TECHNICAL SPECIFICATION

ISO/TS 13141

First edition
2010-02-15

Electronic fee collection — Localisation augmentation communication for autonomous systems

Perception de télépéage — Communications d'augmentation de localisations pour systèmes autonomes

Reference number
ISO/TS 13141:2010(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order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn.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/TS 13141 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 ISO/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-based positioning to collect data required for charging for the use of roads operate in a so-called autonomous way (i.e. generally without relying on dedicated road-side infrastructure). However, these autonomous systems can, in particular places, need some road-side infrastructure support for proper identification of charge objects. Such assistance might be required at places where satellite-based localisation accuracy or availability is insufficient or at places where the OBE is directly informed about the identity of the relevant charge object.

In an interoperable environment, it is essential that this localisation information be available in a standardized way. This Technical Specification defines requirements for localisation augmentation by dedicated short-range communication (DSRC) between road-side equipment and on-board equipment. This Technical Specification makes no assumptions about the operator of the road-side equipment, in terms of his role according to ISO 17573, i.e. whether the road-side equipment is operated by an entity in the Service Provision role or in the Toll Charging role.

This Technical Specification has been prepared considering the following requirements:

— the localisation augmentation communication (LAC) serves to transmit localisation information to passing OBE without identifying individual OBE;

— the localisation information contains both geographical location independent of charging context, and context-dependent identification of charge objects;

— a single road-side installation is able to provide localisation augmentation for several overlapping EFC contexts;

— this Technical Specification is according to the EFC architecture specified in ISO 17573;

— the communication applies to all OBE architectures;

— this Technical Specification is applicable to various DSRC media, including the CEN DSRC stack;

— the communication supports security services for data origin authentication, integrity and non-repudiation.

This Technical Specification defines an attribute, LACData, which is communicated from the roadside to the OBE by means of an acknowledged writing service, which is implemented through the SET service of DSRC Layer 7 (ISO 15628 and EN 12834). The LAC application is defined as a self-contained DSRC application with its own application identifier (AID). Regarding the DSRC communications stack, this Technical Specification gives definitions for the CEN DSRC stack, as used in EN 15509 and the Annexes C, D and E demonstrate the use of ISO CALM IR, UNI DSRC and ARIB DSRC.

All data relevant for the LAC application have been put into the attribute LACData, in order to create a single standard communications content transmitted by all road-side equipment, and always signed as a whole. LACData can transport both geographic coordinates (Lat, Long, Alt) and the identification of a specific charge object. All elements of LACData are mandatory, but Null values are defined to allow LAC installations to transmit only a selection of all defined data elements.

Access credentials are mandatory for writing LACData in order to protect OBE from non-authentic road-side equipment. LACData are critical for charge determination and need to have evidentiary quality. For these purposes, the authenticators which are defined can be used to provide for data origin authentication, data integrity and non-repudiation for LACData. There are two separate authenticator fields defined to allow for separate authentication and non-repudiation, if required by the institutional arrangements of a toll system.

This Technical Specification is minimal, in order to be able to cover what is required by operational EFC systems and systems planned in the foreseeable future.

Electronic fee collection — Localisation augmentation communication for autonomous systems

1 Scope

This Technical Specification establishes requirements for short-range communication for the purposes of augmenting the localisation in autonomous electronic fee collection (EFC) systems. Localisation augmentation serves to inform OBE about geographical location and the identification of a charge object. This Technical Specification specifies the provision of location and heading information and security means to protect from the manipulation of the OBE with false road-side equipment (RSE).

The localisation augmentation communication takes place between an OBE in a vehicle and fixed road-side equipment. This Technical Specification is applicable to OBE in an autonomous mode of operation.

This Technical Specification defines attributes and functions for the purpose of localisation augmentation, by making use of the DSRC communication services provided by DSRC Layer 7, and makes these LAC attributes and functions available to the LAC applications at the RSE and the OBE. Attributes and functions are defined on the level of ADUs (Application Data Units, see Figure 1).

As depicted in Figure 1, this Technical Specification is applicable to:

— the application interface definition between OBE and RSE;

— the interface to the DSRC application layer, as specified in ISO 15628 and EN 12834;

— the use of the DSRC stack.

The localisation augmentation communication is suitable for a range of short-range communication media. This Technical Specification gives specific definitions regarding the CEN DSRC stack as used in EN 15509, and Annexes C, D and E give the use of ISO CALM IR, UNI DSRC and ARIB DSRC.

This Technical Specification contains a protocol implementation conformance statement (PICS) proforma and informative transaction examples. This Technical Specification is not applicable to test specifications.

