SVENSK STANDARD
SS-EN ISO 14906:2018

Fastställd/Approved: 2018-12-18
Utgåva/Edition: 3
Språk/Language: engelska/English
ICS: 03.220.20; 03.240; 35.240.60

SWEDISH STANDARDS INSTITUTE

Vägtrafikinformatik – Elektronisk vägavgiftsupptagning – Applikationsgränssnitt för korthållskommunikation (ISO 14906:2018)

Electronic fee collection – Application interface definition for dedicated short-range communication (ISO 14906:2018)

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Europastandarden EN ISO 14906:2018 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av EN ISO 14906:2018.

Denna standard ersätter SS-EN ISO 14906:2011, utgåva 2 och SS-EN ISO 14906:2011/AC:2013, utgåva 1 och SS-EN ISO 14906:2011/A1:2015, utgåva 1

The European Standard EN ISO 14906:2018 has the status of a Swedish Standard. This document contains the official version of EN ISO 14906:2018.

This standard supersedes the SS-EN ISO 14906:2011, edition 2 and SS-EN ISO 14906:2011/AC:2013, edition 1 and SS-EN ISO 14906:2011/A1:2015, edition 1

Denna standard är framtagen av kommittén för Vägtrafikinformatik, SIS/TK 255.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 14906

December 2018

ICS 35.240.60; 03.220.20

Supersedes EN ISO 14906:2011, EN ISO

English Version

Electronic fee collection - Application interface definition for dedicated short-range communication (ISO 14906:2018)

Perception du télépéage - Définition de l'interface d'application relative aux communications dédiées à courte portée (ISO 14906:2018)

Elektronische Gebührenerhebung - Anwendungsschnittstelle zur dezidierten Nahbereich- Kommunikation (ISO 14906:2018)

This European Standard was approved by CEN on 6 September 2018.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN ISO 14906:2018: E

Contents

Page

European foreword

This document (EN ISO 14906:2018) has been prepared by Technical Committee ISO/TC 204 "Intelligent transport systems" in collaboration with Technical Committee CEN/TC 278 “Intelligent transport systems” the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 2019, and conflicting national standards shall be withdrawn at the latest by June 2019.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO 14906:2011.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 14906:2018 has been approved by CEN as EN ISO 14906:2018 without any modification.

Introduction

This document specifies an application interface for electronic fee collection (EFC) systems, which is based on dedicated short-range communication (DSRC). It supports interoperability between EFC systems on an EFC-DSRC application interface level. This document is intended for DSRC charging applications, but specifically the definition of EFC data elements is valid beyond the use of a DSRC charging interface and might be used for other DSRC applications (e.g. compliance checking communication) and/or on other interfaces (e.g. the application interface of autonomous systems).

This document provides specifications for the EFC transaction model, EFC data elements (referred to as attributes) and functions, from which an EFC transaction can be built. The EFC transaction model provides a mechanism that allows handling of different versions of EFC transactions and associated contracts. A certain EFC transaction supports a certain set of EFC attributes and EFC functions as defined in this document. It is not envisaged that the complete set of EFC attributes and functions be present in each piece of EFC equipment, on-board equipment (OBE) or roadside equipment (RSE).

This document provides the basis for agreements between operators, which are needed to achieve interoperability. Based on the tools specified in this document, interoperability can be reached by operators recognising each others' EFC transactions (including the exchange of security algorithms and keys) and implementing the EFC transactions in each others' RSEs, or they can reach an agreement to define a new transaction (and contract) that is common to both. Considerations should also be made by each operator so that the RSE has sufficient resources to implement such additional EFC transactions.

In order to achieve interoperability, operators should agree on issues such as

— which optional features are actually being implemented and used,

— access rights and ownership of EFC application data in the OBE,

— security policy (including encryption algorithms and key management, if applicable),

— operational issues, such as how many receipts may be stored for privacy reasons, how many receipts are necessary for operational reasons (for example as entry tickets or as proof of payment),

— the agreements needed between operators in order to regulate the handling of different EFC transactions.

In this edition of this document, users are faced with issues related to backward compatibility. This issue can be managed by using the following:

— EfcModule ASN.1 module, including a version number;

— Efc-ContextMark (incl. the ContextVersion), denoting the implementation version, provides a means to ensure co-existence of different implementation versions by means of a look-up table and associated appropriate transaction processing. This will enable the software of the RSE to determine the version of the OBE and his capabilty to accept the new features introduced by this edition of ISO 14906.

