INTERNATIONAL STANDARD

ISO 12813

Second edition
2019-11

Electronic fee collection — Compliance check communication for autonomous systems

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

Reference number
ISO 12813:2019(E)

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

Published in Switzerland

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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

This second edition cancels and replaces the first edition (ISO 12813:2015), which has been technically revised. It also incorporates the Amendment ISO 12813:2015/Amd 1:2017.

The main changes compared to the previous edition are as follows:

— inclusion of the changes of ISO 12813:2015/Amd 1:2017(E), i.e. it defines the electronic fee collection compliance check communication using the WAVE communication stack as defined in IEEE;

— reverting the length of attribute GnssStatus back to 23 octets and removing the data element of type Altitude;

— allowing a maximum of two instances of AID = 20 in the ApplicationList in the VST;

— adding values goSuspicion (5) and noGoPaymentMeans (4) to the data element statusIndicator as well as updating and clarifying the semantic definitions of all statuses and when they change;

— updating the OBEStatusHistory – timeWhenChanged and ExtendedOBEStatusHistory -timeWhenChanged/timeWhenChangedToPrevious based on the updated sematic definition of statusIndicator;

— clarifing the relationship between the LLLL element in VehicleClass and the LocalVehicleClassId (imported from ISO 17575-3);

— clarifing that ExtendedOBEStatusHistory - timeWhenChangedToPrevious shall be set to zero in case no previous value is available;

— clarifing that VehicleWeightHistory – timeWhenChangedToCurrentValue changes not only due to changes in the attribute VehicleCurrentMaxTrainWeight but also changes in the assignment of the LocalVehicleClassId or the LLL element within VehicleClass;

— adding the EFC attributes ExtendedOBUStatusHistoryPart1, ExtendedOBUStatusHistoryPart2 and UserConfirmation;

— updating Annex C by adding the attributes VehicleCurrentMaxTrainWeight and AttributeUpdateInterval to the information in virtual memory according to ETSI ES 200 674-1 communication stack usage for CCC applications.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

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 roadside infrastructure). The OBE will record the amount of road usage in all toll charging systems it passes through.

This document 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 17573-1. See Figure 1.

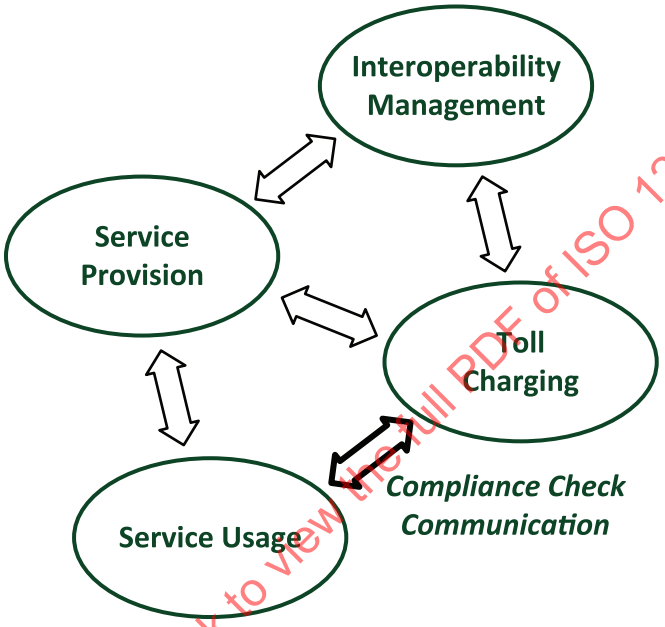

Figure 1 — Compliance check communication in EFC architecture according to ISO 17573-1

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 roadside 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 document defines attributes required on all OBE for reading by an interrogator.

This document has been prepared to fulfil the following statements:

a) Collected evidence can be used as court proof. Data is 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 is read only, since the operator of the interrogator does not interfere with the working of the OBE.

c) All attributes, standardised at the time of personalisation of the OBE, are 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 document.

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

e) The attributes apply to all OBE architectures, and especially to both thin (edge-light) and fat (edge heavy) client architectures. The interrogator is intended to receive essentially the same information irrespective of the type of OBE.

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 operational 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 operation of the OBE and for the payment by the user. Hence, as long as the OBE signals "green" and the user fulfils its other obligations (e.g. 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 soon as practicable. 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 document 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 nationwide 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 document builds on the concept that regarding compliance, there is no notion of toll context as far as possible (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 document 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 document 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) In this case, "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 this document is defined in the corresponding edition of ISO 13143-1 and ISO 13143-2.

