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)

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order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn.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.

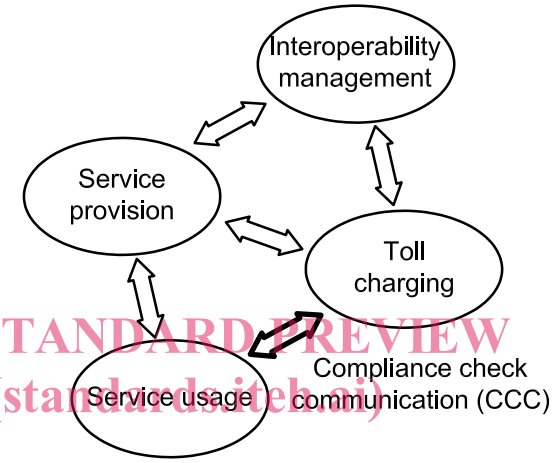


Figure 1 — Compliance check communication in EFC architecture as per ISO 17573

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,

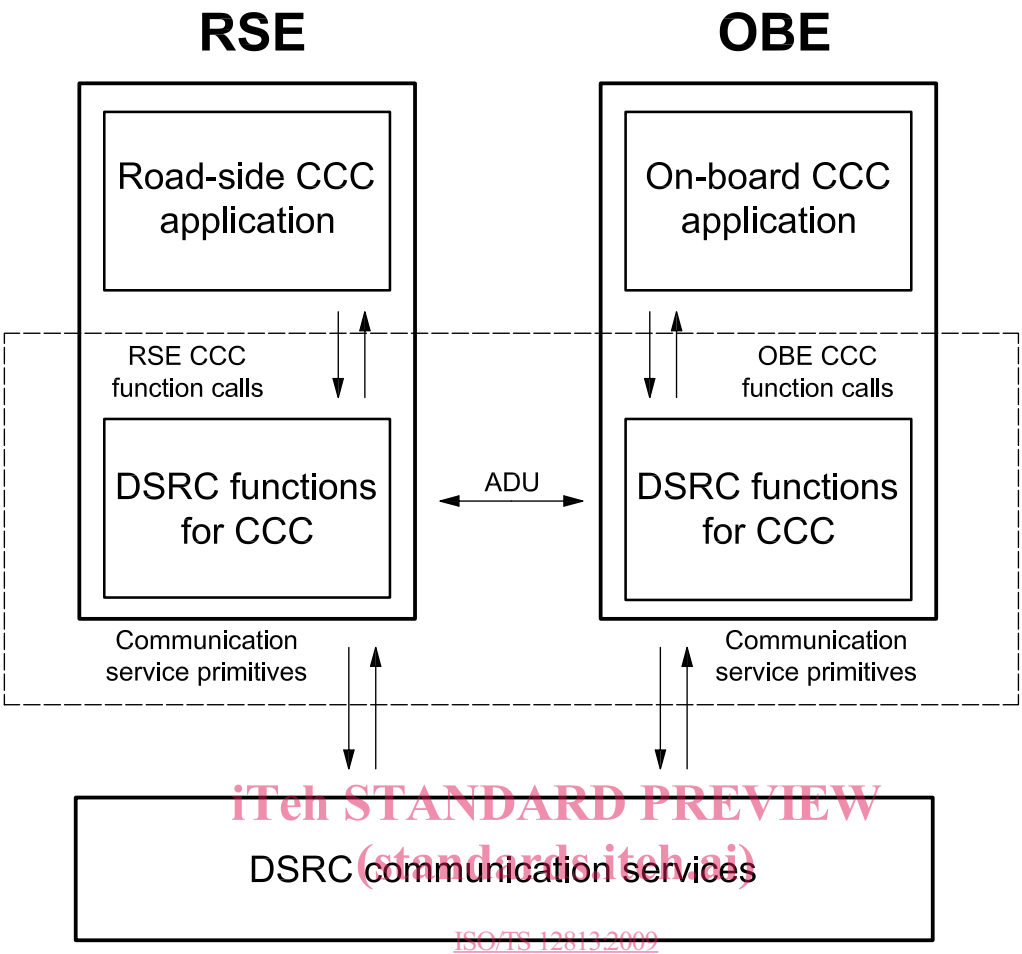
— use of the generic DSRC application layer as specified in ISO 15628 and EN 12834,

— 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.