Annex A provides the normative ASN.1 specifications of the used data types (EFC action parameters and attributes).

Annex B presents an informative example of a transaction based on the CARDME specification, including bit-level specification.

Annex C presents informative examples of EFC transaction types, using the specified EFC functions and attributes.

Annex D presents an informative mapping table from LatinAlphabetNo2 & 5 to LatinAlphabetNo1 to ease for a Service Provider the use of LatinAlphabetNo1 to encode an OBE for data available wiitten with non-Latin1 characters.

Annex E presents an informative mapping table between EFC vehicle data attributes and European registration certificates to ease the task of a service provider in the OBE personalisation with vehicle data.

Annex F presents the security calculations according to the data encryption standard (DES). This annex is based on EN 15509:2014, Annex B.

Annex G presents the security computations examples for DES. This annex is based on EN 15509:2014, Annex E.

Annex H presents the security calculations for advanced encryption standard (AES). This annex is the adaptation of EN 15509:2014, Annex B for the case of AES.

Annex I presents the security computations examples for AES. This annex is the adaptation of EN 15509:2014, Annex E for the case of AES.

This application interface definition can also be used with other DSRC media which do not use a layer 7 according to ISO 15628/EN 12834. Any DSRC medium which provides services to read and write data, to initialise communication and to perform actions is suitable to be used as a basis for this application interface. Adaptations are medium specific and are not further covered here. As Annex B describes in detail a transaction for central account systems, this document can also be used for on-board account systems, in conjunction with ISO 25110, which provides examples of systems based on on-board accounts.

Electronic fee collection — Application interface definition for dedicated short-range communication

1 Scope

This document specifies the application interface in the context of electronic fee collection (EFC) systems using the dedicated short-range communication (DSRC).

The EFC application interface is the EFC application process interface to the DSRC application layer, as can be seen in Figure 1 below. This document comprises specifications of:

— EFC attributes (i.e. EFC application information) that can also be used for other applications and/or interfaces,

— the addressing procedures of EFC attributes and (hardware) components (e.g. ICC and MMI),

— EFC application functions, i.e. further qualification of actions by definitions of the concerned services, assignment of associated ActionType values and content and meaning of action parameters,

— the EFC transaction model, which defines the common elements and steps of any EFC transaction,

— the behaviour of the interface so as to ensure interoperability on an EFC-DSRC application interface level.

