INTERNATIONAL STANDARD

**ISO 25110**

First edition
2017-11

# Electronic fee collection — Interface definition for on-board account using integrated circuit card (ICC)

*Perception du télépéage — Définition d'interface pour compte de bord utilisant une carte à circuit intégré (ICC)*

Reference number
ISO 25110:2017(E)



ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

# 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

This first edition cancels and replaces the second edition of ISO/TS 25110:2013.

The main changes compared to the previous edition are as follows:

— the document has been converted from a Technical Specification to an International Standard;

— terms have been amended, in order to reflect harmonization of terms across electronic fee collection (EFC) standards.

# Introduction

### Background and motivation

There are two payment systems dealing with electronic fee collection (EFC). The first is the central account system using a one-piece on-board unit (OBU) and the second is the on-board account system using a payment media such as the integrated circuit card (ICC).

ICCs have been widely used for public transport cards such as subway and bus payment means and electronic money cards for general purpose payments, as well as for credit cards and banking cards. The ICC is expected to be used for EFC payment means along with these global trends and provides convenience and flexibility.

Currently, the descriptions in the existing EFC-related International Standards are focused on the central account system, which is rather simple and gives more feasibility for EFC interoperability than the on-board account system, which is complex and has more items to be settled.

With consideration of the widespread use for transport cards or electronic money cards, a new International Standard relating the on-board account system using those ICCs is strongly required as shown in Figure 1. Furthermore, a state-of-the-art mobile phone integrated with ICC functions, a so-called "mobile electronic purse", has been used for public transport or retail shopping as a payment means in some countries so rapidly that standardization on this theme is important and essential for considering future EFC payment methods as well.

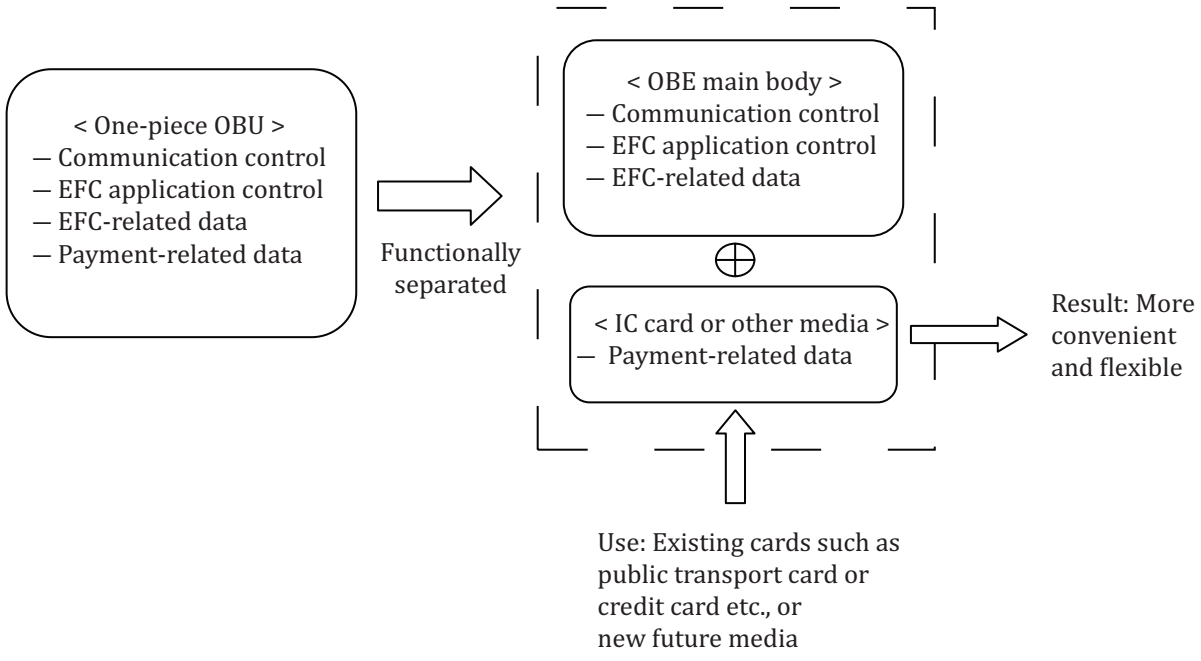



**Figure 1 — Motivation for on-board account using ICC**

Figure 2 shows the scope of the EFC standards, in which the OBU is used as a communication means and the ICC carries the payment means.

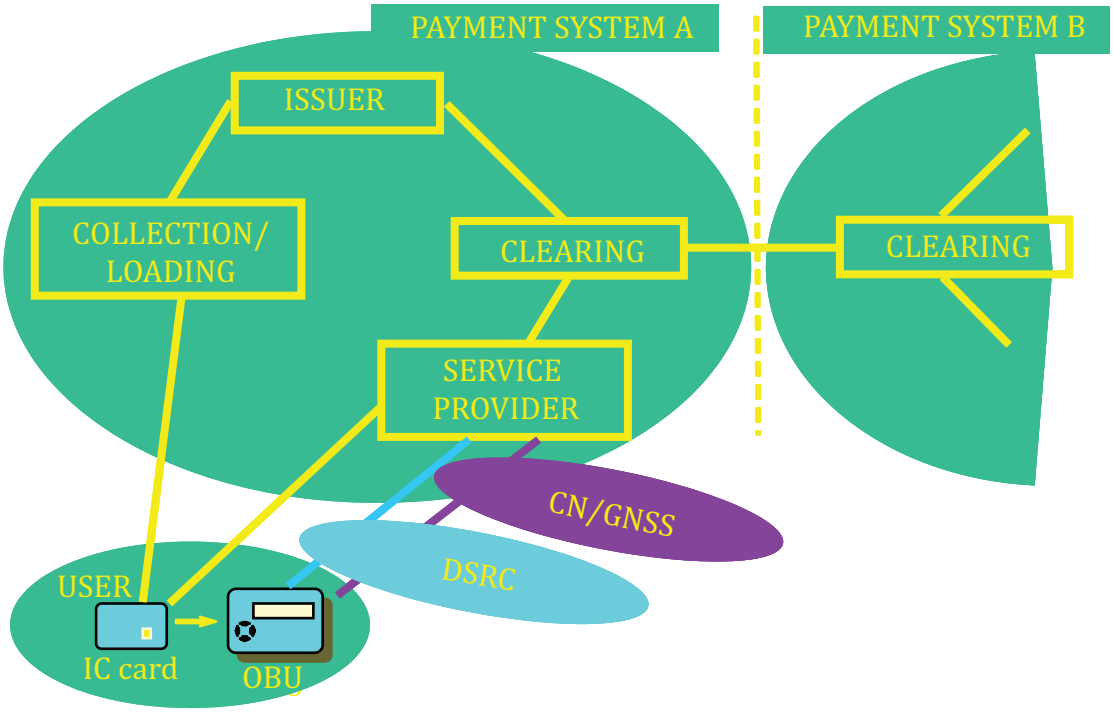



**Figure 2 — Illustration of the scope of the EFC standards**

**Objective**

The objective of this document is to classify data transfer models based on operational requirements and define a specific ICC access interface for on-board accounts using the ICC for each model. Furthermore, this document provides practical examples of transactions in Annex B, for consideration and easy adoption by toll road operators.

**Use**

This document provides a common technical platform for on-board accounts using ICCs to deal with various operational requirements and practical examples of on-board accounts actually used or planned in several countries.

Each toll road operator can establish their own specification by selecting an example of the models in this document (like a tool box) so as to meet their requirements.

# Electronic fee collection — Interface definition for on-board account using integrated circuit card (ICC)

## 1 Scope

This document defines the data transfer models between roadside equipment (RSE) and integrated circuit card (ICC) and the interface descriptions between the RSE and on-board equipment (OBE) for on-board accounts using the ICC. It also provides examples of interface definitions and transactions deployed in several countries.

This document covers:

— data transfer models between the RSE and ICC which correspond to the categorized operational requirements and the data transfer mechanism for each model;

— interface definition between the RSE and OBE based on each data transfer model;

— interface definition for each model;

— functional configuration;

— RSE command definitions for ICC access;

— data format and data element definitions of RSE commands;

— a transaction example for each model in Annex B.

Figure 3 shows the configuration of an on-board account and the scope of this document. The descriptions in this document focus on the interface between the RSE and OBU to access the ICC.

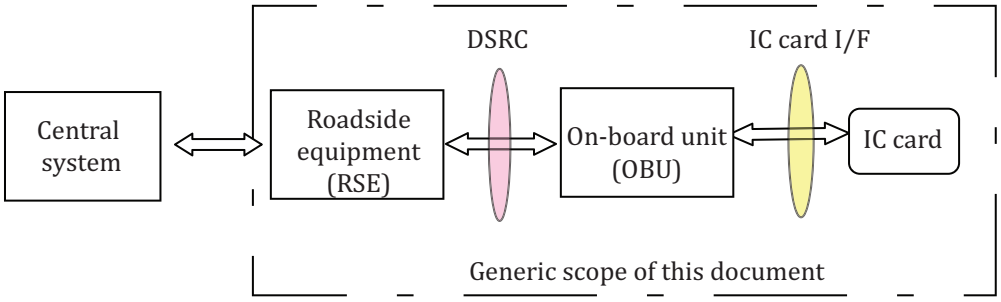



**Figure 3 — Configuration of an on-board account and the scope of this document**

Figure 4 shows the layer structure of the RSE, OBU and ICC where the mid-layer of application interfaces are denoted as the practical scope of this document.

NOTE The existing standards for physical and other protocol layers both between the RSE and OBE, and between OBE and ICC, are outside the scope of this document. For example, DSRC-related items (L-1, L-2 and L-7) and ICC-related items (ICC commands, data definition, etc.) are outside the scope of this document.

There are two types of virtual bridges contained in an OBU. The first type is Bridge-1 on which an RSE command sent from the RSE is decomposed and the ICC access command contained in the application protocol data unit (APDU) part of the RSE command is transferred to ICC I/F to access the ICC. The second type is Bridge-2 in which an RSE command sent from the RSU is transformed to ICC access command and transferred to ICC I/F to access the ICC.

Bridge-1 corresponds to the transparent type and the buffering type defined in this document, whereas Bridge-2 corresponds to the cashing type.

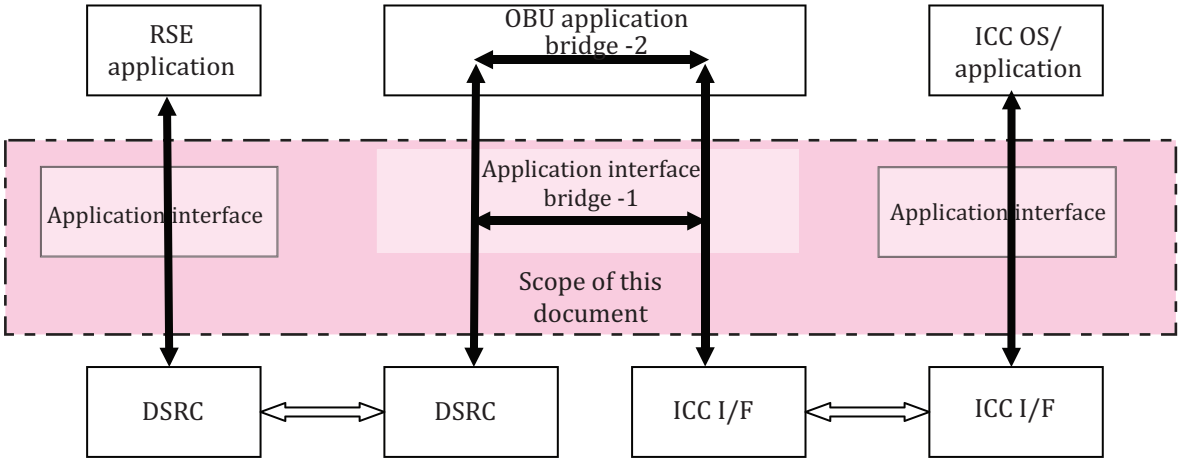



**Figure 4 — Application interfaces of RSE, OBU and ISS and the scope of this document**

## 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 14906, *Electronic fee collection — Application interface definition for dedicated short-range communication*

ISO 15628, *Intelligent transport systems — 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

Note 1 to entry: The access credentials carry information needed to fulfil access conditions in order to perform the operation on the addressed element in the *OBE* (3.10). The access credentials can carry passwords as well as cryptographic-based information such as *authenticators* (3.3).

