TECHNICAL SPECIFICATION

ISO/TS 25110

Second edition
2013-05-15

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/TS 25110:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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

ISO/TS 25110 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*, and CEN/TC 278, *Road transport and traffic telematics.*

This second edition cancels and replaces the first edition (ISO/TS 25110:2008), which has been technically revised.

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. 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 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.

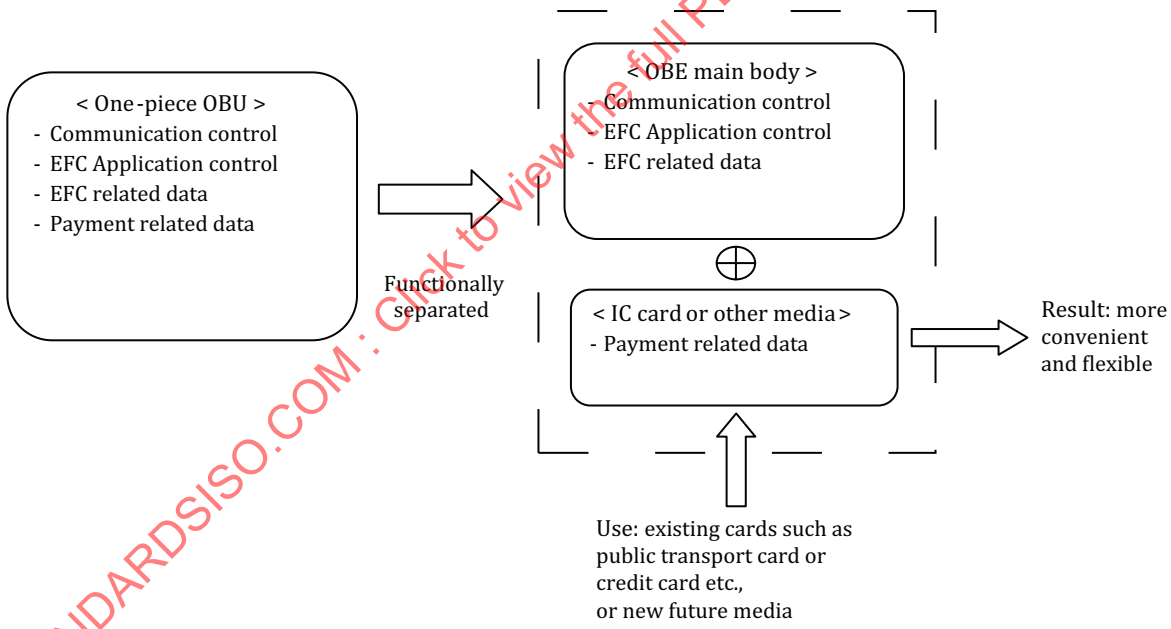


Figure 1 — Motivation for on-board account using ICC

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.

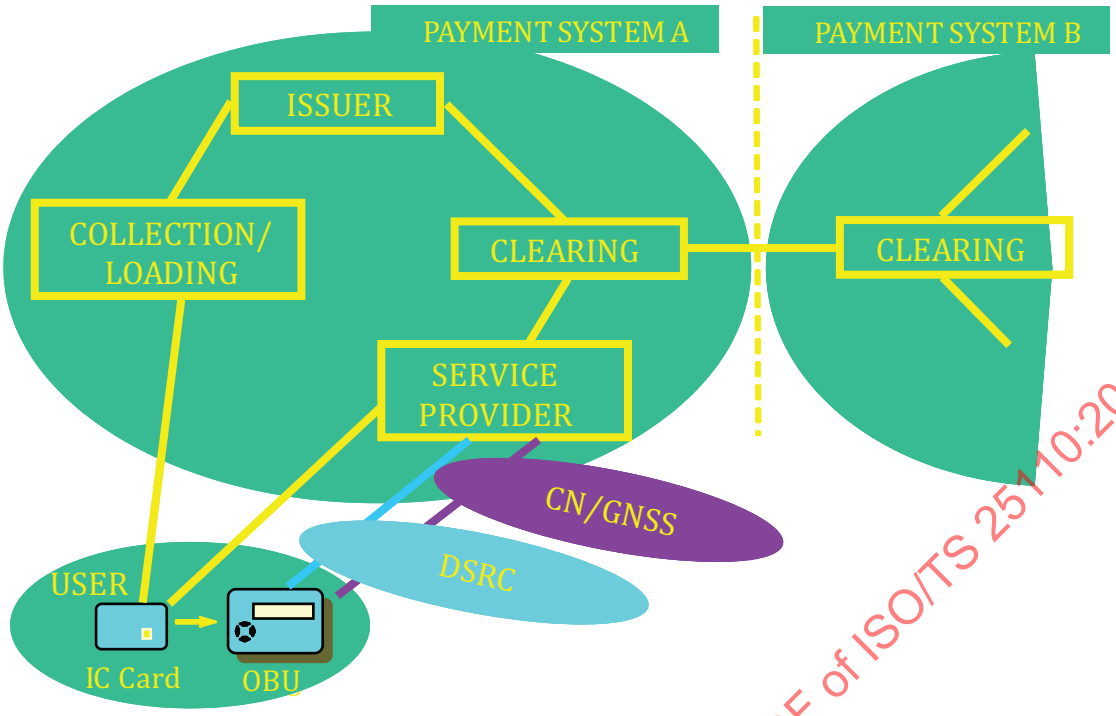


Figure 2 — Illustration of the scope of the EFC standards

Objective

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

Use

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

This Technical Specification covers:

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

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

— interface definition for each model comprises

— functional configuration,

— RSE command definitions for ICC access, and

— data format and data element definitions of RSE commands;

— a transaction example for each model in Annex B.

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

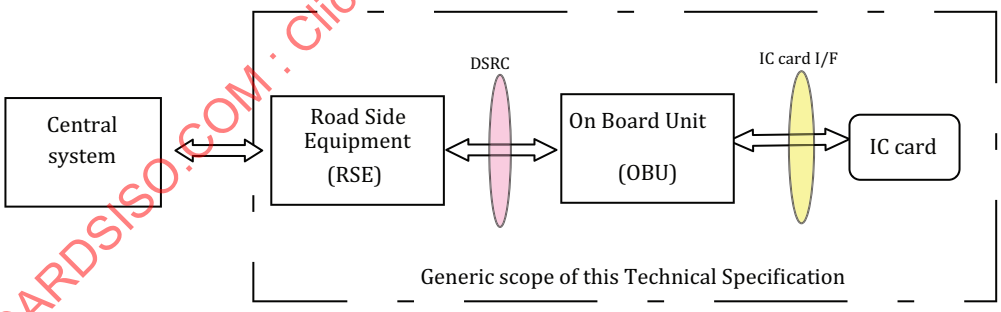


Figure 3 — Configuration of on-board account and generic scope of ISO/TS 25110

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

NOTE The existing standards for physical and other protocol layers both between RSE and OBE, and between OBE and ICC, are outside the scope of this Technical Specification. 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 Technical Specification.

