. The OBE verifies the access credentials and in the positive case executes the command.

The authentication key is used during a compliance check communication to generate a MAC over (a part of) the data sent by the OBE to the RSE (e.g. using the authenticated data retrieval function according to 6.1.4 with the algorithms according to 6.2.2).

The toll charger can verify the MAC in order to check the OBE's data integrity and its authenticity. This can be done at the RSE or at the toll charger's central system.

The non-repudiation key is used during CCC to generate a MAC over (a part of) the data sent by the OBE to the RSE. If necessary (e.g. if the toll charger suffers from a repudiation attack) the toll charger can either

— ask the service provider to check the MAC, or

— check the MAC using the SAM which has been distributed to him (optionally).

Annex H
(informative)

Use of this International Standard for the EETS

H.1 General

In 2004 an EU 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 EU-Directive calls for the establishment of a European Electronic Toll Service (EETS).

In 2009 an 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 International Standard.

H.2 Overall relationship between European standardization and the EETS

The EU 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 is 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 on how this International 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 EC-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 EC-Directive, further European standards could be referenced there as well.

In 2011 the European Commission has also published 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 was intended to be updated on regular basis.

H.3 European standardization work supporting the EETS

Many of the standards developed by CEN/TC278 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 co-operation between CEN working groups and the EC.

It should be noted that no CEN/ISO standards are "turn key" 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 the task of the owner(s) of the EETS.

It should also be noted that CEN/ISO has 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.

H.4 Correspondence between this International Standard and the EETS

This International Standard defines requirements for GNSS/CN based EFC schemes to check if users have fulfilled their obligation to cooperate. This is using a proper OBE associated with a functional payment means as well as having set the OBE to the currently correct variable configuration parameters determining the local vehicle class and with this the applicable tariff.

This International Standard is intended to be implemented in all EETS-compliant OBE providing all specified functional elements with no options.

This International Standard defines requirements that correspond to the requirements listed in EC-decision 2009/750/EC:

Table H.1 — ISO 12813 and EC-Decision 2009/750/EC

Clause(s)/subclause(s) of this CEN/ISO standard	Essential Requirements of EC Decision 2009/750/EC	Qualifying remarks/Notes
Whole standard except the informative annexes and the Bibliography	Annex II Clause 3.(b)	Real-time compliance checking transactions

Bibliography

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

[2] ISO 21214, *Intelligent transport systems — Communications access for land mobiles (CALM) — Infra-red systems*

[3] EN 12253:2004, *Road transport and traffic telematics — Dedicated Short Range Communication — Physical layer using microwave at 5.8 GHz*

[4] EN 12795:2003, *Road transport and traffic telematics — Dedicated Short Range Communication (DSRC) — DSRC data link layer: medium access and logical link control*

[5] ARIB[5)] STD-T75, *Dedicated Short-Range Communication*

[6] ITU-R.M1453-2, *Intelligent Transport Systems — Dedicated Short Range Communications at 5.8 GHz*

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

[8] ISO/TS 17574:2009, *Electronic fee collection - Guidelines for security protection profiles*

[9] STANAG 4294, *NAVSTAR Global Positioning System (GPS) System Characteristics*

[10] Directive EU 2004/52/EC, *on the interoperability of electronic road toll systems in the community*

[11] ETSI/ES 200 674-1 version 2.4.1 (2013-05), *Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communications (DSRC); Part 1: Technical characteristics and test methods for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band*

[12] EC-decision 2009/750/EC, *on the definition of the European Electronic Toll Service and its technical elements*

[13] ISBN 978-92-79-18637-0, *Guide for the Application of Directive on the Interoperability of Electronic Road Toll Systems*

[14] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations

[15] ISO/TS 13143-1:2011, *Electronic fee collection — Evaluation of on-board and roadside equipment for conformity to ISO/TS 12813 — Part 1: Test suite structure and test purposes*

[16] ISO/TS 13143-2:2011, *Electronic fee collection — Evaluation of on-board and roadside equipment for conformity to ISO/TS 12813 — Part 2: Abstract test suite*

[17] ISO/TS 19299:2015, *Electronic fee collection — Security framework*

[18] CEN/TS 16072-1:2014*Electronic fee collection — Secure monitoring for autonomous toll systems - Part 1: Compliance checking*

[19] CEN/TS 16072-2:2015*Electronic fee collection — Secure monitoring for autonomous toll systems - Part 2: Trusted recorder*

[20] ISO/TS 13141, *Electronic fee collection — Localisation augmentation communication for autonomous systems*

[21] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

5) Association of Radio Industries and Businesses (ARIB), a Japanese Standards Development Organisation.

[22] ASME Y14.5:2009 — *Dimensioning and Tolerancing*

ICS 03.220.20; 35.240.60

Price based on 42 pages