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)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 25110:2017
https://standards.iteh.ai/catalog/standards/sist/98e43d44-8f96-4807-a1f9-172d94a8d49f/iso-25110-2017

Reference number
ISO 25110:2017(E)

© ISO 2017

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 25110:2017
https://standards.iteh.ai/catalog/standards/sist/98e43d44-8f96-4807-a1f9-172d94a8d49f/iso-25110-2017

COPYRIGHT PROTECTED DOCUMENT

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO 2017 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 25110:2017
https://standards.iteh.ai/catalog/standards/sist/98e43d44-8d6-4807-a1d9-172d9aa8d491/iso-25110-2017

© ISO 2017 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO 25110:2017
https://standards.iteh.ai/catalog/standards/sist/[illegible]-a1f9-172d94a8d49f/iso-25110-2017

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.

 © ISO 2017 – All rights reserved

Introduction

Background and motivation

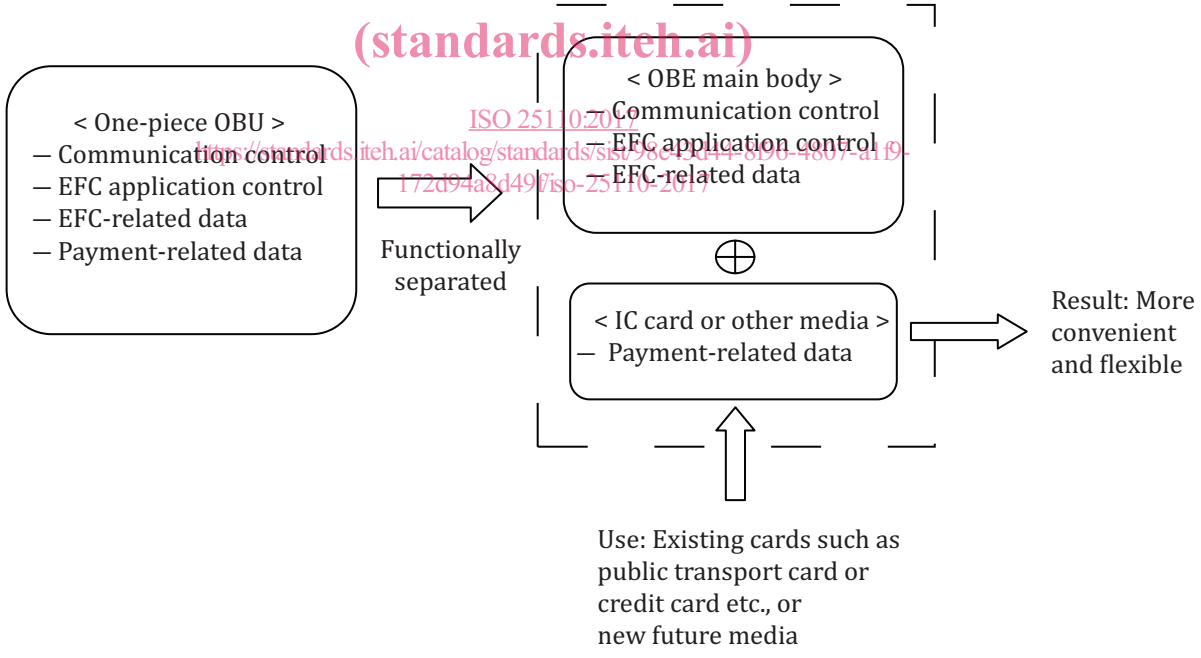
There are two payment systems dealing with electronic fee collection (EFC). The first is the central account system using a one-piece on-board unit (OBU) and the second is the on-board account system using a payment media such as the integrated circuit card (ICC).