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

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

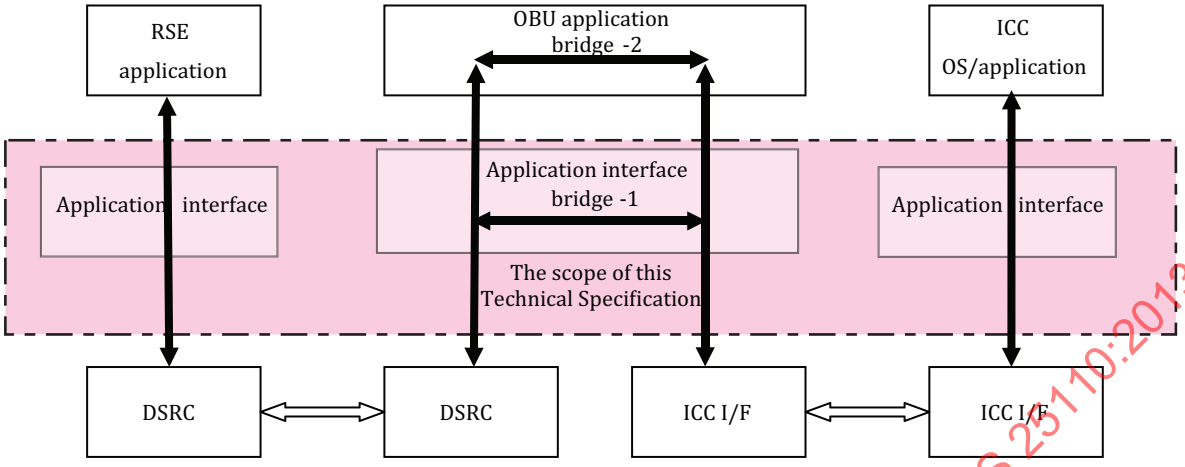


Figure 4 — Scope of ISO/TS 25110

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 14906:2011, *Electronic fee collection — Application interface definition for dedicated short-range communication*

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

3 Terms and definitions

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

3.1
access credentials
data that is transferred to on-board equipment (OBE), in order to establish the claimed identity of a roadside equipment (RSE) application process entity

[ISO 14906, definition 3.1]

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. The access credentials can carry passwords as well as cryptographic based information such as authenticators.

3.2
action
function that an application process resident at the roadside equipment can invoke in order to make the on-board equipment (OBE) execute a specific operation during the transaction

[ISO 14906, definition 3.2]

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

[ISO 14906, definition 3.3]

3.4
authenticator
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and/or the integrity of the data unit and protect against forgery

[ISO 14906, definition 3.4]

3.5
channel
information transfer path

[ISO 7498-2:1989, definition 3.3.13; and ISO 14906, definition 3.5]

3.6
component
logical and physical entity composing an on-board equipment, supporting a specific functionality

[ISO 14906, definition 3.6]

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

[ISO 14906, definition 3.7]

3.8
cryptography
discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

[ISO 7498-2:1989, definition 3.3.20; and ISO 14906, definition 3.8]

3.9
data group
collection of closely related EFC data attributes which together describe a distinct part of an EFC transaction

[ISO 14906, definition 3.9]

3.10
data integrity
property in which data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2:1989, definition 3.3.21; and ISO 14906, definition 3.10]

3.11
element
⟨DSRC⟩ directory containing application information in the form of attributes

[ISO 14906, definition 3.11]

3.12
issuer
entity responsible for the payment system and responsible for issuing the payment means to the user

3.13
on-board equipment
OBE
equipment fitted within or on the outside of a vehicle and used for toll purposes

[ISO 14906, definition 3.13]

Note 1 to entry: The OBE does not need to include payment means.

3.14
on-board unit
minimum component of an on-board equipment, whose functionality always includes at least the support of the DSRC interface

[ISO 14906, definition 3.14]

3.15
roadside equipment
equipment located along the road transport network, for the purpose of communication and data exchanges with on-board equipment

[ISO 14906, definition 3.16]

3.16
secure application module
SAM
physically, electrically and logically protected module intended to contain algorithm(s), related keys, security procedures and information to protect an application in such a way that unauthorized access is not possible

[ISO/TS 17574, definition 3.22]

3.17
service
⟨EFC⟩ road transport related facility provided by a service provider

Note 1 to entry: Normally a type of infrastructure, the use of which is offered to the user for which the user may be requested to pay.

Note 2 to entry: Adapted from ISO 14906.

3.18
service primitive
⟨communication⟩ elementary communication service provided by the application layer protocol to the application processes

[ISO 14906, definition 3.18]

Note 1 to entry: The invocation of a service primitive by an application process implicitly calls upon and uses services offered by the lower protocol layers.

3.19
service provider
⟨EFC⟩ operator that accepts the user's payment means and in return provides a road-use service to the user

3.20
session
exchange of information and interaction occurring at a specific EFC station between the roadside equipment and the user/vehicle

[ISO 14906, definition 3.19]

3.21
transaction
whole of the exchange of information between the roadside equipment and the on-board equipment necessary for the completion of an EFC operation over the DSRC

[ISO 14906, definition 3.24]

3.22
transaction model
functional model describing the general structure of electronic payment fee collection transactions

[ISO 14906, definition 3.25]

3.23
user
customer of a toll service provider

EXAMPLE One liable for toll, the owner of the vehicle, a fleet operator, a driver, etc., depending on the context.

Note 1 to entry: Adapted from ISO 14906.

3.24
transport service provider
person, company, authority or abstract entity offering a transport service to the user for which the user has to pay a toll

Note 1 to entry: The fee will in some cases be zero, e.g. emergency vehicles.

Note 2 to entry: See ISO 17573.

4 Abbreviations

For the purposes of this document, the following abbreviations apply throughout the document unless otherwise specified.

AID	Application Identifier
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One (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 (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 model

5.1 Overview

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

5.1.1 Transparent type

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

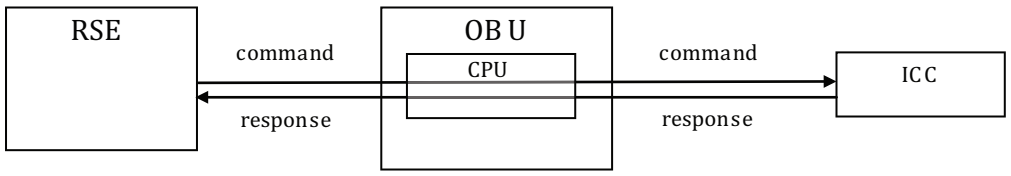


Figure 5 — Generic structure of transparent type

5.1.2 Caching type

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

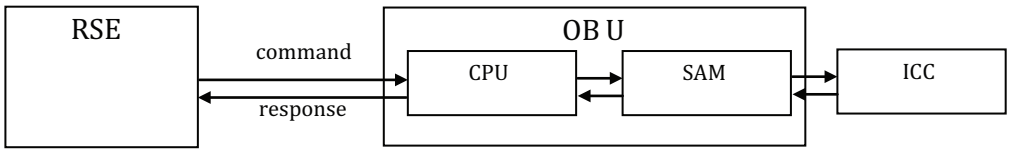


Figure 6 — Generic structure of caching type

5.1.3 Buffering type

The EFC related data which is limited to non-sensitive data are read from 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 RSE. See Figure 7.