Electronic fee collection — Compliance check communication for autonomous systems

1 Scope

This document 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 interrogator (roadside 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 17573-1. 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 document 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 not a communication sequence. All the attributes defined herein are required in any OBE claimed to be compliant with this document, 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 in the data retrieval phase, 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, ARIB DSRC and WAVE 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 application layer, with the CCC attributes and functions made available to the CCC applications at the roadside 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;

— CCC data type specifications given in Annex A;

— a protocol implementation conformance statement (PICS) proforma is given in Annex B;

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

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

— an example CCC transaction is presented in Annex G;

— the informative Annex I highlights how to use this document for the European electronic toll service (as defined in Commission Decision 2009/750/EC).

Test specifications are not within the scope of this document.

NOTE A test suite for checking an OBE or RSE implementation for compliance with this document is defined in the corresponding edition of ISO 13143-1 and ISO 13143-2.

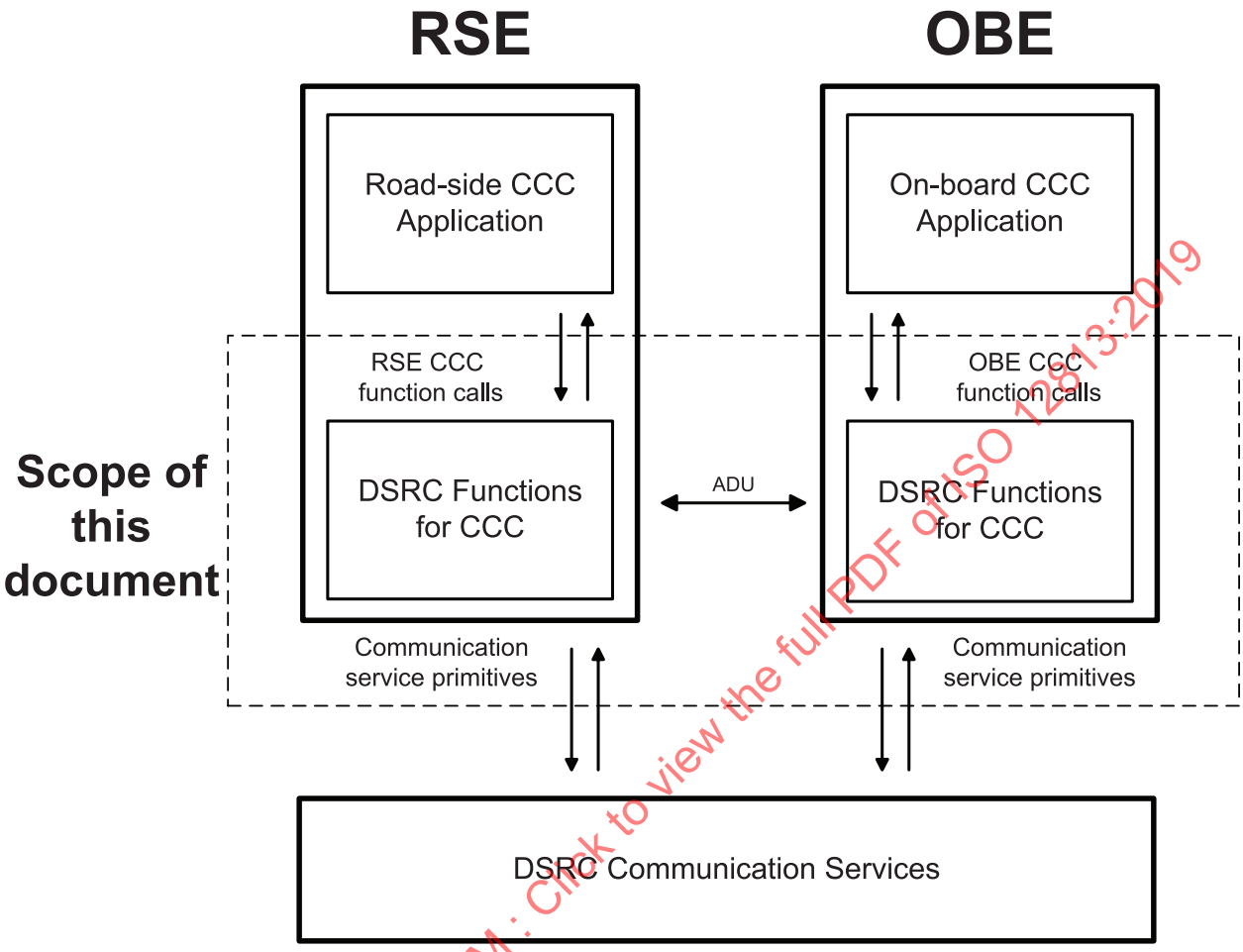

Figure 2 — CCC application interface

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 8824-1:2015, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

