International Standard

ISO 25110

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

Perception de télépéage — Définition d'interface pour compte embarqué utilisant une carte à circuit(s) intégré(s)

Second edition
2025-04

Reference number
ISO 25110:2025(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO 25110:2017), which has been technically revised.

The main changes are as follows:

— Clause 3 has been updated and ISO 17573-2 has been made the primary source for terms and definitions;

— in Clause 6, a provision related to the EFC functions invoked by roadside equipment to instruct the on-board equipment has been changed from a recommendation to a requirement for conformance to ISO 14906.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 Background and motivation

Two payment systems currently exist for dealing with electronic fee collection (EFC):

1) the central account system, which uses a one-piece on-board unit (OBU), and

2) the on-board account system, which uses a payment media such as the integrated circuit card (ICC) inserted in an element of on-board equipment (OBE).

ICCs are widely used for public transport cards such as subway and bus payment means, and electronic money cards are used for general purpose payments, as well as for credit cards and banking cards. In the future, ICCs are expected to also be used for EFC payment means, providing convenience and flexibility; see Figure 1.

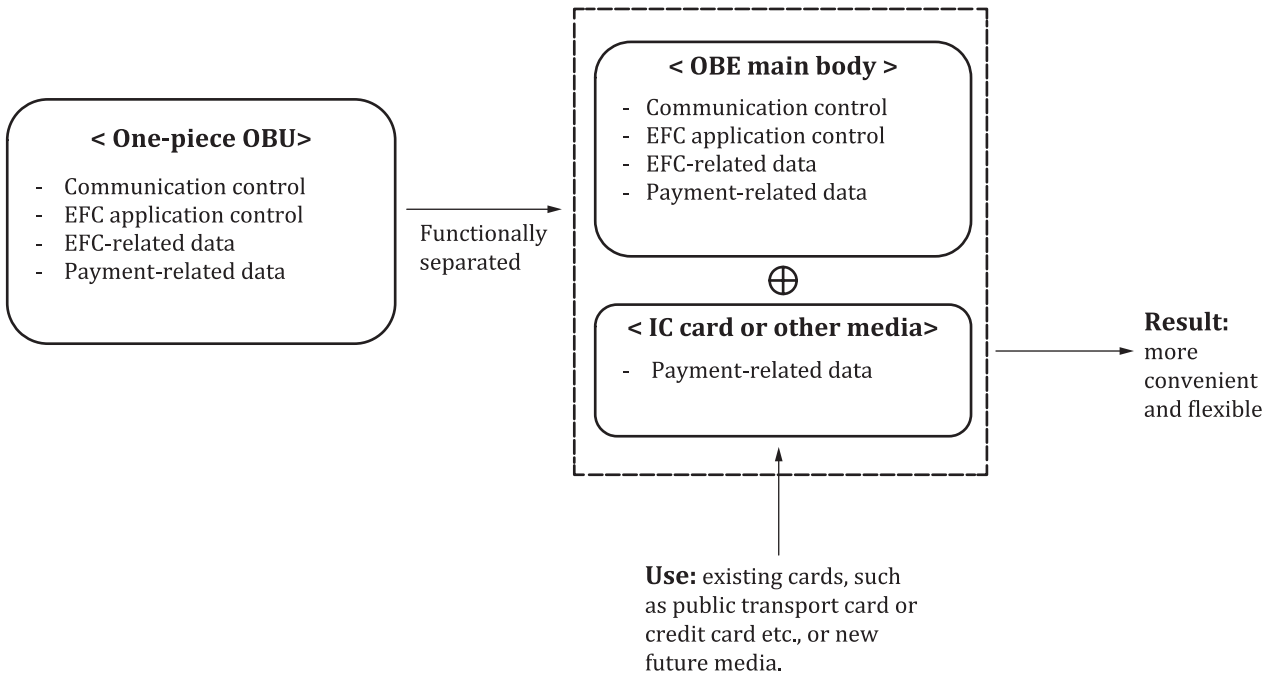


Figure 1 — Motivation for on-board accounts using ICCs

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

Figure 2 shows the basic model of EFC, in which the OBE is used as a communication means and the ICC carries the payment means.

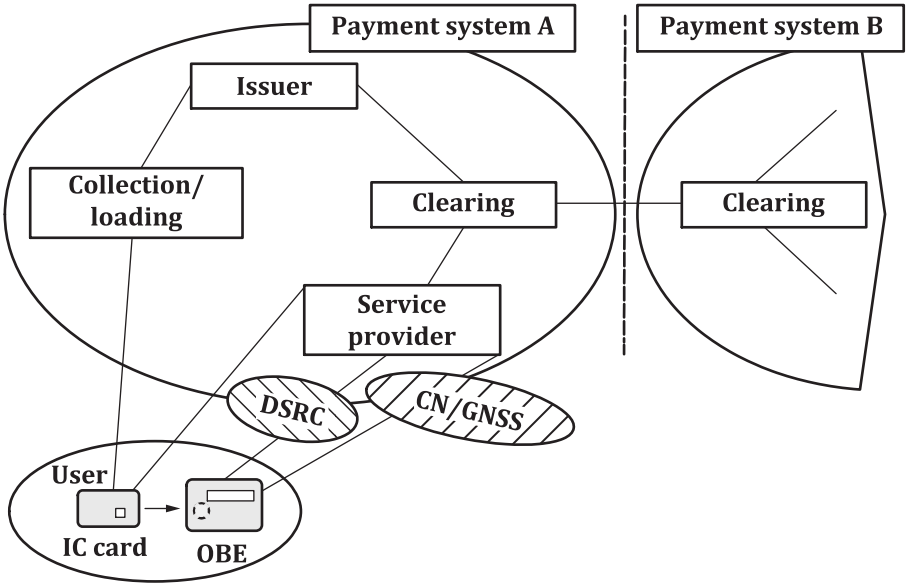


Figure 2 — The basic model of EFC

Considering the widespread use of transport cards or electronic money cards, a new International Standard for an on-board account system using ICCs is required. Furthermore, the rapid development in certain regions of the use of state-of-the-art mobile phones integrated with ICC functions as a payment means for public transport or retail shopping (a "mobile electronic purse"), makes standardization on this theme essential when considering future EFC payment methods.

0.2 Objective and use

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

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

Each toll road operator can establish their own specification by selecting one example in the models of this document (like a toolbox) to meet their requirements.

Figure 3 shows the principle of an on-board account architecture and the scope of this document. The descriptions in this document focus on the interface (I/F) between the RSE and OBE to access the ICC.

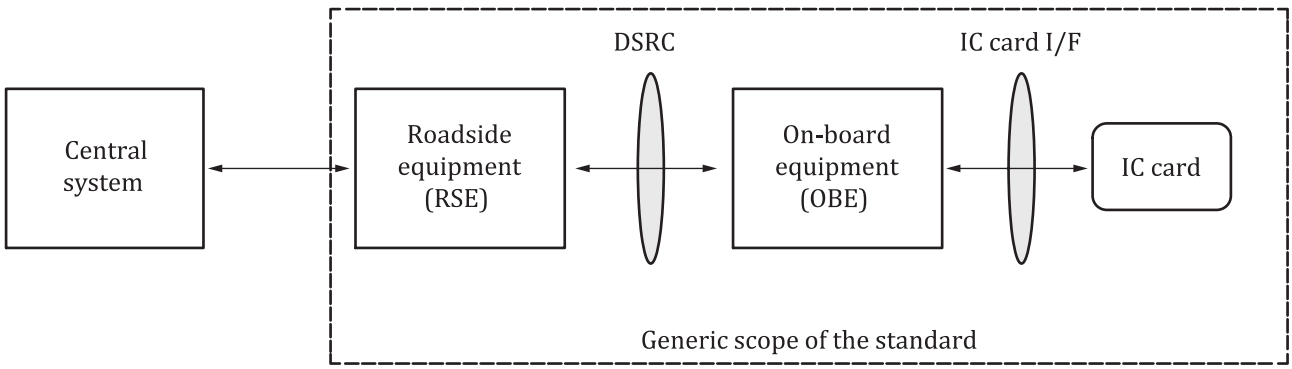


Figure 3 — Principle of an on-board account architecture and scope of this document

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

1 Scope

This document specifies the data transfer models between roadside equipment (RSE) and integrated circuit cards (ICCs) and the interface descriptions between the RSE and on-board equipment (OBE) for on-board accounts using an 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;

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

— the interface definition for each model;

— the functional configuration;

— RSE command definitions for ICC access;

— the data format and data element definitions of RSE commands;

— a transaction example for each model (Annex B).

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

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

ISO 17573-2:2025[1)], *Electronic fee collection — System architecture for vehicle related tolling — Part 2: Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 17573-2:2025[2)] and the following apply.

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

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

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

1) Under preparation. Stage at the time of publication: ISO/DIS 17573-2:2025.

2) Under preparation. Stage at the time of publication: ISO/DIS 17573-2:2025.

3.1
Element
dedicated short-range communication (DSRC) directory containing application information in the form of attributes

[SOURCE: ISO 14906:2022, 3.8]

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
ATR	answer to reset
ATS	answer to select
BST	beacon service table
CPU	central processing unit
DSRC	dedicated short-range communication
EAL	evaluation assurance level
EFC	electronic fee collection
EID	Element identifier
EVENT-RT	EVENT-Report
IC	integrated circuit(s)
ICC	integrated circuit(s) card (IC card)
I/F	interface
IFMS	interoperable fare management system
MAC	medium access control
OBE	on-board equipment
SAM	secure application module

5 Data transfer models

5.1 General

5.1.1 Overview

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

The data transfer models are as follows:

— the transparent type;

— the caching type;

— the buffering type.

Figure 4 shows the layer structure of the RSE, OBE and ICC, where the mid-layer of application interfaces is the focus of this document.

NOTE Subjects covered by 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.

There are two types of virtual bridges contained in an OBE. The first type is Bridge-1, in 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 the 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 the 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 caching type.