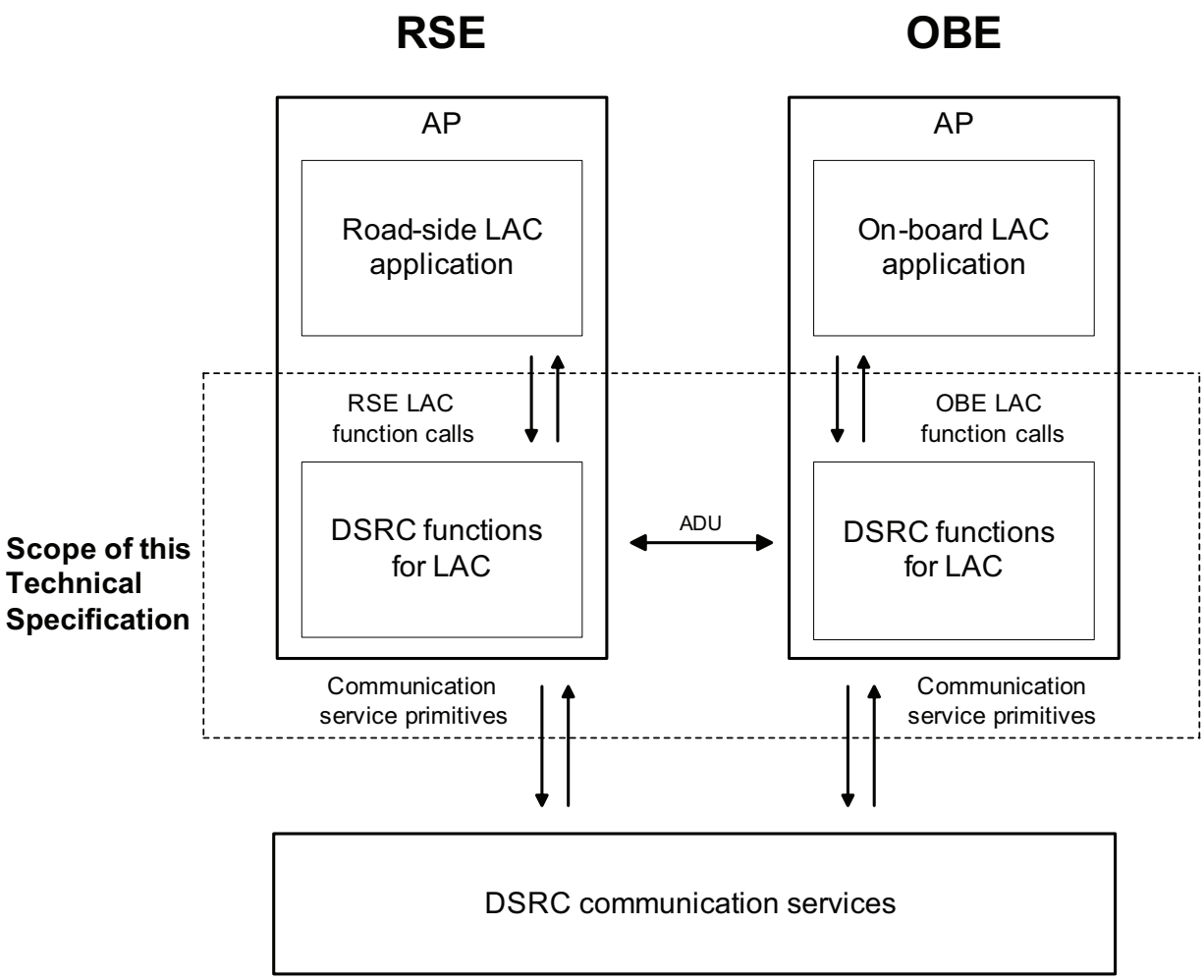

Figure 1 — The LAC application interface

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/TS 12813, *Electronic fee collection — Compliance check communication for autonomous systems*

ISO 14906:—[1)], *Road transport and traffic telematics — Electronic fee collection — Application interface definition for dedicated short-range communication*

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

ISO/IEC 8824-1:2002, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

1) To be published. (Revision of ISO 14906:2004).

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

EN 12834, *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 are transferred to on-board equipment in order to establish the claimed identity of a road-side equipment application process entity

[ISO 14906]

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

NOTE Adapted from ISO 14906:—, definition 3.3.

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

NOTE Adapted from ISO 14906:—, definition 3.4.

3.4
charge object
geographic object where a charge for the use of infrastructure is due according to the definition in the toll regime

3.5
contract
expression of an agreement between two or more parties concerning the use of the road infrastructure

[ISO 14906]

3.6
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[ISO 14906]

3.7
road-side equipment
equipment installed at a fixed position along the road transport network, for the purposes of communication and data exchange with the on-board equipment of passing vehicles

[ISO 14906]

3.8
on-board equipment
equipment located within the interrogated vehicle and supporting the information exchange with the road-side equipment

3.9
service
toll service
service enabling users having a contract and an OBE to use a vehicle in one or more toll domains

3.10
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.

3.11
toll regime
set of rules defining a toll scheme, i.e. the rules defining the charge and the charging processes for a specific road-user charging measure

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

3.13
transaction
whole of the exchange of information between the road-side equipment and the on-board equipment necessary for the completion of a toll or compliance checking operation

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

ADU Application data unit (see ISO 14906)

AID Application identifier (see ISO 15628 and EN 12834)

ASN.1 Abstract syntax notation one (see ISO/IEC 8824-1:2002)

BST Beacon service table (see ISO 14906)

CCC Compliance check communication

DSRC Dedicated short-range communication (see ISO 14906)

EID Element identifier (see ISO 15628 and EN 12834)

EFC Electronic fee collection (see ISO 14906)

IR Infrared

LAC Localisation augmentation communication

MAC Media Access control (see ISO 14906) or Message authentication code

OBE On-board equipment (see ISO 14906)

PICS Protocol implementation conformance statement

RSE Road-side equipment (see ISO 14906)

VST Vehicle service table (see ISO 14906)

5 Application interface architecture

5.1 General

This clause gives an insight into the LAC architecture by identifying the functions, the use of DSRC communication primitives, and the attributes addressed. A detailed description of the functions is given in Clause 6, while details of the attributes are in Clause 7.

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

5.2 Services provided

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

— writing of data in order for the RSE to communicate location data to the OBE;

— authentication of the RSE by the OBE by means of access credentials.

There is no read service provided within the LAC communication. The RSE transmits data to the OBE using the underlying acknowledged communication services, in order to verify that the data indeed are properly transmitted over the DSRC interface.