[SOURCE: EN 15509:2014, 3.1]

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

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

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

[SOURCE: EN 15509:2014, 3.3]

**3.4**
**channel**
information transfer path

[SOURCE: ISO 7498-2:1989, 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

[SOURCE: EN 15509:2014, 3.6]

**3.6**
**data group**
class of closely related *attributes* (3.2)

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

**3.7**
**data integrity**
property in which data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 14906:2011, 3.10 — modified]

**3.8**
**Element**
<DSRC> directory containing application information in the form of *attributes* (3.2)

[SOURCE: ISO 14906:2011, 3.11]

**3.9**
**issuer**
entity responsible for issuing the payment means to the user

[SOURCE: ISO/TS 16785:2014, 3.9]

**3.10**
**on-board equipment**
**OBE**
all required equipment on-board a vehicle for performing required EFC functions and communication services

**3.11**
**on-board unit**
single electronic unit on-board a vehicle for performing specific EFC functions and for communication with external systems

**3.12**
**roadside equipment**
equipment located along the road, either fixed or mobile

**3.13**
**secure application module**
**SAM**
physical module that securely executes cryptographic functions and stores keys

[SOURCE: ISO/TS 19299:2015, 3.35]

**3.14**
**service primitive**
<communication> elementary communication service provided by the application layer protocol to the application processes

[SOURCE: ISO 14906:2011, 3.18]

**3.15**
**transaction**
whole of the exchange of information between two physically separated communication facilities

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

**3.16**
**transaction model**
functional model describing the general structure of electronic payment fee collection transactions

[SOURCE: ISO 14906:2011, 3.25]

**3.17**
**transport service provider**
entity providing a transport-related service, such as provision of roads

## 4 Abbreviated terms

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

| | |
|---|---|
| AID | Application Identifier |
| APDU | Application Protocol Data Unit |
| ASN.1 | Abstract Syntax Notation One (see ISO/IEC 8824-1) |
| ATR | Answer to Reset |
| ATS | Answer to Select |
| BST | Beacon Service Table |
| DSRC | Dedicated Short-Range Communication |
| EAL | Evaluation Assurance Level |
| EFC | Electronic Fee Collection |
| EID | Element Identifier |
| ERP | Electronic Road Pricing |
| EVENT-RT | EVENT-Report (see ISO 15628) |
| MAC | Medium Access Control |

| | |
|---|---|
| ICC | Integrated Circuit(s) Card (IC card) |
| IFMS | Interoperable Fare Management System |
| OBE | On-Board Equipment |

# 5 Data transfer models

## 5.1 General

There are three types of data transfer models for on-board accounts using the ICC to cope with the operational requirements described in Annex A.

### 5.1.1 Transparent type

The ICC command data are transferred directly from the RSE to the ICC through the OBU. The OBU temporarily stores the ICC command data and response data in the buffer memory. See Figure 5.

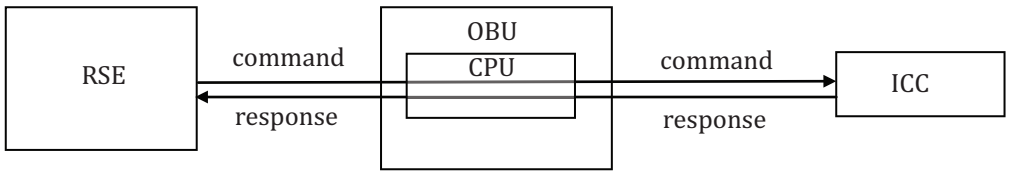



**Figure 5 — Generic structure of transparent type**

### 5.1.2 Caching type

The EFC-related data are read out from the ICC at the presentation and stored in the SAM of the OBU. In the DSRC communication, the EFC-related data in the SAM is transferred to the RSE. See Figure 6.

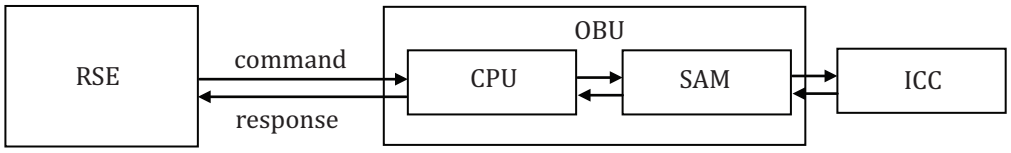



**Figure 6 — Generic structure of caching type**

### 5.1.3 Buffering type

The EFC-related data which is limited to non-sensitive data are read from the ICC at the presentation and stored in the buffer memory in the OBU. In the DSRC communication, the EFC-related data in the buffer memory is transferred to the RSE. See Figure 7.

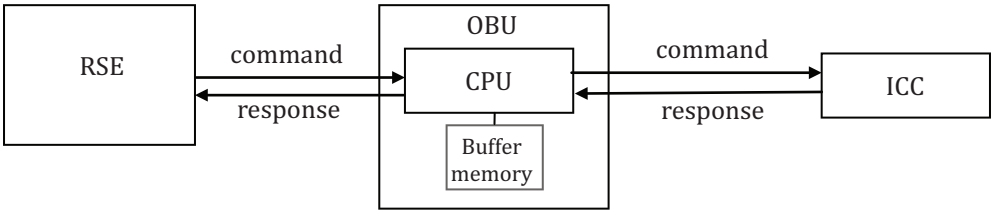



**Figure 7 — Generic structure of buffering type**

## 5.2 Symbols

In the data transfer mechanism of each model, the symbols given in Figure 8 are applied.

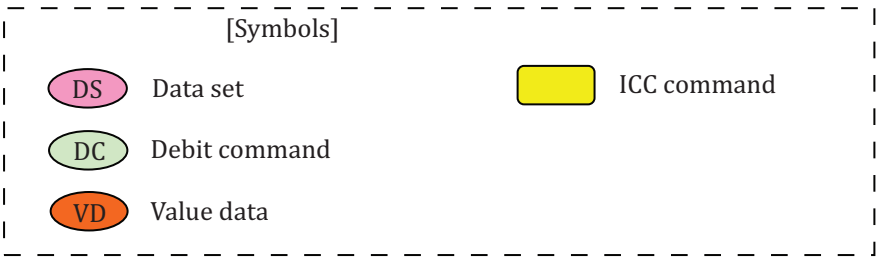



**Figure 8 — Definition of symbols**

## 5.3 Transparent type

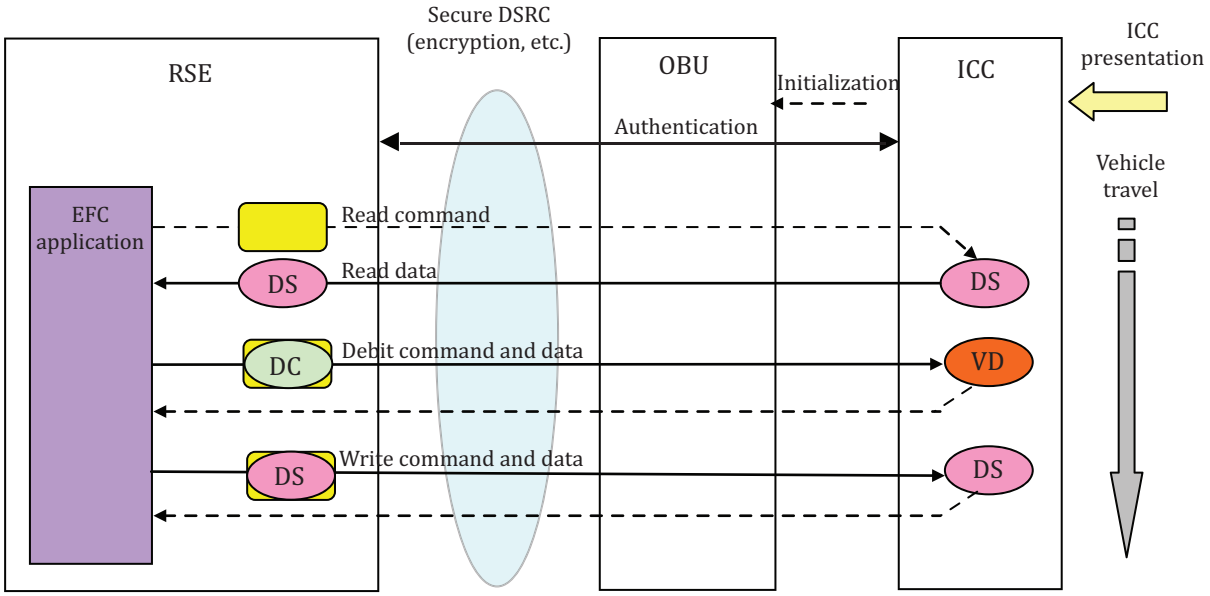
### 5.3.1 General

In this model, the maximum vehicle speed depends on the data transfer rate between the ICC and OBU so that the vehicle has to stop or go through slowly under an RSE antenna in case a conventional contact ICC is used. The feature of the transparent type is to make the OBU simple by eliminating the secure memory inside of the OBU and the performance will be improved according to the developing ICC with high transfer data rate.

### 5.3.2 Data transfer process

In this model, data exchanges between the RSE and ICC are processed directly after establishing DSRC communication and authentication between the RSE and OBU is completed. Mutual authentication between the ICC and RSE is processed directly before the application data are exchanged and value data are accessed.

In the reading sequence, the READ command is sent from the RSE to the ICC through the OBU to read out the data set stored in the ICC. In the READ response, the data set stored in the ICC is transferred from the ICC to the RSE through the OBU. In the writing sequence, the same procedure is processed. In case of prepaid payment, the debit command is sent from the RSE and the same procedure is processed, as shown in Figure 9.




NOTE Debit command is used in case of prepaid payment.

**Figure 9 — Data transfer process of transparent type**

## 5.4 Caching type

### 5.4.1 General

In this model, the OBU reads out datasets from the ICC and stores them in a secure memory inside the OBU, upon insertion and completion of the authentication. The feature of this type is that the high data exchange rate between the RSE and OBU is performed even when the ICC with slow data rate is used. With this caching type, maximum vehicle speed is enhanced up to DSRC communication performance irrelevant to the data transfer rate of the ICC.

### 5.4.2 Data transfer process

In this model, read out data from the ICC is stored in a secure memory such as a SAM inside the OBU to ensure information security.

The feature of this type is to cope with high vehicle speed by processing high data exchange rate between the RSE and OBU irrelevant to type of the ICC. See Figure 10.