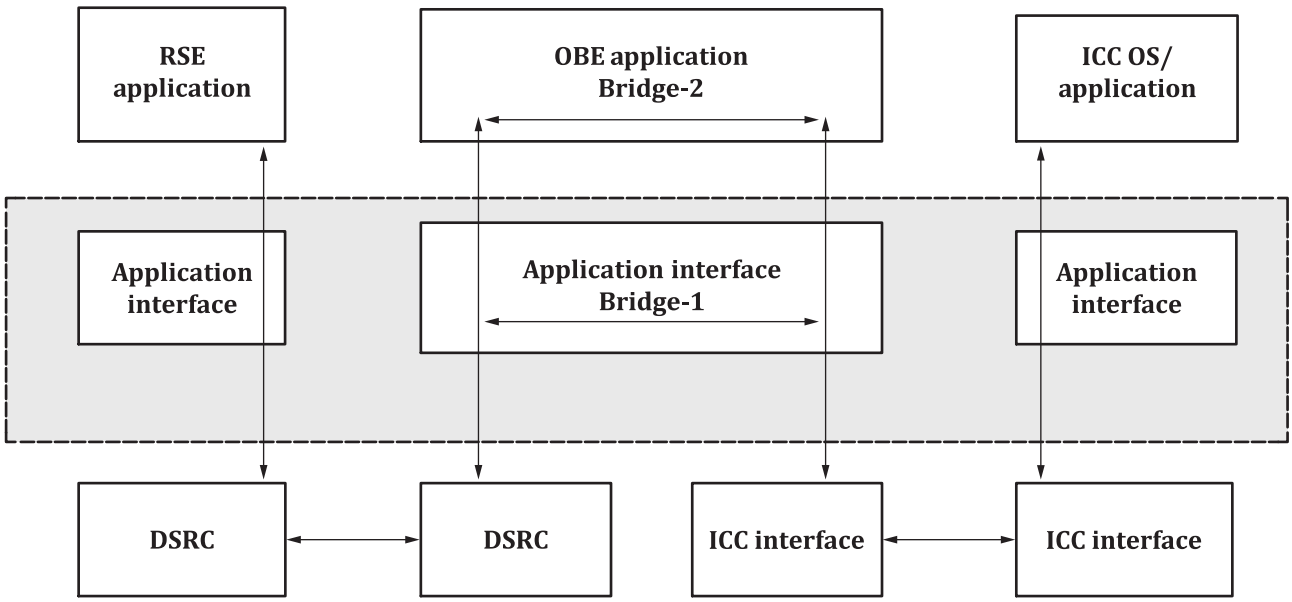
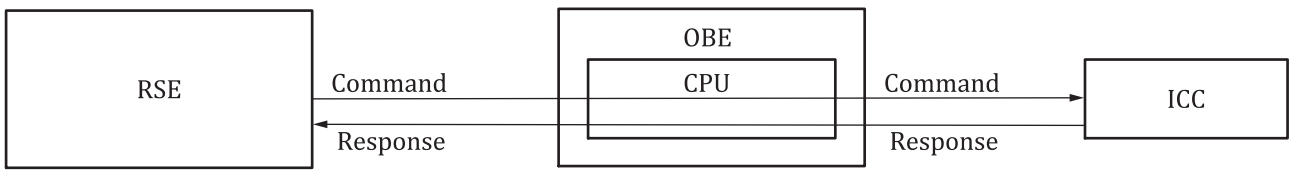


Figure 4 — Application interfaces of RSE, OBE and ICC

5.1.2 Transparent type

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



Key

CPU central processing unit

Figure 5 — Generic structure of transparent type

5.1.3 Caching type

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

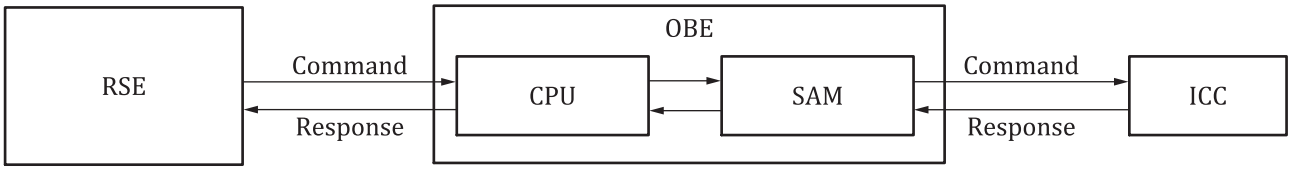


Figure 6 — Generic structure of caching type

5.1.4 Buffering type

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

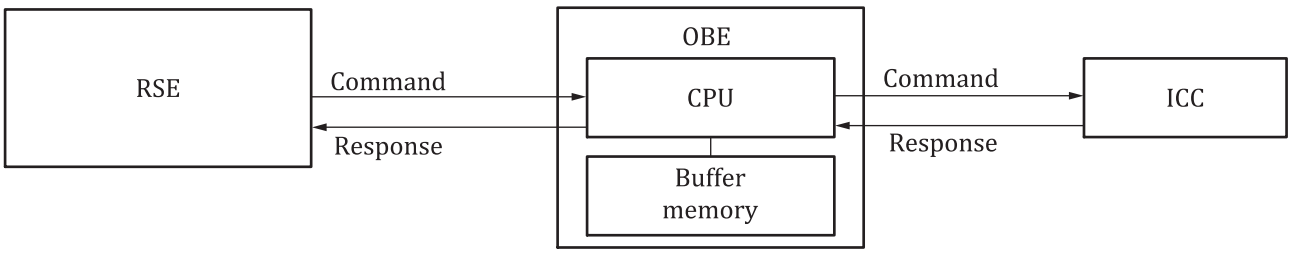


Figure 7 — Generic structure of buffering type

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 — definition

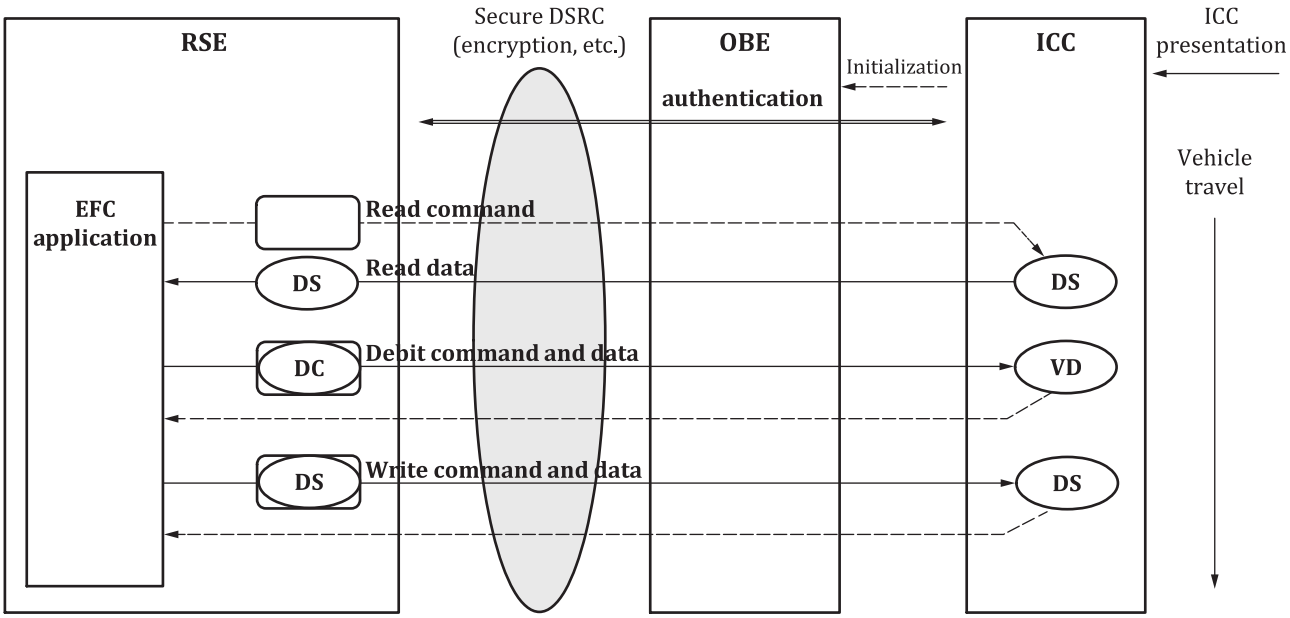
5.3.1 General

In this model, the maximum vehicle speed is limited by the data transfer rate between the ICC and OBE so that the vehicle has to stop or pass slowly beneath an RSE antenna when a conventional contact ICC is used. The key feature of this type is that the OBE is simplified by eliminating the secure memory inside of the OBE and by using high transfer rate ICCs.

5.3.2 Data transfer process

In this model, data exchanges between the RSE and ICC are processed directly after establishing DSRC communication and when authentication between the RSE and OBE 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 OBE 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 OBE. 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 — definition

5.4.1 General

In this model, the OBE reads out datasets from the ICC and stores them in a secure memory inside the OBE, upon insertion and completion of the authentication. The key feature of this type is that a high data exchange rate between the RSE and OBE is achieved even when using ICC with a slow data rate. With this caching type, maximum vehicle speed is enhanced up to DSRC communication performance, regardless of 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 OBE to ensure information security.

This type can cope with high vehicle speed by processing between the RSE and OBE at a high data exchange rate, regardless of the type of ICC. See Figure 10.

