TECHNICAL REPORT

ISO/TR 14906

First edition
1998-12-15

Road Transport and Traffic Telematics (RTTT) — Electronic Fee Collection (EFC) — Application interface definition for dedicated short range communications

Télématique de la circulation et du transport routier — Perception du télépéage — L'interface applicative relative aux communications dédiées aux courtes portées

Reference number
ISO/TR 14906:1998(E)

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The main task of technical committees is to prepare International Standards, but in exceptional circumstances a technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

ISO/TR 14906, which is a Technical Report of type 2, was prepared by European Committee for Standardization (CEN) in collaboration with ISO Technical Committee ISO/TC 204, *Transport information and control systems,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Internet iso@iso.ch

Printed in Switzerland

This document is being issued in the Technical Report (type 2) series of publications (according to subclause G.3.2.2 of part 1 of the ISO/IEC Directives, 1995) as a "prospective standard for provisional application" in the field of *transport information and control systems* because there is an urgent need for guidance on how standards in this field should be used to meet an identified need.

This document is not to be regarded as an "International Standard". It is proposed for provisional application so that information and experience of its use in practice may be gathered. Comments on the content of this document should be sent to the ISO/TC 204 Secretariat.

A review of this Technical Report (type 2) will be carried out not later than three years after its publication with the options of: extension for another three years; conversion into an International Standard; or withdrawal.

Annex A forms an integral part of this Technical Report. Annexes B to D are for information only.

CONTENTS

Foreword

This European Prestandard has been prepared by Technical Committee CEN/TC 278 "Road transport and traffic telematics", the secretariat of which is held by NNI, in collaboration with Technical Committee ISO/TC 204 "Transport information and control systems".

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this European Prestandard: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

Introduction

This European Pre-Standard specifies an application interface for Electronic Fee Collection (EFC) systems, which are based on the Dedicated Short-Range Communication (DSRC), enabling interoperability between open EFC systems (i.e. between different EFC system operators) on an EFC-DSRC application interface level.

The European Pre-Standard 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 European Pre-Standard. It is not envisaged that the complete set of EFC attributes and functions is present in each piece of EFC equipment, be OBE or RSE.

This European Pre-Standard provides the basis for agreements between operators, which are needed to achieve interoperability. Based on the tools specified in this European Pre-Standard, 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 RSE, or they may reach an agreement to define a new transaction (and contract) that is common to both. Considerations also have to be made by each operator that the RSE has sufficient resources to implement such additional EFC transactions.

In order to achieve interoperability, operators have to agree on issues like:

- which optional features are actually being implemented and used;
- 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 (e.g. as entry tickets or as proof of payment);
- the agreements needed between operators in order to regulate the handling of different EFC transactions.

This European Pre-Standard has the following structure. In the first four clauses the scope, normative references, definitions of terms and abbreviations are accounted for. Next, in clause 5, the EFC Application interface architecture is described in terms of its relation to the DSRC communication architecture, including the addressing of data attributes and of components. In the following clause 6, the EFC transaction model is introduced, defining the common steps of each EFC transaction, in particular the initialisation phase. Clauses 7 and 8 are dedicated to the detailed specification of the EFC application functions and of the EFC data attributes, respectively. Four annexes provide

- the normative ASN.1 specifications of the used data types (EFC action parameters and attributes);
- an informative excerpt from DSRC application layer (ENV 12834), and its service primitives, parameters and functions;
- informative examples of EFC transactions using the specified EFC attributes and functions;
- an informative listing of functional requirements, which can be satisfied by using the tools provided by this European Pre-standard.

1 Scope

This European Pre-Standard specifies the application interface in the context of Electronic Fee Collection (EFC) systems using the Dedicated Short-Range Communications (DSRC).

The EFC application interface is the EFC application process interface to the DSRC Application Layer, as can be seen in figure 1 below. The scope of this European Pre-Standard comprises specifications of:

- EFC attributes (i.e. EFC application information);
- 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.

