TECHNICAL SPECIFICATION

ISO/TS 12813

First edition
2009-11-15

Electronic fee collection — Compliance check communication for autonomous systems

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

Reference number
ISO/TS 12813:2009(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

- an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

- an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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.

ISO 12813 was prepared by the European Committee for Standardization (CEN) Technical Committee CEN/TC 278, *Road transport and traffic telematics*, in collaboration with ISO Technical Committee TC 204, *Intelligent transport systems*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

Introduction

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

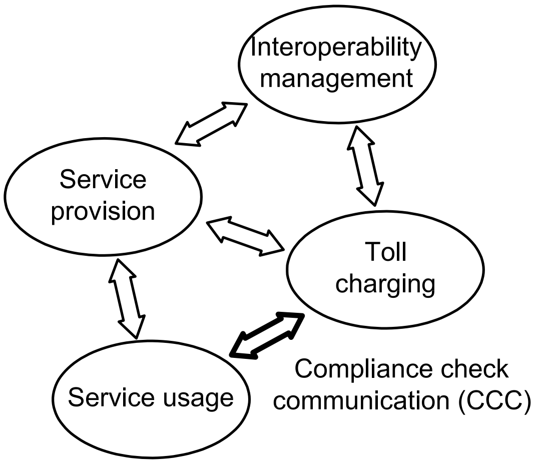

Interoperability management
Service provision
Toll charging
Service usage
Compliance check communication (CCC)

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) 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 Technical Specification defines attributes required on all OBE for reading by an interrogator.

In order to protect users against infringement of their privacy, the entity responsible for interrogation will need to avoid keeping a record of the checked transactions where no indication of non-compliance is detected. Local privacy legislation will apply.

This Technical Specification 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 must be present in the OBE such that an operator of an interrogator 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.

d) The attributes must be abstract from the individual toll regime and 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 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) or by internal mechanisms of the OBE itself (e.g. because of a detected defect or an outdated data set) — the user knows that the OBE is no longer a valid payment means. He then has to use alternative means of toll payment until the problem is remedied and the OBE is “green” again.

Ultimately, the policy of when to signal “green” and when “red” is defined by the service provider. As long as the user is signalled “green”, the service provider has an unconditional payment obligation towards the toll charger for all tolls accrued by the user.

In the case where the OBE status turns “red”, the user has to take action and 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 Technical Specification 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 Technical Specification 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 on quite different principles, the possibilities for doing this in a standardised way are quite limited. This Technical Specification 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 Technical Specification has been prepared with the intention to be “minimalist” in the sense that it covers that which is required by operational systems and systems planned in the foreseeable future. Future editions could include additional provisions were, for example, a trusted device inside the OBE to become standard.

[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.

Electronic fee collection — Compliance check communication for autonomous systems

1 Scope

This Technical Specification defines requirements for short-range communication for the purposes of compliance checking in autonomous electronic fee-collecting (EFC) 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 Technical Specification 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 Technical Specification, even if some values are set to “not defined” in cases where a 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 possible.

The CCC is suitable for a range of short-range communication media. Specific definitions are given for the CEN-DSRC specified in EN 15509, as well as for the use of ISO CALM IR, UNI DSRC 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 ADU (application data units).

The definition of the CCC includes

— the application interface between OBE and RSE,

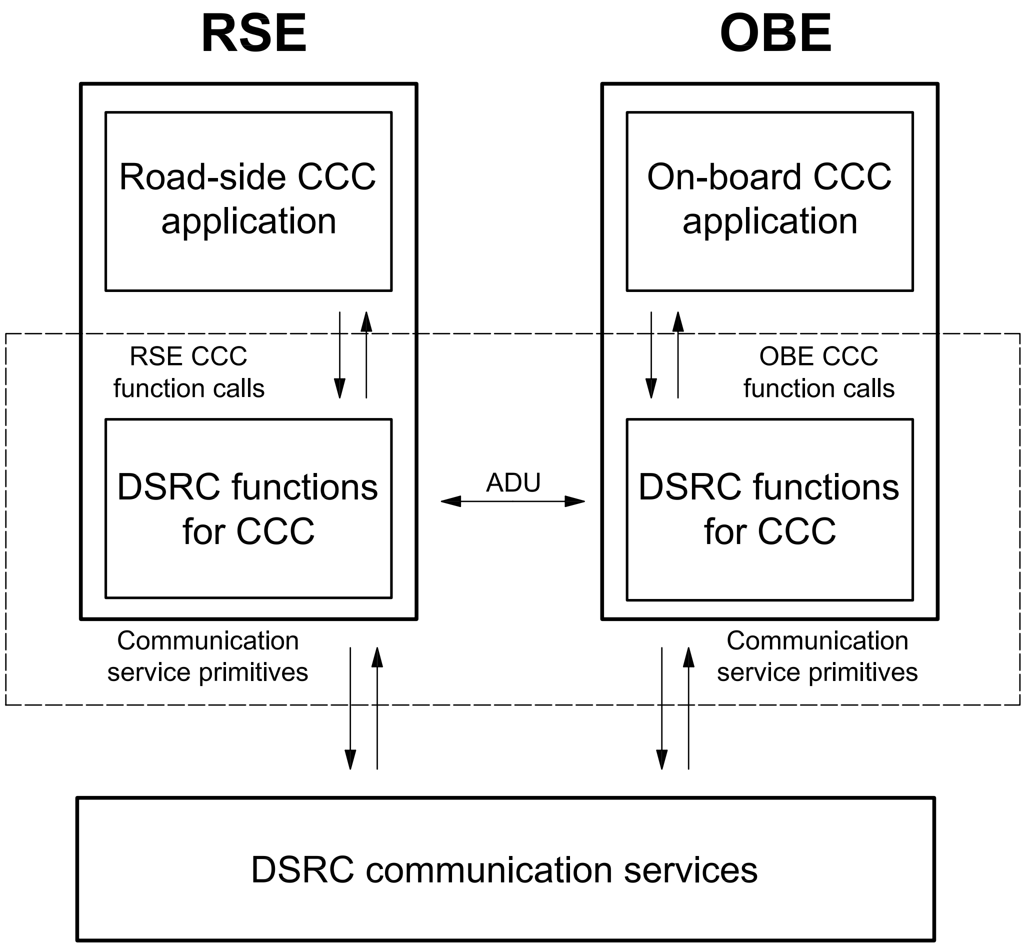
— use of the generic DSRC application layer as specified in ISO 15628 and EN 12834,