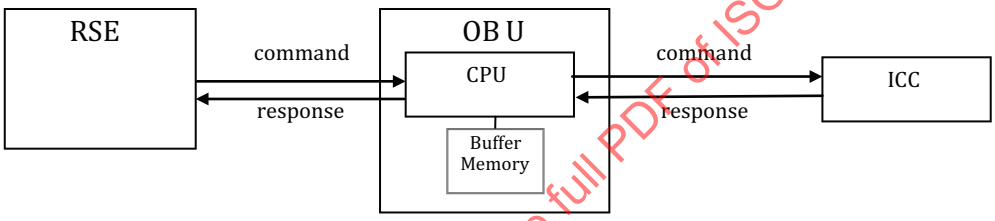


Figure 7 — Generic structure of buffering type

5.2 Symbols

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

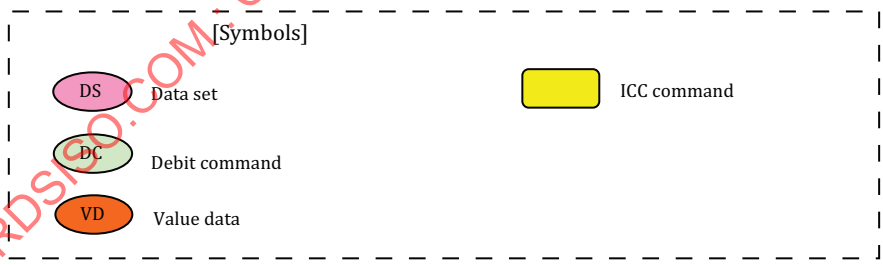


Figure 8 — Definition of symbols

5.3 Transparent type

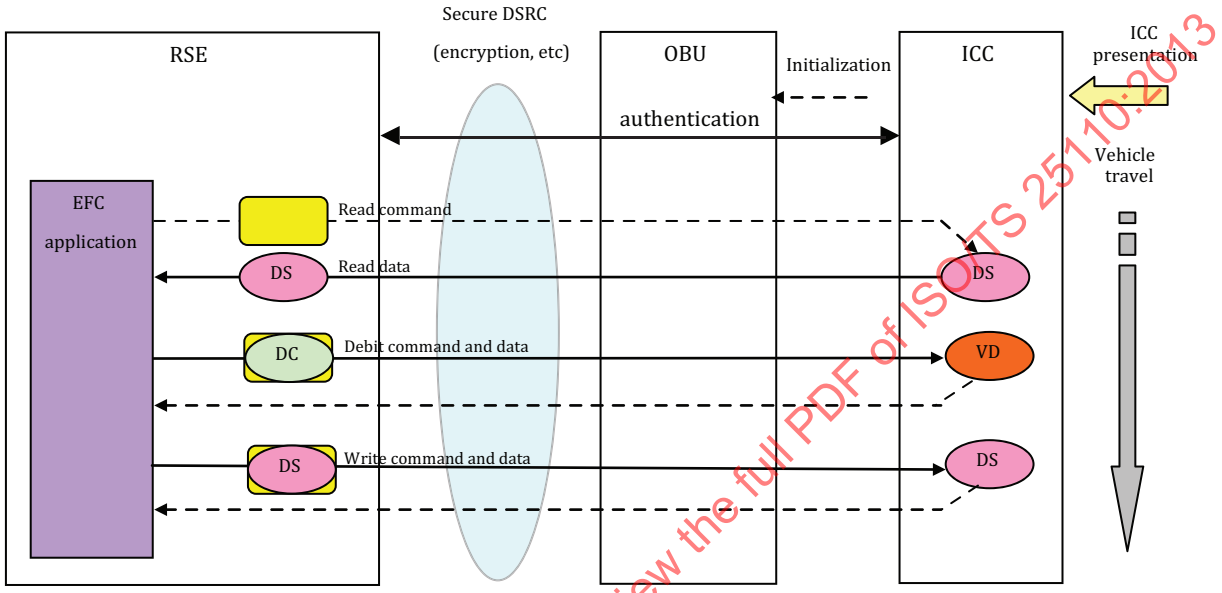
5.3.1 General description

In this model, the maximum vehicle speed depends on the data transfer rate between ICC and OBU, so that the vehicle has to stop or go through slowly under an RSE antenna in case conventional contact ICC is used. The feature of the transparent type is to make OBU simple by eliminating secure memory inside of 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 RSE and ICC are processed directly after establishing DSRC communication and authentication between RSE and OBU is completed. Mutual authentication between 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 RSE to ICC through OBU to read out the data set stored in ICC. In the READ response, the data set stored in ICC is transferred from ICC to RSE through OBU. In the writing sequence, the same procedure is processed. In case of prepaid payment, the debit command is sent from 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 description

In this model, OBU reads out data sets from ICC and stores them in secure memory inside OBU, upon insertion and completion of the authentication. The feature of this type is that high data exchange rate between RSE and OBU is performed even when 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 ICC.