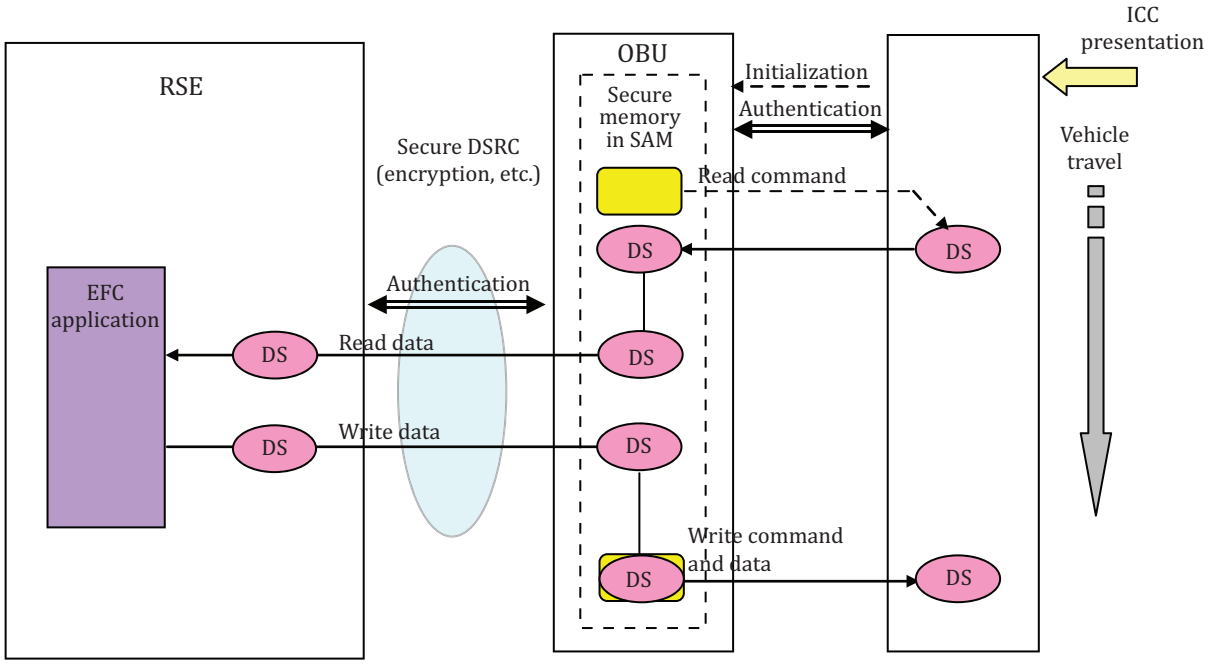



**Figure 10 — Data transfer process of caching type**

## 5.5 Buffering type

### 5.5.1 General

This buffering type has features of both the transparent type and the cashing type. However, datasets stored in the ICC are limited to non-sensitive data not to be suffered from falsification or disclosure. In this buffering type, the data transfer method is the same as the cashing type and datasets of the ICC are read out and stored in a buffer memory inside the OBU when the ICC is inserted into the OBU. Datasets stored in the buffer memory are transferred to the RSE during DSRC read sequence. In case of writing, datasets of RSE are transferred to the OBU and stored in the buffer memory of the OBU and then transferred to the ICC.

### 5.5.2 Data transfer process

The feature of this type is to be able to eliminate the SAM in the OBU and to use even low speed ICC. See Figure 11.

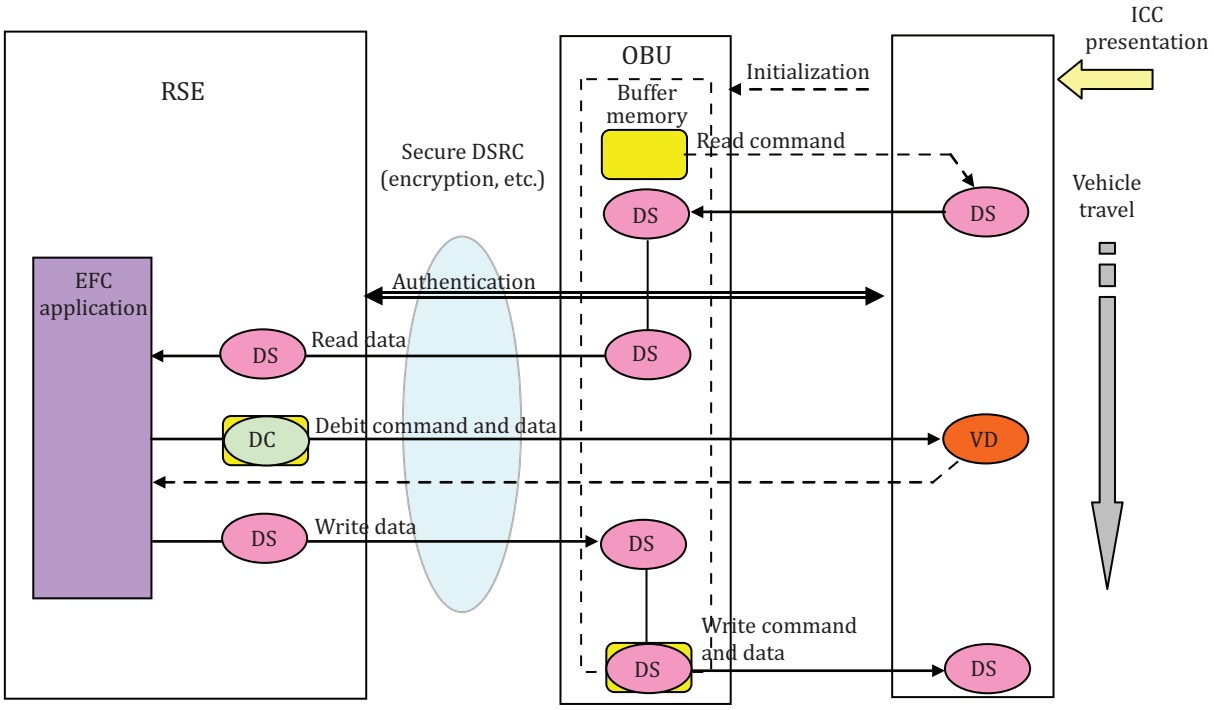



**Figure 11 — Data transfer process of buffering type**

# 6 Interface definition for ICC access

## 6.1 Transparent type

### 6.1.1 Functional configuration

Functional configuration of the transparent type is shown in Figure 12. The RSE sends the RSE command containing ICC access commands in its ADPU so as to execute the ICC read/write operation directly.

The command definition between the OBU and ICC should be based on ISO/IEC 7816-4.

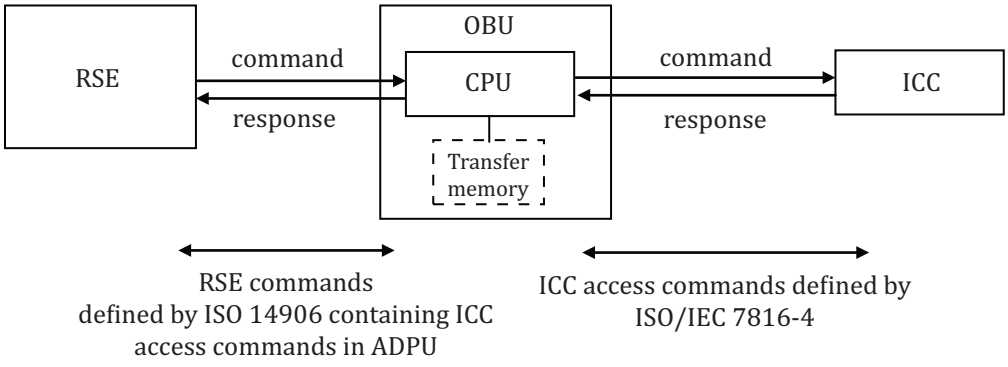



**Figure 12 — Functional configuration of transparent type**

### 6.1.2 Command and response between the RSE and OBU

Transfer Channel defined by ISO 14906 is used as a basic RSE command to access ICC from RSE directly with designating the channel ID in the Action Parameter as channel ID = ICC(3). Refer to Tables 1 and 2.

**Table 1 — TRANSFER_CHANNEL.request**

| Parameter | ASN.1 Type | Value | Remarks |
|---|---|---|---|
| Element Identifier EID | Dsrc-Eid | 0 | |
| Action Type | INTEGER(0..127,..) | 8 | Transfer Channel |
| AccessCredentials | OCTET STRING | | |
| ActionParameter | ChannelRq:: = SEQUENCE {<br>channelId ChannelId,<br>apdu OCTET STRING<br>} | | Always to be present<br>Channel ID = ICC (3) |
| Mode | BOOLEAN | TRUE | |

The apdu in ActionParameter shall contain the ICC command.

**Table 2 — TRANSFER_CHANNEL.response**

| Parameter | ASN.1 Type | Value | Remarks |
|---|---|---|---|
| ResponseParameter | ChannelRs:: = SEQUENCE {<br>channelId ChannelId,<br>apdu OCTET STRING<br>} | | Always to be present |
| Return Code(Ret) | Return Status | | Optional use |

The apdu in ResponseParameter shall contain the ICC response.

## 6.2 Caching type

### 6.2.1 Functional configuration

The functional configuration of the caching type is shown in Figure 13. Datasets stored in the ICC are read out and cached in the SAM of the OBU when the ICC is inserted to the OBU. During DSRC communication, the RSE sends the RSE command including the SAM access command in its ADPU to read data sets cached in the SAM.

The command definition between the SAM and ICC should be based on ISO/IEC 7816-4.

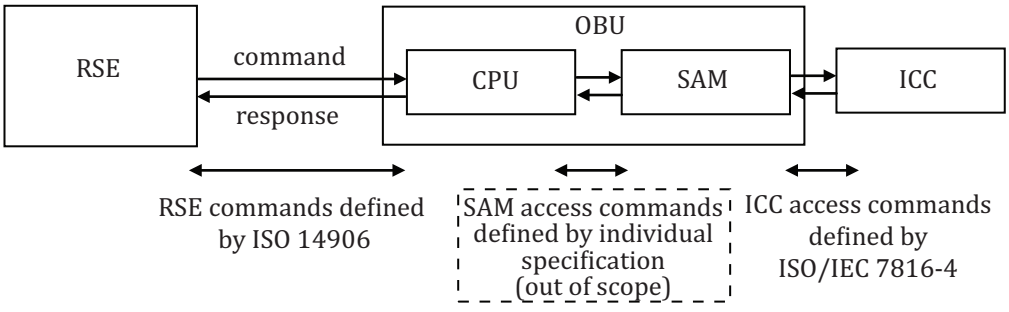



**Figure 13 — Functional configuration of caching type**

### 6.2.2 Command and response between the RSE and OBU

Transfer Channel defined by ISO 14906 is used as the basic RSE command to access SAM of OBU from RSE directly with designating the channel ID in Action Parameter as channel ID = SAM1(1) or SAM2(2). Refer to Tables 3 and 4.

**Table 3 — TRANSFER_CHANNEL.request**

| Parameter | ASN.1 Type | Value | Remarks |
|---|---|---|---|
| Element Identifier EID | Dsrc-Eid | 0 | |
| Action Type | INTEGER(0..127,..) | 8 | Transfer Channel |
| AccessCredentials | OCTET STRING | | |
| ActionParameter | ChannelRq:: = SEQUENCE {<br>channelId ChannelId,<br>apdu OCTET STRING<br>} | | Always to be present<br>Channel ID = SAM1 (1) or SAM2(2) |
| Mode | BOOLEAN | TRUE | |

The apdu in ActionParameter shall contain the ICC command or its data elements.

**Table 4 — TRANSFER_CHANNEL.response**

| Parameter | ASN.1 Type | Value | Remarks |
|---|---|---|---|
| ResponseParameter | ChannelRs:: = SEQUENCE {<br>channelId ChannelId,<br>apdu OCTET STRING<br>} | | Always to be present |
| Return Code(Ret) | Return Status | | Optional use |

The apdu in ResponseParameter shall contain the ICC response or its data elements.

## 6.3 Buffering type

### 6.3.1 Functional configuration

The functional configuration of the buffering type is shown in Figure 14. Datasets stored in the ICC are read out and stored in the buffer memory of the OBU when the ICC is inserted to the OBU. During DSRC communication, the RSE sends the RSE command to read datasets stored in buffer memory.

The command definition between the OBU and ICC should be based on ISO/IEC 7816-4.

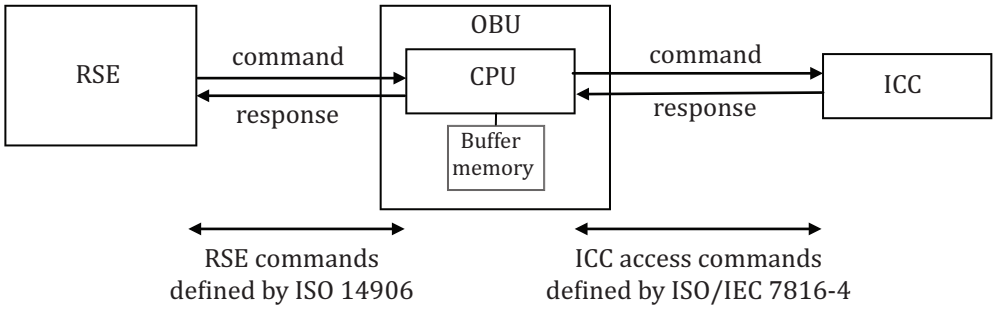



**Figure 14 — Functional configuration of buffering type**

### 6.3.2 Command and response between the RSE and OBU

Since in this buffering type necessary data sets stored in ICC are transferred to buffer memory of OBU, GET or SET primitive is used as the RSE command. Furthermore, Debit or Credit of the EFC function defined by ISO 14906 is used for the prepaid payment process. Refer to Tables 5 and 6.