— 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.

Test specifications are not within the scope of this Technical Specification. See Figure 2.



The scope of ISO/TS 12813 is the area within the dashed line.

Figure 2 — CCC application interface

2 Normative references

The following referenced documents are indispensable for the application 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, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

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

ISO 15628:2007, *Road transport and traffic telematics — Dedicated short range communication (DSRC) — DSRC application layer*

ISO 14906:2004, *Road transport and traffic telematics — Electronic fee collection — Application interface definition for dedicated short range communication*

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

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

3 Terms and definitions

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

3.1
access credentials
data that is transferred to on-board equipment (OBE) in order to establish the claimed identity of a roadside equipment (RSE) application process entity

[ISO 14906]

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.

3.2
attribute
application information formed by one or by a sequence of data elements, used for implementation of a transaction

[ISO 14906]

3.3
authenticator
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and/or the integrity of the data unit and protect against forgery

[ISO 14906]

3.4
contract
expression of an agreement between two or more parties concerning the use of the road infrastructure

[ISO 14906]

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

[ISO 14906]

3.6
fixed roadside equipment
roadside equipment installed at a fixed position along the road transport network, for the purpose of communication and data exchange with the on-board equipment of passing vehicles

[ISO 14906]

3.7
mobile roadside equipment
⟨compliance checking communication⟩ roadside equipment located on-board special vehicles using or standing near the road transport network or hand-held equipment, for the purpose of communication and data exchange with the on-board equipment of passing vehicles

3.8
on-board equipment
OBE
equipment located within the interrogated vehicle and supporting the information exchange with the roadside equipment

[ISO 14906]

3.9
roadside equipment
RSE
equipment located outside the interrogated vehicle for the purpose of interrogating the on-board equipment of vehicles subject to toll

3.10
toll service
service enabling users having a contract and an OBE to use a vehicle in one or more toll domains

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

[ISO 14906]

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

3.12
toll context
logical view of a toll regime as defined by attributes and functions

3.13
toll regime
set of rules defining a toll scheme covering the charge and charging processes for a specific road-user charging measure

3.14
transaction
whole of the exchange of information between the *roadside equipment* and the *on-board equipment* necessary for the completion of a toll or compliance checking operation

[ISO 14906]

4 Abbreviated terms

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

AC_CR	access credentials
ADU	application data unit
ASN.1	abstract syntax notation one
BST	beacon service table
CCC	compliance check communication
DSRC	dedicated short-range communication

EID	element identifier
EFC	electronic fee collection
GNSS/CN	global navigation satellite systems/cellular network
MAC	media access control or message authentication code
OBE	on-board equipment
PICS	protocol implementation conformance statement
RSE	roadside equipment
TS	technical specification
VST	vehicle service table

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, while 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 enforcement 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 validate 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 The policy of whether or not the results 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 Technical Specification.

The above services are realised 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 is used to establish the CCC communication link between RSE and OBE;
- the “data retrieval” function, which is used to retrieve CCC attributes;

- the "authenticated data retrieval" function, which is used to retrieve data with an authenticator from the OBE;
- the "driver notification" function, which is used to invoke an HMI function (e.g. signal "OK" via a buzzer sound);
- the "terminate communication" function, which is used to terminate the CCC communication;
- the "test communication" function, which is used for testing and localising the OBE.

NOTE 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 Technical Specification 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 14906:2004, 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 UNI DSRC	UNI 10607-4 UNI 10607-3	UNI 10607-2 UNI 10607-1	Example implementation in Annex C
ISO CALM IR	ISO 15628 EN 12834	ISO 21214	Example implementation in Annex D
ARIB DSRC	ARIB STD-T75 ISO 15628	ARIB STD-T75 ITU-R.M1453-2	Example implementation in Annex E

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 used.

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 15509:2007, 5.1.2.

Fixed RSE shall comply with EN 15509:2007, 5.2.2.

Mobile RSE shall comply with EN 15509:2007, 5.2.2., excepting *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 functions shall either be provided by the DSRC application layer as specified in ISO 15628 and EN 12834 (services INITIALISATION, GET, and RELEASE) or shall be implemented according to the corresponding EFC functions of ISO 14906 (functions GET_STAMPED, SET_MMI, and ECHO).

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 shall be provided, see Annex C for UNI 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 shall be initiated by the RSE. The invocation of an initialisation request by the RSE attempts to initialise communication between RSE and OBE. 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. 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.

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.

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 with the function "Terminate communication". The invocation of a release request by the RSE attempts to close the communication on application level.

NOTE 1 A termination of the communication on link level is outside of the scope of this Technical Specification.

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

This Technical Specification provides for an authentication service that may serve to prove the identity of the data source and the integrity of the data and 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 Transaction counter according to EN 15509:2007 is not supported by the CCC application.