5.4.2 Data transfer process

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

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

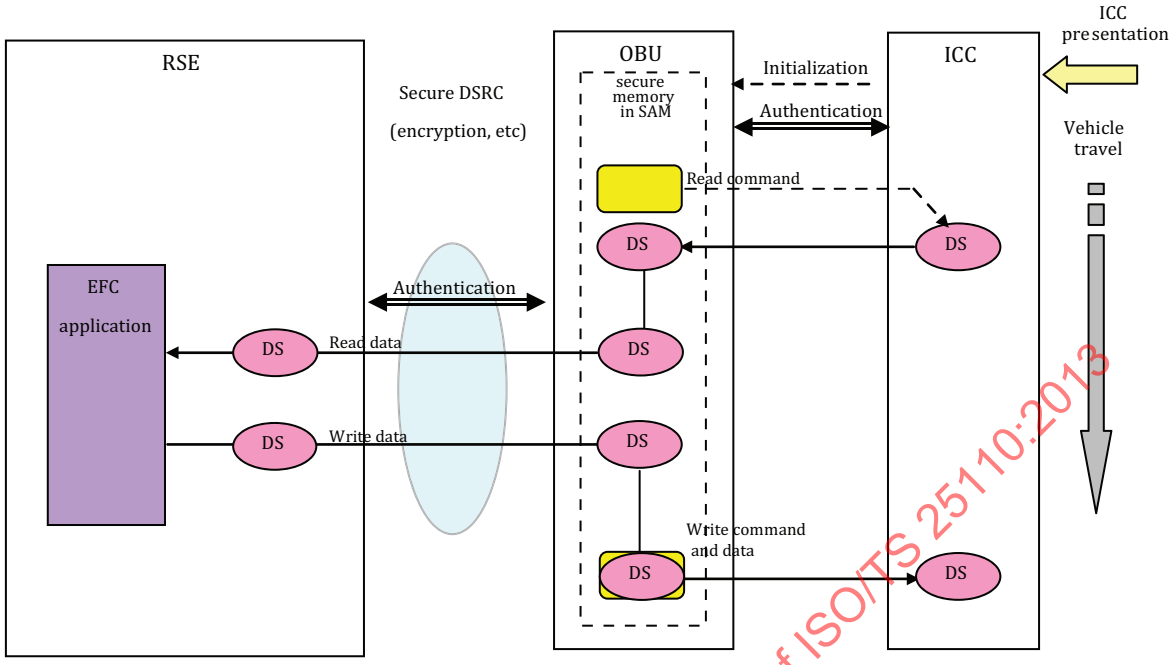


Figure 10 — Data transfer process of caching type

5.5 Buffering type

5.5.1 General description

This buffering type has features of both the transparent type and the cashing type. However, data sets stored in 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 data sets of ICC are read out and stored in buffer memory inside OBU when ICC is inserted into the OBU. Data sets stored in buffer memory are transferred to RSE during DSRC read sequence. In case of writing, data sets of RSE are transferred to OBU and stored in buffer memory of OBU and then transferred to ICC.

5.5.2 Data transfer process

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

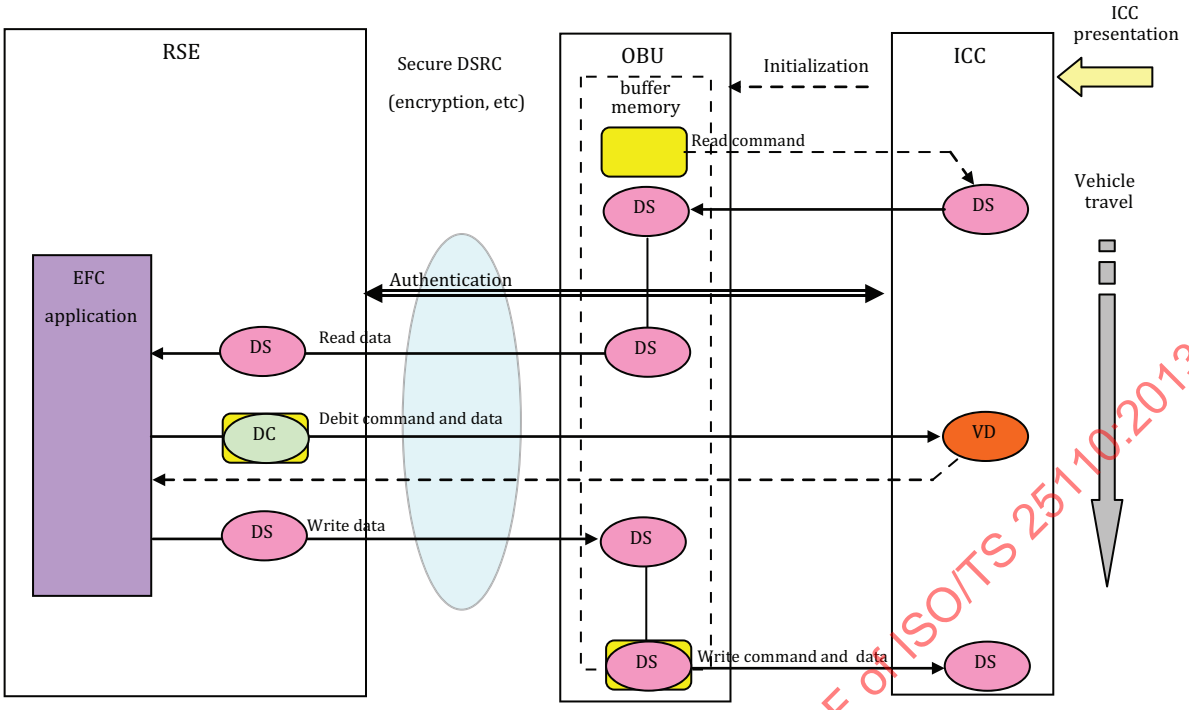


Figure 11 — Data transfer process of buffering type

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. RSE sends the RSE command containing ICC access commands in its ADPU so as to execute the ICC read/write operation directly.

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

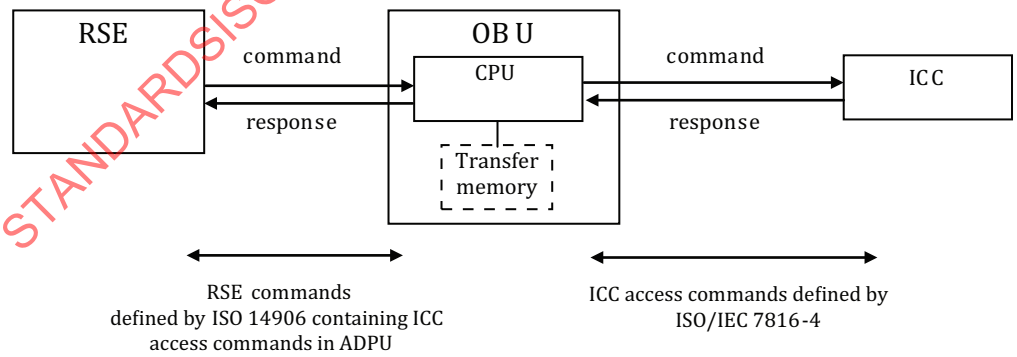


Figure 12 — Functional configuration of transparent type

6.1.2 Command and response between 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).

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)	Return Status		Optional use

The apdu in ResponseParameter shall contain the ICC response.

6.2 Caching type

6.2.1 Functional configuration

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

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

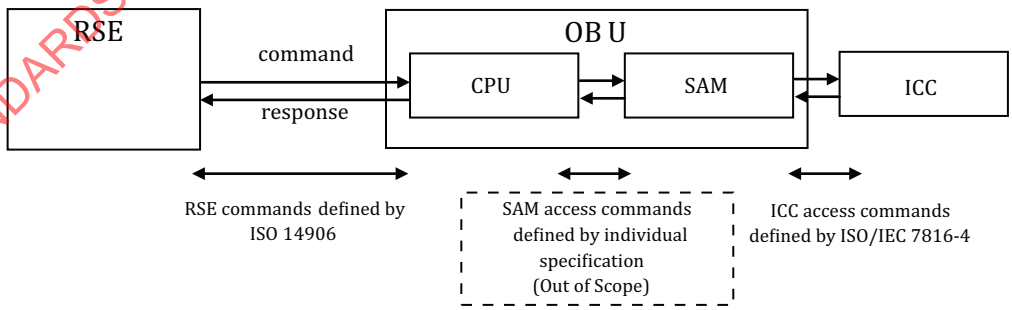


Figure 13 — Functional configuration of caching type

6.2.2 Command and response between 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).

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)	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

Functional configuration of the buffering type is shown in Figure 14. Data sets stored in ICC are read out and stored in buffer memory of OBU when ICC is inserted to OBU. During DSRC communication, RSE send the RSE command to read data sets stored in buffer memory.