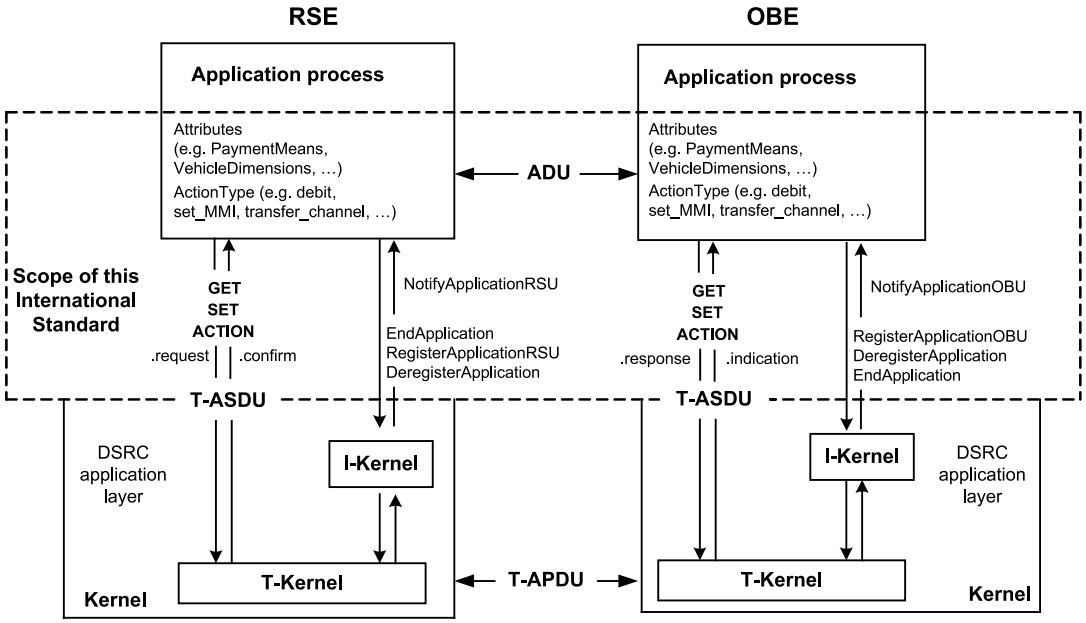

Figure 1 — The EFC application interface

This is an interface standard, adhering to the open systems interconnection (OSI) philosophy (see ISO/IEC 7498-1), and it is as such not primarily concerned with the implementation choices to be realised at either side of the interface.

This document provides security-specific functionality as place holders (data and functions) to enable the implementation of secure EFC transactions. Yet the specification of the security policy (including specific security algorithms and key management) remains at the discretion and under the control of the EFC operator, and hence is outside the scope of this document.

2 Normative references

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

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

ISO 1176, *Road vehicles — Masses — Vocabulary and codes*

ISO 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

ISO 3779, *Road vehicles — Vehicle identification number (VIN) — Content and structure*

ISO 4217, *Codes for the representation of currencies*

ISO/IEC 7812-1, *Identification cards — Identification of issuers — Part 1: Numbering system*

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

ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO 14816:2005, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure*

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

ISO/IEC 18033-3:2010, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

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

3 Terms and definitions

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

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

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

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

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

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

[SOURCE: ISO 17575-1:2016, definition 3.2]

3.3
authenticator
data, possibly encrypted, that is used for authentication

3.4
channel
information transfer path

[SOURCE: ISO 7498-2:1989, definition 3.3.13]

3.5
cryptography
principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorized use

3.6
data group
class of closely related attributes

[SOURCE: ISO 17575-1:2016, definition 3.10]

3.7
data integrity
property that data has not been altered or destroyed in an unauthorised manner

3.8
Element
DSRC directory containing application information in the form of attributes

3.9
on-board equipment
all required equipment on-board a vehicle for performing required EFC functions and communication services

3.10
on-board unit
single electronic unit on-board a vehicle for performing specific EFC functions and for communication with external systems

3.11
roadside equipment
equipment located along the road, either fixed or mobile

3.12
toll charger
entity which levies toll for the use of vehicles in a toll domain

3.13
toll domain
area or part of a road network where a toll regime is applied

[SOURCE: ISO 17573:2010, definition 3.18]

3.14
toll service
service enabling users to pay toll

3.15
toll service provider
entity providing toll services in one or more toll domains

3.16
transaction
whole of the exchange of information between two physically separated communication facilities

[SOURCE: ISO 17575-1:2016, definition 3.21]

3.17
transaction model
functional model describing the structure of electronic payment transactions

4 Abbreviated terms

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

AP	Application Process
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One (ISO/IEC 8824-1)
BST	Beacon Service Table
CCC	Compliance check communication
cf	Confirm
DSRC	Dedicated Short-Range communication
EFC	Electronic Fee Collection
EID	Element Identifier
GNSS	Global Navigation Satellite System
ICC	Integrated Circuit(s) Card
IID	Invoker Identifier
I-Kernel	Initialisation Kernel
ind	Indication
L1	Layer 1 of DSRC (Physical Layer)
L2	Layer 2 of DSRC (Data Link Layer)
L7	Application Layer Core of DSRC
LAC	Localisation Augmentation Communication
LID	Logical Link Control Identifier
LLC	Logical Link Control
LPDU	LLC Protocol Data Unit
MAC	Medium Access Control
MMI	Man-Machine Interface
n.a.	Not applicable
OBE	On-Board Equipment
PDU	Protocol Data Unit
PER	Packed Encoding Rules (ISO/IEC 8825-2)

req	Request
rs	Response
RSE	Roadside Equipment
SAM	Secure Application Module
T-APDU	Transfer-Application Protocol Data Unit
T-ASDU	Transfer-Application Service Data Unit
T-Kernel	Transfer Kernel
VST	Vehicle Service Table

5 EFC application interface architecture

5.1 Relation to the DSRC communication architecture

The DSRC services are provided to an application process by means of the DSRC Application Layer service primitives, which are abstract implementation interactions between a communication service user and a provider. The services are offered by the DSRC communication entities by means of its DSRC Application Layer (EN 12834/ISO 15628) as shown in Figure 2.