**Table 5 — DEBIT.request**

| Parameter | ASN.1 Type | Value | Remarks |
|---|---|---|---|
| Element Identifier EID | Dsrc-Eid | | Unequal 0 |
| Action Type | INTEGER(0..127,..) | 13 | |
| AccessCredentials | OCTET STRING | | Optional use |
| ActionParameter | DebitRq:: = SEQUENCE {<br>debitPaymentFee PaymentFee,<br>nonce OCTET STRING<br>keyRef INTEGER(0..255)<br>} | | Always to be present |
| Mode | BOOLEAN | TRUE | |

Each parameter in ActionParameter shall contain data elements of the debit command for ICC.

**Table 6 — DEBIT.response**

| Parameter | ASN.1 Type | Value | Remarks |
|---|---|---|---|
| ResponseParameter | DebitRs:: = SEQUENCE {<br>debitResult ResultFin,<br>debitAuthenticator OCTET STRING<br>} | | Always to be present |
| Return Code(Ret) | Return Status | | Optional use |

Each parameter in ResponseParameter shall contain data elements of the debit response for ICC.

# Annex A
(informative)

# On-board account requirements

## A.1 Operational requirements for on-board account

The major factors of operational requirements for EFC are vehicle speed and information security level as shown in Figure A.1, which both largely influence the design of the EFC system. The information security levels in Figure A.1, referred to as evaluation assurance levels (EALs), are defined in the ISO 15408 series.

Category-4 is performed by a specially designed security mechanism such as an SAM embedded in the OBU in addition to the ICC security mechanism, while Categories-1, -2 and -3 security mechanisms are performed by the ICC.

Category-4 covers all EFC services with high security level. Category-1 covers parking payment and drive-through payment where the vehicle stops for a moment or goes through at low speed under the roadside antenna. Category-2 covers Category-1 and EFC services in a single lane. Category-3 covers Category-2 and EFC/ERP in a multi-lane free flow, where the vehicle goes through at high speed under the roadside antenna.

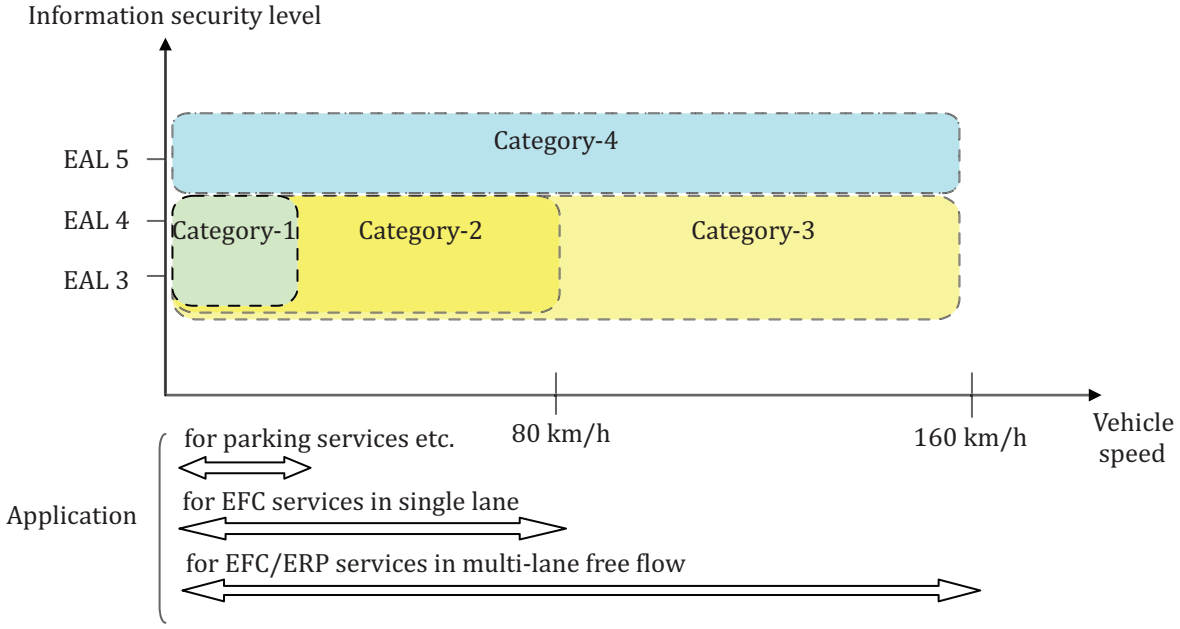



**Figure A.1 — Operational requirements**

## A.2 Types of ICC

The ICC used for on–board accounts is classified as described in Figure A.2. The contact type ICC based on the ISO/IEC 7816 series is largely used by financial cards, such as bank and credit cards. The contact-less ICC based on the ISO/IEC 14443 series or ISO/IEC 18092 is largely used by the public transport sector, as a payment means and for ticketing. The hybrid type ICC has both functions defined by the ISO/IEC 7816 series and the ISO/IEC 14443 series or ISO/IEC 18092 as well and is used for multi-function cards such as EFC cards and public transport cards.

There are several options when the ICC is used for EFC. One option is to use it just for payment. Another option is to use it both for payment and data storage for EFC-related data.

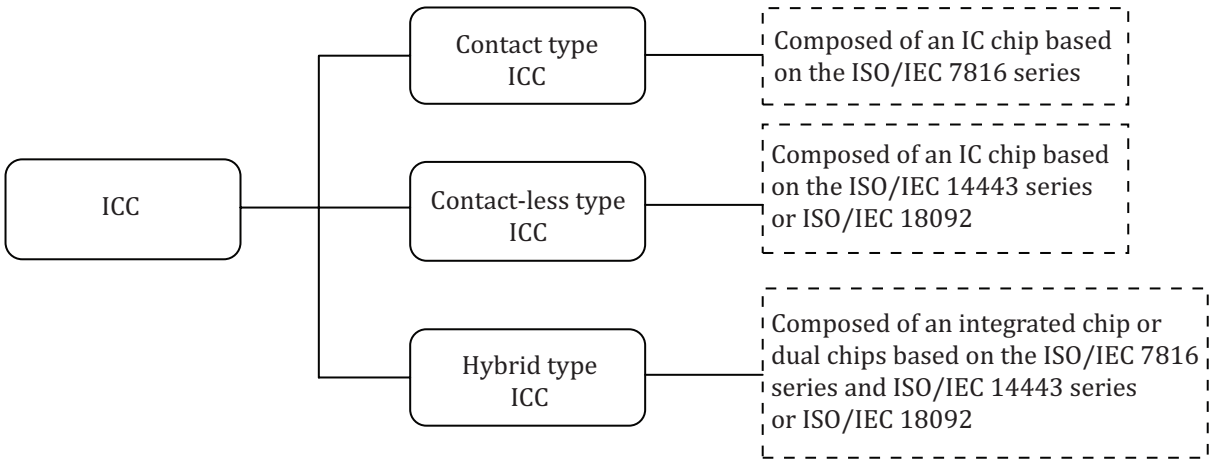



**Figure A.2 — Types of IC cards**

## A.3 Interoperability requirements for the ICC

For its feature of secure and portable aspects, the ICC is potentially required to have interoperability with other services as a common payment means. The interoperability level required for the ICC is assumed to be classified into the following three levels.

Level-1: Interoperability within the group of contracted toll road operators

Level-2: Interoperability expanded for public transport applications

Level-3: Interoperability expanded further for retail applications

Especially with regard to Level-2, the interoperability scheme should be considered based on the collaboration with EFC architecture and IFMS architecture of public transport.

Annex C shows the operational interoperability relation where the ICCs issued for EFC are required to be used for public transport and/or retail applications.

## A.4 Performance of each transfer model

Table A.1 shows the relation with category domains defined from operational requirements and data transfer models.

**Table A.1 — Relation with category domains and data transfer models**

| Category | Data transfer model | | |
|---|---|---|---|
| | Transparent type | Caching type | Buffering type |
| Category-1 | × | | |
| Category-2 | × | | |
| Category-3 | × | | × |
| Category-4 | | × | |

NOTE In the case of the transparent type, each category depends on the transfer rate of the ICC type.

# Annex B
(informative)

# Example of an ICC access method

## B.1 Transparent type model

### B.1.1 Transparent type model-1 (for prepaid payment)

#### B.1.1.1 General

As an example of this transparent type, the transparent type model-1, the ICC is accessed by using the transfer channel function defined in ISO 14906.

— Command: TRANSFER_CHANNEL defined by ISO 14906

— AID: Electronic fee collection (EFC) as AID = 1 by ISO 14906

— Channel ID: ICC defined as ChannelID = icc(3) by ISO 14906

— ICC type: Contact-less type prepaid ICC

#### B.1.1.2 Data type definition

a) Definition of APDU contents in TransferChannel.rq

```
ICCcommand:: = SEQUENCE{
opCommandBody OCTET STRING – ICC command ISO/IEC 7816-4

}
```

b) Definition of APDU contents in TransferChannel.rs

```
ICCresponse:: = SEQUENCE{
opCommandBody OCTET STRING – ICC response ISO/IEC 7816-4

}
```

#### B.1.1.3 Transaction

##### B.1.1.3.1 ETC distance-based charging (closed system)

a) Entrance system

At the entrance, the mutual authentication between RSE and ICC is done, and entrance information is recorded in the ReceiptServicePart of the OBU memory, see Figure B.1.

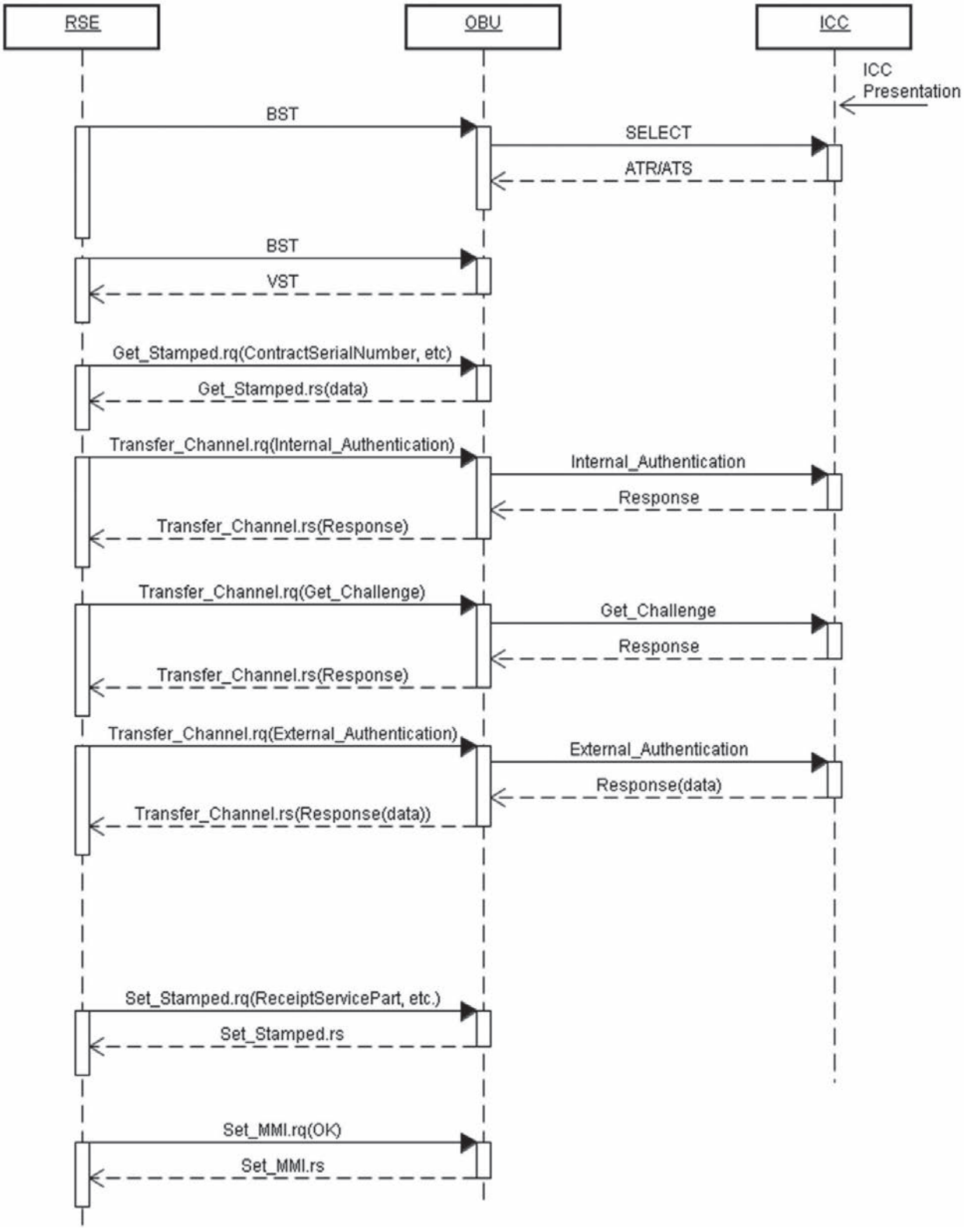



**Figure B.1 — Sequence flow of entrance system**

b) Exit system

At the exit, RSE reads the entrance information from the OBU and keeps it in the memory of RSE and the mutual authentication between RSE and ICC is done. RSE calculates the fee according to the entrance

information, and sends the debit command to the ICC directly via OBU by using the transfer channel function, see Figure B.2.