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

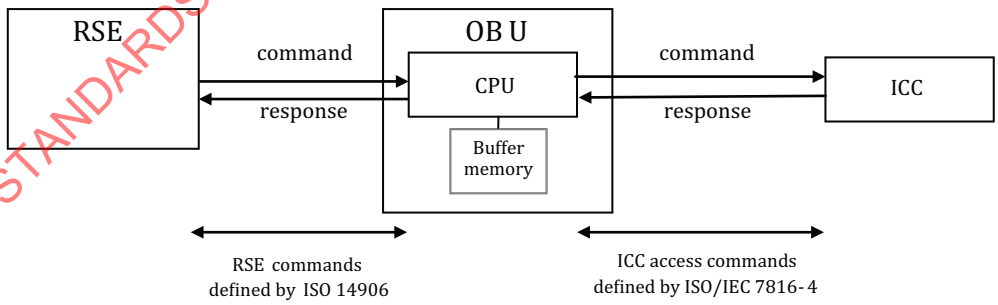


Figure 14 — Functional configuration of buffering type

6.3.2 Command and response between 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.

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 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)	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 the figure, referred to as evaluation assurance levels (EALs), are defined in ISO 15408.

Category-4 is performed by a specially designed security mechanism such as 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 multi-lane free flow, where the vehicle goes through at high speed under the roadside antenna.

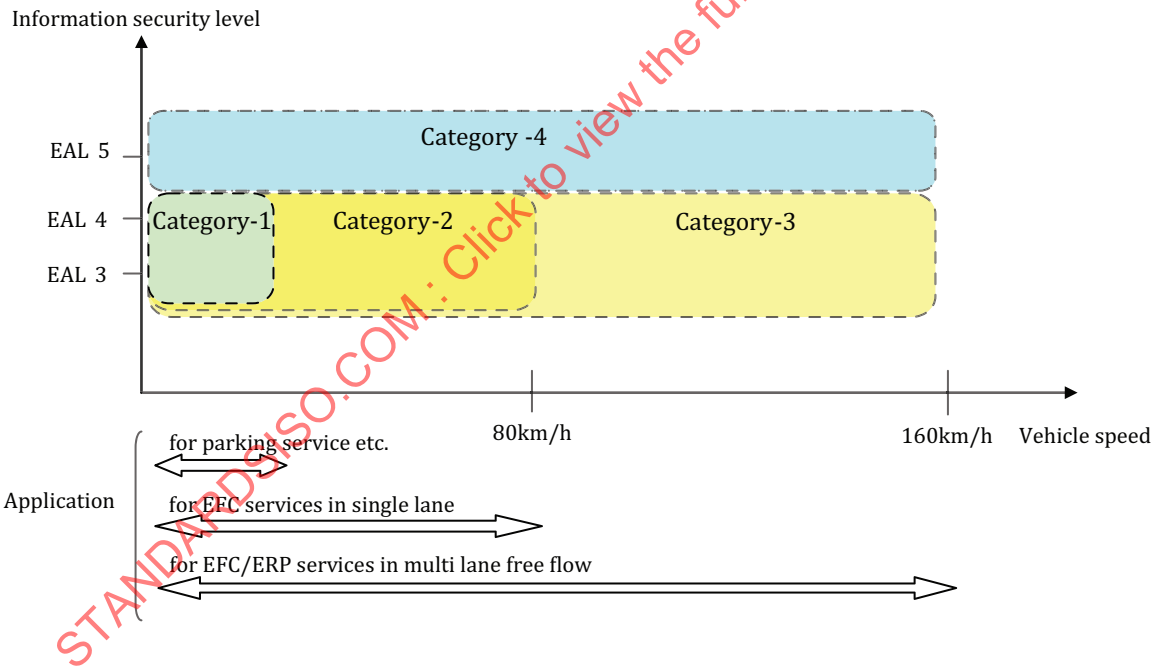


Figure A.1 — Operational requirements

A.2 Type of ICC

ICC used for on–board account 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 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.

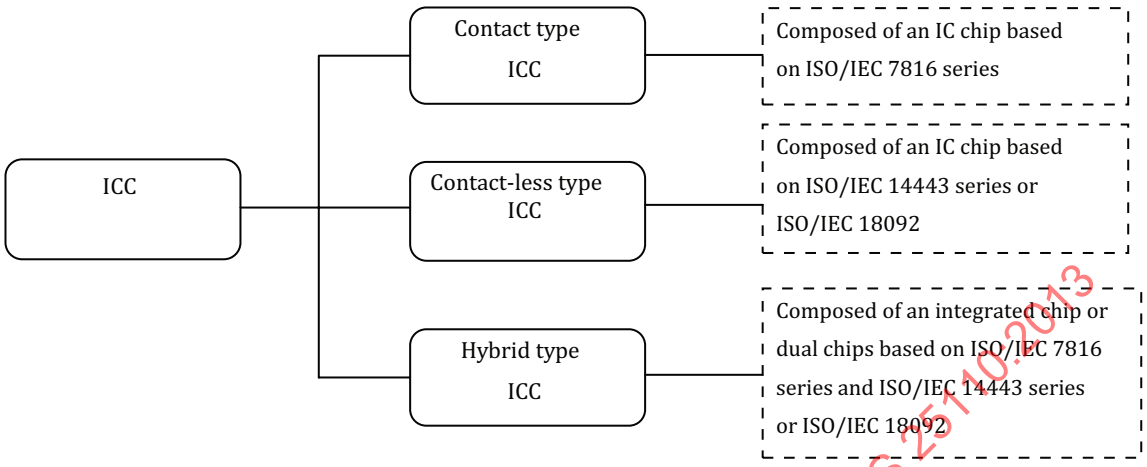


Figure A.2 — Type of IC card

A.3 Interoperability requirements for ICC

For its feature of secure and portable aspects, ICC is potentially required to have interoperability with other services as a common payment means. The interoperability level required for 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 ReceitServicePart of the OBU memory.