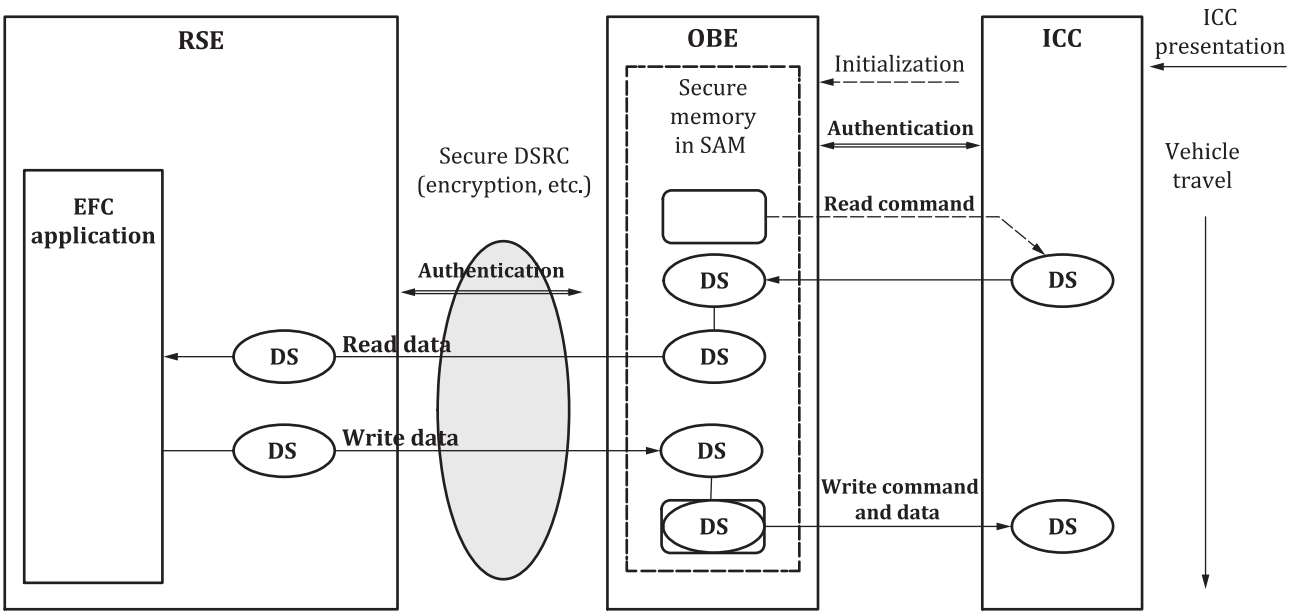


Figure 10 — Data transfer process of caching type

5.5 Buffering type — definition

5.5.1 General

This model shares features with both the transparent and caching type. However, in the buffering type, datasets stored in the ICC are limited to non-sensitive data to avoid tampering or disclosure of sensitive data. In the buffering type, the data transfer method is the same as in the caching type and datasets of the ICC are read out and stored in a buffer memory inside the OBE when the ICC is inserted into the OBE. Datasets stored in the buffer memory are transferred to the RSE during the DSRC read sequence. In case of writing, RSE datasets are transferred to the OBE and stored in the buffer memory of the OBE and then transferred to the ICC.

5.5.2 Data transfer process

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

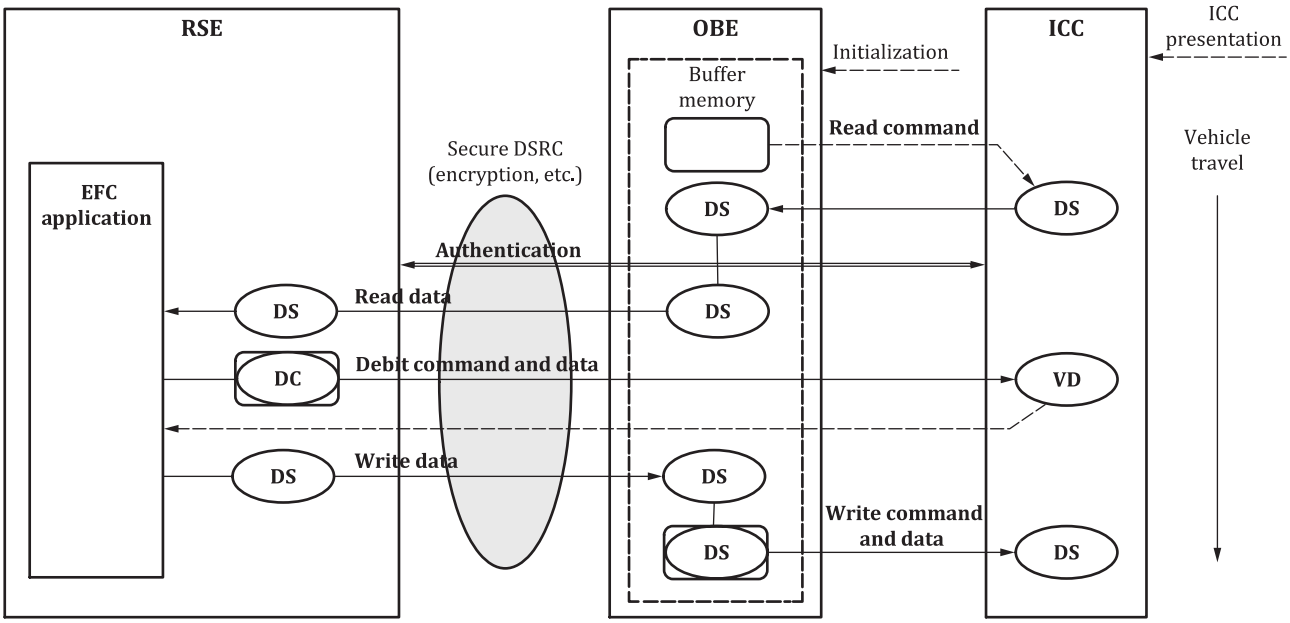


Figure 11 — Data transfer process of buffering type

6 Interface definition for ICC access

6.1 Transparent type

6.1.1 Functional configuration

The functional configuration of the transparent type is shown in Figure 12. RSE commands containing ICC access commands are sent in its ADPU to execute the ICC "Read" or "Write" command, or both commands directly.

The command definition between the OBE and ICC shall conform to ISO/IEC 7816-4.

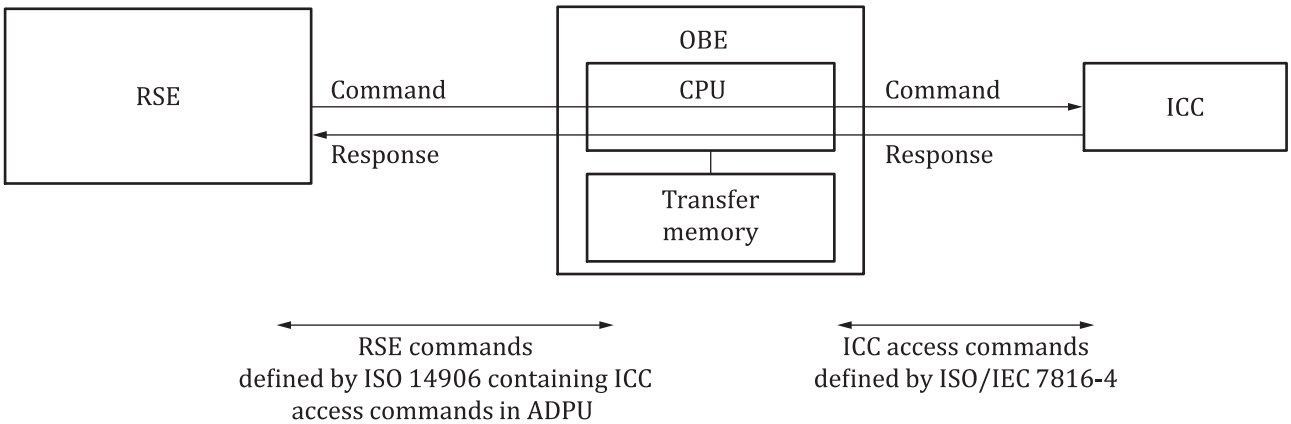


Figure 12 — Functional configuration of transparent type

6.1.2 Command and response between the RSE and OBE

The transfer channel defined by ISO 14906 shall be used as a basic RSE command to access ICC from RSE directly with the `channelId` designated 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 {
	channelId ChannelId,
	APDU OCTET STRING
	}
			Always to be present
			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 {
	channelId ChannelId,
	APDU OCTET STRING
	}
			Always to be present

Return Code(Ret)	ReturnStatus		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 OBE when the ICC is inserted in the OBE. 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 the ICC shall be based on ISO/IEC 7816-4.

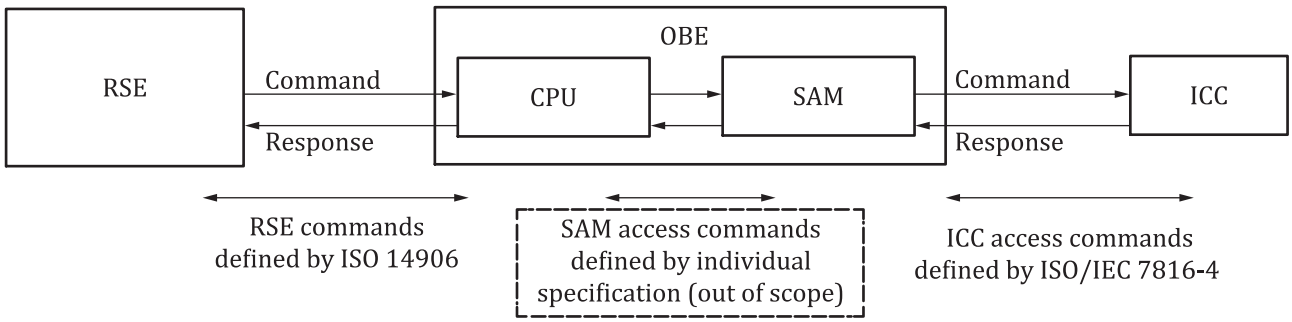


Figure 13 — Functional configuration of caching type

6.2.2 Command and response between the RSE and the OBE

The transfer channel defined by ISO 14906 shall be used as the basic RSE command to access the SAM of the OBE from the RSE directly with designating the `channelId` 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 {
	channelId ChannelId,
	APDU OCTET STRING
	}
			Always to be present
			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 {
	channelId ChannelId,
	APDU OCTET STRING
	}
			Always to be present

Return Code(Ret)	ReturnStatus		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 OBE when the ICC is inserted in the OBE. During DSRC communication, the RSE sends the RSE command to read datasets stored in the buffer memory.