ISO/IEC 8825-2:2015, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) — Part 2*

ISO 14906:2018, *Electronic fee collection — Application interface definition for dedicated short-range communication*

ISO 14906:2018/Amd 1[2)], *Electronic fee collection — Application interface definition for dedicated short-range communication — Amendment 1*

2) To be published. Current stage: 40.99.

ISO 17575-3:2016, *Electronic fee collection — Application interface definition for autonomous systems — Part 3: Context data*

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.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
access credentials
AC_CR
trusted attestation or secure module that establishes the claimed identity of an object or application

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 V1.1.1:1998, 3]

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

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

[SOURCE: ISO 7498-2:1989, 3.3.21]

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 electronic fee collection (EFC) functions and communication services

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

3.10
service primitive
elementary communication service provided by the application layer protocol to the application processes

3.11
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

3.12
toll regime
set of rules, including enforcement rules, governing the collection of a toll in a toll domain

3.13
toll service provider
TSP
entity providing toll services in one or more toll domains

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 abbreviated terms 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	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 service 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 on 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 document.

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 roadside for checking the compliance of a vehicle are given in detail in Clause 7.

All attributes defined in this document 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 14906:2018, 5.3.

Multiple instances of attributes are not supported.

5.4 Toll context

An OBE may be in several tolling contexts at once.

NOTE This can occur, e.g. in situations where a motorway toll geographically overlaps with an area-based charging system.

In these different tolling contexts, the OBE might run different charging applications or several instances of one charging application in parallel.

This document builds on the concept that for compliance checking, there is basically no need to distinguish between tolling contexts. In certain circumstances and in the cases specified in the semantic definition, the toll service provider shall ensure that the attribute content complies with the specifications of the toll charger (e.g. for local vehicle classes).

The OBE should hold only one CCC context, represented by a single element as specified in ISO 14906. However, for backwards compatibility reasons, one additional CCC context, represented by a second element may be used to support ISO 12813:2015 (see also 8.2.3).

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 EN 12795 and EN 12253 have been adopted in ITU-R.M 1453–2.			

Table 1 *(continued)*

Medium	Application layer	Lower layers	Detailed specifications
WAVE DSRC	IEEE 1609.11-2010 ISO 15628	IEEE 1609.3-2010 IEEE 1609.4-2016 IEEE 802.11	Implementation example in Annex F
NOTE 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.

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, Annex E for ARIB microwave DSRC and Annex F for WAVE 5.9 GHz 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.

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 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 document provides for generic security services. The detailed implementations are media-specific.

This document 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

NOTE 1 It is assumed that privacy protection requirements are covered by the access credentials mechanism.

NOTE 2 Transaction counter according to EN 15509:2014 is not supported by the CCC application.

NOTE 3 The security measures defined in the following subclauses fulfil the CCC interface security countermeasures defined in ISO/TS 19299:2015, 7.3.3.

6.2.2 Authentication/non-repudiation

Authenticated reading of data is provided by the function "Authenticated data retrieval". Authenticators are defined as ASN.1 OCTET STRING type. 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 1 as defined in EN 15509:2014, 6.1.5.3;

— the RSE shall be able to calculate authenticators to security level 1 as defined in EN 15509:2014, 6.1.5.3;

— 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, E or F, 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 document. 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, 6.1.5.3.

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 ISO 14906 and 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	13 to 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[b]	

[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	23	
51	DistanceRecordingStatus	6	
52	ActiveContexts	Variable 1+(x *4)[b]	
53	OBEStatusHistory	13	
64	AttributeUpdateInterval	1	
55	VehicleCurrentMaxTrainWeight	2	Vehicle
60	VehicleWeightHistory	12	
61	ExtendedOBEStatusHistory	18	Status
62	ExtendedVehicleAxlesHistory	10	Vehicle
63	LocalVehicleClassId	2	
99	ExtendedOBUStatusHistoryPart1	36	Status
100	ExtendedOBUStatusHistoryPart2	28	
101	UserConfirmation	13	

[a] For information only.