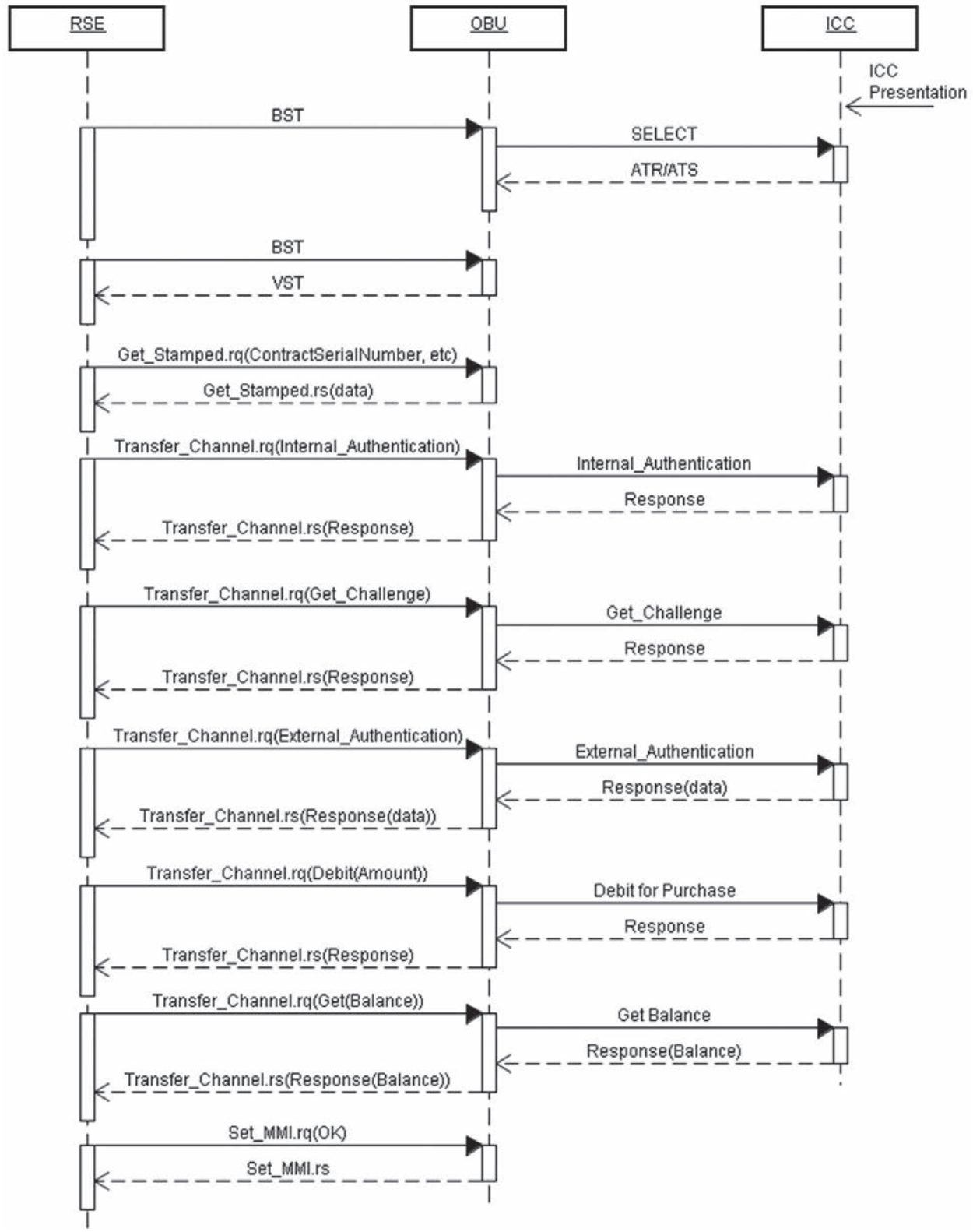



**Figure B.2 — Sequence flow of exit system**

### B.1.2 Transparent type model-2 (for post payment)

#### B.1.2.1 General

As an example of this transparent type model-b, the ICC access method defined in the "DSRC basic application interface" established by the ITS Forum in Japan is introduced.

The "DSRC basic application interface" is established so as to provide multiple information services such as traffic and road information, traveller's information and parking information, etc., with identifying application ID as AID = 18 registered in ISO 15628. In addition to these major information services, the ICC access is defined for parking payment application.

In this subclause, Send Message defined in the "DSRC basic application interface" is introduced as an equivalent method of Transfer Channel described in ISO 14906:2011, 7.1.

— Command definition: Defined by DSRC basic application interface (ITS Forum RC-004 in Japan)

— Command: TRANSFER_CHANNEL defined by ISO 14906

— AID: Electronic fee collection (EFC) as AID = 1 by ISO 14906

— Channel ID: ICC defined as ChannelID = icc(3) by ISO 14906

— ICC type: Contact-type ICC with credit payment

#### B.1.2.2 Data type definition

a) Definition of APDU contents in TransferChannel.rq

```
CCAccessCommand:: = SEQUENCE{
   versionIndex   Version,
   accessCommand  AccessCommand
}
Version:: = SEQUENCE{
   version INTEGER(0..15),
   fill     BIT STRING(SIZE(4)) –0 fill
}
AccessCommand:: = CHOICE{
   dummy                  [0]     NULL,
   operationCommand       [1]     OperationCommand,
   accreditationInfoCommand[2]    AccreditationInfoCommand,
   dummy                  [3–254] NULL,
   obuDenialResponse      [255]   ObuDenialResponse
}
```

```
operationCommand:: = SEQUENCE{
   opCommandType   OpCommandType,
   opSecurityProfileOpSecurityProfile,
   opCommandBody   OCTET STRING – ICC command/response ISO/IEC 7816-4
}
OpCommandType:: = ENUMERATED{
   iCCCommand          (0),    – ICC command send
   reservedForFutureUse        (1),
   endRequest          (2),
   initRequest         (3),
   reservedForFutureUse        (4–127),
   iCCResponse         (128),  – ICC response send
   reservedForFutureUse        (129),
   endResponse         (130),
   initResponse        (131),
   reservedForFutureUse        (132–255)
}
```

b) Definition of APDU contents in TransferChannel.rs

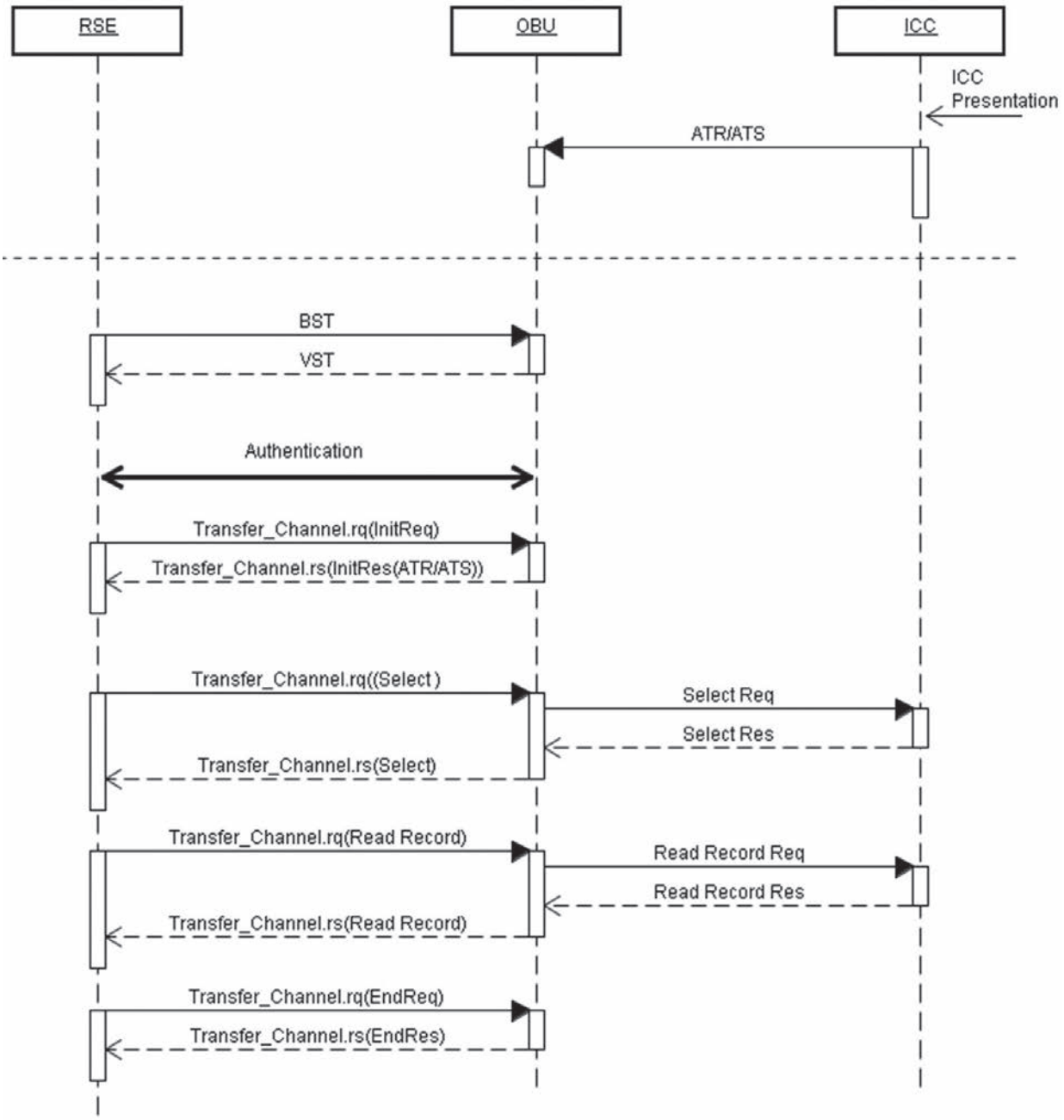
```
ICCAccessResponse:: = SEQUENCE{
   versionIndex   Version,
   accessCommand  AccessCommand
}
```

#### B.1.2.3 Transaction

##### B.1.2.3.1 Parking system

a) Simple system (centre chaining method)

In this system, the parking fee should be paid by the credit card number registered to the centre system in which the credit card number and the membership number are chained. In order to contract membership and payment, the credit card number has to be registered to the centre system beforehand, see Figure B.3.