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

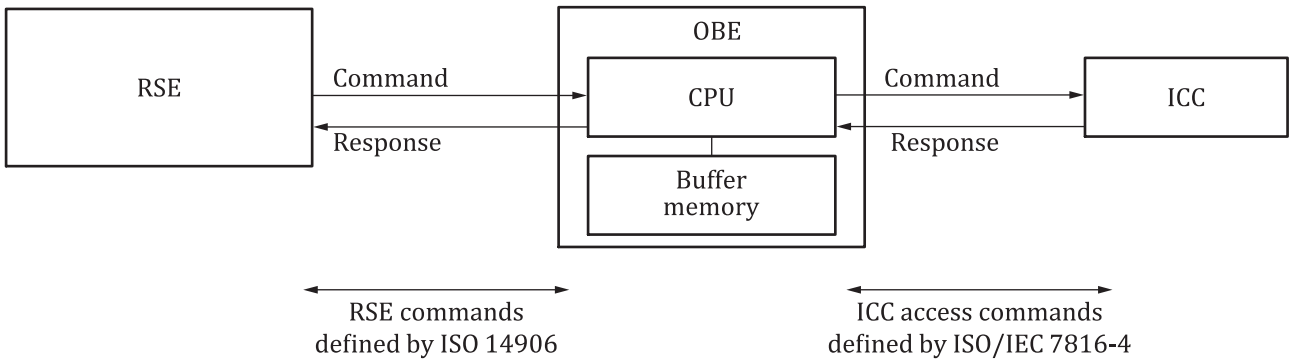


Figure 14 — Functional configuration of buffering type

6.3.2 Command and response between the RSE and the OBE

In this buffering type, necessary data sets stored in the ICC are transferred to buffer memory of OBE. `GET` or `SET` primitive is therefore used as the RSE command. `Debit` or `Credit` of the EFC function defined by ISO 14906 shall be 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 {
	debitPaymentFee PaymentFee,
	nonce OCTET STRING
	keyRef INTEGER(0..255)
	}
			Always to be present

Mode	BOOLEAN	TRUE	

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

Table 6 — DEBIT.response

Parameter	ASN.1 Type	Value	Remarks

ResponseParameter	DebitRs:: = SEQUENCE {
	debitResult
	ResultFin,
	debitAuthenticator OCTET STRING
	}
			Always to be present

Return Code(Ret)	ReturnStatus		Optional use

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

Annex A
(informative)

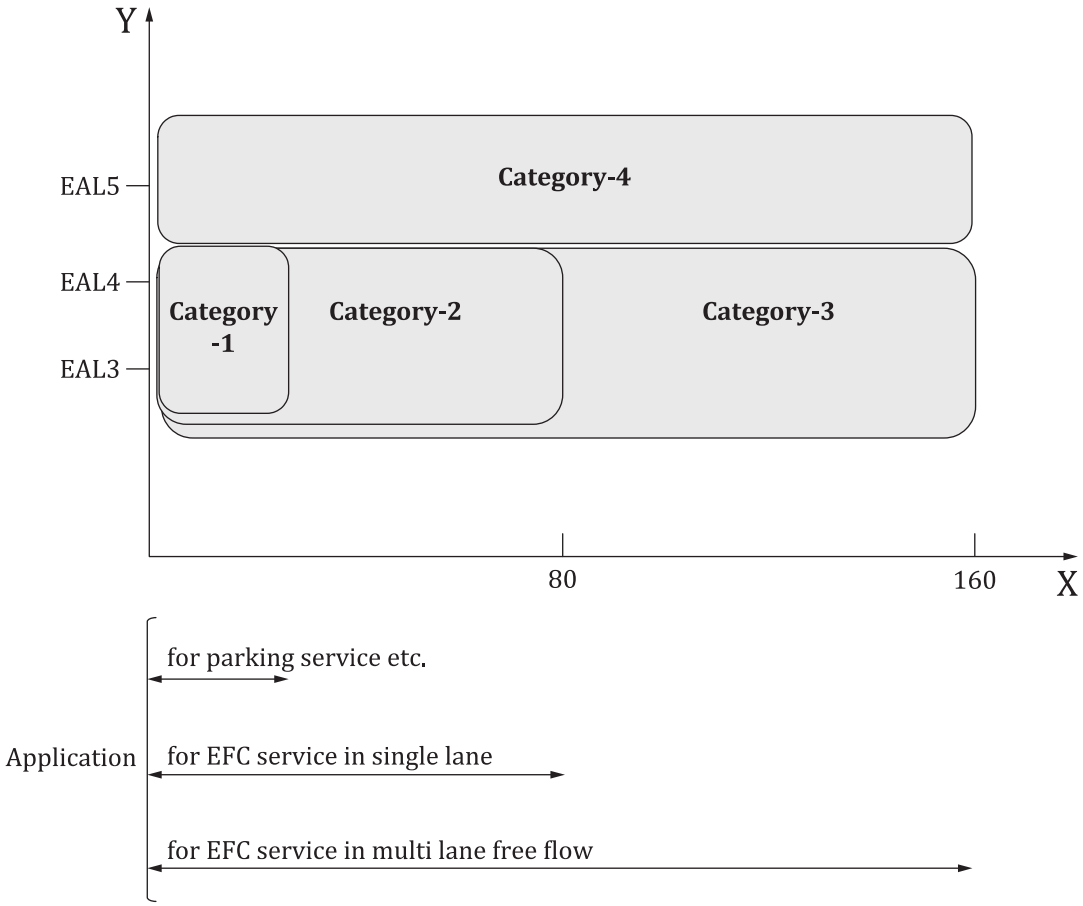
On-board account requirements

A.1 Operational requirements for the on-board account

The major factors of operational requirements for EFC are vehicle speed and information security level, as shown in Figure A.1, both of which 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 a SAM embedded in the OBE, in addition to the ICC security mechanism, while Category-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 in a multi-lane free flow, where the vehicle goes through at high speed under the roadside antenna.



Key

X vehicle speed (km/h)

Y information security evaluation assurance level

Figure A.1 — Operational requirements

A.2 Types of ICC

The type of 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 contactless 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, 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.

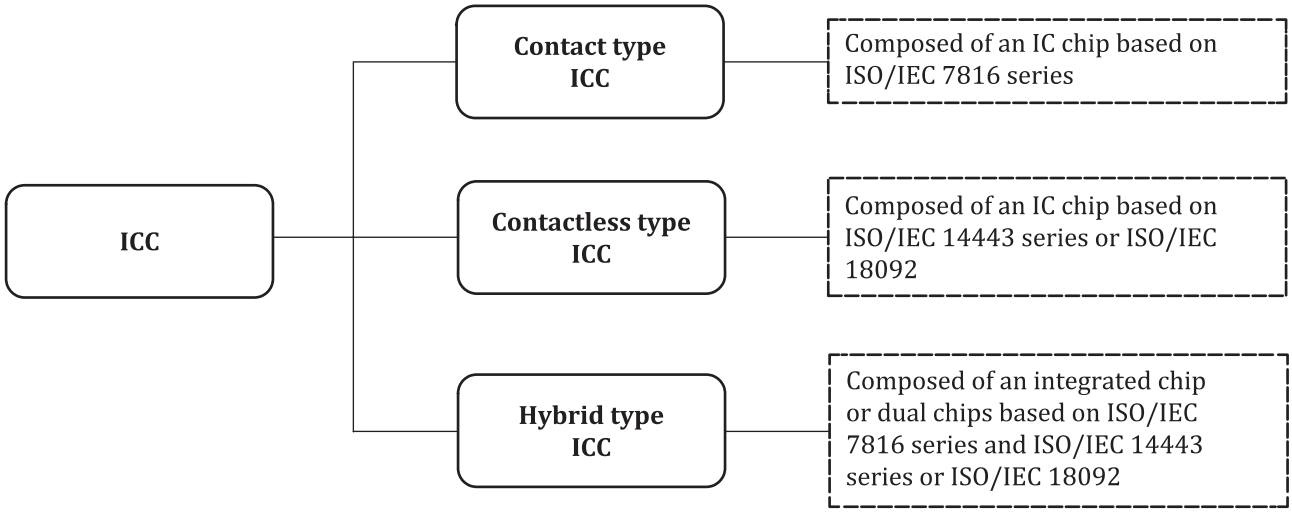


Figure A.2 — Types of IC cards

A.3 Interoperability requirements for the ICC

For its 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 regarding Level-2, the interoperability scheme should be considered based on the collaboration with EFC architecture and the interoperable fare management system (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 1 In the case of the transparent type, each category depends on the transfer rate of the ICC type.			
NOTE 2 × means "to be applied".			

Annex B
(informative)

Examples of 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 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 Channel ID = ICC(3) by ISO 14906

— ICC type: Contactless 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 — ETC distance-based charging (closed system)

a) Entrance system

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

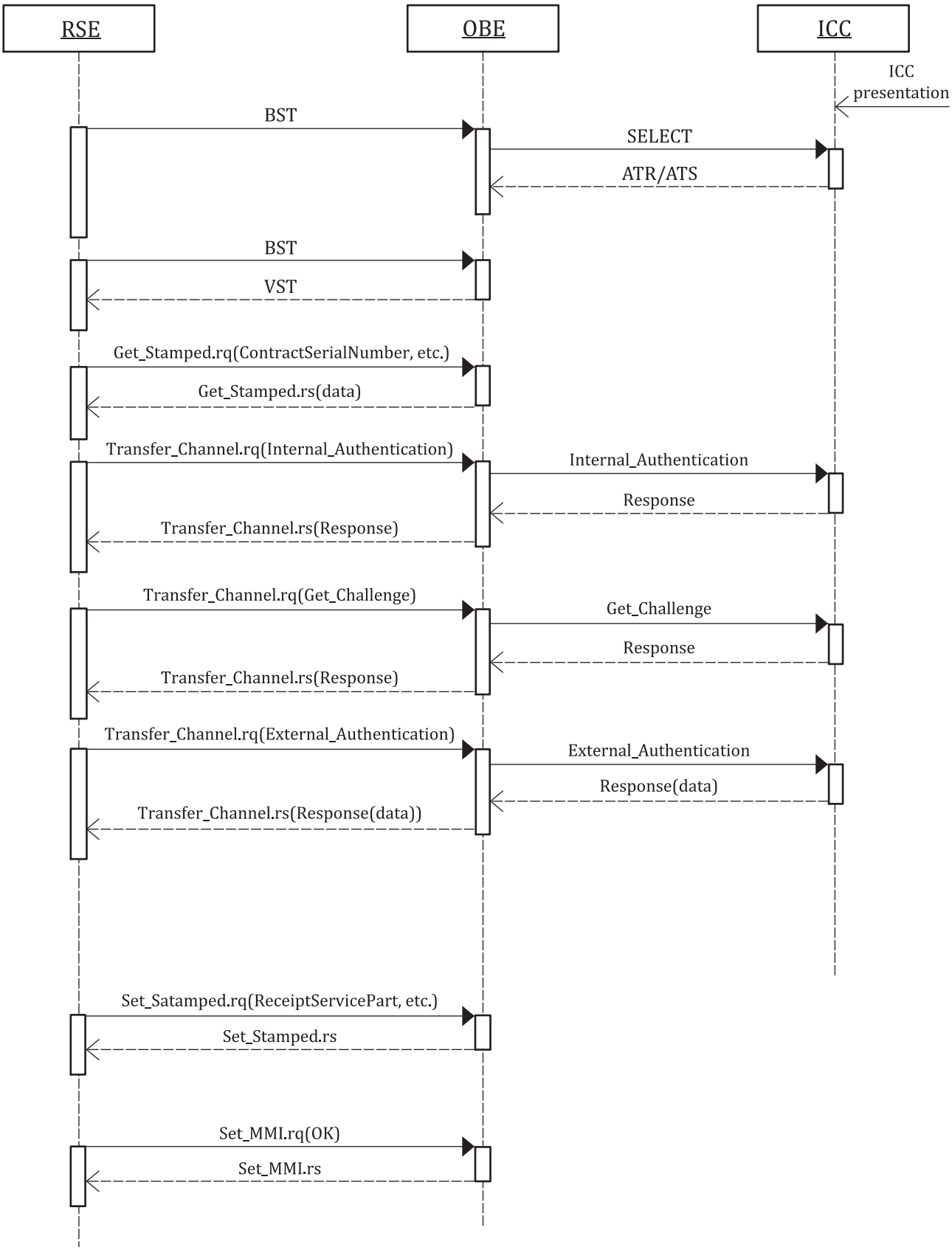


Figure B.1 — Sequence flow of entrance system

b) Exit system

At the exit, the RSE reads the entrance information from the OBE and keeps it in the memory of the RSE, and the mutual authentication between RSE and ICC is completed. The RSE calculates the fee according to the entrance information and sends the debit command to the ICC directly via the OBE by using the transfer channel function; see Figure B.2.