6.2.2 Authentication/non-repudiation

Authenticated reading of data is 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 1 as defined in EN 15509:2007, 5.1.5.3;
- the RSE shall able to calculate authenticators to security level 1 as defined in EN 15509:2007, 5.2.5.3.

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

Authenticators shall primarily pertain to values and prove the source and/or the integrity of the data unit, protect against forgery and/or provide non-repudiation. Authenticators are to 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 Technical Specification. 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 15509:2007, 5.1.5.3.

The RSE shall be able to calculate access credentials to security level 1 as defined in EN 15509:2007, 5.2.5.3.

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]	

[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	Status
49	CommunicationStatus	8	
50	GnssStatus	23	
51	DistanceRecordingStatus	6	
52	ActiveContexts	Variable (×*4)	
53	OBEStatusHistory	13	

[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

EFC attribute	Data element	Definition of semantics	Informative remarks
ActiveContexts	ContextId	Identification of the context(s) the OBE has currently loaded. The coding all zero indicates that a generic context is active (e.g. thin clients).	Can be used to check if the current context(s) are active in the OBE.
	ContextVersion	Version number(s) of the active context.	Can include versions of context parameters and maps (if required in that context).
OBEStatusHistory	StatusIndicator	Set to the same value as a go/no-go user indicator. TRUE shall mean that the OBE indicates operating in a compliant status (“GO”).	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.	
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.	
CommunicationStatus	TimeOfLast Transmission	Date and time of the end of the last successful data transmission to the central system.	Can be used to check if the toll data communication is operational (not tampered with).
	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	LastGnssFixLon	Latest geographic longitudinal coordinate the GNSS sensor of the OBE has determined. Value in microdegrees, reference model WGS84.	Can be used to check if GNSS reception is operational (not tampered with).
	LastGnssFixLat	Latest geographic latitudinal coordinate the GNSS sensor of the OBE has determined. Value in microdegrees, reference model WGS84.	
	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 localisation augmentation message was received; identification of the operator of the localisation augmentation communication; identifier of the operator’s RSE.	Can be used to check if the localisation augmentation communication is operational (not tampered with).
DistanceRecordingStatus	OdometerActive	Indicates the presence of an interface to the vehicle distance measurement (e.g. odometer) and correct reception of a signal.	Value range: interface not present; interface present and signal received; interface present and signal not received.
	AccumulatedTravelled Distance	Accumulated travelled distance of the vehicle since OBE installation. Value not relevant if interface not 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 measurement indicates higher speed. Value not relevant if interface not present.	Can be used to check quality of the odometer’s signal.

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.	The usage is according to ISO 14906 but more specific and limited in scope. Claimed licence plate of the vehicle. The length of the padded LPN is fixed to 14 octets (i.e. 17 octets including the country code, alphabet indicator, length determinant and the LPN).
VehicleClass	Same as in EN 15509.	See EN 15509.	Service provider specific information pertaining to the vehicle. Includes trailer attached, the basic vehicle class and the local vehicle class.
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.
VehicleWeightLimits	Same as in ISO 14906.	See EN 15509.	Includes vehicle max laden weight, vehicle train max weight and vehicle weight unladen.
VehicleSpecificCharacteristics	Same as in ISO 14906.	See ISO 14906.	Includes information on engine fuel type, EURO emission class and CO_2 emission rating.

8 Transaction model

8.1 General

The transaction model related to the CCC application interface for DSRC shall comply with ISO 14906:2004, 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 a response is mandatory.

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 BST.

NOTE This does not exclude the BST (beacon service table) 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 15509:2007, Annex A, corresponding to security level 1.