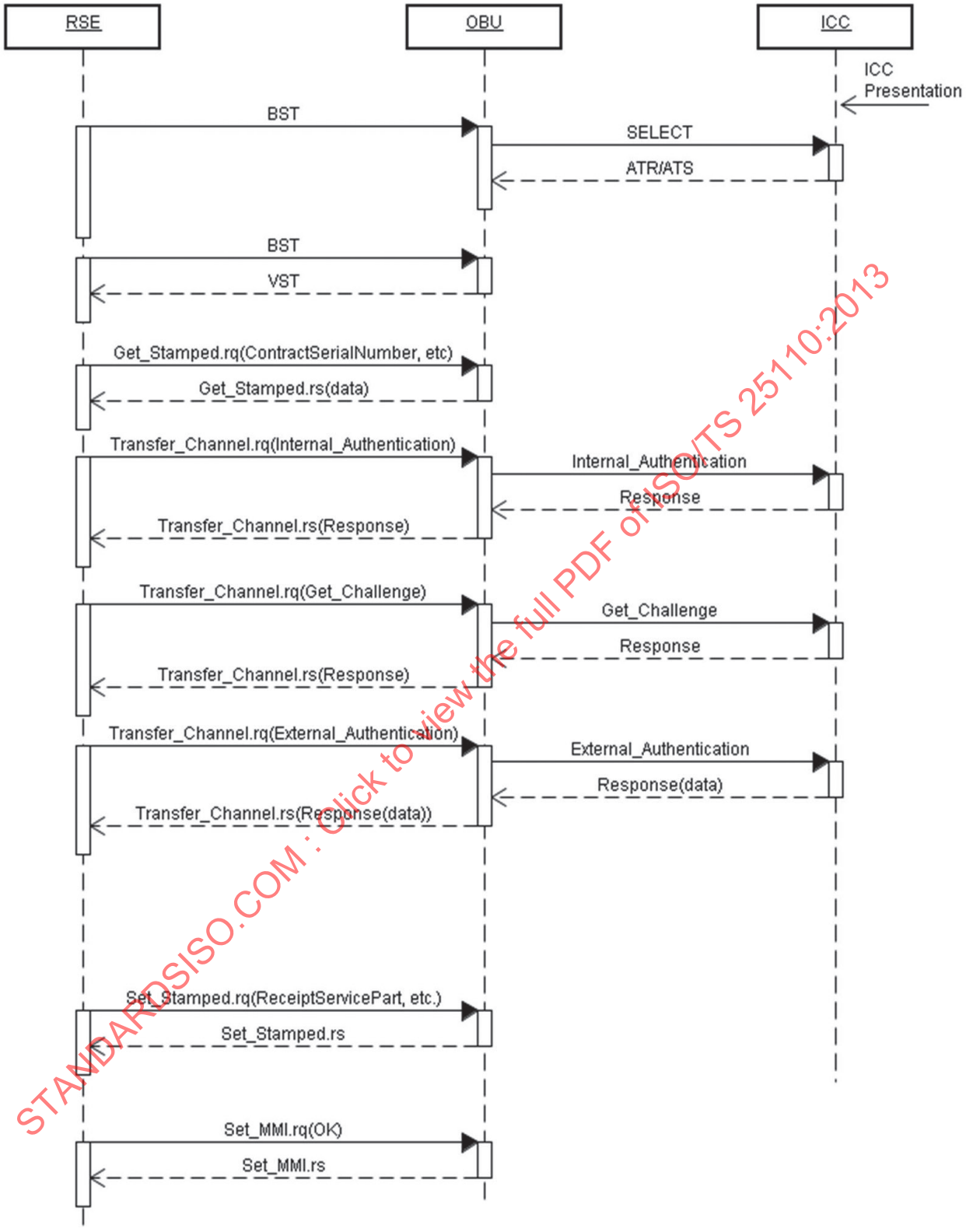


Figure B.1 — Sequence flow of entrance system

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.

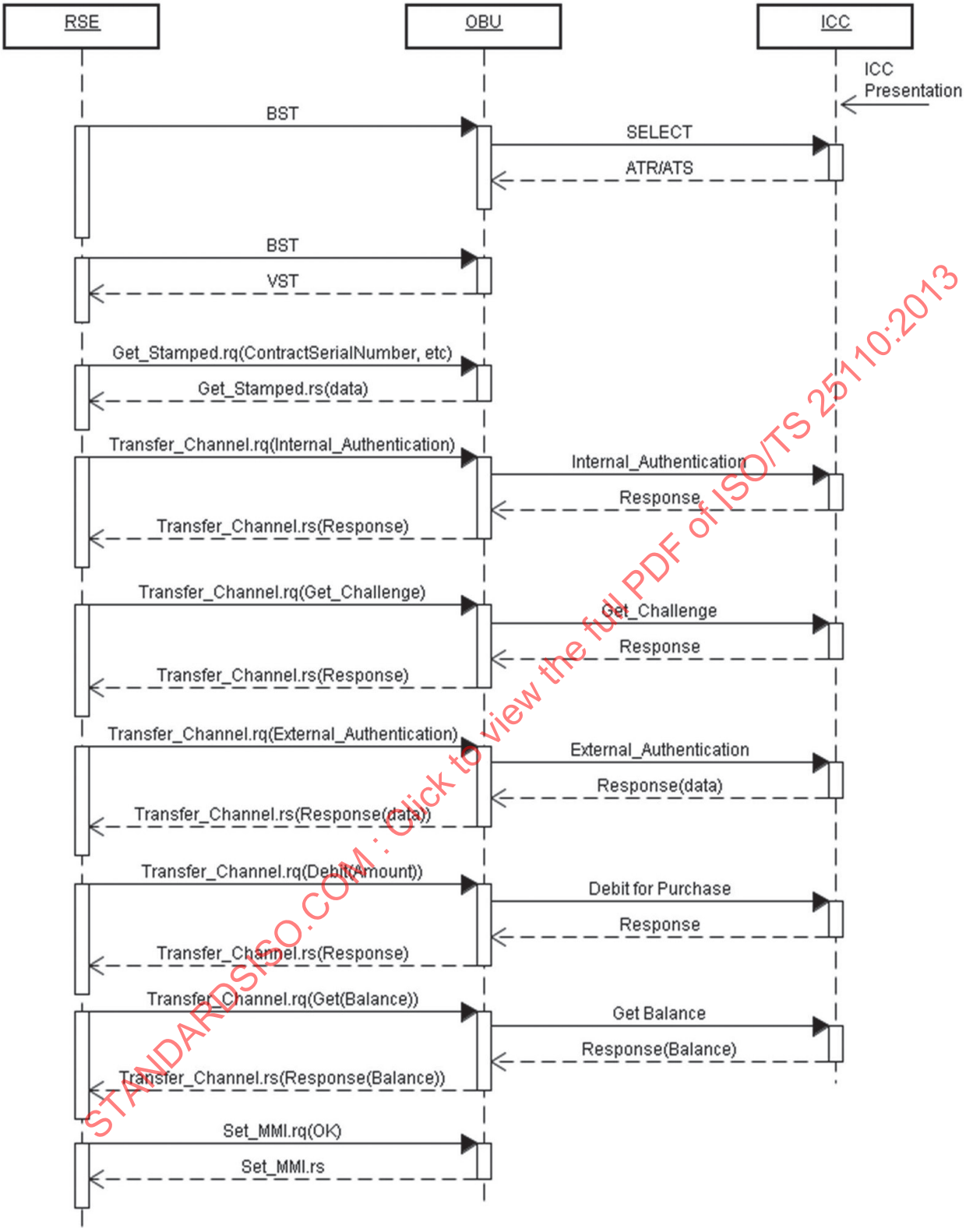


Figure B.2 — Sequence flow of exit system

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 "DSRC basic application interface" established by ITS Forum in Japan is introduced.