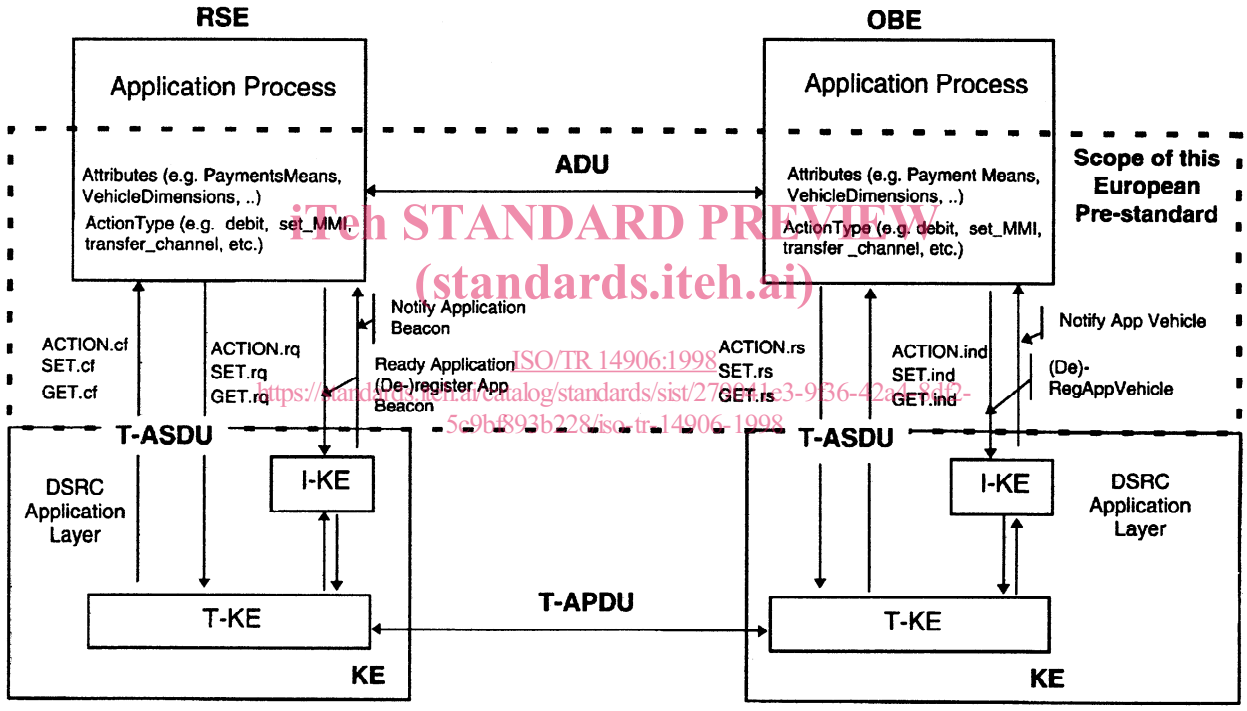


Figure 1: The EFC application interface

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

This European Pre-Standard 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 European Pre-Standard.

2 Normative references

This European Pre-Standard incorporates by dated or undated reference, provisions from other publications.

These normative references are cited at the appropriate places in the text and the publications are listed hereafter.

For dated references, subsequent amendments to or revisions of any of these publications apply to this European Pre-Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

ISO 612:		Vehicle Measurement Definition
ISO 1176:		Vehicle Weight Definitions
ISO 3166:		Codes for the representation of names of countries
ISO 3779:	1983	Road Vehicles - Vehicle Identification Number (VIN) Content and Structure
ISO 3780:	1983	Road Vehicles World manufacturer identification code (WMI)
ISO 4217:		Codes for the representation of currencies and funds
ISO 7498-1:	1994	Information Processing Systems - Open Systems Interconnection - Basic Reference model
ISO/IEC 8824-1:	1995	Information processing systems - Open Systems Interconnection - Specification of abstract syntax notation one (ASN.1)
ISO/IEC 8825-2:	1996	Information processing systems - Open Systems Interconnection - ASN.1 encoding rules: Specification of Packed encoding rules
ENV 1545-1	1998	Identification card systems - Surface transport applications - Part 1 : General data elements
ENV 1545-2	1998	Identification card systems - Surface transport applications - Part 2 : Transport payment related data elements
prENV ISO 14816:	1998	Road Traffic and Transport Telematics (RTTT), Automatic Vehicle and Equipment Identification - Numbering and Data Structures (ISO/DTR 14816 : 1998)
ENV 12834:	1997	Road Traffic and Transport Telematics (RTTT), Dedicated Short-Range Communication (DSRC) - Application Layer

3 Definitions

For the purposes of this European Pre-Standard, the following definitions apply:

3.1 access credentials Data that is transferred to *On-Board Equipment,* in order to establish the claimed identity of an RSE application process entity.

NOTE: The access credentials carries information needed to fulfil access conditions in order to perform the operation on the addressed element in the OBE. The access credentials can carry passwords as well as cryptographic based information such as authenticators.