8.3 Transaction phase

After completion of the initialisation phase, the RSE application is 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 Technical Specification 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 ASN.1 (abstract syntax notation one) 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 apply.

```
CccModule {iso standard 12813 modules(0) ccc(0) version(1)}
DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
EquipmentOBUId, PaymentMeans, LPN, VehicleClass, VehicleDimensions, VehicleAxles,
VehicleWeightLimits, VehicleSpecificCharacteristics, EFC-ContextMark, Provider,

-- Imports data attributes and elements from EFC which are used for CCC

GetStampedRq, GetStampedRs, SetMMIRq

-- Imports function parameters from the EFC Application Interface Definition

FROM EfcModule {iso standard 14906 modules(0) efc(0) version(1)}

Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList,
AttributeList, Attributes, BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-
Request, Event-Report-Response, EventType, Get-Request, Get-Response, Initialisation-
Request, Initialisation-Response, ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs,
VST

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition, i.e.
the lower interface within the CCC scope

FROM DSRCData {iso standard 14906 modules (0) dsrc (1) version (1)};

--Note the following are the definitions of the CCC functions:

CCC-InitialiseComm-Request ::= BST

CCC-InitialiseComm-Response ::= VST

CCC-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid,
accessCredentials (SIZE(4)), attrIdList})

CCC-DataRetrieval-Response::= Get-Response (WITH COMPONENTS {..., eid, iid ABSENT})

CCC-AuthDataRetrieval-Request::= Action-Request (WITH COMPONENTS {mode (TRUE), eid,
actionType (0), accessCredentials (SIZE(4)), actionParameter })
-- uses actionParameter (GetStampedRq)

CCC-AuthDataRetrieval-Response::= Action-Response (WITH COMPONENTS {..., iid ABSENT,
responseParameter PRESENT}) -- uses responseParameter (GetStampedRs)
```

```
CCC-Notification-Request::= Action-Request (WITH COMPONENTS {mode, eid (0), actionType
(10), actionParameter }) -- uses actionParameter (SetMMIRq)

CCC-Notification-Response::= Action-Response (WITH COMPONENTS {..., eid (0), iid ABSENT,
responseParameter ABSENT})

CCC-TerminateComm::= Event-Report-Request  (WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})

CCC-TestComm-Request::= Action-Request (WITH COMPONENTS {..., eid (0), actionType (15),
accessCredentials ABSENT, iid ABSENT})

CCC-TestComm-Response::= Action-Response (WITH COMPONENTS {..., fill (SIZE(1)), eid (0),
iid ABSENT})

-- NOTE: The following are the definitions of the CCC attributes:

ActiveContext ::= SEQUENCE OF SEQUENCE{
    contextId             Provider,
    contextVersion        INT1
    }

CCC-ContextMark ::= EFC-ContextMark

CommunicationStatus ::=   SEQUENCE {
    timeOfLastTransmission       Time,
    pendingSince                 Time    -- pending since when
    }

DistanceRecordingStatus ::= SEQUENCE {
    odometerStatus               OdometerStatus,
    accumulatedTravelledDistance  INT4, -- in meter modulo max
    deviationFromGnss            INT1Signed --in 0.1%, positive indicates GNSS is faster,
                                 averaged over one hour, standing still periods removed
    }

GnssStatus ::= SEQUENCE {
    lastGnssFixLon           Longitude,
    lastGnssFixLat           Latitude,
    lastGnssFixTime          Time,
    currentHDOP              CurrentHDOP,
    lastLAC                  LastLAC
    }

OBEStatusHistory ::= SEQUENCE {
    statusIndicator          INTEGER{
        noGo       (0),
        go         (1)
        -- (2..255) are reserved for future use
        }          (0..255),
    timeWhenChanged          Time,
    timeWhenActived          Time,
    timeWhenObePowered       Time
    }

VehicleAxlesHistory ::=   SEQUENCE {
    timeWhenChanged          Time,
    previousVehicleAxles     VehicleAxles

    }

VehicleLicensePlateNumber ::= LPN (WITH COMPONENTS {..., licencePlateNumber (SIZE(14))})

-- NOTE: The following are the definitions of data elements in the CCC attributes:

CurrentHDOP::= SEQUENCE {
    hDOP                     INT1,      -- HDOP value, keep max
    numberOfUsedSatellites   INT1       -- Number of satellites from which a GNSS signal
is received
    }
```

```
INT1 ::= INTEGER(0..255)
INT1Signed::= INTEGER (-128..127)
INT2 ::= INTEGER(0..65535)
INT4 ::= INTEGER(0..4294967295)
INT4Signed ::= INTEGER(-2147483648..2147483647)

LastLAC ::= SEQUENCE {
    timeOfLAC                 Time,       -- Time received in the LAC
    lACOperator               Provider,   -- Operator of the LAC
    rSEId                     INT2        -- Id of the LAC RSE
    }

Latitude ::= INT4Signed   --in micro degrees, >0 =north, <0=south, absolute value shall
not exceed 90 degrees

Longitude ::= INT4Signed --in micro degrees, >0 =east, <0 =west, absolute value shall not
exceed 180 degrees

OdometerStatus::= ENUMERATED {
    odometerInterfaceNotPresent   (1),
    presentAndSignalReceived      (2),
    presentAndSignalNotReceived   (3),
    reservedForFutureUse          (4)
    }

--Note: the following is the extension of the Layer 7 module

ApplicationContextMark::= SEQUENCE {
    cCC-ContextMark           CCC-ContextMark,
    aC-CR-Reference           OCTET STRING (SIZE (2)),
    rndOBE                    OCTET STRING (SIZE (4))
}

Container::=CHOICE{
integer         [0]     INTEGER,
bitstring       [1]     BIT STRING,
octetstring     [2]     OCTET STRING (SIZE (0..127), ...),
universalString    [3] UniversalString,
beaconId        [4]     BeaconID,
t-apdu          [5]     T-APDUs,
dsrcApplicationEntityId   [6] DSRCApplicationEntityID,
dsrc-Ase-Id     [7]     Dsrc-EID,
attrIdList      [8]     AttributeIdList,
attrList        [9]     AttributeList,
time            [15]    Time,
gstrq           [17]    GetStampedRq,
gstrs           [18]    GetStampedRs,
efccontext      [32]    EFC-ContextMark,
vehlpn          [47]    LPN, -- vehicle licence plate number
vehclass        [49]    VehicleClass,
vehdims         [50]    VehicleDimensions,
vehaxles        [51]    VehicleAxles,
vehwtlims       [52]    VehicleWeightLimits,
vehspchars      [54]    VehicleSpecificCharacteristics,
equOBUId        [56]    EquipmentOBUId,
paymeans        [64]    PaymentMeans,
setmmirq        [69]    SetMMIRq,
contCCC1        [81]    VehicleAxlesHistory,
contCCC2        [82]    CommunicationStatus,
contCCC3        [83]    GnssStatus,
contCCC4        [84]    DistanceRecordingStatus,
contCCC5        [85]    ActiveContext,
contCCC6        [86]    OBEStatusHistory
--Defines the CCC Container types as the next values in the row after the efc data types
--of ISO 14906
}

END
```

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 Technical Specification 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.1 to B.14) 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.

a) **Identification of PICS**

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

b) **Identification of the implementation and/or system**

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

c) **Identification of the OBE supplier**

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

d) **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	

e) **Identification of ISO/TS 12813**

Item No.	Question	Response
1	Title, reference no., publication date	
2	ISO/TS 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) [1] ……………

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.