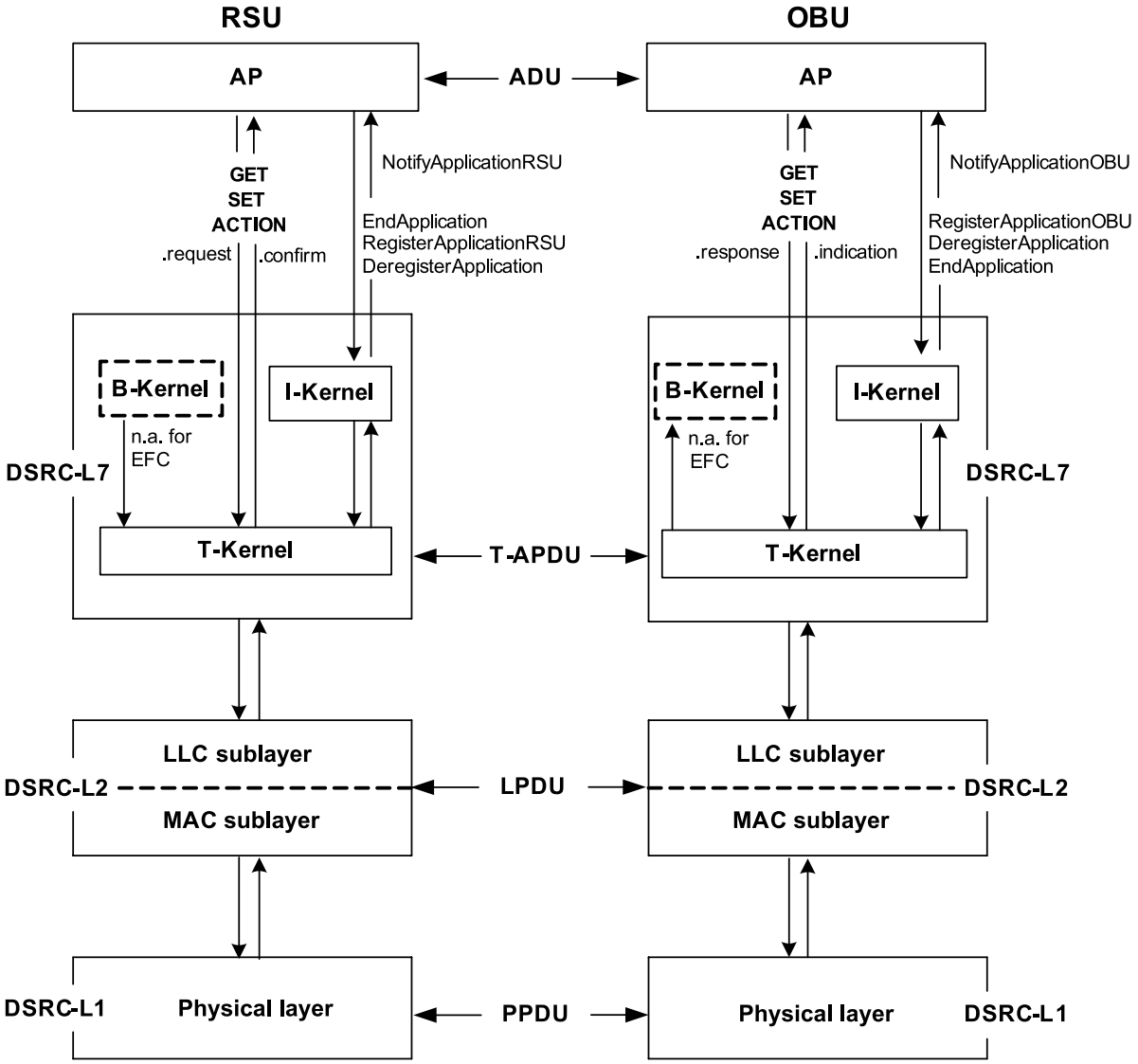

Figure 2 — The EFC application process on top of the DSRC communication stack

NOTE The abbreviated terms used in Figure 2 are defined in Clause 4.