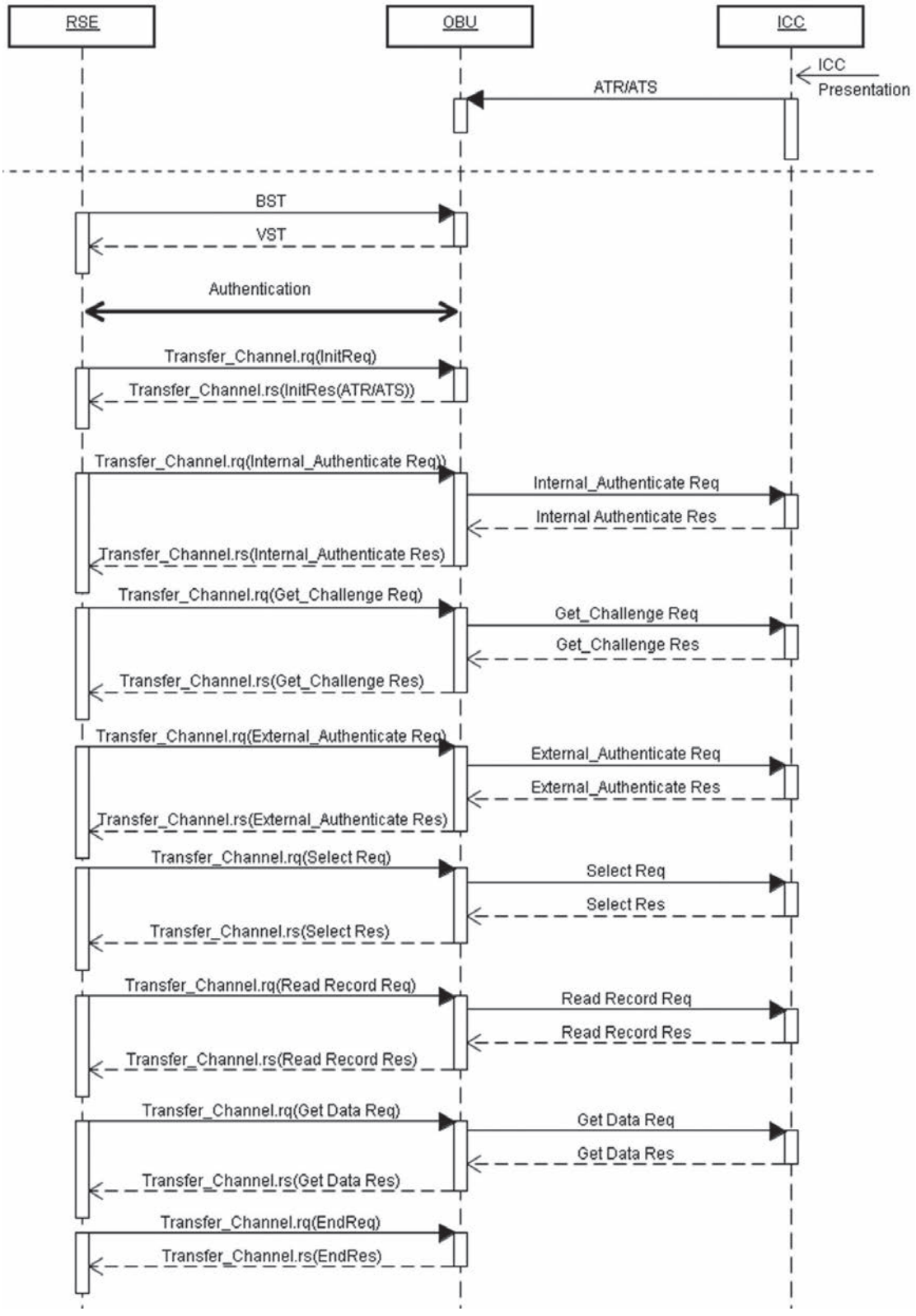



NOTE The membership number is contained in the Read Record Res.

**Figure B.3 — Sequence flow of simple system (centre chaining method)**

b) Complex system (direct method)

In this system, the parking fee should be paid by the credit card number read out from the credit ICC directly, see Figure B.4.




NOTE The credit card number is contained in the Read Record Res.

**Figure B.4 — Sequence flow of complex system (direct method)**

## B.2 Caching type model

### B.2.1 General

As an example of this caching type model, the ICC access method used for Japanese ETC is described. In Japanese ETC, distribution of the OBU is based on retailing at auto-shops and any manufacturer can participate in the OBU market by getting type approval from the testing institute. Therefore, the data security level for ICC and toll collection-related data stored in the OBU require high level and the approved OBU manufacturers have to equip SAM provided from certified SAM manufacturers by the trusted third party (see NOTE 1 below).

— Command definition: Defined by the DSRC interface standard (ETC-B02230P) using for Japanese ETC

— Command: TRANSFER_CHANNEL defined by ISO 14906

— AID: Electronic Fee Collection (EFC) as AID = 1 or Multi-Purpose Payment (MPP) defined as AID = 14 by ISO 14906 (see NOTE 2 below)

— ICC type: Contact-type ICC for credit payment

NOTE 1 The reasons why the SAM is adopted in Japanese ETC are:

— to implement a caching mechanism in the OBU to ensure high performance even when using low-speed contact-type ICC;

— to ensure compatibility with regard to the ETC application and the security mechanism between the RSE and OBU. The SAM contains not only a security mechanism but also an ETC application to perform caching and data handing processes with the ICC;

— to maintain competitiveness and to spread OBU nationwide quickly.

NOTE 2 Explanation of AID = 14:

— AID = 14 usage is described in ISO 14906.

— AID equal to 14 identifies the multi-purpose payment context. In Japan, ISO 14906 specifies the application interface for DSRC used for multi-purpose payment (when the AID = 14 is used in Japan, the EID and parameter fields are defined through the BST).

### B.2.2 Data type definition

a) Definition of ADPU contents in TransferChannel.rq

```
RSECommand:: = SEQUENCE{
   eid            Dsrc-EID,
   parameter      OCTET STRING                  -Parameter not included in
                  (SIZE(0..255)),               subcommand
   subCommandList SEQUENCE(0..255) OF           -Sub command list
                  SubCommand
}
SubCommand:: = CHOICE{
   dgetRq              [0]     DgetRq,
   dgetRs              [1]     DgetRs,
   dget_instanceRq     [2]     Dget_instanceRq,
```

```
   dget_instance Rs    [3]     Dget_instanceRs,
   dsetRq              [4]     DsetRq,
   dsetRs              [5]     DsetRs,
   dendRq              [6]     DendRq,
   dendRs              [7]     DendRs,
   dummy               [8–31]  NULL – Future use
}
DgetRq:: = SEQUENCE{
   fill              BIT STRING (SIZE(3)),
   attributeIdList  AttributeIdList
}
DsetRq:: = vSEQUENCE{
   fill              BIT STRING (SIZE(2)),
   delete            BOOLEAN,
   attributeIdList   AttributeIdList,
   dataList          DataList
}
DataList:: = SEQUENCE(0..255) OF Data
Data:: = OCTET STRING(1..255)
AttributeIdList:: = SEQUENCE(0..255)OF attributeID
attributeID:: = INTEGER(0..127,..)
```

b) Definition of ADPU in TransferChannel.rs

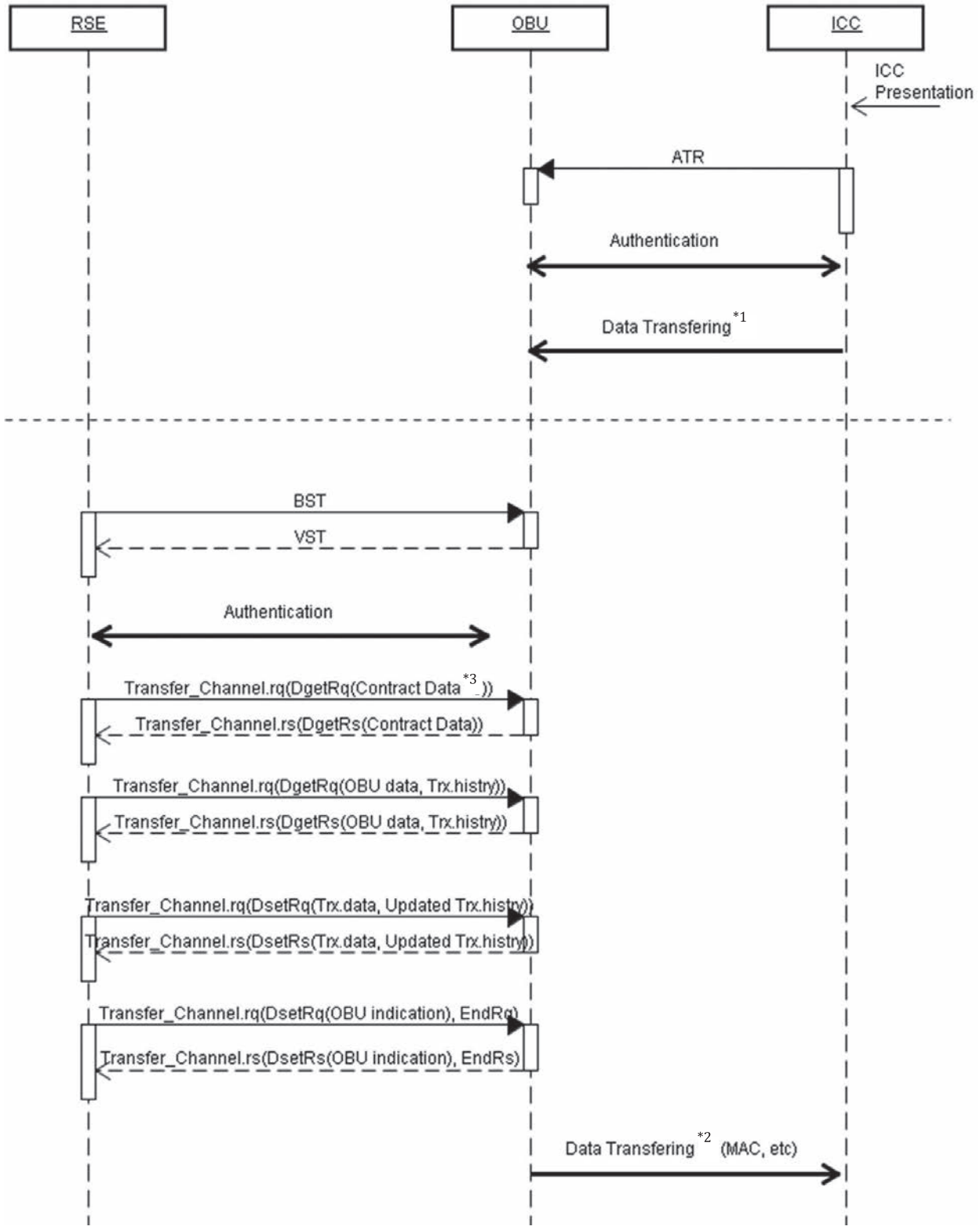
```
RSECommand:: = SEQUENCE{
   eid            Dsrc-EID,
   parameter      OCTET STRING                -Excluded parameter in Sub
                  (SIZE(0..255)),             command
   subCommandList SEQUENCE(0..255) OF         -Sub command list
                  SubCommand
}
DgetRs:: = SEQUENCE{
   fill       BIT STRING (SIZE(3)),
   ret        INTEGER(0..255),
   dataList   DataList
}
```

```
DsetRs:: = SEQUENCE{
   fill        BIT STRING (SIZE(3)),
   ret         INTEGER(0..255),
}
```

### B.2.3 Transaction example

#### B.2.3.1 ETC flat rate charging (open system) and credit payment

Refer to Figure B.5.




**Key**

*1 The following ICC datasets are transferred to the OBU after ICC Presentation Contract data, Transaction history data (Trx histry).

*2 The following datasets are transferred to the ICC after completion of DSRC Transaction (Trx.) data, Transaction (Trx) history data.