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

The services are provided by the following functions:

— the “Initialise communication” function, which is used to establish the LAC communication link between the RSE and OBE;

— the “Write data” function, which is used to send LAC attributes to the OBE;

— the “Terminate communication” function, which is used to terminate the LAC communication.

5.3 Attributes

There is a single attribute defined for localisation augmentation. This attribute contains a set of data in order for the OBE to be able to determine its localisation with better accuracy and availability or to directly receive a charge object identification related to the local toll context. This set of data contains:

— geographic coordinates (latitude, longitude and altitude);

— charge object reference.

When the RSE writes this attribute to the OBE, it shall transmit geographic coordinates or charge object reference or both.

5.4 Contract and toll context

Regarding LAC, the OBE shall identify itself in the initialisation phase with a single LAC Context Mark in the VST. This Context Mark identifies the user contract in terms of the service provider, type of contract and version information. This information enables the RSE to decide whether the OBE carries a contract which it can support, and if so, to choose the corresponding security elements.

A RSE can provide the OBE with localisation augmentation for several overlapping contexts simultaneously, by writing the LAC attribute (which includes the applicable toll context) several times in one transaction.

NOTE The LAC works in a broadcast fashion, where the roadside has only minimal information about the OBE and is not able to assess the liability of a vehicle for tolls. For this reason, the OBE can receive LAC information which is not applicable.

5.5 Use of lower layers

5.5.1 Supported DSRC communication stacks

The LAC 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 Annexes C, D and E.

Table 1 — Supported short-range communication stacks

Medium	Application layer	Lower layers	Detailed specifications
CEN-DSRC	ISO 15628 and EN 12834	EN 12795 EN 12253	Specification in 5.5.2
Italian UNI DSRC	UNI 10607-4:2007 UNI 10607-3:2007	UNI 10607-2:2007 UNI 10607-1:2007	Example implementation in Annex C
ISO CALM IR	ISO 15628 and EN 12834	ISO 21214	Example implementation in Annex D
ARIB DSRC	ARIB STD-T75 and 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, the OBE shall respond to RSE interrogations on the same medium as the RSE has used.

5.5.2 The use of the CEN DSRC stack

The LAC application shall be used with the CEN DSRC communication stack in the following ways:

— the OBE shall comply with EN 15509:2007, 5.1.2;

— the RSE shall comply with EN 15509:2007, 5.2.2.

Compliance with EN 15509 implies compliance of the DSRC stack with ISO 15628 and EN 12834 regarding the application layer, and EN 12795 and EN 12253 for the lower layers.

6 Functions

6.1 Functions in detail

6.1.1 General

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

For CEN-DSRC, the functions shall be provided by the DSRC application layer as specified in ISO 15628 and EN 12834 (services INITIALISATION, SET and RELEASE).

Only the functions for CEN DSRC are defined in 6.1.2 to 6.1.4. 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 Initialising communication

Initialisation of the communication shall be carried out 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. the beacon serial number) and absolute time. The initialisation notification on the RSE side shall carry the LAC application identity and also the data required for the security services (e.g. random number and 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 (see LAC-InitialiseComm-Request and LAC-InitialiseComm-Response).

6.1.3 Writing of data

The function “Write data” shall be provided by the application layer SET service as specified in ISO 15628 and EN 12834, and is defined in Annex A (see LAC-DataTx-Request and LAC-DataTx-Response).

NOTE The “mode” parameter in the LAC-DataTx-Request indicates whether or not the corresponding response is expected. If mode=false, the response primitive is not used and the reception is only acknowledged by the OBE on lower layers.

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

The SET shall always carry access credentials.

6.1.4 Termination of 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 the application level.

NOTE 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, and is defined in Annex A (see LAC-TerminateComm).

6.2 Security

6.2.1 General

Security is an essential part of LAC applications. This specification provides for both communication-related security services and communication-transparent data elements, which may provide security characteristics.

This specification for localisation augmentation communication provides for a “Write data” function and uses access credentials as a mandatory communication security provision. Access credentials provide for protection against unauthorized writing of LAC data, and hence for authentication of the LAC RSE and the LAC data to the OBE. The detailed implementations of the communication security services are media-specific (see 6.2.2 for CEN DSRC and the annexes for other media).

NOTE 1 Authentication of the OBE to the RSE according to EN 15509 is not supported, as the identity of the OBE and contract are not relevant for the LAC application.

This specification provides for data elements, which may provide data origin authentication, data integrity and non-repudiation characteristics to the LAC Data. The LAC application is transparent to these authenticators, which may be stored together with the other LAC data elements as a data packet, which is protected against forgery and/or protected against repudiation (between e.g. the user and the LAC Operator).

NOTE 2 This specification does not provide for an encryption service. No privacy sensitive data are transferred by LAC.

6.2.2 Authentication of RSE: access credentials

Access credentials shall be used to manage access to the LAC attribute. Access credentials are mandatory. The “Write data” function shall always carry access credentials.

The CEN DSRC OBE shall support the calculation of access credentials according to security level 1, as defined in EN 15509:2007, 5.1.5.3.

The CEN DSRC RSE shall be able to calculate access credentials according 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.

6.2.3 Authentication of LAC Data

The data elements MAC1 and MAC2 (see 7.5) may contain authenticators, as well as key references for the calculation of those authenticators, and are provided as a means to guarantee data origin authentication, integrity and non-repudiation characteristics to the LAC data.

The two data elements are provided to allow for separate elements for authentication and non-repudiation, if required. The LAC application is transparent to these authenticators, which implies that it supports various system security concepts.

The data elements MAC1 and MAC2 are defined as being of ASN.1 type OCTET STRING. The semantics of the data elements are media-independent.

7 Attributes

7.1 General

Within the LAC context, the attributes and data elements given in Table 2 shall be made available.