3.2 action Function that an application process resident at the *Roadside Equipment* can invoke in order to make the *On-Board Equipment* execute a specific operation during the *Transaction.*

3.3 attribute Application information formed by one or by a sequence of data elements, and is managed by different actions used for implementation of a *transaction.*

3.4 authenticator Data appended to, or a cryptographic transformation (see cryptography) 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.

3.5 channel An information transfer path [ISO/IEC 7498-2].

3.6 component Logical and physical entity composing an *On-Board Equipment*, supporting a specific functionality.

3.7 contract Expression of an agreement between two or more parties concerning the use of the road infrastructure.

3.8 cryptography The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification or/and prevent its unauthorised use [ISO/IEC 7498-2].

3.9 data group A collection of closely related EFC data attributes which together describe a distinct part of an Electronic Fee Collection transaction.

3.10 data integrity The property that data has not been altered or destroyed in an unauthorised manner [ISO 7498-2].

3.11 element In the context of DSRC, a directory containing application information in form of *Attributes.*

3.12 on-board equipment Equipment located within the vehicle and supporting the information exchange with the *Road Side Equipment.* It is composed of the *On-Board Unit* and other sub-units whose presence have to be considered optional for the execution of a *Transaction.*

3.13 on-board unit Minimum component of an *On-Board Equipment*, whose functionality always includes at least the support of the DSRC interface.

3.14 roadside equipment Equipment located at a fixed position along the road transport network, for the purpose of communication and data exchanges with the *On-Board Equipment* of passing vehicles.

3.15 service (EFC) Road transport related facility provided by a *Service Provider*. Normally a type of infrastructure, the use of which is offered to the *User* for which the *User* may be requested to pay.

3.16 service primitive (communication) Elementary communication service provided by the Application layer protocol to the application processes.

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

3.17 service provider (EFC) The operator that accepts the user's payment means and in return provides a road-use service to the user.

3.18 session The complete exchange of information and interaction occurring at a specific Electronic Fee Collection station between the *Roadside Equipment* and the user/vehicle.

3.19 transaction The whole of the exchange of information between the *Roadside Equipment* and the *On-Board Equipment* necessary for the completion of an Electronic Fee Collection operation over the DSRC.

NOTE: A transaction may require more than one session in order to be achieved, e.g. an entry session and an exit session.

3.20 transaction model Functional model describing the general structure of Electronic Fee Collection transactions.

3.21 user The entity that uses transport services provided by the *Service Provider* according to the terms of a *Contract*.

4 Abbreviations

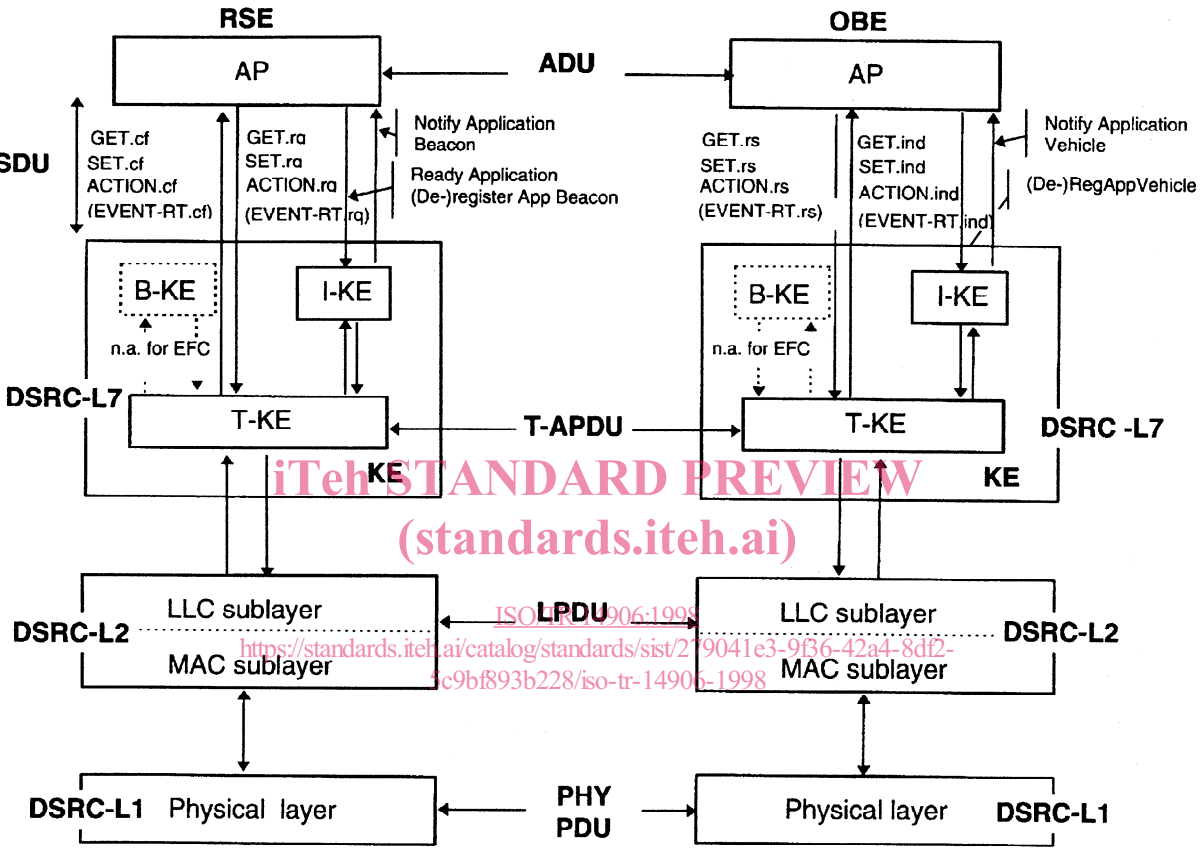
For the purpose of this European Pre-Standard, the following abbreviations apply throughout the document unless otherwise specified:

ADU	Application Data Unit
APDU	Application Protocol Data Unit
AP	Application Process
ASN.1	Abstract Syntax Notation One
BST	Beacon Service Table (DSRC Application Layer)
DSRC	Dedicated Short-Range Communications
EID	Element ID
EFC	Electronic Fee Collection
GPS	Global Positioning System
ICC	Integrated Circuit(s) Card
I-KE	Initialisation Kernel Element (DSRC Application Layer)
IID	Invoker ID
LID	Link ID
MMI	Man-Machine Interface
OBE	On-Board Equipment
OBU	On-Board Unit
PDU	Protocol Data Unit
PER	Packed Encoding Rules
RSE	Road-Side Equipment
RTTT	Road Traffic and Transport Telematics
SAM	Secure Application Module
T-APDU	Transport-Application Protocol Data Unit (DSRC Application Layer)
T-ASDU	Transport-Application Service Data Unit (DSRC Application Layer)
T-KE	Transport Kernel Element (DSRC Application Layer)
VST	Vehicle Service Table (DSRC Application Layer)

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 provider. The services are offered by the DSRC communication entities by means of its DSRC Application Layer (ENV 12834).



Additional abbreviations used only in this figure (for all other abbreviations see clause 4.)

B-KE	Broadcast-Kernel Element
LLC	Logical Link Control
LPDU	Link Protocol Data Unit
MAC	Medium Access Control
PHY-PDU	Physical Link Protocol Data Unit
req/ind/rs/cf	request/indication/response/confirm
EVENT-RT	EVENT-REPORT
n.a.	not applicable

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

The Transfer Kernel Element (T-KE) 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. a 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 (see clause 7.4) 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 I-KE as defined in ENV 12834, which in its turn is configured by the application(s) wishing to execute applications over the DSRC link.

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 ENV 12834):

- The INITIALISATION services:
  - (De-)Register Application RSE (at RSE)
  - Notify Application Beacon (at RSE)
  - Ready Application (at RSE)
  - (De-)Register Application OBE (at OBE)
  - Notify Application Vehicle (at OBE)

  are used to realise the EFC-specific initialisation mechanism (see clause 6)
- The GET service is used to retrieve EFC attributes (see annex B.2.1. For attribute specifications see clause 8)
- The SET-service is used to set EFC attributes (see annex B.2.2)
- 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 clause 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 Ready Application of ENV 12834). 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. All data elements of an ASN.1 type are mandatory. To each data element an unambiguously defined name is associated.

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:

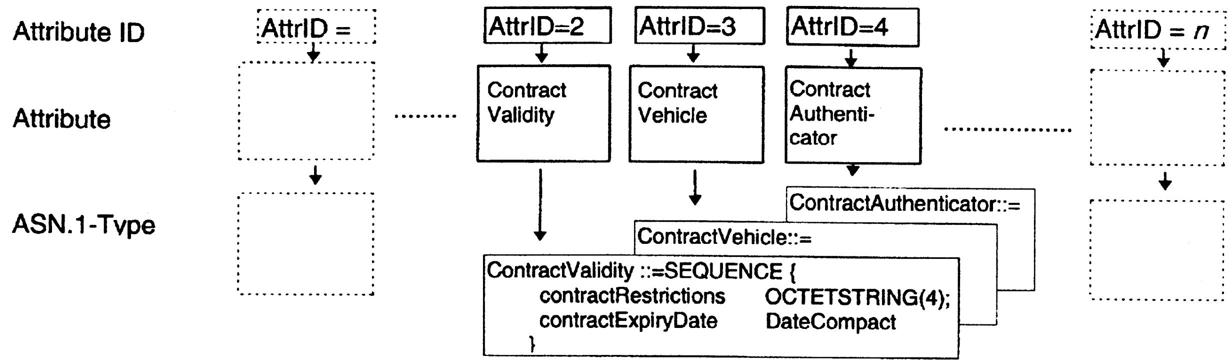


Figure 3: Basic addressing mechanism

5.3.2 Role of the EID

The DSRC-EID (different from 0) is used to identify an EFC context, given by the EFC-ContextMark (see clause 6.1.3), in which Attributes can be addressed unambiguously by AttributeIDs. In the VST, the OBE may specify several of these EFC contexts, each corresponding to a set of EFC Attributes and EFC functions supported by it.

EXAMPLE:

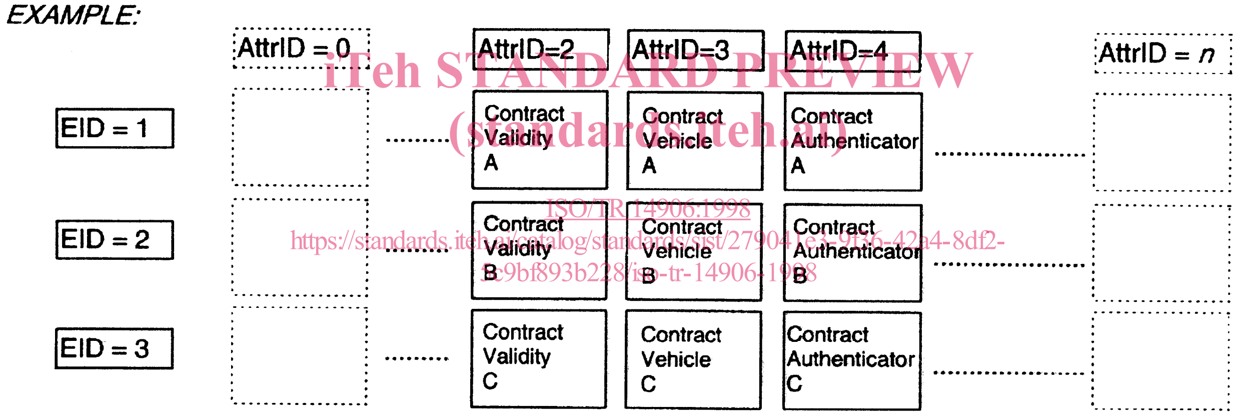


Figure 4: Role of the EID

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

5.3.3 Multiple Instances of Attributes

There may be n instances of an Attribute available in an 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:

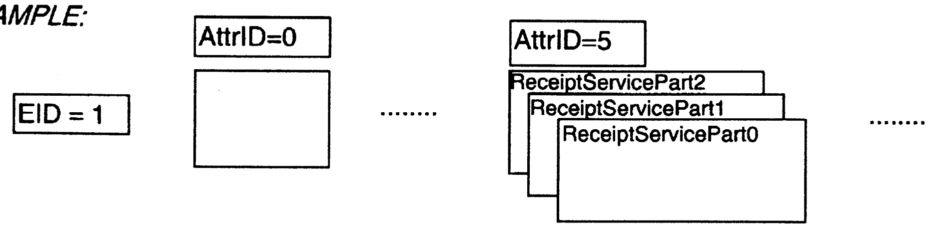


Figure 5: Multiple instances (0-2) of attribute 5

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 clause 7.2.5 for GET_INSTANCE and clause 7.2.6 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
- Beeper
- Printer
- Serial interface
- Parallel interface
- GPS
- Tachograph

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 clause 7.2.9) supports this functionality.

EXAMPLE: 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 OBU components. In this case, the operating system of the OBU will address the corresponding components. The EFC function SET_MMI supports this functionality (see clause 7.2.11).

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

> *NOTE: In addition, the OBE may use a kind of implicit addressing. In an implementation, specific attributes or data elements may activate some MMI function (e.g. a SET command on the attribute ReceiptText might display the text on an LCD display. A SET command on the attribute ReceiptServicePart with data element SessionResultOperational other than SessionOK might activate an alert beep).*