"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, ICC access is defined for parking payment application.

In this subclause, Send Message defined in "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]   ObuDenialResponsse
```

```
}
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

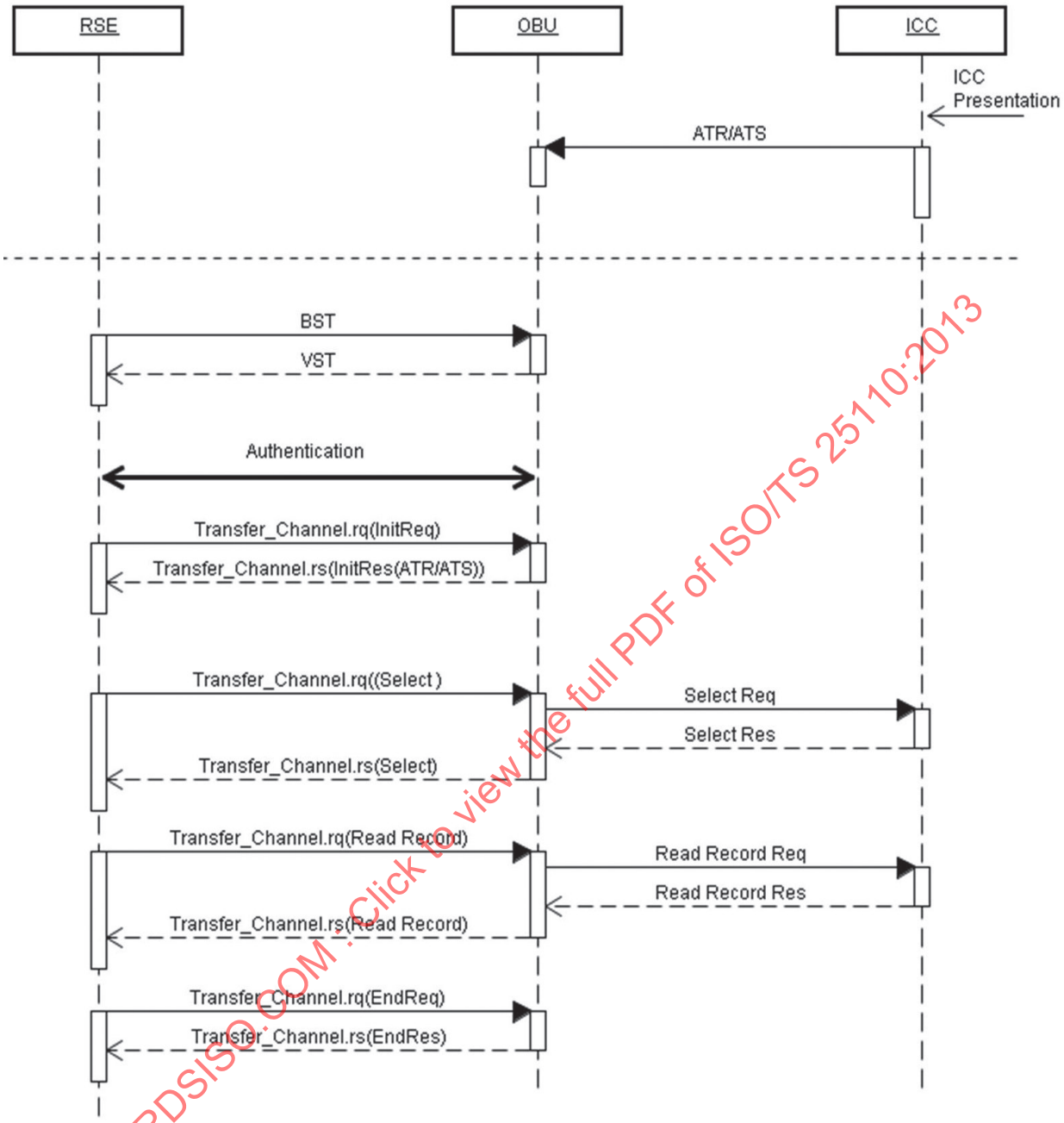
```
ICCAccessResponse::=SEQUENCE{
    versionIndex        Version,
    accessCommand       AccessCommand

}
```

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.