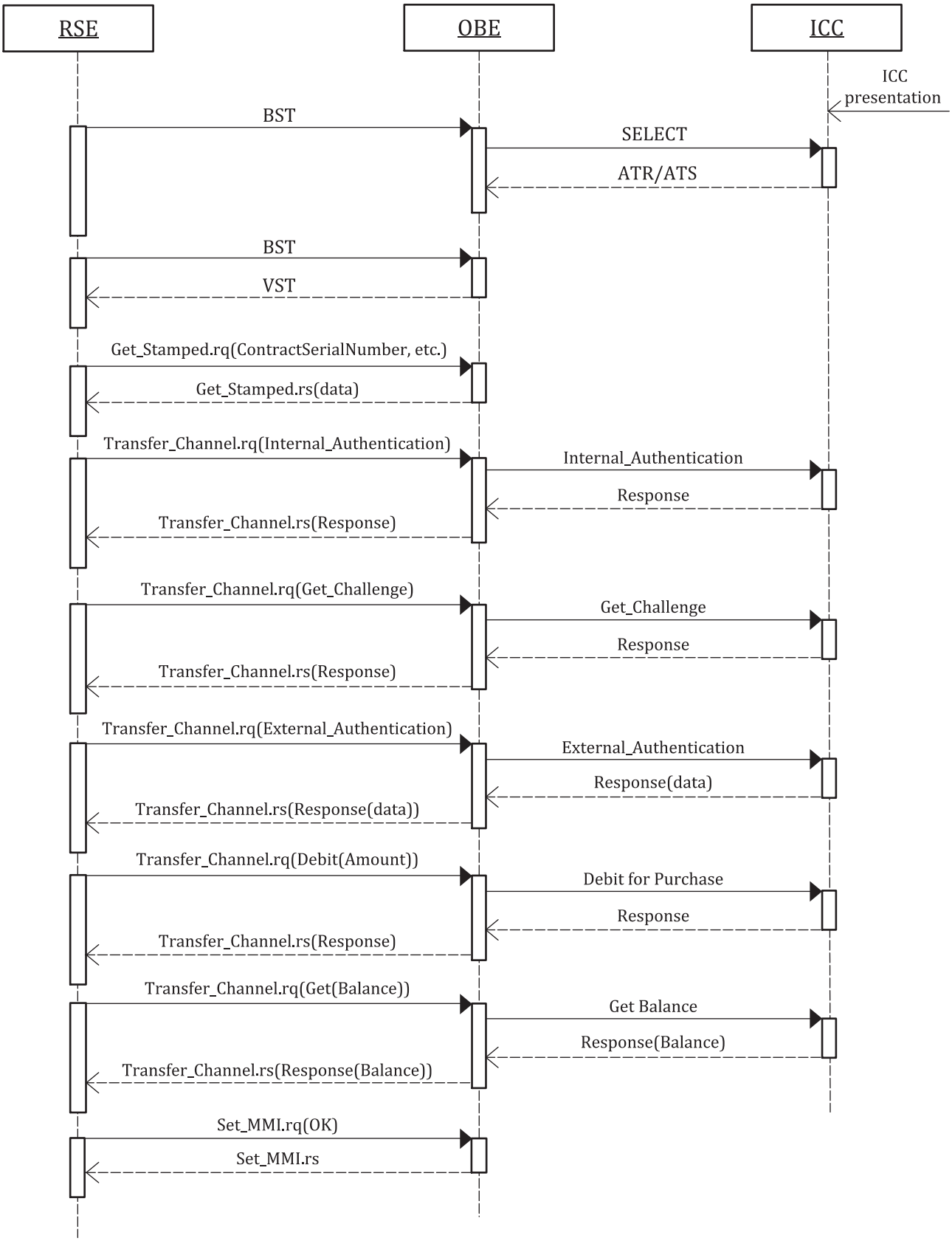


Figure B.2 — Sequence flow of exit system

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

B.1.2.1 General

As an example of the transparent type model-2, this subclause describes the ICC access method defined in the “DSRC basic application interface”.[19]

The “DSRC basic application interface” is established to provide multiple information services such as traffic and road information, traveller information and parking information, with the 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.

— Command definition: Defined by DSRC basic application interface (ITS Forum RC-004[19] 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 Channel ID = 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{
   versionIndexVersion,
   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,
   obeDenialResponse        [255]  ObeDenialResponse
}
operationCommand:: = SEQUENCE{
   opCommandType  OpCommandType,
   opSecurityProfile OpSecurityProfile,
   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

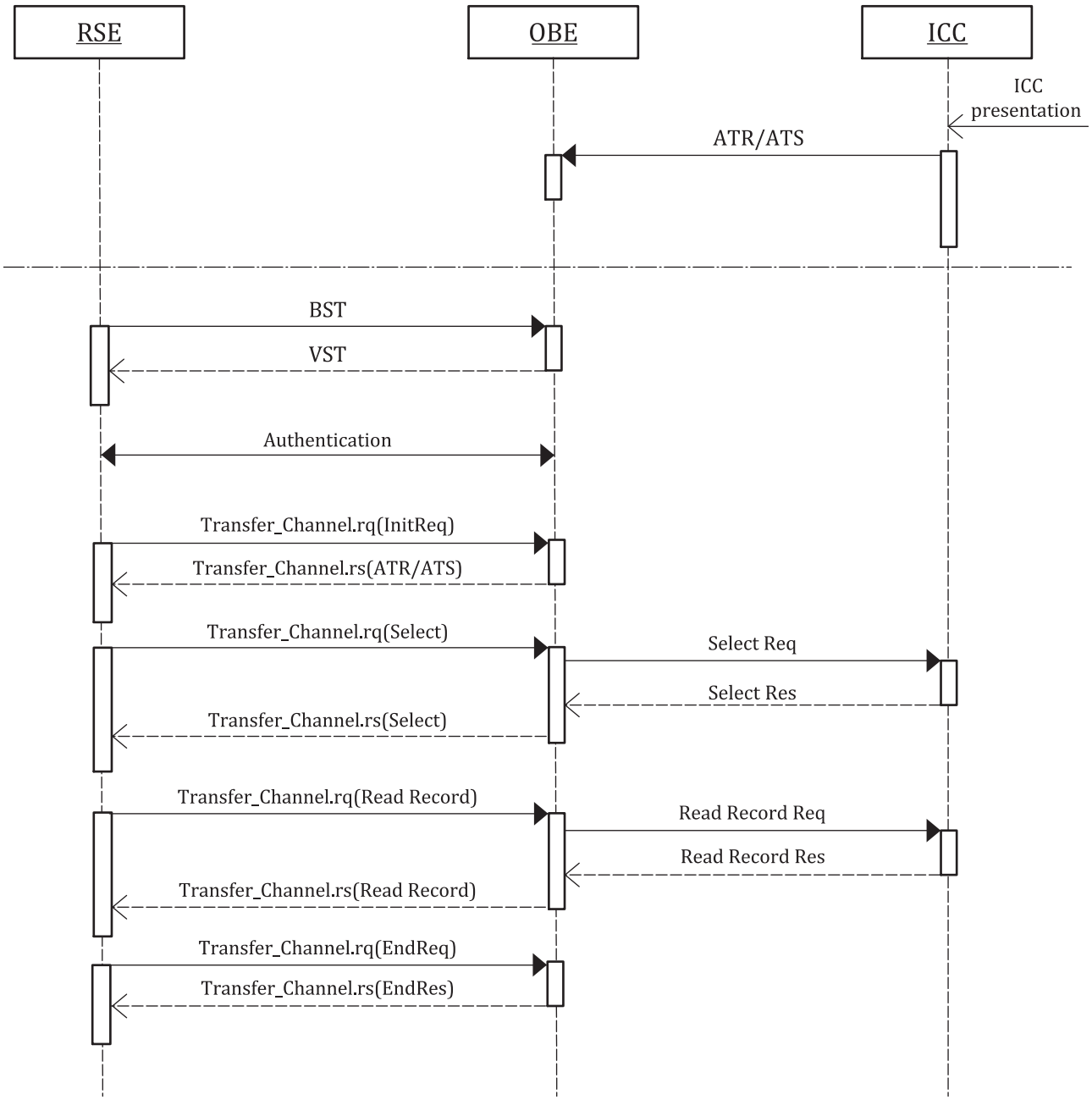
```
ICCAccessResponse:: = SEQUENCE{
   versionIndexVersion,
   accessCommand  AccessCommand
```

}

B.1.2.3 Transaction — Parking system

a) Simple system (centre chaining method)