[b] where 'x' means the number of toll contexts active in the OBE: x value is given in the first byte.

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 a correct (GO) operational status to the user and does it operate properly regarding core technical functionality?

The EFC attribute ExtendedOBUStatusHistoryPart1 provides, compared to the data elements in ExtendedOBEStatusHistory, additional information about geographical position of the change of the status indicator and the possibility to submit a toll service provider individual information code. The EFC attribute ExtendedOBUStatusHistoryPart2 provides two additional earlier historic values of the OBU status.

NOTE 1 The OBE provides all the attributes ExtendedOBEStatusHistory, ExtendedOBUStatusHistoryPart1 and ExtendedOBUStatusHistoryPart2.

The RSE decides which of those attributes to request, e.g. either

— ExtendedOBEStatusHistory or

— ExtendedOBUStatusHistoryPart1 or

— ExtendedOBUStatusHistoryPart1 and ExtendedOBUStatusHistoryPart2 or

— none of the three options above.

Table 5 — Data regarding status

EFC attribute	EFC attribute	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 to the CCC 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 to the identifier of the VersionID as specified in ISO 17575-1	Can include versions of context parameters and maps (if required in that context).

Table 5 *(continued)*

EFC attribute	EFC attribute	Definition of semantics	Informative remarks
OBEStatusHistory	statusIndicator	The statuses are divided into the two classes "GO" and "NO-GO". In case several status conditions from both the "GO" and "NO-GO" class are fulfilled the status shall be set to one of the statuses of the "NO-GO" class. The condition to set statuses in the "GO" class is that: the OBE is functioning correctly and the user is fulfilling its obligations to cooperate. Statuses and conditions in the "GO"-class are: — go (1): shall be set when the "GO" condition is fulfilled and the status is not set to goSuspicion(5). — goSuspicion (5): may be set when the "GO" condition seems to be fulfilled and there is suspicion of technical manipulation, where the exact definition of what constitutes "suspicion of technical manipulation" shall be defined by the toll service provider.	The data element statusIndicator contains information on the correct functioning of the OBE and the fulfillment of the user's obligations to cooperate with toll scheme requirements. The statusIndicator is not necessarily completely reflected on the user HMI. There are cases where the HMI will report that the user is not allowed to drive the vehicle without the statusIndicator having a "NO-GO"-value, for example during OBE upstart. To evaluate and report suspicious technical behaviour is an OBE option, not a requirement. Examples: An OBE with status "go" (1) is shut down. During subsequent boot of this OBE the HMI indicates that the vehicle is not allowed to drive for a short time while performing some internal boot checks. After that, it indicates that the user can drive the vehicle. These changes shall not lead to changes of the data elements statusIndicator or previousStatusIndicator.
		The condition to set statuses in the "NO-GO" class is that: the OBE is not functioning correctly excluding non-functioning in short time periods (such as for example during a shutdown followed by immediate upstart, or a reboot) or detection of the user not fulfilling its obligations to cooperate Statuses in the "NO-GO"-class are:	The automatic tolling function is actively switched off by the user. The data element statusIndicator contains "noGoUserSwitchedOff" (3). Later, the user turns on again automatic tolling, the data element statusIndicator switches back to "go" (1).

Table 5 *(continued)*

EFC attribute	EFC attribute	Definition of semantics	Informative remarks
		— noGo (0): shall be set when the "NO-GO" condition is fulfilled and the status is not set to another status in the "NO-GO" class. — noGoContractual (2): may be set when the "NO-GO" condition is fulfilled due to contractual aspects. — noGoUserSwitchedOff (3): may be set when the "NO-GO" condition is fulfilled and the OBE has been switched off due to user action or driving behaviour. — noGoPaymentMeans (4): may be set when the "NO-GO" condition is fulfilled due to insufficient payment means, where the exact definition of what constitutes "insufficient payment means " shall be defined by the toll service provider. NOTE The responsibility for defining “insufficient payment means” can be with a separate Payment Means Provider, or this responsibility can be assumed by the toll service provider directly.	These changes shall lead to changes of the data elements statusIndicator and previousStatusIndicator with the respective points of time.
	timeWhenChanged	Time when GO/NO-GO status was changed to current status.	