Table 2 — Supported short-range communication stacks

AttributeID[a]	Attribute	Data element	Length in Octets[b]
n.a.	LAC-ContextMark	ContractProvider	3
		TypeOfContract	2
		ContextVersion	1
54	LACData	LACOperator	3
		RSEId	2
		Latitude	4
		Longitude	4
		Altitude	2
		TollCharger	6
		ChargeObject	10
		DistanceToObject	2
		LACTime	4
		MAC1	1+8
		MAC2	1+8
87-127	ReservedForPrivateUse	—	—

[a] The assignment of attribute IDs is aligned with ISO 14906 and ISO/TS 12813. Attributes 87 to 127 are assigned for private use. All other remaining IDs are reserved for future use.

[b] Length information is informative. For the type OCTET STRING, the length determinant, as defined in ISO/IEC 8825-2, is explicitly stated.

The attribute LAC-ContextMark shall be part of ApplicationContextMark as specified in Annex A.

NOTE LAC-ContextMark is not an addressable attribute. It is part of the VST and can neither be read nor written by the RSE as part of the LAC application.

In the following clauses, LAC Attributes and data elements are specified in terms of

— the names of the data elements forming the LAC 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 location reference

The data element Latitude shall contain the latitudinal coordinate of the centre of the road surface covered by the specific LAC implementation, in micro degrees, using the reference model WGS84. The data type shall be as defined in ISO/TS 12813.

The data element Longitude shall contain the longitudinal coordinate of the centre of the road surface covered by the specific LAC implementation, in micro degrees, using the reference model WGS84. The data type shall be as defined in ISO/TS 12813.

The data element Altitude shall contain the altitudinal coordinate of the centre of the road surface covered by the specific LAC implementation, in 0,25 m resolution.

In case no geographic coordinates are provided, a coding of all zero shall be used (Latitude, Longitude and Altitude equal to zero).

NOTE 1 The location indicated by the coding for “no geographic coordinates provided” is not on land surface and does not need to be supported.

The data element ChargeObject shall identify the charge object for which LAC is operated, according to the local definition of the Toll Charger owning the respective toll scheme. The data element is the same as ChargeObjectId defined in CEN ISO/TS 17575-1. It shall contain the Toll Charger's identifier of the toll regime it belongs to (regimeId), and a designation (chargeObjectDesignation).

In case no toll charger dependent information is provided, a coding of all zero shall be used (TollCharger and ChargeObjectId equal to zero).

NOTE 2 The data element ChargeObjectId can be used to identify any kind of charge object, e.g. road section, passage of cordon. Identification of lanes can be provided in accordance with the restrictions of the communication medium.

The data element DistanceToObject, shall contain the distance, in metres, to the charge object as identified by the element ChargeObjectId, from the point of operation of the LAC. Negative values indicate that the charge object precedes the RSE in the sense of direction of traffic.

NOTE 3 In order to avoid charging errors, it is advisable to not allow vehicles to exit to another road after receiving the LAC message and without using the charge object.

7.3 Operational data

The data element LACOperator shall identify the organization that operates LAC, i.e. the entity responsible for data content of the LAC transaction. The data element is as defined in ISO 14906. It contains the country code and the Id of the operator assigned on a national basis.

The data element RSEId shall contain an operator-specific identification of the RSE which operates LAC.

The data element TollCharger shall identify the Toll Charger which owns the toll scheme for which LAC is operated. The data element is as defined CEN ISO/TS 17575-1.

The data element LACTime shall contain the time at which the LAC transaction occurred. The data element is as defined in ISO 14906.

7.4 OBE contractual data

The data element LAC-ContextMark shall identify the user contract in terms of the service provider, type of contract and version information. It is the same as the EFC-ContextMark defined in ISO 14906.

The coding and usage of this data element is service-provider specific. It shall be used as a minimum to manage and distinguish OBE supporting different future versions of this Technical Specification and to identify the related LAC security elements.

NOTE It is assumed that the OBE supports only this edition of this Technical Specification (in order to reduce the OBE's complexity) and that the LAC RSE will support all existing OBE conforming to different editions of this Technical Specification.

7.5 Security-related data

The data elements MAC1 and MAC2 may contain security-related data regarding the other nine data elements of the attribute LACData. This may comprise authenticators, as well as key references. The calculation, the coding and the applicability of those data elements are outside of the scope of this Technical Specification.

8 Transaction model

8.1 General

The transaction model related to the LAC Application Interface for DSRC shall comply with ISO 14906, Clause 6, with the restrictions and amendments defined in 8.2 and 8.3, for implementation using the CEN DSRC communication stack. Details on the transaction model and addressing for other communication media (if any) are given in the relevant annexes.

The transaction model comprises two phases, the initialisation phase and the transaction phase.

8.2 Initialisation phase

8.2.1 Initialisation phase — General

Initialisation of the communication shall be carried out by the RSE by means of the function “Initialise communication”.

The OBE evaluates the initialisation request to decide whether the LAC application is supported. If the OBE does not support the LAC application, it shall not respond to the initialisation request. If the OBE supports the LAC application, a response is mandatory.

8.2.2 Initialisation phase — LAC application-specific contents of the BST

AID=21 shall be used for the LAC application.

The RSE shall initialise only one instance of the LAC application; this means that there shall be only one instance of AID=21 in the BST.

NOTE This does not exclude the BST from carrying information related to other applications, which may be active at the RSE (e.g. the CCC application as given in ISO/TS 12813).

The LAC application shall be qualified as a mandatory application. EID shall not be transmitted in the BST related to the EFC application. No Parameter shall be transmitted in the BST related to the LAC application.