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



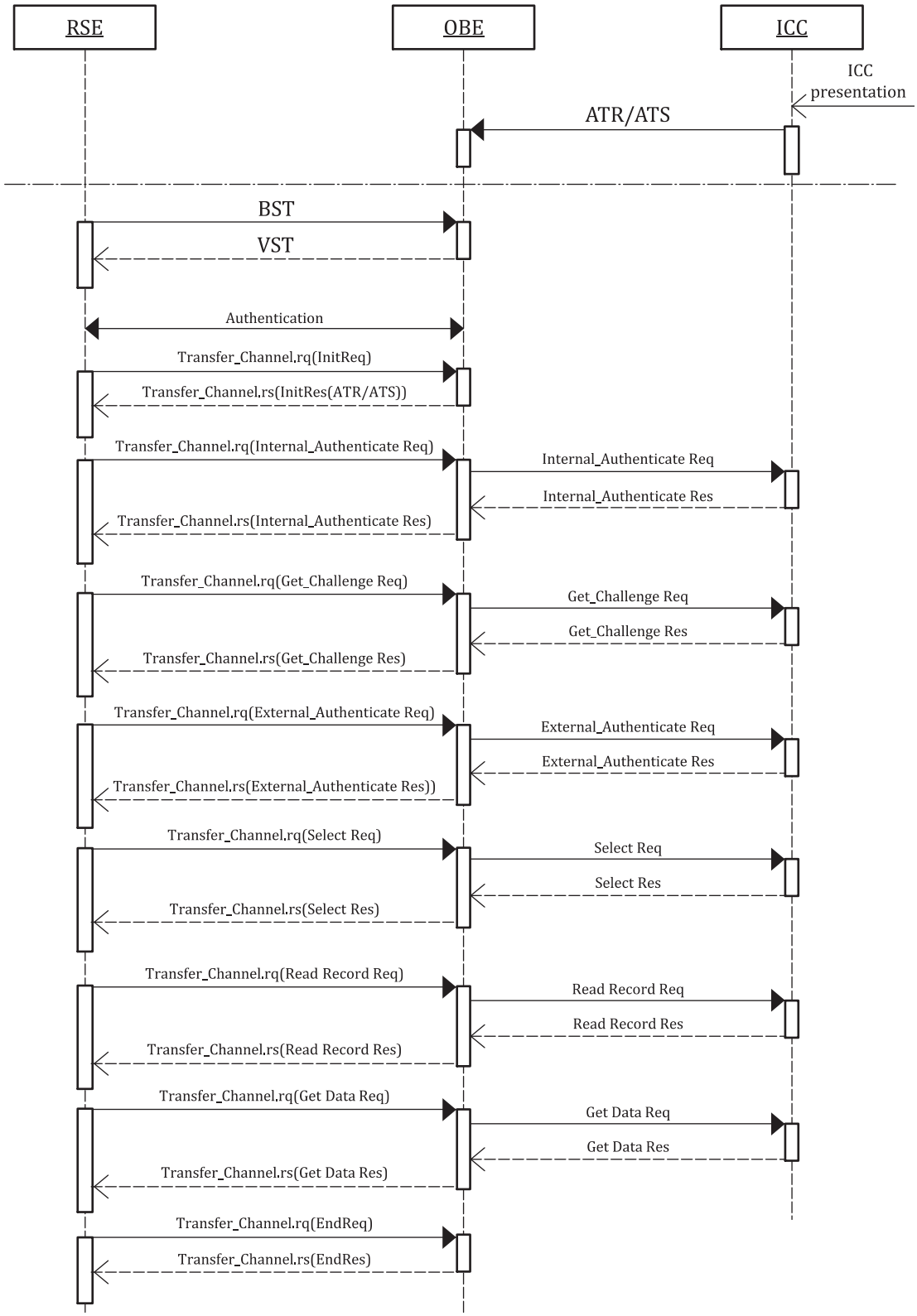
NOTE 1 The membership number is contained in the Read Record Response.

NOTE 2 'Req' is 'Request' and 'Res' is 'Response'.

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

b) Complex system (direct method)

In this system, the parking fee is paid with the credit card number read out from the credit ICC directly; see Figure B.4.



NOTE 1 The credit card number is contained in the Read Record Res.

NOTE 2 'Req' is 'Request' and 'Res' is 'Response'.

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 OBE is based on retailing at auto-shops. Any manufacturer can participate in the OBE market by getting type approval from the testing institute. Therefore, the data security level for ICC and toll collection-related data stored in the OBE is required to be high level and the approved OBE manufacturers are required to use SAM provided from certified SAM manufacturers by the trusted third party (see Note 1).

— Command definition: Defined by the DSRC interface standard (ETC-B02230P[20]) used 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)

— ICC type: Contact-type ICC for credit payment

NOTE 1 The reasons for adopting the SAM in Japanese ETC are:

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

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

— to maintain competitiveness and to spread OBE 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{
   eidDsrc-EID,
   parameterOCTET STRING (SIZE(0..255)),  --Parameter not in subcommand
   subCommandList SEQUENCE(0..255) OF SubCommand--Sub command list
}
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)),
   attributeIdListAttributeIdList
}
DsetRq:: = vSEQUENCE{
   fill  BIT STRING (SIZE(2)),
   deleteBOOLEAN,
   attributeIdListAttributeIdList,
```

```
   dataList DataList
}
DataList:: = SEQUENCE(0..255) OF Data
Data:: = OCTET STRING(1..255)
AttributeIdList:: = SEQUENCE(0..255)OF attributeID
attributeID:: = INTEGER(0..127,..)
```

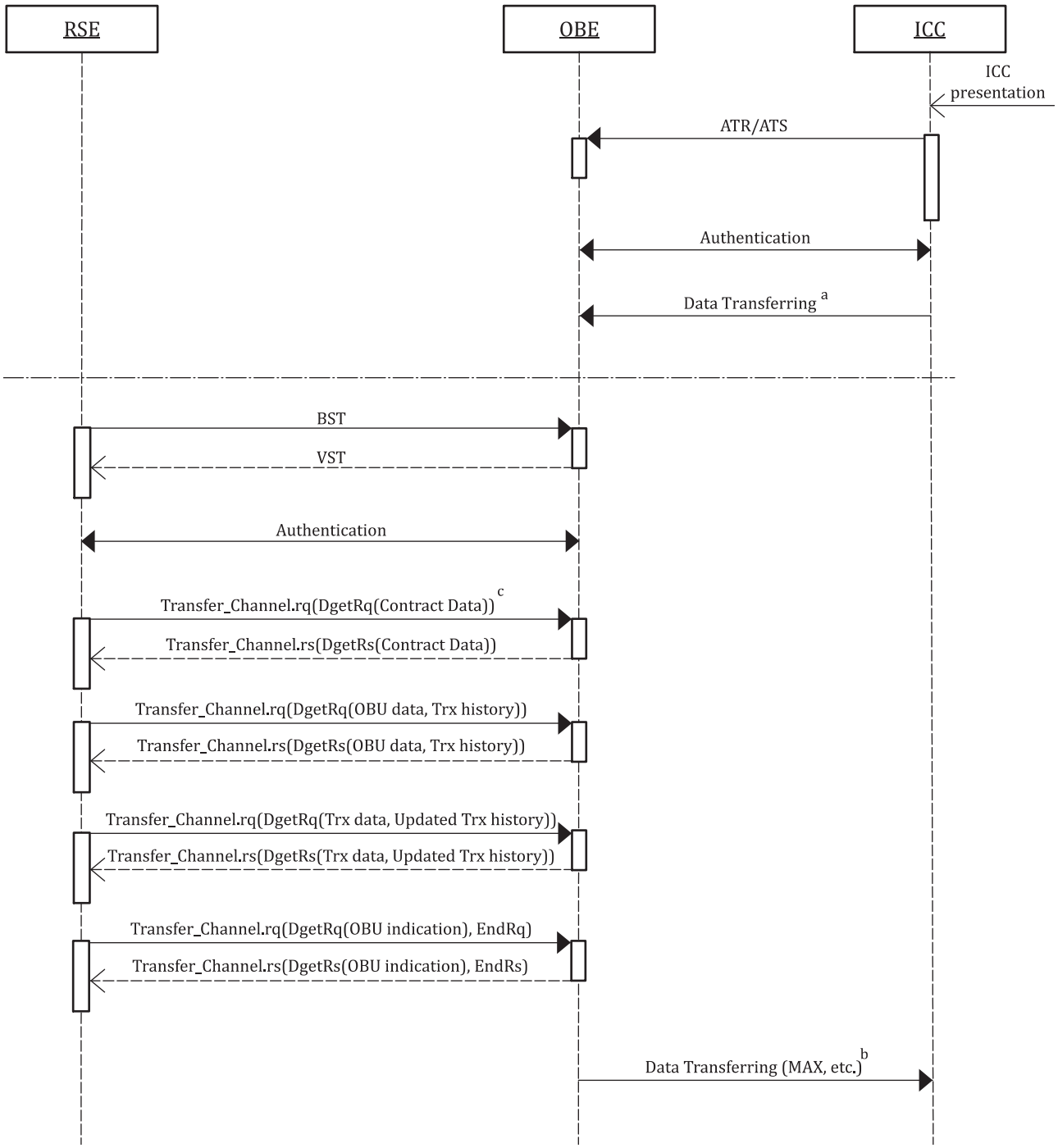
b) Definition of ADPU in TransferChannel.rs