Table 5 *(continued)*

EFC attribute	EFC attribute	Definition of semantics	Informative remarks
	timeWhenActivated	Last time the OBE started to evaluate current time, place and other parameters to determine if any toll context rules apply, and in this case start to operate accordingly.	Used to prevent fraud by incorrect deactivation while in transit. EXAMPLE 1: A specific OBE implementation has a button allowing the user to turn it off. A cheating user keeps this OBE turned off while driving on a tolled road but turns the OBE on just before a known CCC spotcheck location. Then timeWhenActivated shall be set to the time when the user turns it on. EXAMPLE 2: A specific OBE implementation does not feature any possibility to turn it off causing timeWhenActivated to normally be the same as time of installation in vehicle. However, a cheating user disconnects the OBE from vehicle power and runs up the battery power causing a complete shutdown, then reconnects the OBE to vehicle power just before a known CCC spotcheck location. Then timeWhenActivated shall be set to the time when the OBE is operational again, in this case the value will be very close to or identical to timeWhenPowered (depending for example on time for boot up sequence).
	timeWhenObePowered	Last time the OBE was connected to vehicle power.	
ExtendedOBEStatusHistory	statusIndicator timeWhenChanged	same as in OBEStatusHistory	
	previousStatusIndicator	Shall contain the previous value of data element statusIndicator, if this value has changed. However, the OBU may avoid storing changes due to on-off power switching already recorded in the statusIndicator data element.	May be used to detect fraud by manipulation of the OBE status claiming the excuse that it happened recently. Not recording in history on-off status changes means, e.g., that NOGO transitions due to long switch off or parking may not be present in the previousStatusIndicator and timeWhenChangedToPrevious. This helps in preventing the occurrence of false positives.
	timeWhenChangedToPrevious	The time of the change of data element previousStatusIndicator. The data element shall be set to 0 and the previousStatusIndicator shall be set to 0 if no previousStatusIndicator is available.	
	timeWhenActivated timeWhenOBEPowered	same as in OBEStatusHistory	

Table 5 *(continued)*

EFC attribute	EFC attribute	Definition of semantics	Informative remarks
ExtendedOBUStatusHistoryPart1	statusIndicator timeWhenChanged	same as in OBEStatusHistory	
	tspStatus	An information or error code that is specific to the toll service provider and corresponds to statusIndicator.	This date element can provide additional information about the reasons for a specific statusIndicator. As an example, if statusIndicator is set to "noGo", the tspStatus can provide additional information on the reason for setting this statusIndicator.
	position	The position of the vehicle when statusIndicator was set. The data elements GnssLon and GnssLat shall be set to 0 if no corresponding position is available.	
	previousStatusIndicator	The previous value of data element statusIndicator, if this value has changed. The data element shall be set to 0 and the timeWhenChangedToPrevious shall be set to 0 if no previousStatusIndicator is available.	May be used to detect fraud by manipulation of the OBE status claiming the excuse that it happened recently
	timeWhenChangedToPrevious	The time of the change of data element previousStatusIndicator. The data element shall be set to 0 and the previousStatusIndicator shall be set to 0 if no previousStatusIndicator is available.	
	previousTspStatus	An information or error code that is specific to the toll service provider and corresponds to previousStatusIndicator.	
	previousPosition	The position of the vehicle when previousStatusIndicator was set. The data elements GnssLon and GnssLat shall be set to 0 if no corresponding position is available.	
	timeWhenActivated timeWhenOBEPowered	Same as in OBEStatusHistory	
ExtendedOBUStatusHistoryPart2	previousStatusIndicator2	The previous value of data element previousStatusIndicator in ExtendedOBUStatusHistory21, if this value has changed. The data element shall be set to 0 and the timeWhenChangedToPrevious2 shall be set to 0 if no previousStatusIndicator2 is available.	