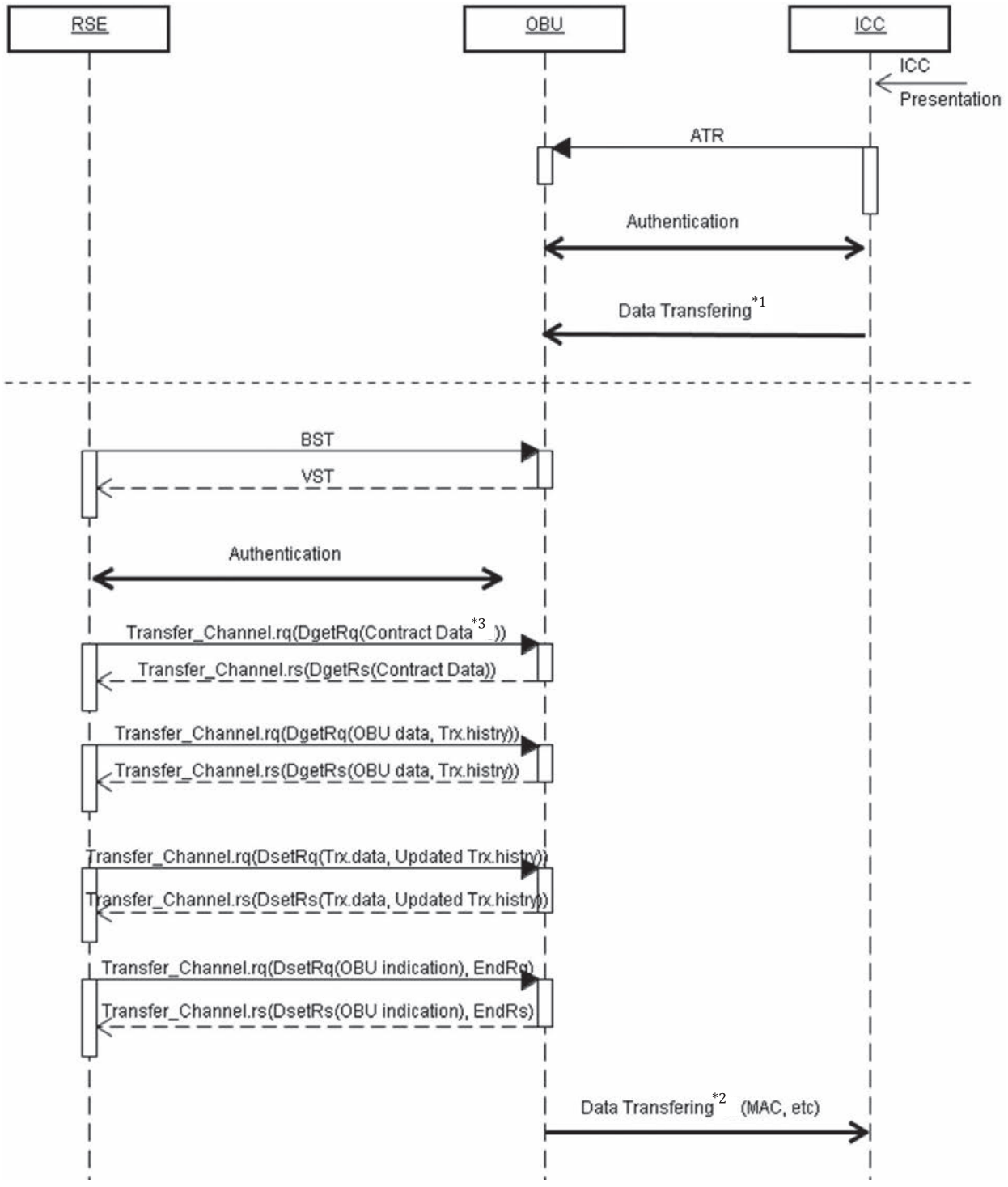
*3 The IC card number is included.

**Figure B.5 — Sequence flow of ETC flat rate charging (open system) and credit payment**

#### B.2.3.2 ETC distance rate charging (closed system) and credit payment

Refer to Figure B.6.

a) Entrance transaction




**Key**

*1 The following ICC datasets are transferred to the OBU after ICC Presentation Contract data, Transaction history data (Trx histry).

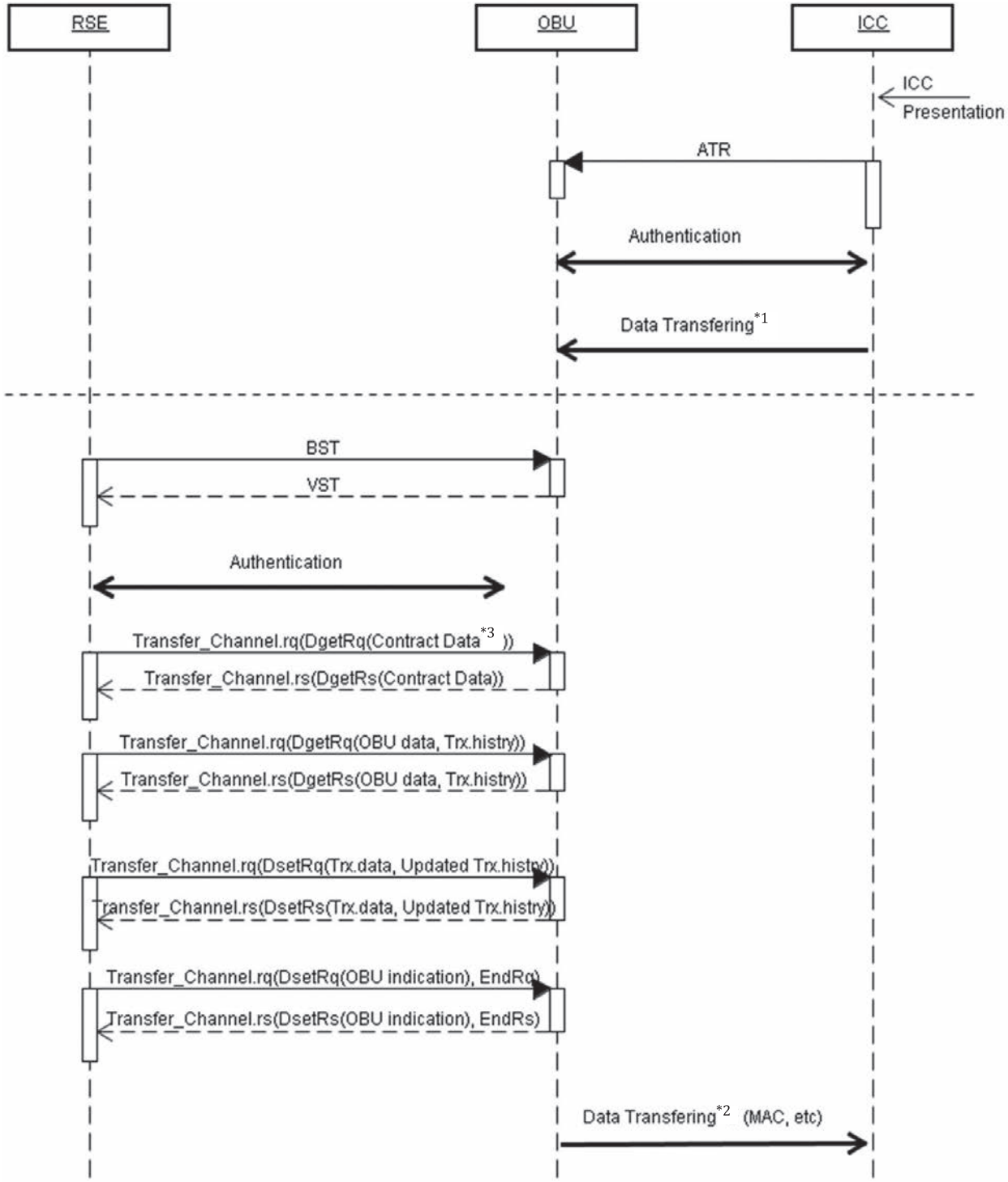
*2 The following datasets are transferred to the ICC after completion of DSRC Transaction (Trx.) data, Transaction (Trx) history data.

*3 The IC card number is included.

**Figure B.6 — Sequence flow of entrance transaction**

b) Exit transaction

Refer to Figure B.7.




**Key**

*1 The following ICC datasets are transferred to the OBU after ICC Presentation Contract data, Transaction history data (Trx histry).

*2 The following datasets are transferred to the ICC after completion of DSRC Transaction (Trx.) data, Transaction (Trx) history data.

*3 The IC card number is included.

**Figure B.7 — Sequence flow of exit transaction**

## B.3 Buffering type model

### B.3.1 General

As an example of this buffering type model, the ICC access method used in Korean ETC is introduced. In Korean ETC, the hybrid type ICC is used not only for ETC but also for Touch and Go, where the driver can go through a toll lane by touching his/her ICC to the roadside reader.

— Command definition: Defined by Korean ETC standards

— Command: Initialize, Action (Debit, Set-secure), Get and Release as defined by ISO 14906

— AID: Electronic fee collection (EFC) as AID = 1 by ISO 15628

— ICC type: Hybrid card with prepaid payment

### B.3.2 RSE command definition

#### B.3.2.1 Debit command

Nonce in ActionParameter includes data for ICC Debit command (S2, PSAM ID, etc.)

* Definition of nonce

```
nonce:: = SEQUENCE{
   length    OCTET STRING (SIZE(1)),  – length of nonce
   PPSAM     OCTET STRING (SIZE(3)),  – PSAM Provider ID
   PSAM      OCTET STRING (SIZE(8)),  – PSAM ID
   NTPSAM    OCTET STRING (SIZE(4)),  – PSAM Transaction Number
   S2        OCTET STRING (SIZE(4)),  – Signature S2
   RFU       OCTET STRING (SIZE(5)),  – reserved for future use
}
```

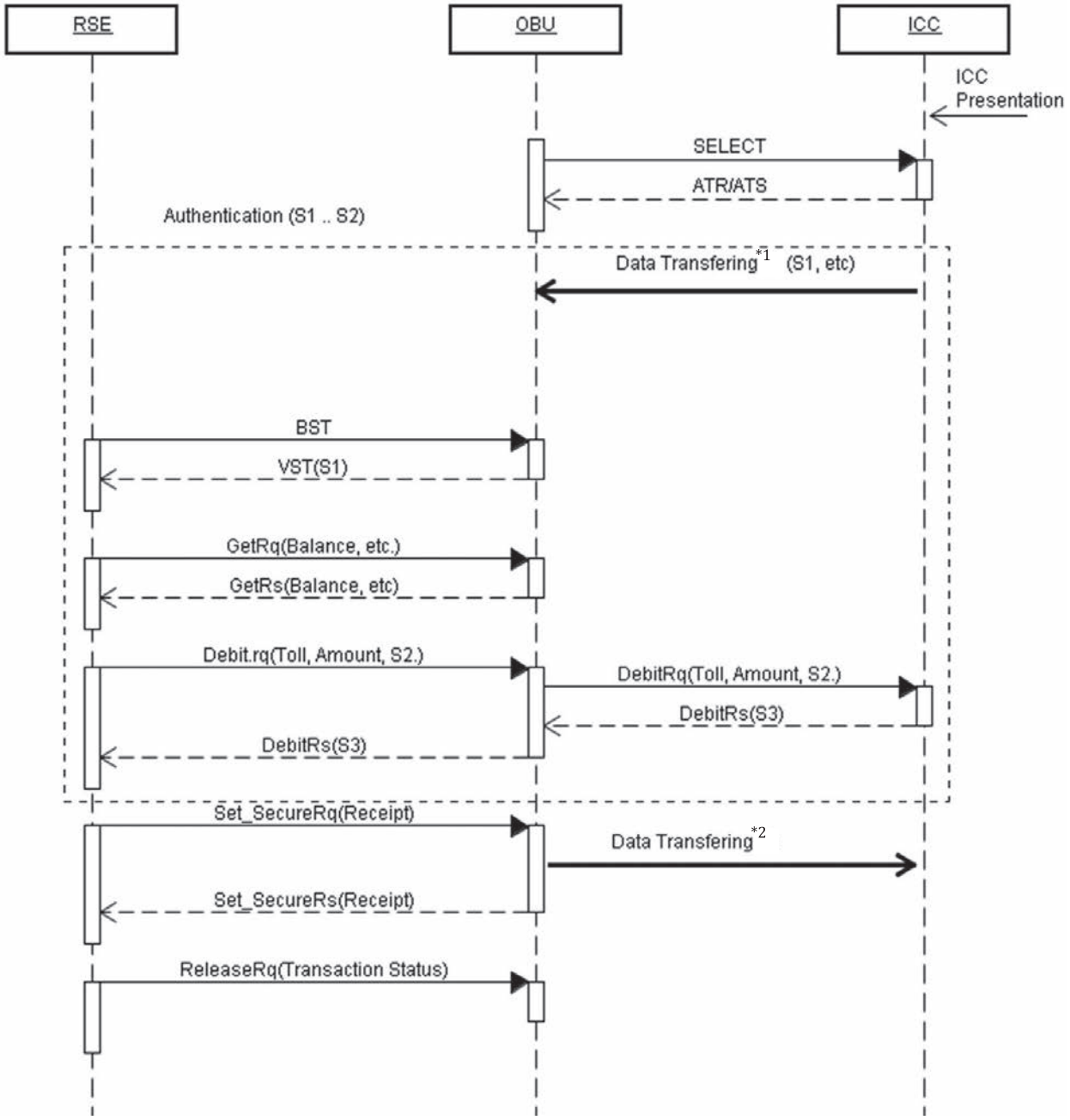
* Definition of debitAuthenticator

```
debitAuthenticator:: = SEQUENCE{
   parameterLen  OCTET STRING (SIZE(1)),  – length of S3
   S3            OCTET STRING (SIZE(4))   – Signature S3
}
```

### B.3.3 Transaction

a) ETC fast transaction algorithm and prepaid payment

Refer to Figure B.8.