The Transfer Kernel of DSRC Application Layer offers the following services to application processes (see also Figure 2 above):

— GET: The invocation of a GET service request results in retrieval (i.e. reading) of application information (i.e. Attributes) from the peer service user (i.e. the OBE application process), a reply is always expected.

— SET: The invocation of a SET service request results in modification (i.e. writing) of application information (i.e. Attributes) of the peer service user (i.e. the OBE application process). This service may be requested in confirmed or non-confirmed mode, a reply is only expected in the former case.

— ACTION: The invocation of an ACTION service request results in a performance of an action by the peer service user (i.e. the OBE application process). An action is further qualified by the value of the ActionType. This service may be requested in confirmed or non-confirmed mode, a reply is only expected in the former case.

— EVENT-REPORT: The invocation of an EVENT-REPORT service request forwards a notification of an event to the peer service user.

— INITIALISATION: The invocation of an initialisation service request by RSE results in an attempt to initialise communication between a RSE and each OBE that has not yet established communication with the concerned RSE. The Initialisation service is only used by the Initialisation Kernel as defined in EN 12834/ISO 15628.

5.2 Usage of DSRC application layer by the EFC application interface

EFC uses the following services offered by DSRC Application Layer (as defined in ISO 15628):

— The INITIALISATION services:

  — Notify Application RSU (at RSE);

  — End Application (at RSE);

  — Register Application RSU (at RSE);

  — Deregister Application (at RSE and OBE);

  — Notify Application OBU (at OBE);

  — Register Application OBU (at OBE)

  are used to realise the EFC-specific initialisation mechanism (see Clause 6);

— The GET service is used to retrieve EFC attributes (For attribute specifications see Clause 8);

— The SET service is used to set EFC attributes;

— The ACTION services are applied to realise additional EFC specific functionality needed to support EFC application processes, such as TRANSFER_CHANNEL, SET_MMI and ECHO (see 7.2).

In the following, the EFC-specific usage of the DSRC Layer 7 services is specified in detail.

NOTE The EVENT-REPORT-service can be implicitly used by EFC application processes. It is e.g. used indirectly as part of an already defined command to release an application process (see EN 12834/ISO 15628, Ready Application). However as the EVENT-REPORT-service is not explicitly used by EFC application processes, this service is not further referred to in this document.

5.3 Addressing of EFC attributes

5.3.1 Basic mechanism

EFC Attributes are used to transfer the EFC application-specific information.

EFC Attributes are composed of one or more data elements of specified ASN.1 types. Each data element is associated with, within the context of this document, an unambiguous name.

To each EFC Attribute, an AttributeID is associated. The AttributeID enables to unambiguously identify and address an EFC Attribute.

EXAMPLE Figure 3 illustrates the basic addressing mechanism.

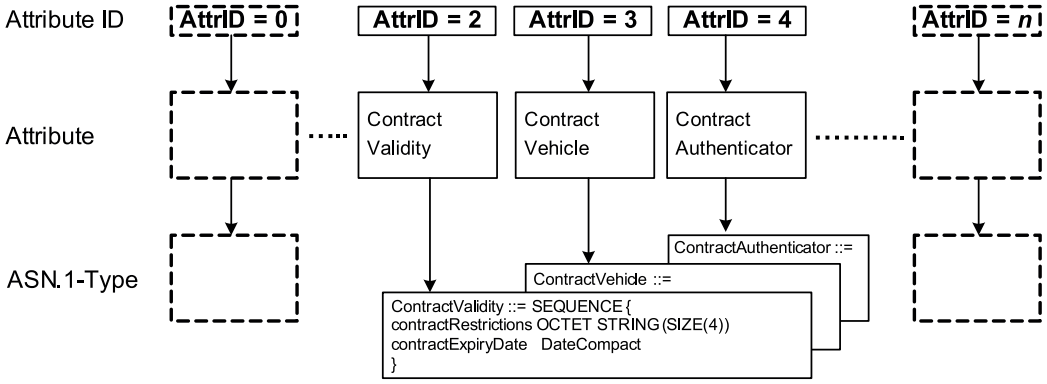

Figure 3 — Basic addressing mechanism

5.3.2 Role of the EID

In a given OBE, the DSRC-EID (different from 0) is used to address an EFC context, identified by the EFC-ContextMark (see 6.2.3), in which Attributes can be addressed unambiguously by AttributeIDs inside an Element of the OBE. In the VST, the OBE specifies one or several of these EFC contexts, each corresponding to an EFC ContextMark and the EID to be used for addressing the attributes and using the EFC functions supported by it.