Table 5 *(continued)*

EFC attribute	EFC attribute	Definition of semantics	Informative remarks
	timeWhenChangedToPrevious2	The time of the change of data element previousStatusIndicator2. The data element shall be set to 0 and the previousStatusIndicator2 shall be set to 0 if no previousStatusIndicator2 is available.	
	previousTspStatus2	An information or error code that is specific to the toll service provider. and corresponds to previousStatusIndicator2.	
	previousPosition2	The position of the vehicle when previousStatusIndicator2 was set. The data elements GnssLon and GnssLat shall be set to 0 if no corresponding position is available.	
	previousStatusIndicator3	The previous value of data element previousStatusIndicator2, if this value has changed. The data element shall be set to 0 and the timeWhenChangedToPrevious3 shall be set to 0 if no previousStatusIndicator3 is available.	
	timeWhenChangedToPrevious3	The time of the change of data element previousStatusIndicator3. The data element shall be set to 0 and the previousStatusIndicator3 shall be set to 0 if no previousStatusIndicator3 is available.	
	previousTspStatus3	An information or error code that is specific to the toll service provider and corresponds to previousStatusIndicator3.	
	previousPosition3	The position of the vehicle when previousStatusIndicator3 was set. The data elements GnssLon and GnssLat shall be set 0 if no corresponding position is available.	
CommunicationStatus	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. pendingSince shall be set to "0" when no transmission is pending.	

Table 5 *(continued)*

EFC attribute	EFC attribute	Definition of semantics	Informative remarks
GnssStatus [a]	lastGnssFixLon	Latest geographic longitudinal coordinate the GNSS sensor of the OBE has determined. Value in microdegrees[a]. 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.	
	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 satellites being tracked.	
	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).
UserConfirmation	timeOfConfirmation	The time when the user confirms an OBE message or indication.	The TSP is free to define the HMI and the way how the user can confirm a message (e.g. by pushing a button)
	positionOfConfirmation	The position of the vehicle when the user confirms an OBE message or indication. The data elements GnssLon and GnssLat shall be set to 0 if no corresponding position is available.	
	tspStatus	An information or error code that is specific to the toll service provider and corresponds to the user confirmation.	Can be used to transmit a TSP individual code of the error message that is displayed to the user and which the user needs to confirm.

Table 5 *(continued)*

EFC attribute	EFC attribute	Definition of semantics	Informative remarks
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 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.
AttributeUpdateInterval	attributeUpdateInterval	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.

[a] To translate **lastGnssFixLon** (the longitude) and **lastGnssFixLat** (the latitude) 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 2 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.	

Table 6 *(continued)*

EFC Attribute	Data element	Definition of semantics	Informative remarks
VehicleClass	Same as in EN 15509.	See EN 15509. Shall correspond with the first entry of ActiveContexts. The LLLL element within the VehicleClass shall contain the LocalVehicleClassId. In case it is not coded the LLLL element shall be set to 0000'B.	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 17575-3:2016.	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 LocalVehicleClassDefinition 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 axles number (lifted or not).
VehicleAxlesHistory	timeWhenChanged	Date and time of the last change of the value of any data element 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.	
ExtendedVehicleAxlesHistory	timeWhenChanged	Date and time of the last change of the value of any data element of the attribute VehicleAxles.	
	previousVehicleAxles	Value of the attribute VehicleAxles before last change.	
	timeWhenChangedToPrevious	Date and time of the previous change of number of vehicle axles.	Can be used to detect fraud by quickly switching the declaration of vehicle axles to reset the history.
VehicleWeightLimits	Same as in ISO 14906.	See EN 15509.	Includes vehicle max laden weight, vehicle train max weight and vehicle weight unladen.
VehicleCurrentMaxTrainWeight	Same as in ISO 14906.	See ISO 14906.	This weight may be lower than VehicleTrainMaximumWeight as it represents the current maximum train weight and not the maximum design mass.
VehicleWeightHistory	timeWhenChangedToCurrentValue	Indicates the most recent time when the value of VehicleCurrentMaxTrainWeight or LocalVehicleClassId or the LLLL element within VehicleClass was changed.	May be used to detect a fraudulently 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 of the value of VehicleCurrentMaxTrainWeight. The data element shall be set to 0 if no previous weight is available.	

Table 6 *(continued)*

EFC Attribute	Data element	Definition of semantics	Informative remarks
	previousLocalVehicle ClassID	Indicates the settings of local vehicle class ID before the last change. The data element shall be set 0 and the time-WhenChangedToPrevious shall be set to 0 if no previous local vehicle class ID is available.	
	timeWhenChangedTo Previous	Indicates the time when the previous settings were set. The data element shall be set 0 and the previousLocalVehicleClassID shall be set to 0 if no previous local vehicle class ID is available.	
VehicleSpecific Characteristics	Same as in ISO 14906.	See ISO 14906.	Includes information on engine fuel type, EURO emission class and CO_2 emission rating, plus reserve.
TrailerCharacter-istics	Same as in ISO 14906.	See ISO 14906.	Includes information on trailers such if present, general type and allowed weight.