8.2.3 Initialisation phase — LAC application-specific contents of the VST

There shall be only one instance of AID=21 in the ApplicationList in the VST. This instance shall contain the parameter 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.

The transaction phase may be performed as a sequence of one or more “Write data” functions on the LAC attribute. Each “Write data” function shall write the LAC data for one particular toll context for which the LAC service is provided. “Write data” functions may be concatenated as far as allowed by the specific communication medium.

NOTE To ease the implementation of an OBE supporting the LAC application, the LAC data attribute can be implemented as an instance attribute which stores various instances of the LAC attribute, which are written during one single LAC transaction using subsequent write functions.

The OBE shall respond to the functions invoked by the RSE and shall not initiate any functions.

The RSE may terminate the communication using the function “Terminate communication”.

Annex A
(normative)

LAC data type specifications

This clause contains the ASN.1 definition of

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

— the data types related to the LAC attributes described in Clause 7, and

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

using the Abstract Syntax Notation One (ASN.1) technique in accordance with ISO/IEC 8824-1. The packed encoding rules, in accordance with ISO/IEC 8825-2, shall be applied.

```
LacModule {iso standard 13141 modules(0) lac(0) version(1)}

DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
EFC-ContextMark, Provider
FROM EfcModule {iso standard 14906 modules(0) efc(0) version(1)}

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

Longitude, Latitude
FROM CccModule {iso standard 12813 modules(0) ccc(0) version(1)}

-- imports data attributes and elements from CCC

TollCharger, ChargeObjectId
FROM ChargingModule {iso standard 17575 modules(0) efc(0) version(1)}

-- imports data attributes and elements from ISO 17575-1

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

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition

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

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

LAC-InitialiseComm-Request ::= BST

LAC-InitialiseComm-Response ::= VST

LAC-DataTx-Request::= Set-Request (WITH COMPONENTS {..., accessCredentials (SIZE(4)), iid
ABSENT})

LAC-DataTx-Response::= Set-Response (WITH COMPONENTS {..., iid ABSENT, ret PRESENT})

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

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

ChargeObject ::= ChargeObjectId (WITH COMPONENTS {regimeId, chargeObjectDesignation})

LAC-ContextMark ::= EFC-ContextMark
```

```
LACData::= SEQUENCE{
    lACOperator         Provider,
    rSEId               INT2,
    latitude            Latitude,
    longitude           Longitude,
    altitude            INT2Signed,
    tollCharger         TollCharger,
    chargeObject        ChargeObject,
    distanceToObject    INT2Signed,
    lACtime             Time,
    mAC1                OCTET STRING (SIZE (8)),
    mAC2                OCTET STRING (SIZE (8))
}

-- NOTE: The following are the definitions of the LAC (sub) data elements

INT2 ::= INTEGER(0..65535)

INT2Signed::= INTEGER (-32768..32767)

INT4 ::= INTEGER(0..4294967295)


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

-- The following is the definition of the LAC Container type as the next values in the row
after the CCC data types of ISO 12813

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,
vector                      [16]    SEQUENCE (SIZE(0..255)) OF INTEGER(0..127,...),
contLAC                     [87]    LACData
-- Container CHOICE type values [88..127] are reserved for private use and intended for
the addressing of the corresponding private attribute identifiers.

}

END
```

Annex B
(normative)

PICS proforma for the data elements in the attribute

B.1 General

This annex gives the protocol implementation conformance statement (PICS) proforma to be used for the attributes defined in Clause 7 and Annex A.

To evaluate conformance of a particular implementation, a statement of which capabilities and options have been implemented shall be provided. Such a statement is called an implementation conformance statement (ICS) or more specifically, in case it covers transactions, a PICS. This annex provides PICS templates, which shall 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 requirements defined in this Technical Specification may provide information about the implementation in a standardized manner.

The PICS proforma is subdivided into the following categories of information:

— identification of the implementation;

— identification of the protocol;

— global statement of conformance;

— PICS proforma tables.

B.3 Instruction for completing the PICS proforma

B.3.1 Definition of support

A capability is said to be supported if the Implementation Under Test (IUT) is able to:

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

— 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 some 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 indicates the level of support required for conformance to the ISO/IEC standard. The values are as follows:

m mandatory support is required;

o optional support is permitted for conformance to the standard. If implemented, it shall conform to the specifications and restrictions contained in the standard. These restrictions may affect the optionality of other items.

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 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 are:

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, not erasing nor making the original entry illegible, and writing the new entry alongside. All such alterations to records shall be initialised by the staff making them.

B.3.4 Item reference numbers

Each line within the PICS proforma, which requires that implementation details be entered, is numbered on the left-hand edge of the line. This numbering is included as a means 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 carried out in the following sequence:

— a reference to the smallest enclosing the relevant item;

— a solidus character, '/';

— the reference number of the row in which the response appears;

— if, and only if, more than one response occurs in the row identified by the reference number, then each possible entry is implicitly labelled a, b, c, etc., from left to right and this letter is appended to the sequence.

B.4 PICS proforma for the OBE

B.4.1 Identification of the implementation

Table B.1 — Identification of PICS

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

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

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

Table B.3 — Identification of the OBE supplier

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

Table B.4 — Identification of the OBE

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

B.4.2 Identification of the standard

Table B.5 — Identification of the standard

Item No.	Question	Response
1	Title, reference no., publication date of the Technical Specification	
2	Technical Specification edition number	
3	Implemented annexes	
4	Implementer's Guide version no.	
5	Implementation defect reports (ref. no.)	
6	Other information	

B.4.3 Global statement of conformance

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

NOTE 1 Answering “No” to this question indicates non-conformance with the specification. Non-supported mandatory capabilities are identified in the ICS, with an explanation of why the implementation is non-conforming, on pages attached to the ICS proforma.