See Tables B.1 to B.7.

Table B.1 — Security requirements

Item no.	Element	Reference	Status	Support
1	Security level 1	EN 15509:2007, 5.1.5.3	m	
2	Authenticator calculation	EN 15509:2007, 5.1.5	m	
3	AccessCredentials calculation	EN 15509:2007, 5.1.5.3	m	

Table B.2 — 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	

[1] 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.3 — Implemented DSRC stacks

Item no.	Element	Reference	Status [a]	Support
1	CEN-DSRC	5.5.2	o.	
2	UNI DSRC	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.4 — 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.5 — 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	VehicleAxlesHistory	7.3	m			
4	CommunicationStatus	7.3	m			
5	GnssStatus	7.3	m			
6	DistanceRecording Status	7.3	m			

Table B.6 — 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	VehicleDimensions	7.4	m			
4	VehicleAxles	7.4	m			
5	VehicleWeightLimits	7.4	m			
6	VehicleSpecific Characteristics	7.4	m			

Table B.7 can be used to provide any other relevant information about the OBE relevant for testing but not covered in the above items. This may include additional features such as other communication media or other proprietary attributes for local use.

Table B.7 — Other information

Item no.	Other Information

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.

a) **Identification of PICS**

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

b) **Identification of the implementation and/or system**

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

c) **Identification of the RSE supplier**

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

d) **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	

e) **Identification of ISO/TS 12813**

Item No.	Question	Response
1	Title, reference no., publication date	
2	ISO/TS 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) [2]..............

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.

Table B.8 — Security requirements

Item No.	Element	Reference	Status	Support
1	Security level 1	EN 15509:2007, 5.1.5.3	m	
2	Authenticator calculation	EN 15509:2007, 5.1.5	m	
3	AccessCredentials calculation	EN 15509:2007, 5.1.5.3	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.9 — 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.10 — Implemented DSRC stacks

Item No.	Element	Reference	Status[a]	Support
1	CEN-DSRC	5.5.2	o	
2	UNI DSRC	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.11 — 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.12 — 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	VehicleAxlesHistory	7.3	m			
4	CommunicationStatus	7.3	m			
5	GnssStatus	7.3	m			
6	DistanceRecording Status	7.3	m			

Table B.13 — 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	VehicleDimensions	7.4	m			
4	VehicleAxles	7.4	m			
5	VehicleWeightLimits	7.4	m			
6	VehicleSpecificCharacteristics	7.4	m			

Table B.7 can be used to provide any other relevant information about the RSE relevant for testing but not covered in the above items. This may include additional features such as other communication media or other proprietary attributes for local use.

Table B.14 — Other information

Item No.	Other Information

Annex C
(informative)

Using the UNI DSRC communication stack for CCC applications

C.1 General

This annex lists the requirements for CCC application using the UNI DSRC communication stack defined in UNI 10607 as the communications media. It shows how CCC generalised communication functions are mapped onto UNI DSRC service primitives, gives an example of how CCC information types can be stored in, and information retrieved from, a UNI DSRC-compliant OBE.

The security algorithms and calculations, as well as the transaction model, should be those specified in UNI 11310, [UNI Profile], on DSRC interoperability (see Reference [14]).

C.2 UNI DSRC requirements

The following are required in order for the UNI communication stack for transferring CCC data means to be compliant with the four specifications that constitute UNI 10607 (see References [10] to [13]):

— [UNI DSRC1];

— [UNI DSRC2];

— [UNI DSRC3];

— [UNI DSRC4].

It is also recommended that the OBE equipment be compliant with UNI 11310.

C.3 Function correspondences

Table C.1 presents the correspondences between CCC functions and primitives defined in the UNI stack. Different UNI service primitives are used to access data that are located in different memory regions.

After the first interaction to initialise the communication link, an A-SLT service request should be 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.

These recommendations are implemented in the transaction example given in C.5.

The address of the CCC application (AID parameter) corresponds to the Called AP Invocation Identifier parameter in the A-Associate service primitive.

Table C.1 — Functions correspondences

CCC Function	UNI primitive(s)
Initialise communication	A-Associate, [UNI DSRC3], concatenated with A-Get_Nonce, [UNI DSRC4]
Data retrieval	*Data location* *Service primitive* Master core Get_Context, [UNI DSRC3] Master record Get_Context_Record, [UNI DSRC4] Application core Get_ASO_Context, [UNI DSRC3] Application record GET [UNI DSRC3]
Authenticated data retrieval	Concatenation of: Get_Credentials, [UNI DSRC4] A Get operation (according to the requested data, see GET above in this table)
Driver notification	A-Alert_Extrn, [UNI DSRC4]
Terminate communication	A-Release [UNI DSRC3]
Test communication	A-SLT [UNI DSRC3]

C.4 Data storage and retrieval

C.4.1 Data storage

The main characteristics of OBE data addressing in the UNI standards is that data are referenced by position, i.e. by specifying their location in the OBE virtual memory (whose structure is described in [UNI DSRC4]). Table C.2 presents an example of how CCC application data could be referenced. In no way should it be assumed that the choice of CCC attributes or the memory structure depicted in Table C.2 represents a real implementation. The choice of data types to be used for CCC application, and their positioning in the OBE memory structure, are to be defined in an appropriate CCC interoperability profile.