**Key**

*1 The following ICC datasets are transferred to the OBU after ICC Presentation Balance data, Card Information. Then, initial ICC Authentication data (S1) are generated and transferred to the OBU.

*2 Receipt data are successfully written to the ICC only after the MAC generated by the RSE (i.e. SAM) is verified by the ICC.

**Figure B.8 — ETC fast transaction algorithm and prepaid payment**

# Annex C
(informative)

# Interoperability relation with other sectors

Figure C.1 indicates the operational interoperability relation where the ICCs issued for EFC are required to be used for public transport and/or retail application.

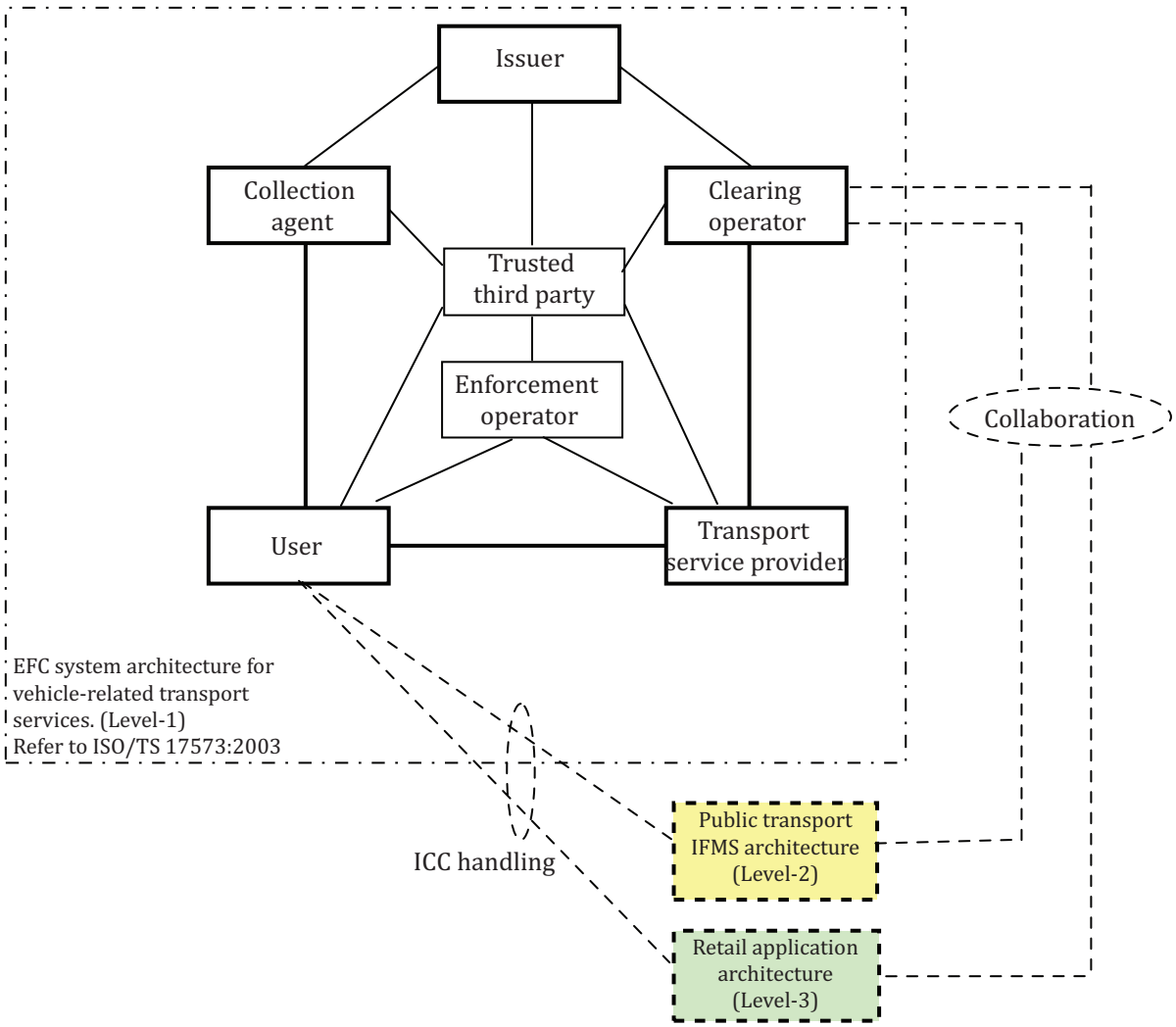



**Figure C.1 — Interoperability model of the EFC service with other services**

On the contrary, Figure C.2 indicates the other operational interoperability relations where the ICCs issued for public transport, where an ICC is treated as a portable electronic medium or retail payment are required to be used for EFC.

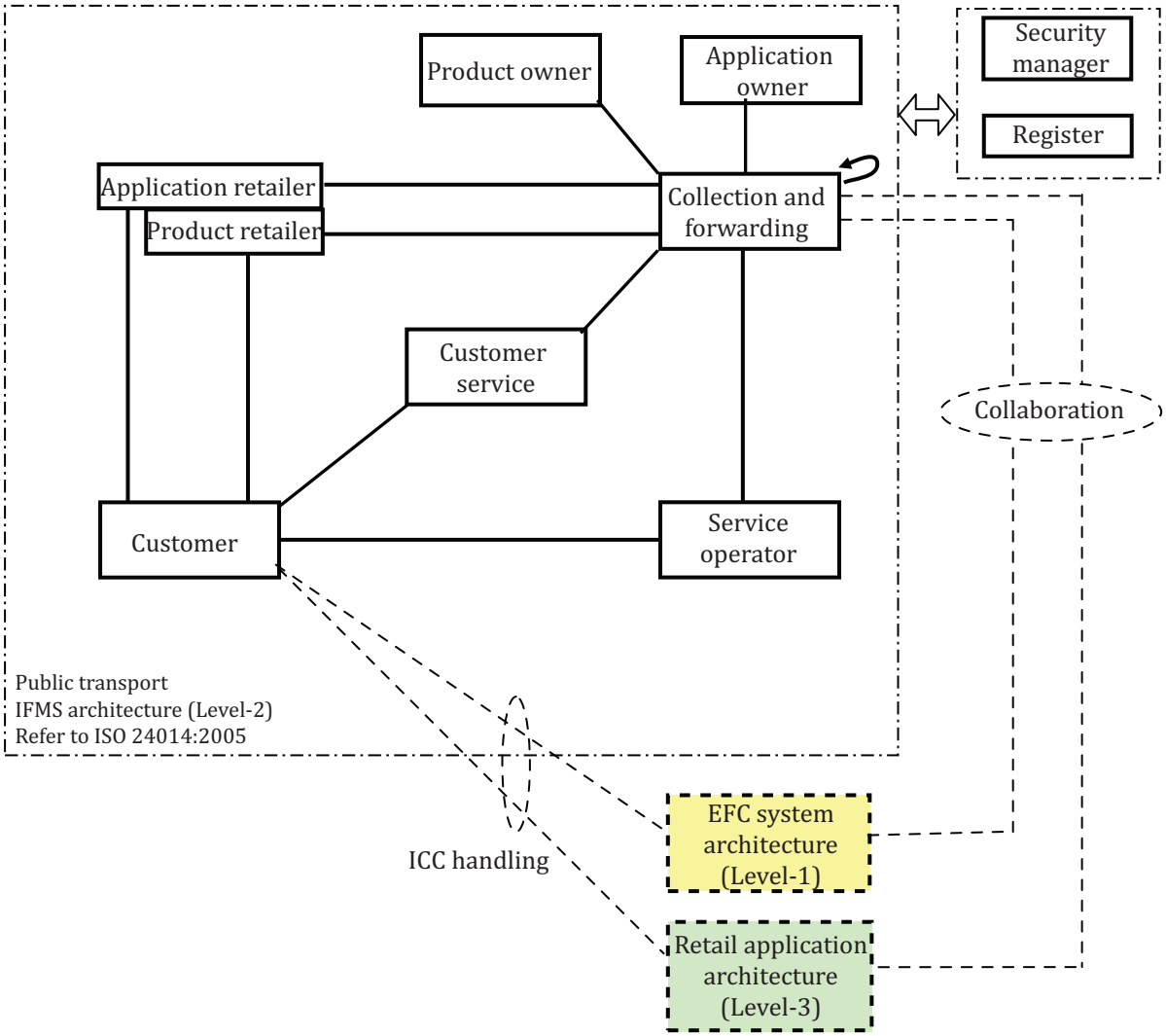



**Figure C.2 — Interoperability model of the IFMS service with other services**

# Bibliography


[1] ISO/IEC 7482-2:1989, *Information processing systems — Open Systems Interconnection Basic Reference Model — Part 2: Security Architecture*

[2] ISO/IEC 7816-1, *Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics*

[3] ISO/IEC 7816-2, *Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimensions and location of the contacts*

[4] ISO/IEC 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

[5] ISO/IEC 7816-4, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

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

[7] ISO/TS 14907-1, *Electronic fee collection — Test procedures for user and fixed equipment — Part 1: Description of test procedures*

[8] ISO/TS 14907-2, *Electronic fee collection — Test procedures for user and fixed equipment — Part 2: Conformance test for the on-board unit application interface*

[9] ISO/IEC 14443-1, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 1: Physical characteristics*

[10] ISO/IEC 14443-2, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 2: Radio frequency power and signal interface*

[11] ISO/IEC 14443-3, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 3: Initialization and anticollision*

[12] ISO/IEC 14443-4, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 4: Transmission protocol*

[13] ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

[14] ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

[15] ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

[16] ISO/TS 16785:2014, *Electronic fee collection (EFC) — Interface definition between DSRC-OBE and external in-vehicle devices*

[17] ISO 17573, *Electronic fee collection — Systems architecture for vehicle-related tolling*

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

[19] ISO/TS 17575-1:2016, *Electronic fee collection — Application interface definition for autonomous systems — Part 1: Charging*

[20] ISO/IEC 18092, *Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)*

[21] ISO/TS 19299:2015, *Electronic fee collection — Security framework*

[22] ISO 24014-1, *Public transport — Interoperable fare management system — Part 1: Architecture*

[23] EN 15509-1:2014, *Electronic fee collection — Interoperability application profile for DSRC*

[24] ENV 14062-1, *Identification card systems — Surface transport applications. Electronic fee collection. Part 1: Physical characteristics, electronic signals and transmission protocols*

[25] ENV 14062-2, *Identification card systems — Surface transport applications. Electronic fee collection. Part 2: Message requirements*

**ICS 03.220.01; 35.240.60**

Price based on 34 pages