NOTE Depending on the layout of an EFC cluster the actual **VehicleClass** and the **LocalVehicleClassId** can 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 14906:2018, 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 applications.

The RSE shall initialise 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 can be active at the RSE.

8.2.3 CCC application-specific contents of VST

There shall be a minimum of one instance and a maximum of two instances of AID = 20 in the ApplicationList in the VST.

In those instances, the parameter ApplicationContextMark shall be as defined in ISO 14906:2018, Annex A, corresponding to security level 1, with the first 6 octets containing the CCC-ContextMark instead of the EFC-ContextMark.

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.

One instance of the CCC application-specific context shall be present and comply with this document. A second instance is optional and if present should comply with ISO 12813:2015.

NOTE 1 The Service Provider can use the CCC-ContextMark to identify to which specific version of the CCC application interface definition the OBE complies. This can be useful when creating a region of interoperable toll systems to support gradual migration to newer updates of the standard by mandating that the RSE handles not only the most recent application interface definition but also others that are existing within the OBE population.

NOTE 2 To ensure compatibility with all former versions of the standard and to limit the number of CCC contexts that need to be handled to only two.

The RSE shall only carry out a CCC transaction with an OBE that has transmitted a CCC-ContextMark valid for the toll context.

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 document 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 DSRC application layer,

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 ASN.1 Module's Object Identifier has been assigned in accordance to the requirements of ISO 14813-6.

The actual ASN.1 module is contained in the attached file "ISO12813(2019)EfcCccV4.asn", which can be directly imported in a compiler found at http://standards.iso.org/iso/12813/ed-2/en.

The syntax and semantics of the data types in the ASN.1 types in the attached file "ISO12813(2019) EfcCccV4.asn" that are imported shall comply with ISO 14906:2018/Amd 1 and ISO 17575-3:2016, respectively.

NOTE 1 The above referenced file(i.e. "ISO12813(2019)EfcCccV4.asn") is freely available for download via hyperlink at www.itsstandards.eu/index.php/efc#EFCstandards and is available at http://standards.iso.org/iso/12813/ed-2/en

Table A.1 provides the SHA-256 cryptographic hash digest for the referenced file, offering a means to verify the integrity of the file. The SHA-256 algorithm is specified in NIST 180-4.

Table A.1 — SHA-256 cryptographic hash digest

File Name	SHA-256 cryptographic hash digest
ISO12813(2019)EfcCccV4.asn	479C5738203ED8A5470E7B098EDB6E97416F28C07CDBA140284BDBBEDF598091

NOTE 2 Pasting the text of the file into one of the hash digest computation pages available on the web can result in a non-matching hash digest due to changes in the underlying coding.

Annex B
(normative)

PICS proforma

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 the concerned equipment supplier or its representative.

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 document 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 shall 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 shall 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)[3] .....

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	
5	WAVE DSRC	Annex F	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			

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.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			
8	ExtendedOBUStatusHistoryPart1	7.3	m			
9	ExtendedOBUStatusHistoryPart2	7.3	m			
10	UserConfirmation	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	VehicleCurrentMaxTrainWeight	7.4	m			
10	VehicleWeightHistory	7.4	m			
11	VehicleSpecificCharacteristics	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) [4] .....

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.

4) 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	
5	WAVE DSRC	Annex F	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	o[a]			
4	CommunicationStatus	7.3	m			
5	GnssStatus	7.3	m			
6	DistanceRecording Status	7.3	m			
7	AttributeUpdateInterval	7.3	m			
8	ExtendedOBUStatusHistoryPart1	7.3	o[a]			

[a] Either ExtendedOBEStatusHistory or both elements ExtendedOBUStatusHistoryPart1 and ExtendedOBUStatusHistoryPart2 shall be supported.

Table B.21 *(continued)*

Item No.	Element	Reference	Status	Support read protection	Support write protection	Support coding
9	ExtendedOBUStatusHistoryPart2	7.3	o[a]			
10	UserConfirmation	7.3	m			

[a] Either ExtendedOBEStatusHistory or both elements ExtendedOBUStatusHistoryPart1 and ExtendedOBUStatusHistoryPart2 shall be supported.