Table C.2 — Example of OBE storing of CCC data

Application context/field			Field length (octets)	Description
Master	header	core-len	1	Core length = 5.
		record-len	1	Record length = 11 octets.
		record-number	1	There is 1 record (in case of only CCC application present in the OBE).
		current-record	1	The current record (addressed application) is the first one.
	core		5	OBE-specific (manufacturer) information (reserved).
	record 1	application-id	2	This is the CCC Application identifier.
		reserved	1	
		EFC-ContextMark	6	ISO 14906, AttrId 0.
		AC_CR-KeyReference	2	Reserved for key reference for AC-CR, see [EFC IAP] [a].
CCC Application	header	core-len	1	Core length = 53
		record-len	1	Record length = 42 octets + k (length of GnssStatus) +ActiveContexts length
		record-number	1	There is 1 record
		current-record	1	The current record is the first one
	core	VehicleLicencePlateNumber	17	ISO 15509
		VehicleClass	1	ISO 14906, AttrId 17
		VehicleAxles	2	ISO 14906, AttrId 19
		VehicleWeightLimits	6	ISO 14906, AttrId 20
		CommunicationStatus	8	CCC specific attribute
		PaymentMeans	14	ISO 14906, AttrId 32
		EquipmentOBUId	5	ISO 14906, AttrId 24
	record 1	StatusIndicator	1	CCC specific attribute
		TimeWhenChanged	4	CCC specific attribute
		TimeWhenActivated	4	CCC specific attribute
		TimeWhenObePowered	4	CCC specific attribute
		VehicleAxlesHistory	6	CCC specific attribute
		GnssStatus	k	CCC attribute
		DistanceRecordingStatus	3	CCC specific attribute
		OBEStatusHistory	13	CCC specific attribute
		VehicleDimensions	3	ISO 14906, AttrId 18
		VehicleSpecificCharacteristics	4	ISO 14906, AttrId 22
		ActiveContexts	2n	CCC specific attribute. Length is a variable multiple of 2 including 0.

Reading or writing of the above data is performed by a set of functions that is specific for each identified memory region, namely: Master Core, Master Record, Application Core and Application Record (see [UNI DSRC3] and [UNI DSRC4]). The means of accessing the above data is specified in C.4.2.

[a] Electronic fee collection (EFC) interoperability application profile (IAP) for DSRC, EN 15509.

C.4.2 Data retrieval

Table C.3 shows how to access data with the functions defined above.

Table C.3 — Example data access

CCC Attribute	Access via UNI communication primitives
EFC-ContextMark	Get_Master_Record (Offset=3, Length=6)
AC_CR-KeyReference	Get_Master_Record (Offset=9, Length=2)
VehicleLicence PlateNumber	Get_ASO_Context (Offset=0, Length=17)
VehicleClass	Get_ASO_Context (Offset=17, Length=1)
VehicleAxles	Get_ASO_Context (Offset=18, Length=2)
VehicleWeightLimits	Get_ASO_Context (Offset=20, Length=6)
CommunicationStatus	Get_ASO_Context (Offset=26, Length=8)
PaymentMeans	Get_ASO_Context (Offset=34, Length=14)
EquipmentOBUId	Get_ASO_Context (Offset=48, Length=4)
StatusIndicator	Get (Offset=0, Length=1)
TimeWhenChanged	Get (Offset=1, Length=4)
TimeWhenActivated	Get (Offset=5, Length=4)
TimeWhenObePowered	Get (Offset=9, Length=4)

Reading or writing multiple attributes in a single instance of a service primitive (Get or Set) is possible in the UNI case for attributes that are stored sequentially in the same memory region. This can be accomplished by specifying a displacement corresponding to the first attribute to be read or written, and a length equal to the sum of the attributes' lengths.

EXAMPLE Getting the OBEStatusHistory attribute, which is made of Status Indicator, TimeWhenChanged, TimeWhenActivated and TimeWhenObePowered, can be accomplished by means of a Get (Where=Current, Offset=0, Length=13).

C.5 CCC transaction example

C.5.1 General

In this example, the RSE uses the PaymentMeans field to calculate the OBE authenticator, and the random number received by the OBE, together with the AC_CR-KeyReference field, to compute its authenticator.

The memory structure of the OBE for this example is as indicated in Table C.2.

The transaction is performed in two phases: initialisation and data retrieval. There is no prescription on how DSRC interactions should be split in the two phases, nor any limit to the number of DSRC interactions, the only limitation being the amount of application data exchanged in a single DSRC interaction.

a) In the first phase, a connection is established between the RSE and the OBE, some information is retrieved, including the EFC-ContextMark and the AC_CR-KeyReference, and the RSE calculates its authenticator. These operations are performed in a single DSRC interaction.

b) In the second phase, the RSE authenticates itself, asks for OBE authentication, and asks for some information, including CommunicationStatus, PaymentMeans, EquipmentOBUId, and other CCC specific attributes stored in the Application Record (see Table C.2). MMI signals are then transmitted to the OBE for display. These operations are performed by three DSRC interactions.

The transaction flow is shown in terms of the interactions that take place between the RSE and the OBE.

C.5.2 Initialisation phase

This interaction is aimed at retrieving the following public and private OBE information:

— RndOBE

— EFC-ContextMark

— AC_CR-KeyReference

The RSE reads the EFC-ContextMark and AC_CR-KeyReference fields by means of a concatenated set or primitives. The sequence of service primitives and related exchanges of protocol messages is presented in Table C.4.