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

NOTE 2 For definition of the security levels, see 6.2 and Annex D.

B.4.4 PICS proforma tables

This part of the PICS proforma identifies the supported application context, the communication services and attributes (ADUs).

Table B.6 — Security requirements

Item No.	Element	Reference	Status	Support
1	Security level 1 — Access credentials	EN 15509, 5.1.5.3	m	

Table B.7 — Required Layer 7 functions

Item No.	Element	Subclause No./Reference	Status	Support
1	INITIALISATION	6.1.2	m	
2	SET	6.1.3	m	
5	EVENT_REPORT	6.1.4	m	

Table B.8 — Implemented DSRC stacks

Item No.	Element	Subclause No./Reference	Status	Support
1	CEN DSRC	5.5.2	o[a]	
2	CALM IR	Annex D	o[a]	
3	UNI DSRC	Annex C	o[a]	
4	ARIB DSRC	Annex E	o[a]	

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

Table B.9 — Data requirements regarding the LAC-Context Mark

Item No.	Element	Subclause No./Reference	Status	Support coding
1	LAC-ContextMark	7.4	m	

Table B.10 — Data requirements regarding location reference

Item No.	Element	Subclause No./Reference	Status	Support read protection	Support coding
1	LACOperator	7.3	m		
2	RSEId	7.3	m		
3	Latitude	7.2	m		
4	Longitude	7.2	m		
5	Altitude	7.2	m		
6	TollCharger	7.3	m		
7	ChargeObjectId	7.2	m		
8	DistanceToObject	7.2	m		
9	LACTime	7.3	m		
10	MAC1	7.5	m		
11	MAC2	7.5	m		

The following table (Table B.11) can be used to provide any other relevant information.

NOTE This table can be used to add information regarding the OBE, which is relevant for testing, but not covered in the items above. This can include additional features, such as other communication media or other proprietary attributes for local use.

Table B.11 — Other information

Item No.	Other information

B.5 PICS proforma for the RSE

B.5.1 Identification of the implementation

Table B.12 — Identification of PICS

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

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

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

Table B.14 — Identification of the RSE supplier

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

Table B.15 — Identification of the RSE

Item No.	Question	Response
1	Brand Name	
2	Type, Version	
3	Manufacturer ID	
4	Serial numbers of supplied units	
5	Other information	

Table B.16 — Identification of the standard

Item No.	Question	Response
1	Title, reference no., publication date of the Technical Specification	
2	Technical Specification edition number	
3	Implemented annexes	
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).....

NOTE 1 Answering “No” to this question indicates non-conformance to the specification. Non-supported mandatory capabilities are identified in the ICS, with an explanation of why the implementation is non-conforming, on pages attached to the ICS proforma.

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

NOTE 2 For definition of the security levels, see 6.2 and Annex D.

B.5.3 PICS proforma tables

This part of the PICS proforma identifies the supported application context, the communication services and attributes (ADUs).

Table B.17 — Security requirements

Item No.	Element	Reference	Status	Support
1	Security level 1 – Access credentials	EN 15509, 5.2.5.3	m	

Table B.18 — Required Layer 7 functions

Item No.	Element	Subclause No./Reference	Status	Support
1	INITIALISATION	6.1.2	m	
2	SET	6.1.3	m	
5	EVENT_REPORT	6.1.4	m	

Table B.19 — Implemented DSRC stacks

Item No.	Element	Subclause No./Reference	Status	Support
1	CEN DSRC	5.5.2	o[a]	
2	CALM IR	Annex D	o[a]	
3	UNI DSRC	Annex C	o[a]	
4	ARIB DSRC	Annex E	o[a]	
[a] One or more DSRC stacks shall be implemented.				

Table B.20 — Data requirements regarding the LAC-Context Mark

Item No.	Element	Subclause No./Reference	Status	Support coding
1	LAC-ContextMark	7.4	m	

Table B.21 — Data requirements regarding location reference

Item No.	Element	Subclause No./Reference	Status	Support write protection	Support coding
1	LACOperator	7.3	m		
2	RSEId	7.3	m		
3	Latitude	7.2	m		
4	Longitude	7.2	m		
5	Altitude	7.2	m		
6	TollCharger	7.3	m		
7	ChargeObjectId	7.2	m		
8	DistanceToObject	7.2	m		
9	LACTime	7.3	m		
10	MAC1	7.5	m		
11	MAC2	7.5	m		

The following table (Table B.22) can be used to provide any other relevant information:

NOTE This table can be used to add information regarding the OBE, which is relevant for testing, but not covered in the items above. This can include additional features, such as other communication media or other proprietary attributes for local use.

Table B.22 — Other information

Item No.	Other information

Annex C
(informative)

UNI DSRC communication stack usage for LAC communications

C.1 General

This annex:

— lists the requirements which should be fulfilled by an LAC application in order to use the UNI DSRC [UNI 10607 (all parts)] standard as a communication media;

— shows how LAC generalized communication functions are to be mapped on to UNI DSRC service primitives;

— gives an example of how LAC information types can be stored in an UNI DSRC compliant OBE.

Security algorithms and calculations, as well as the transaction model, should be as specified in the UNI DSRC Interoperability profile, UNI 11310.

C.2 UNI DSRC requirements

Using the UNI communication stack for transferring LAC data means being compliant to the four documents which constitute the [UNI 10607 (all parts)] standard ([UNI DSRC1], [UNI DSRC2], [UNI DSRC3] and [UNI DSRC4]). It also recommended that the OBE equipment be compliant to the UNI Interoperability profile [UNI Profile].