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	VehicleCurrentMaxTrainWeight	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 ETSI ES 200 674-1, Annex D.

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 ETSI ES 200 674-1, Clause 11. 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

Table C.1 *(continued)*

CCC Function	ES 200 674–1 directive
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

Table C.4 *(continued)*

Area	Displacement	Length	Description
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	2	VehicleCurrentMaxTrainWeight
	152	2	Altitude
	154	1	AttributeUpdateInterval
	155	1	LocalVehicleClassId
	156	36	ExtendedOBUStatusHistoryPart1
	192	28	ExtendedOBUStatusHistoryPart2
	220	13	UserConfirmation
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 14906:2018, 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 14906:2018, 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 ISO 14906:2018, Clause 6 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 ISO 15628:2013, A.2.

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 document are met.

Annex F
(informative)

Using the WAVE communication stack for CCC applications

F.1 General

This Annex specifies the use of the WAVE system based on the standards IEEE 1609.4, IEEE 802.11-2016, IEEE 1609.0, IEEE 1609.3 and IEEE 1609.11-2010.

F.2 Communication requirements

The communication requirements are defined in IEEE 1609.11-2010, A.2.

The contents of the beacon service table (BST), defined in 8.2.2, along with optional application-specific information, should be transmitted as the Provider Service Context (PSC) of a WAVE service advertisement (WSA) message, as defined in IEEE 1609.11-2010.

F.3 CCC functions

F.3.1 General

The CCC functions are defined in IEEE 1609.11-2010, A.3.1, Table 1. Table F.1 shows the correspondences between the WAVE primitives, the DSRC application layer primitives and the EFC functions.

Table F.1 — CCC functions correspondence

CCC function	DSRC application layer primitive (ISO 15628)	EFC function (ISO 14906)	WAVE primitive(s) (IEEE 1609.3-2010)
Initialise communication	INITIALISATION		WME-ProviderService.request, WME-UserService.request
Data retrieval	GET		WSM-WaveShortMessage.request, WSM-WaveShortMessage.indication
n.a.	SET		
n.a.		GET_STAMPED	
n.a.		GET_INSTANCE	
Driver Notification		SET_MMI	
Test Communication		ECHO	
Secure data retrieval		GET_SECURE	
n.a.		SET_SECURE	
Terminate communication		RELEASE	WME-ProviderService.request

The WAVE communication stack provides a CCC function called “Secure data retrieval” as an alternative to “Authenticated data retrieval”.

F.3.2 Secure data retrieval

The function “Secure data retrieval” should be implemented by the EFC function GET_SECURE as specified in ISO 14906 and with additional specification in IEEE 1609.11-2010, A.3.2.

GET_SECURE should not carry access credentials.

NOTE GET_SECURE according to IEEE 1609.11–2010 carries encrypted application data in the form of an encrypted AttributeList and an authenticator calculated by the recipient over the requested data.

F.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 14906:2018, 5.3. For CCC application data, EID should always be used. Multiple instances of attributes are not supported.

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

The RSE should support any OBE that is compliant.

F.5 Security requirements

F.5.1 General

This Annex 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.

It provides for an encryption service that also deals with control of access to the OBE data, both for protection of user privacy

F.5.2 Authentication/non-repudiation

Authenticated reading of data is provided by the function “Secure data retrieval”. Authenticators are defined as being of ASN.1 type OCTET STRING. When using the WAVE communication stack,

— the OBE should be able to calculate authenticators according to IEEE 1609.11-2010, A.5;

— the RSE should able to calculate authenticators according to IEEE 1609.11-2010, A.5;

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

F.5.3 Encryption

Encryption of payload data should be used to manage access to attributes by the function “Secure data retrieval”. Encryption is mandatory for all attributes defined in this document.

The OBE should support encryption as defined in IEEE 1609.11-2010, A.5.

The RSE should support encryption as defined in IEEE 1609.11-2010, A.5.

F.6 Transaction requirements

F.6.1 General

The EFC transaction model complies with ISO 14906:2018, Clause 6, and IEEE 1609.11-2010 A.5, with the restrictions and amendments given in F.6.2 to F.6.3.

F.6.2 Initialisation phase

F.6.2.1 CCC application-specific contents of BST

As defined in 8.2.2.

F.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 IEEE 1609.11-2010, A.5.

F.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 document are met.