Table C.4 — Example Initialisation phase

RSE		Protocol Message		OBE
A-Associate.Request	→	Open-Rq	→	A-Associate.Indication
A-Get_Nonce.Request		Get-TBA-Random-Rq		A-Get_Nonce.Indication
(Length='4'D)		(Length=’4’D)		(Length=’4’D)
A-Get_Context_Record.Request		Get-Mast-Rec-Rq		A-Get_Context_Record.Indication
(Offset=’3’D, Length=’8’D)		(Offset=’3’D, Length=’8’D)		(Offset=’3’D, Length=’8’D)
A-Release.Request		Close-Rq		A-Release.Indication
A-Get_Nonce.Confirm	←	Get-TBA-Random-Rs	←	A-Get_Nonce.Response
(Data)		(Data)		(Data)
A-Get_Context_Record.Confirm		Get-Mast-Rec-Rs		A-Get_Context_Record.Response
(Data)		(Data)		(Data)

On receipt of the requested information, the following data processing is performed on the RSE side:

Calculation of RSE access credentials, using the RndOBE and the AC_CR-KeyReference fields (see the UNI DSRC Interoperability profile [UNI Profile]).

C.5.3 Data retrieval phase

This interaction is aimed at transmitting the RSE authenticator, verifying the OBE authenticator and retrieving the following public and private OBE information:

— CommunicationStatus;

— PaymentMeans;

— issuer authenticator calculated on PaymentMeans and KeyRef_Iss (1);

— EquipmentObuID;

— StatusIndicator;

— TimeWhenChanged;

— TimeWhenActivated;

— TimeWhenObePowered.

The following information is transmitted from the RSE to the OBE:

Operator Authenticator calculated on EFC-ContextMark and KeyRef_Op (1).

The interaction is performed in three sub-phases, corresponding to three different protocol exchanges.

In the first interaction, the RSE selects the specified OBE, issues its credentials, requires the OBE credentials by offering a random value and selecting key reference = 1 (no key is specified in the A-Get_Credentials.Request), and reads the CommunicationStatus, the PaymentMeans and the EquipmentObuID fields by means of a set of concatenated primitives. The sequence of service primitives and related exchanges of protocol messages in the first interaction is presented in Table C.5.

Table C.5 — Example Data retrieval phase: first interaction

RSE		Protocol message		OBE
A-Associate.Request		Open-Rq		A-Associate.Indication
A-SLT.Request		Select-TBA-Id-Rq		A-SLT.Indication
(Tba-length=’4’D, Tba-id)		(Tba-length=’4’D, Tba-id)		(Tba-length=’4’D, Tba-id)
A-Set_Credential.Request		Set-Credential-Rq		A-Set_Credential.Indication
(Length=’4’D, Credential)		(Length=’4’D, Credential)		(Length=’4’D, Credential)
A-Get_Credential.Request	→	Get-Credential-Rq	→	A-Get_Credential.Indication
(Offset=’0’D, Length=’14’D,		(Offset=’0’D, Length=’14’D,		(Offset=’0’D, Length=’14’D,
NonceLength=’4’D, Nonce)		NonceLength=’4’D, Nonce)		NonceLength=’4’D, Nonce)
A-Get_ASO_Context.Request		Read-Appl-Core-Rq		A-Get_ASO_Context.Indication
(Offset=’26’D, Length=’26’D)		(Offset=’26’D, Length=’26’D)		(Offset=’26’D, Length=’26’D)
A-Release.Request		Close-Rq		A-Release.Indication
A-Get_Credential.Confirm		Get-Credential-Rs		A-Get_Credential.Response
(Authenticator)		(Authenticator)		(Authenticator)
A-Get_ASO_Context.Confirm	←	Read-Appl-Core-Rs	←	A-Get_ASO_Context.Response
(CommunicationStatus, PaymentMeans and EquipmentObuID)		(CommunicationStatus, PaymentMeans and EquipmentObuID)		(CommunicationStatus, PaymentMeans and EquipmentObuID)

On receipt of the requested information, the following data processing is performed on the RSE side:

— check if PaymentMeans and/or EquipmentObuID is/are in white list;

— check the CommunicationStatus.

After this first interaction, the RSE has two choices:

a) perform further checks by requesting and verifying other attributes, or

b) decide that the OBE is non-compliant, issue a warning alert and close the transaction.

In the following, it is assumed that the first interaction does not show any compliance problems, so the second interaction is initiated. The following attributes are requested: StatusIndicator, TimeWhenChanged, TimeWhenActivated and TimeWhenObePowered.

For the purposes of this example, the RSE issues again its credentials, e.g. for security reasons. There is no need, however, for it to ask again for the OBE's credentials, as the OBE is explicitly addressed by means of an A-SLT primitive.

The sequence of service primitives and related exchanges of protocol messages in the second interaction is presented in Table C.6.

Table C.6 — Example data retrieval phase — Second interaction

RSE		Protocol message		OBE
A-Associate.Request	→	Open-Rq	→	A-Associate.Indication
A-SLT.Request		Select-TBA-Id-Rq		A-SLT.Indication
(Tba-length='4'D, Tba-id)		(Tba-length='4'D, Tba-id)		(Tba-length='4'D, Tba-id)
A-Set_Credential.Request		Set-Credential-Rq		A-Set_Credential.Indication
(Length='4'D, Credential)		(Length='4'D, Credential)		(Length='4'D, Credential)
A-Get.Request		Read-Appl-Record-Rq		A-Get.Indication
(Offset='0'D, Length='13'D)		(Offset='0'D, Length='13'D)		(Offset='0'D, Length='13'D)
A-Release.Request		Close-Rq		A-Release.Indication
A-Get.Confirm	←	Read-Appl-Record-Rs	←	A-Get.Response
(Data)		(Data)		(Data)

On receipt of the requested information, the attributes are examined for compliance.

According to the results of the compliance check, different MMI commands may be issued to the OBE. This is done in the third sub-phase with a separate DSRC interaction.