C.3 Function correspondences

Table C.1 shows the correspondence between LAC functions and the primitives defined in the UNI stack. For each UNI service primitive, an indication of the standard number is given. Different UNI service primitives are used to access data, which are located in different memory regions.

Table C.1 — Functions correspondences

LAC function	UNI primitive(s)	
Initialise communication	A-Associate, [UNI DSRC3], concatenated with A-Get_Nonce, [UNI DSRC4], concatenated with A-Get_Context_Record [UNI DSRC4]	
Data Writing	Data location	Service primitive
	Application core	Set_ASO_Context, [UNI DSRC3]
	Application record	SET [UNI DSRC3]
Authenticated data writing	Concatenation of: Set_Credentials, [UNI DSRC4] A Set operation (according to the requested data, see Data writing above in this table)	
Terminate communication	A-Release [UNI DSRC3]	

It is recommended that:

a) after the first interaction to initialise the communication link, an A-SLT service request be concatenated to all other requests;

b) if the write transaction spans a number of DSRC interactions, the RSE repeats its authentication, as long as there is room for authentication data and primitives in that interaction.

The above recommendations are implemented in the transaction example in C.5.

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

C.4 Data storage and addressing

C.4.1 Data storage

The main characteristic 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. The OBE virtual memory structure is described in [UNI DSRC4]. Table C.2 gives an example of how LAC application data could be referenced. By no means should it be assumed that the choice of LAC attributes or the memory structure depicted in the table represents a real implementation. The choice of data types to be used for LAC application and their positioning in the OBE memory structure, should be defined in an appropriate LAC interoperability profile.

Table C.2 — Example of OBE storing of LAC 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 LAC 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 LAC Application identifier
		Reserved	1	
		LAC-ContextMark	6	ISO 14906, AttrId 0
		AC_CR-KeyReference	2	Reserved for key reference for AC-CR, see [EFC IAP]
Application	header	core-len	1	Core length = 18
		record-len	1	Record length = 31 octets
		record-number	1	There is 1 record
		current-record	1	The current record is the first one
	core	MAC1	9	LAC specific attribute
		MAC2	9	LAC specific attribute
	record 1	LACOperator	3	LAC specific attribute
		RSEId	2	LAC specific attribute
		Latitude	4	LAC specific attribute
		Longitude	4	LAC specific attribute
		Altitude	2	LAC specific attribute
		TollCharger	6	LAC specific attribute
		ChargeObject	10	LAC specific attribute

Reading or writing of the data in Table C.2 is performed by a set of functions, which is specific for each identified memory region, namely, Master Core, Master Record, Application Core and Application Record (see [UNI DSRC3] and [UNI DSRC4]). The way to access the above data is specified in C.4.2.

C.4.2 Data access

Table C.3 shows how to access data with the functions defined above in C.3. Accessing data is shown by means of Get primitives only for the sake of exemplifying: LAC applications are supposed to only use Set primitives (write-only) for LAC data.

Table C.3 — Example of data access

LAC 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)
MAC1	Get_ASO_Context (Offset=0, Length=9)
MAC2	Get_ASO_Context (Offset=9, Length=9)
LACOperator	Get (Offset=0, Length=3)
RSEId	Get (Offset=3, Length=2)
Latitude	Get (Offset=5, Length=4)
Longitude	Get (Offset=9, Length=4)
Altitude	Get (Offset=13, Length=2)
TollCharger	Get (Offset=15, Length=6)
ChargeObject	Get (Offset=21, Length=10)

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

EXAMPLE Setting the Latitude and Longitude attributes can be accomplished by means of an operation like Set (Where=Current, Offset=5, Length=8).

C.5 LAC transaction example

In this example, the RSE uses the random number received by the OBE, together with the AC_CR-KeyReference field, to compute its authenticator. For the sake of this example, the MAC1 and MAC2 fields are not used.

The memory structure of the OBE for this example is as indicated in Table C.2. The transaction is performed in two phases, namely, initialisation and data writing. There is no prescription on how DSRC interactions should be split in the two phases, nor is there any prescription on 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, and writes all localisation information, as specified in the Application Record. These operations are performed in a single DSRC interaction.

The transaction flow is shown in terms of the interactions which happen between the RSE and the OBE.

C.5.1 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 of primitives. The sequence of service primitives and related exchanges of protocol messages is shown in Table C.4.

Table C.4 — Example of initialisation phase

RSE		Protocol message		OBE
A-Associate.Request		Open-Rq		A-Associate.Indication
A-Get_Nonce.Request (Length='4'D)		Get-TBA-Random-Rq (Length='4'D)		A-Get_Nonce.Indication (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 (Data)		Get-TBA-Random-Rs (Data)		A-Get_Nonce.Response (Data)
A-Get_Context_Record.Confirm (Data)	←	Get-Mast-Rec-Rs (Data)	←	A-Get_Context_Record.Response (Data)

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

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

C.5.2 Data writing phase

This interaction is aimed at transmitting the RSE authenticator and writing the following OBE information:

— LACOperator;

— RSEId;

— Latitude;

— Longitude;

— Altitude;

— TollCharger;

— ChargeObject.

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

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

The sequence of service primitives and related exchanges of protocol messages in the second interaction is presented in Table C.5.