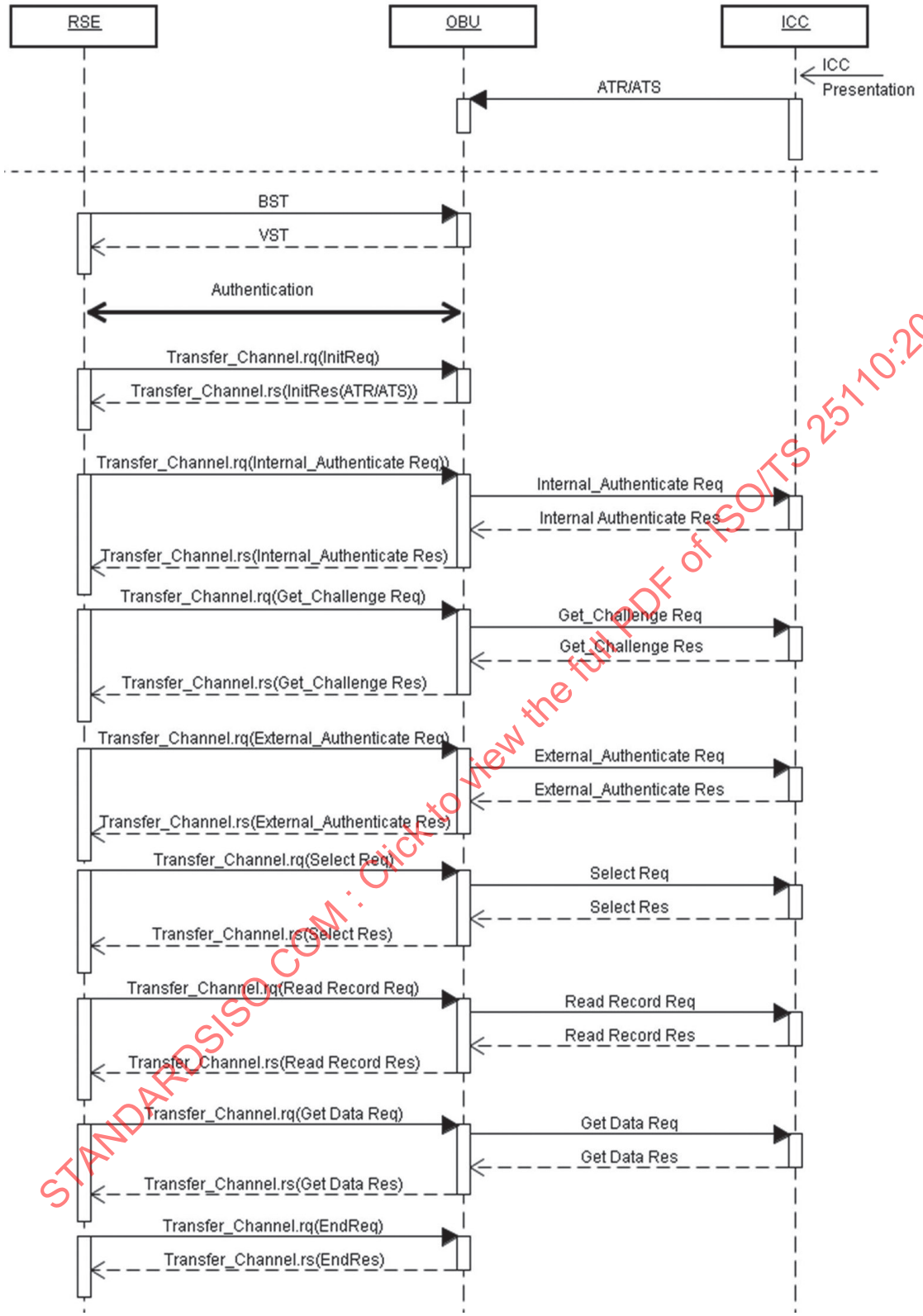


NOTE *1: Membership number is contained in READ RECORD Res.

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.



NOTE *1: Credit card number is contained in Read RecordRes.

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 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 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 SAM is adopted in Japanese ETC are:

— to implement a caching mechanism in 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 RSE and OBU. SAM contains not only a security mechanism but also an ETC application to perform caching and data handing processes with ICC, and

— to maintain competitiveness and to spread OBU nation-wide quickly.

NOTE 2 Explanation of AID = 14:

— AID = 14 usage is described in ISO 14906:2011.

— 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 (SIZE(0..255)),
    subCommandList  SEQUENCE(0..255) OF 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,..)
```

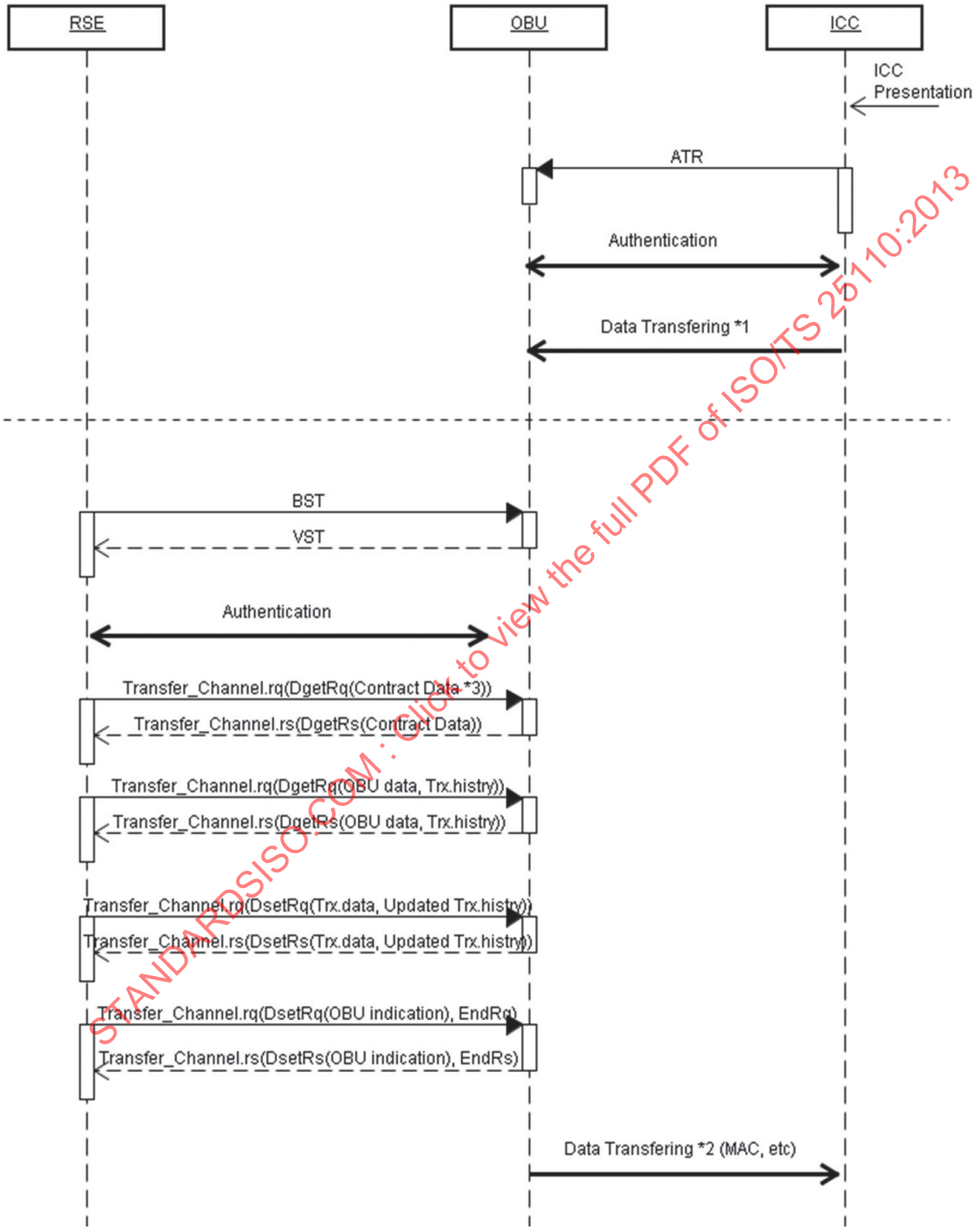
b) Definition of ADPU in TransferChannel.rs

```
RSECommand::=SEQUENCE{
    eid                     Dsrc-EID,
    parameter               OCTET STRING (SIZE(0..255)),
    subCommandList          SEQUENCE(0..255) OF 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



NOTE *1: The following ICC data sets are transferred to OBU after ICC presentation Contract data, Transaction histry data (Trx histry), *2: The following data sets are transferred to ICC after completion of DSRC Transaction (Trx.) data, Transaction (Trx) histry data, *3: IC card-number is included.

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