EXAMPLE Figure 4 illustrates the role of the EID.

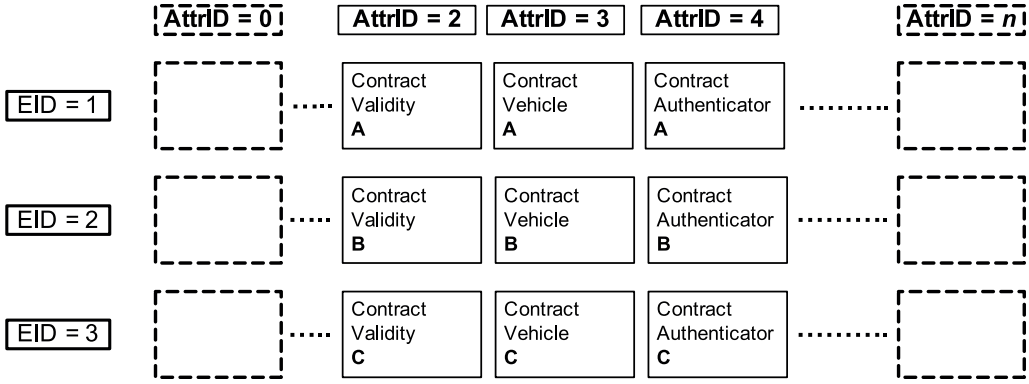

Figure 4 — Role of the EID

EID equals 0 shall be used to address application-independent functions and components, e.g. SET_MMI and TRANSFER_CHANNEL (see 7.2).

5.3.3 Multiple Instances of Attributes

There may be n, where n is an integer, instances of an Attribute available in the OBE.

The maximum number of instances N_{max} of one Attribute may be limited according to the needs of operators and users. The default maximum number of instances is N_{max}=1. The value of N_{max} is determined at the time of OBE configuration.

EXAMPLE Figure 5 illustrates multiple instances (0-2) of attribute 5.

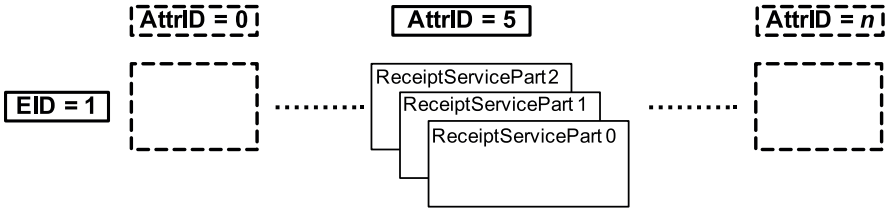

Figure 5 — Multiple instances (0-2) of attribute 5

The handling of multiple instances and the corresponding addressing mechanism are described in detail as part of the behaviour specification of the corresponding functions supporting multiple instances (see 7.2.6 for GET_INSTANCE and 7.2.7 for SET_INSTANCE).

5.4 Addressing of components

Components of an OBE to be addressed via the EFC Application Interface include for example:

— OBU;

— SAM 1;

— SAM 2;

— ICC;

— Display;

— Buzzer;

— Printer;

— Serial interface;

— Parallel interface;

— GNSS;

— Tachograph;

— Bluetooth.

Addressing of these components is enabled on two levels, device-specific and device-independent addressing.

The ***device-specific transparent addressing mechanism*** enables the transfer of information, which shall be processed by the addressed device (such as an ICC-command). The addressed device is identified by a *channel Id*. The EFC function TRANSFER_CHANNEL (see 7.2.10) supports this functionality.

EXAMPLE 1 Transfer of a bit string to an ICC.

The ***device-independent addressing mechanism*** uses a set of commands, which describe a certain functionality, which can be performed by various OBE components. In this case, the operating system of the OBE will address the corresponding components. The EFC function SET_MMI supports this functionality (see 7.2.12).

EXAMPLE 2 Invocation of a SET_MMI(EID=0, ContactOperator) function activates an OBE MMI-device, e.g. a buzzer or a display.