```
RSECommand:: = SEQUENCE{
   eidDsrc-EID,
   parameterOCTET STRING (SIZE(0..255)),  --Excluded parameter in Sub command
   subCommandList SEQUENCE(0..255) OF SubCommand--Sub command list
}
DgetRs:: = SEQUENCE{
   fill  BIT STRING (SIZE(3)),
   retINTEGER(0..255),
   dataList DataList
}
DsetRs:: = SEQUENCE{
   fill  BIT STRING (SIZE(3)),
   retINTEGER(0..255),
}
```

B.2.3 Transaction example

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

Figure B.5 shows the information exchange for a credit payment of a flat rate charging transaction (open system).



a The following ICC datasets are transferred to the OBE after ICC Presentation Contract data, Transaction history data (Trx history).

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

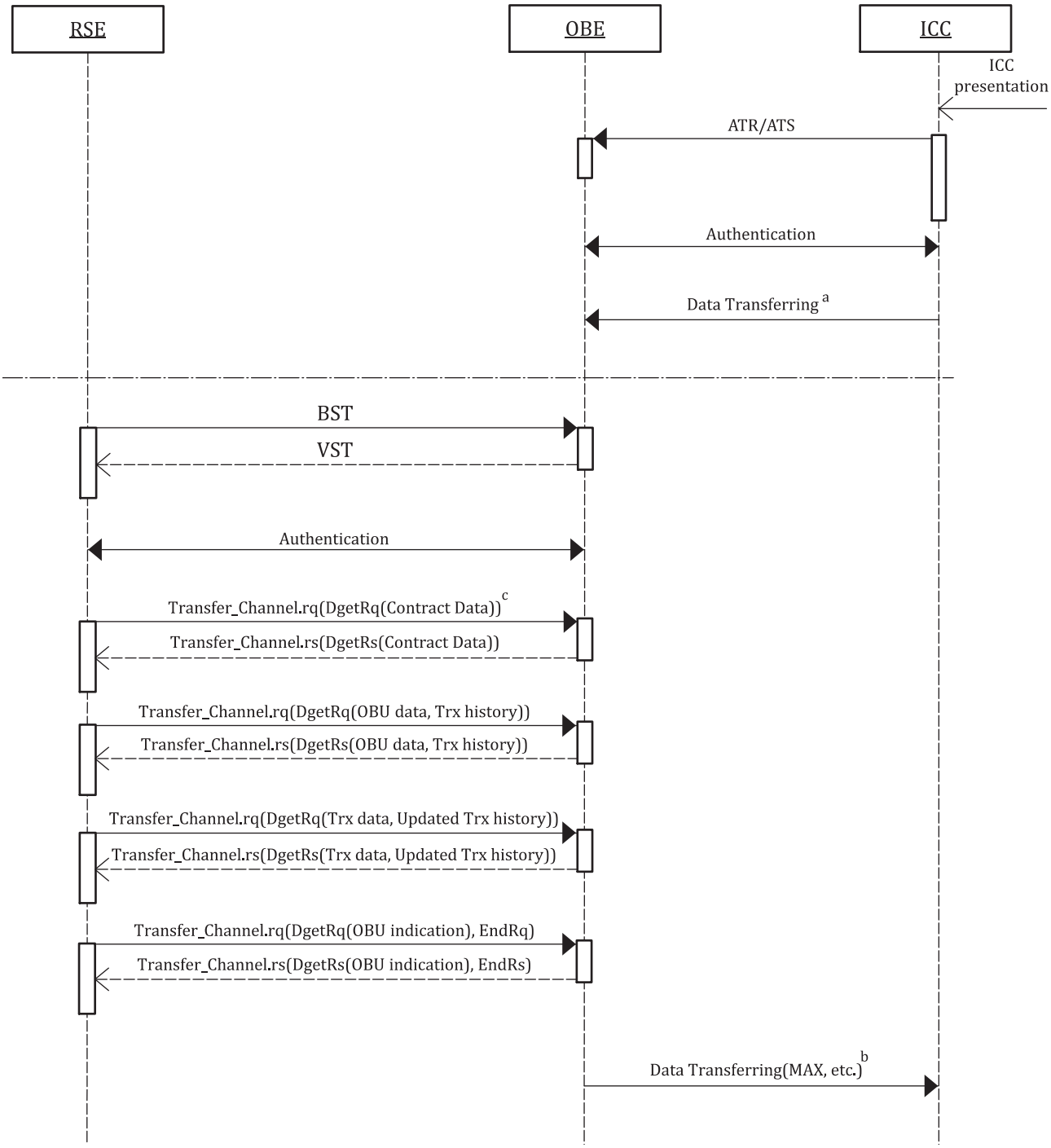
c The IC card number is included.

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

a) Entrance transaction

Figure B.6 shows the information exchange for an entrance transaction.



a The following ICC datasets are transferred to the OBE after ICC Presentation Contract data, Transaction history data (Trx history).

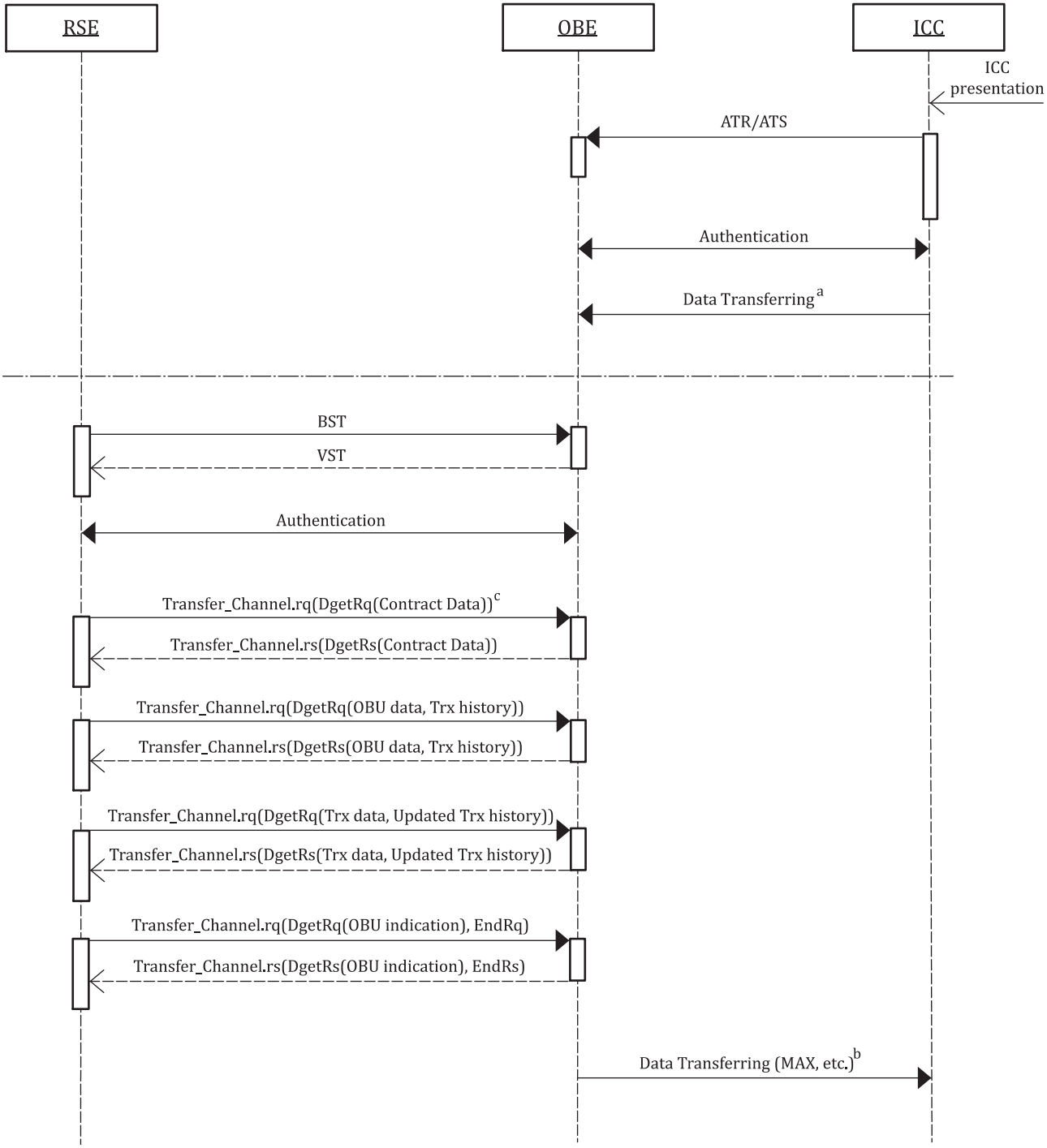
b The following datasets are transferred to the ICC after completion of DSRC Transaction (Trx.) data, Transaction (Trx) history data.

c The IC card number is included.

Figure B.6 — Sequence flow of entrance transaction

b) Exit transaction

Figure B.7 shows the information exchange for an exit transaction.



a The following ICC datasets are transferred to the OBE after ICC Presentation Contract data, Transaction history data (Trx history).

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

c 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, this clause describes the ICC access method used in ETC in the Republic of Korea. In ETC in in the Republic of Korea, the hybrid type ICC is used both for ETC and Touch and Go, where the driver can go through a toll lane by touching their ICC to the roadside reader.

— Command definition: Defined by ETC standards in the Republic of Korea

— 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 — Debit command

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

— Definition of `nonce`

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

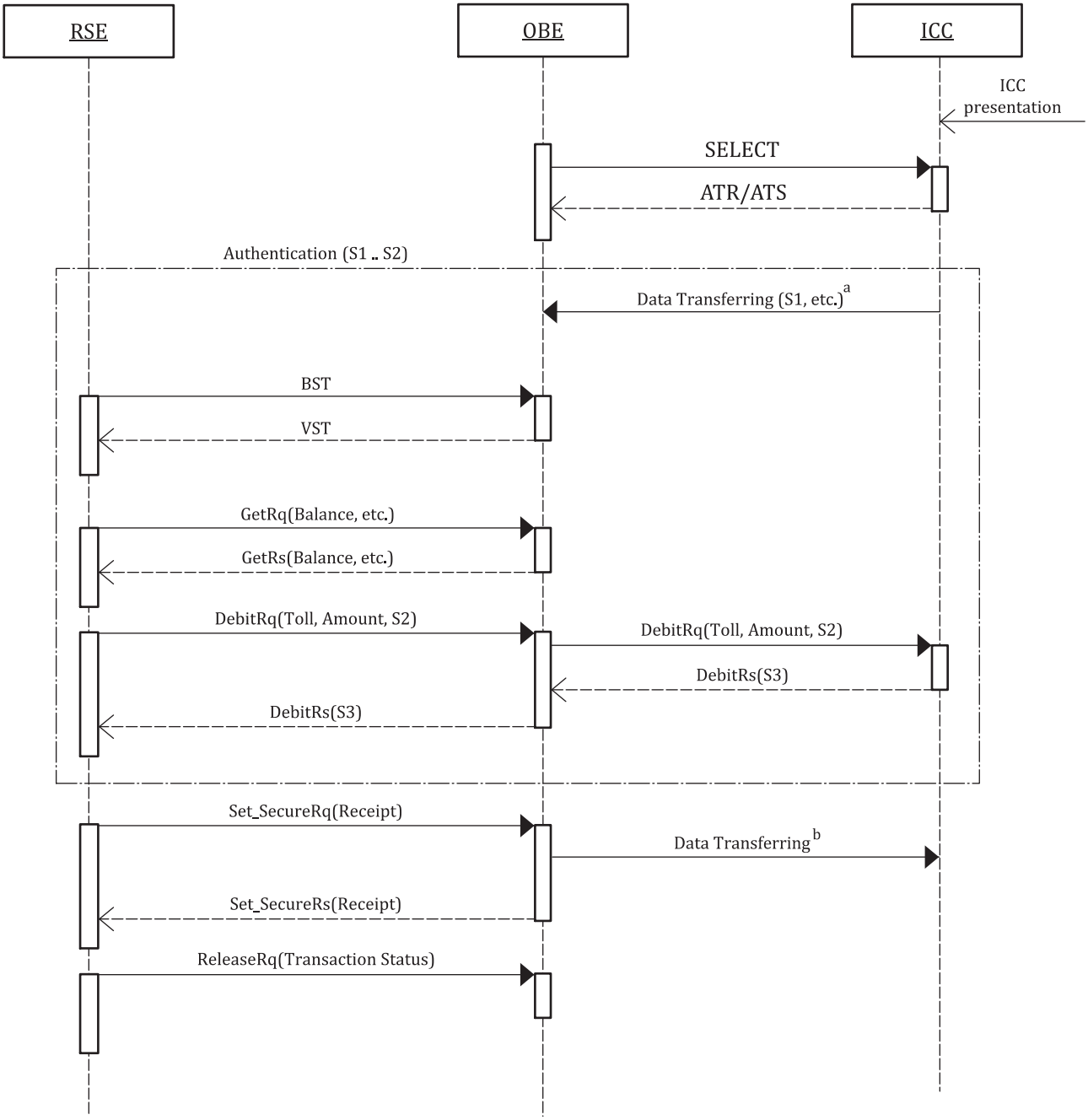
— Definition of `debitAuthenticator`

```
debitAuthenticator:: = SEQUENCE{
   parameterLenOCTET 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

Figure B.8. shows the information exchange for a prepaid payment transaction using a fast transaction algorithm.