For security reasons, in this example the RSE again issues its credentials by means of an A-Set_Credential service primitive, and alerts the user with an A-Alert-Extrn.Request service primitive. The values of the parameters in the A-Alert-Extrn.Request service primitive depend on the result of the compliance check done in the previous interactions. The sequence of service primitives and related exchanges of protocol messages is presented in Table C.7.

Table C.7 — Example Data retrieval phase — Third interaction

RSE		Protocol message		OBE
A-Associate.Request	→	Open-Rq	→	A-Associate.Indication
A-SLT.Request		Select-TBA-Id-Rq		A-SLT.Indication
(Tba-length='4'D, Tba-id)		(Tba-length='4'D, Tba-id)		(Tba-length='4'D, Tba-id)
A-Set_Credential.Request		Set-Credential-Rq		A-Set_Credential.Indication
(Length='4'D, Credential)		(Length='4'D, Credential)		(Length='4'D, Credential)
A-Alert-Extrn.Request		Set-UIF-Rq		A-Alert-Extrn.Indication
(Video-action, Audio-action, number-of-second, count)		(Video-action, Audio-action, number-of-second, count)		(Video-action, Audio-action, number-of-second, count)
A-Release.Request		Close-Rq		A-Release.Indication
A-Release.Confirm (Result, Diagnostic)	←	(No data, only Result and Diagnostic fields)	←	A-Release.Response (Result, Diagnostic)

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 OBE and RSE shall comply with ISO 21214 in the compatibility mode.

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

D.3 Functions

The CCC specific functions shall be implemented in accordance with Clause 6.

D.4 Data requirements

The addressing of the EFC system and application data implemented by the OBE and RSE shall conform to the rules given in ISO 14906:2004, 5.3. For CCC application data only one context is supported. Multiple instances of attributes are not supported.

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

The RSE shall support any OBE that is otherwise compliant.

D.5 Security requirements

The security requirements shall be in accordance with 6.2.

D.6 Transaction requirements

The transaction requirements shall be the same as described 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 shall comply with 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 shall be implemented as DSRC Layer 7 services as defined in ARIB-T75:2001, 4.4.2.1.2.

The SET service is not supported by the CCC application.

GET and GET_STAMPED shall 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 shall conform to the rules defined in section 5.3 in ISO 14906:2004, 5.3. For CCC application data, EID shall always be used. Multiple instances of attributes are not supported.

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

The RSE shall 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 shall comply with ISO 14906:2004, 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 shall be used for the CCC application. There shall be only one instance of AID=20 in the BST.

The CCC application shall be qualified as a mandatory application.

E.6.2.2 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 ApplicationContextMark as defined in ISO 15628:2007, Annex A, corresponding to Security Level 1.

Numbering of AID should be according to ISO 15628 (where AID from 0 to 19 are already defined).

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 Technical Specification 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.

Table F.1 — Example compliance check communication (CCC) transaction

Phase	Roadside Equipment		On-board equipment	Remarks
Initialisation	INITIALISATION.request (BST)	→		RSE periodically sends BST.
(BST – VST)		←	INITIALISATION.response (VST) • CCC-ContextMark • 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 — VehicleLicensePlateNumber — 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 (KeyRefAuth). Retrieval of data from the OBE: remaining identification data and static vehicle data.
		←	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, 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, 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 Technical Specification.

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.

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 Technical Specification);
- 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 Technical Specification)].

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** [3]

      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**

   Protection against false claims by the toll charger [4]

   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 is 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.). In accordance with local legislation, toll chargers should keep no record of the checked transaction when the transaction indicates that the road is used in compliance with the rules.

   3) **Non-authorised 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.

[3] Optional and not strictly needed for compliance checking.

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.	—

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

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 STD-T75, *Dedicated Short-Range Communication*[4)]

[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*[5)]

[8] ISO/TS 17574, *Road transport and traffic telematics — Electronic fee collection (EFC) — Guidelines for EFC security protection profiles*

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

[10] UNI 10607-1:2007, *Road Traffic and Transport Telematics — Automatic Dynamic Debiting Systems and Automatic Access Control Systems Using Dedicated Short-range Communication at 5.8 GHz Part 1: Physical Layer*. [UNI DSRC1] [6)]

[11] UNI 10607-2:2007, *Road Traffic and Transport Telematics — Automatic Dynamic Debiting Systems and Automatic Access Control Systems Using Dedicated Short-range Communication at 5.8 GHz Part 2: Data Link Layer.* [UNI DSRC2] [6)]

[12] UNI 10607-3:2007, *Road Traffic and Transport Telematics — Automatic Dynamic Debiting Systems and Automatic Access Control Systems Using Dedicated Short-range Communication at 5.8 GHz Part 3: Application Layer Service Elements*. [UNI DSRC3] [6)]

[13] UNI 10607-4:2007, *Road Traffic and Transport Telematics — Automatic Dynamic Debiting Systems and Automatic Access Control Systems Using Dedicated Short-range Communication at 5.8 GHz Part 4: The Electronic Fee Collection Service Object*. [UNI DSRC4] [6)]

[14] UNI 11310, *Road traffic and transport Telematics — Automatic Dynamic Debiting Systems and Automatic Access Control Systems using dedicated short-range communication at 5.8 GHz —- Interoperability Application Profile for EETS.* [UNI Profile] [6)]

[4)] Association of Radio Industries and Business (ARIB) of Japan standard.

[5)] To be published. (Revision of ISO/TS 17573:2003)

[6)] English versions of these Italian national standards are available.

ICS 03.220.20; 35.240.60

Price based on 44 pages