Table C.5 — Example of data writing phase

RSE		Protocol message		OBE
A-Associate.Request		Open-Rq		A-Associate.Indication
A-SLT.Request (Tba-length='4'D, Tba-id)		Select-TBA-Id-Rq (Tba-length='4'D, Tba-id)		A-SLT.Indication (Tba-length='4'D, Tba-id)
A-Set_Credential.Request (Length='4'D, Credential)	→	Set-Credential-Rq (Length='4'D, Credential)	→	A-Set_Credential.Indication (Length='4'D, Credential)
A-Set.Request (Mode='Immediate', Offset='0'D, Length='31'D)		Write-Appl-Record-Curr-Conf-Rq (Offset='0'D, Length='31'D)		A-Get.Indication (Mode='Immediate', Offset='0'D, Length='31'D)
A-Release.Request		Close-Rq		A-Release.Indication
A-Set.Confirm	←	Write-Appl-Record-Curr-Conf-Rs	←	A-Set.Response

Annex D
(informative)

IR communication usage for LAC applications

D.1 Using the IR Communication stack (CALM IR)

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

D.1.1 DSRC requirements

The OBE and RSE should be according to ISO 21214 in the compatibility mode.

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

D.1.2 Functions

The LAC specific functions should be implemented as specified in Clause 6.

D.1.3 Data requirements

The addressing of the EFC system and application data implemented by the OBE and RSE should be according to the rules given in ISO 14906:—, 5.3.

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

The RSE should support any OBE that is otherwise compliant.

D.1.4 Security requirements

The security requirements should be as specified in 6.2.

D.1.5 Transaction requirements

The transaction requirements should be as specified in Clause 8.

Annex E
(informative)

ARIB DSRC communication stack usage for LAC applications

E.1 Using the ARIB DSRC communication stack

This annex specifies the use of the ARIB 5.8 GHz microwave DSRC link for localisation augmentation applications.

E.1.1 DSRC requirements

The DSRC should be according to ARIB STD-T75, Clause 2. The DSRC communication stack should be according to ARIB STD-T75, Clause 4.

E.1.2 LAC functions

The LAC functions should be implemented as DSRC Layer 7 services, as defined in ARIB STD-T75, 4.4.2.1.2.

The SET service should always carry AC-CR for secure communication.

E.1.3 Data requirements

The addressing of the EFC system and application data implemented by the OBE and RSE should be according to the rules given in ISO 14906:—, 5.3. For LAC application data, EID should always be used.

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

The RSE should support any OBE that is otherwise compliant.

E.1.4 Security requirements

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

E.1.5 Transaction requirements

The EFC transaction model shall comply with ISO 14906:—, Clause 6, with the restrictions and amendments defined in E.1.5.1 to E.1.5.3.

E.1.5.1 Initialisation phase – LAC application-specific contents of the BST

AID=21 should be used for the LAC application. There should be only one instance of AID=21 in the BST.

The LAC application should be qualified as a mandatory application.

E.1.5.2 Initialisation phase – LAC application-specific contents of the VST

There should be only one instance of AID=21 in the ApplicationList in the VST. This instance should 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.1.5.3 Transaction phase

The transaction requirements should be the same as described in Clause 8.

Annex F
(informative)

LAC transaction example

This annex gives an example of an LAC transaction for the case of an RSE sending localisation augmentation data for two overlapping toll contexts.

For the two toll contexts, the LAC data provided differ in the Toll Charger and can also differ in the identification of the Charge Object and possibly in the LAC Operator. These differences in data content naturally also lead to different message authentication codes.

Table F.1 —LAC transaction example

Phase	Road-side equipment		On-board equipment	Remarks
Initialisation	INITIALISATION.request (BST)	→		RSE periodically sends BST.
(BST – VST)		←	INITIALISATION.response (VST) • LAC-ContextMark • AC_CR-KeyReference • RndOBE	A newly arrived OBE answers with VST. The LAC Context Mark contains information on the toll contract. 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 gives access only when RSE provides the correct access credentials (AC_CR) in the subsequent phases.
Transaction	SET.request • AC_CR LACData LACOperator RSEId Latitude Longitude Altitude TollCharger ChargeObject DistanceToObject LACTime MAC1 MAC2 SET.request AC_CR • LACData LACOperator RSEId Latitude Longitude Altitude TollCharger ChargeObject DistanceToObject LACTime MAC1 MAC2	→		The RSE writes the LAC Data attribute to the OBE twice, corresponding to the two overlapping toll contexts. The SET service contains access credentials that authenticate the RSE.
		←	SET.response SET.response	OBE confirms reception (optional).
Closing	EVENT_REPORT.request (Release)	→		RSE closes the transaction and releases the OBE.

Bibliography

[1] ISO 17573[2)], *Electronic fee collection — Systems architecture for vehicle related tolling*

[2] ISO/TS 17574, *Electronic fee collection — Guidelines for security protection profiles*

[3] ISO/TS 17575-1, *Electronic fee collection — Application interface definition for autonomous systems — Part 1: Charging*

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

[5] EN 12253:2004, *Road transport and traffic telematics — Dedicated short-range communication — Physical layer using microwave at 5.8 GHz*

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

[7] ARIB STD-T75[3)], *Dedicated Short-Range Communication*

[8] ITU-R.M1453-2, *Intelligent transport systems — Dedicated short range communications at 5.8 GHz*

[9] [UNI DSRC1], UNI10607-1:2007, *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 (English version of the UNI standard available)*

[10] [UNI DSRC2], UNI10607-2:2007, *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 (English version of the UNI standard available)*

[11] [UNI DSRC3], UNI10607-3:2007*, 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 (English version of the UNI standard available)*

[12] [UNI DSRC4], UNI10607-4:2007, *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 (English version of the UNI standard available)*

[13] [UNI Profile], UNI11310, *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*

2) To be published. (Revision of ISO/TS 17573:2003).

3) Association of Radio Industries and Businesses (ARIB) of Japan standard.

ICS 03.220.20; 35.240.60

Price based on 35 pages