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

b 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.

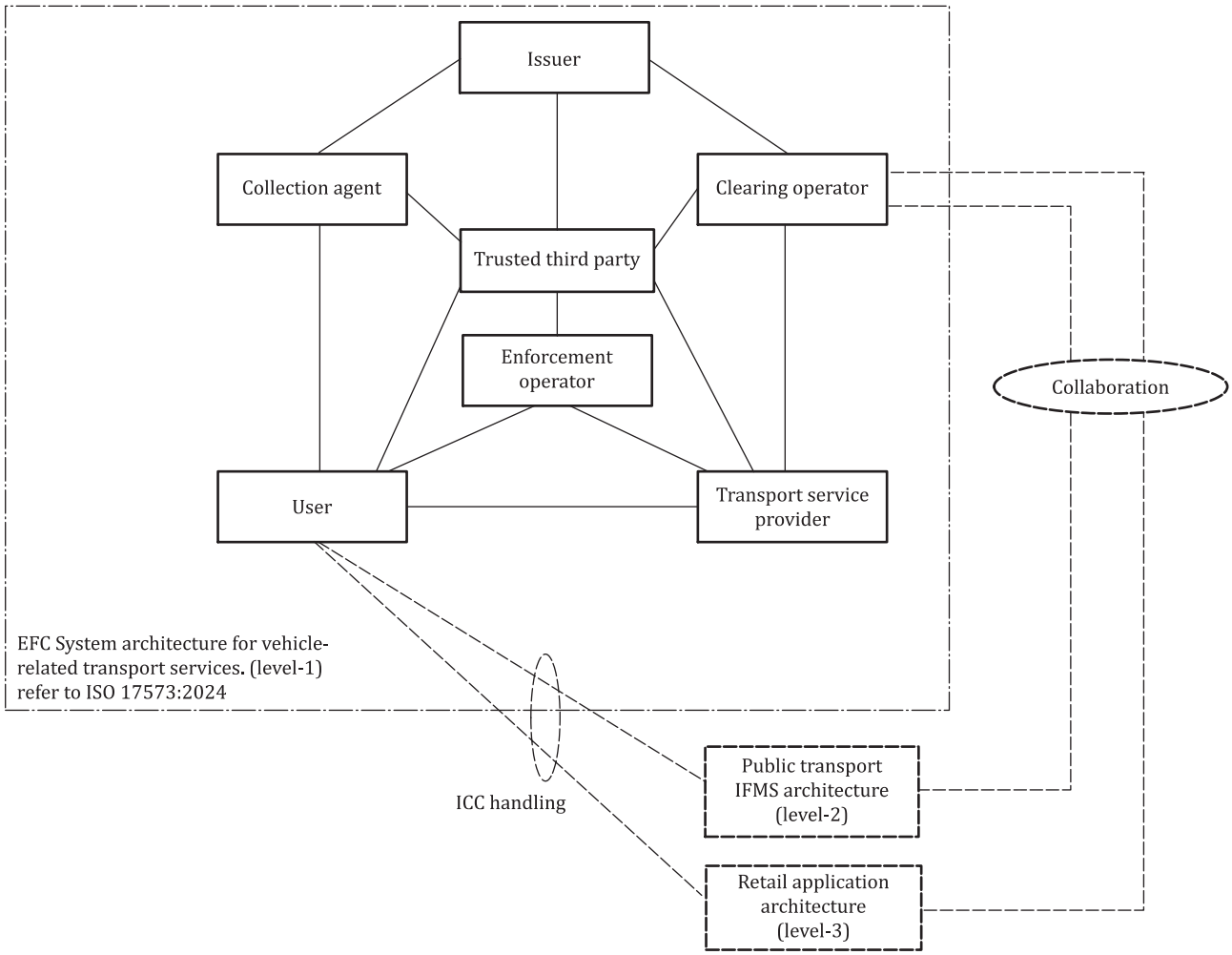


Figure C.1 — Interoperability model of the EFC service with other services

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

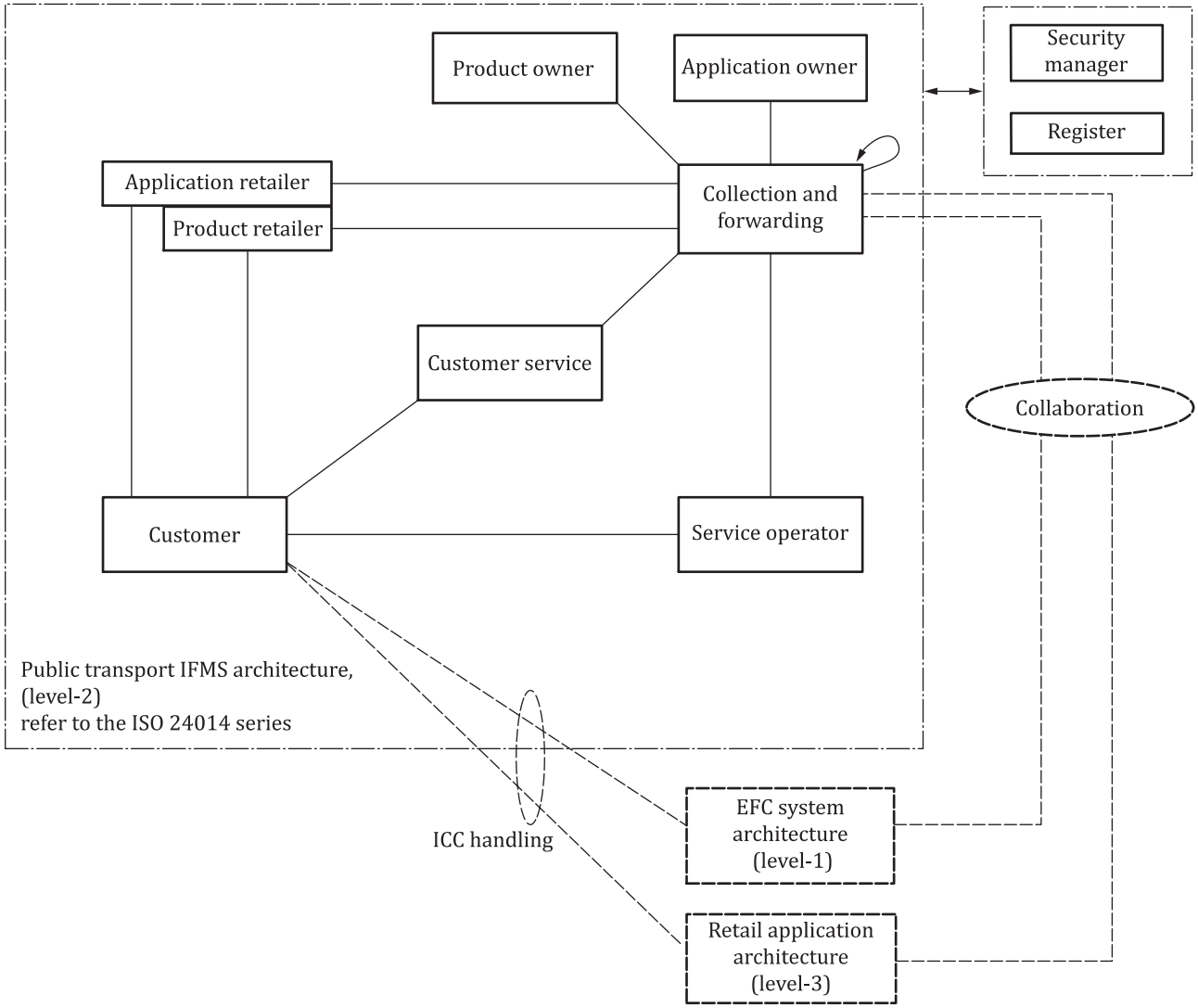


Figure C.2 — Interoperability model of the IFMS service with other services

Bibliography

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

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

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

[4] ISO/IEC 14443-1, *Cards and security devices for personal identification — Contactless proximity objects — Part 1: Physical characteristics*

[5] ISO/IEC 14443-2, *Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface*

[6] ISO/IEC 14443-3, *Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision*

[7] ISO/IEC 14443-4, *Cards and security devices for personal identification — Contactless proximity objects — Part 4: Transmission protocol*

[8] ISO/IEC 15408-1, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

[9] ISO/IEC 15408-2, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

[10] ISO/IEC 15408-3, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

[11] ISO/IEC 15408-4, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

[12] ISO/IEC 15408-5, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

[13] ISO 15628, *Intelligent transport systems — Dedicated short range communication (DSRC) — DSRC application layer*

[14] ISO 17573-1, *Electronic fee collection — System architecture for vehicle-related tolling — Part 1: Reference model*

[15] ISO 17573-3, *Electronic fee collection — System architecture for vehicle-related tolling — Part 3: Data dictionary*

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

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

[18] Forum I.T.S. RC-004, *DSRC basic application interface published by 'ITS info-communication Forum'* in Japan (https://itsforum.gr.jp/E_index.html)

[19] Nippon Expressway Research Institute Company Limited, *5,8 GHz band DSRC interface specification* (ETC-B02230P, November 2022) (https://shop.ri-nexco.co.jp/item/770/)

ICS 03.220.01; 35.240.60

Price based on 29 pages

iso.org