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

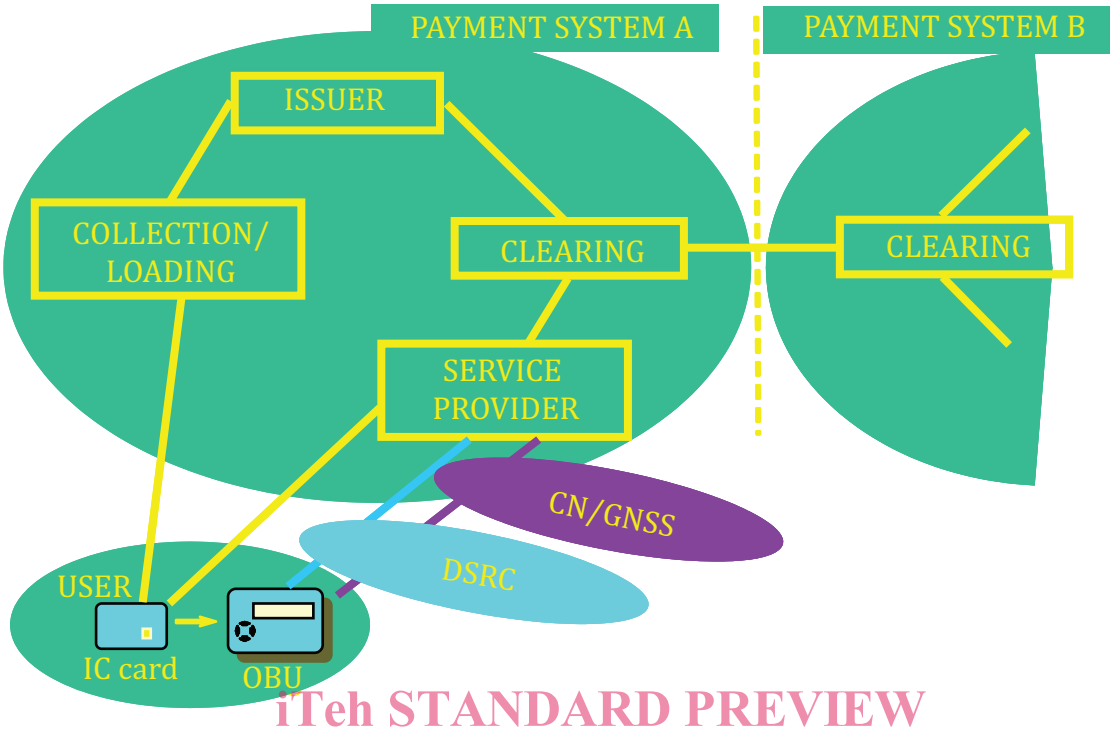


ISO 25110:2017
https://standards.iteh.ai/catalog/standards/sist/9ac42d44-8b6-4807-a1f9-172d94ad496/iso-25110-2017

Figure 1 — Motivation for on-board account using ICC

© ISO 2017 – All rights reserved

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.



iTeh STANDARD PREVIEW
(standards.iteh.ai)

Figure 2 — Illustration of the scope of the EFC standards

ISO 25110:2017
https://standards.iteh.ai/catalog/standards/sist/98e43d44-8f96-4807-a1f9-172d94a8d49f/iso-25110-2017

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.

© ISO 2017 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 25110:2017
https://standards.iteh.ai/catalog/standards/sist/98e43d44-8f06-4807-a1f9-172d94a8d49f/iso-25110-2017

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.

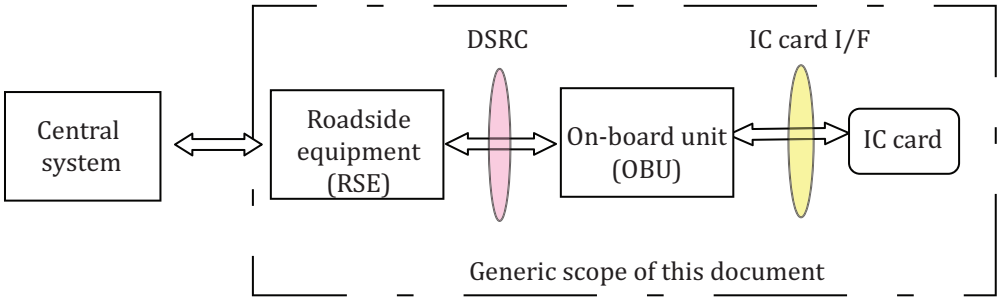


Figure 3 — Configuration of an on-board account and the scope of this document

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.

© ISO 2017 – All rights reserved

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

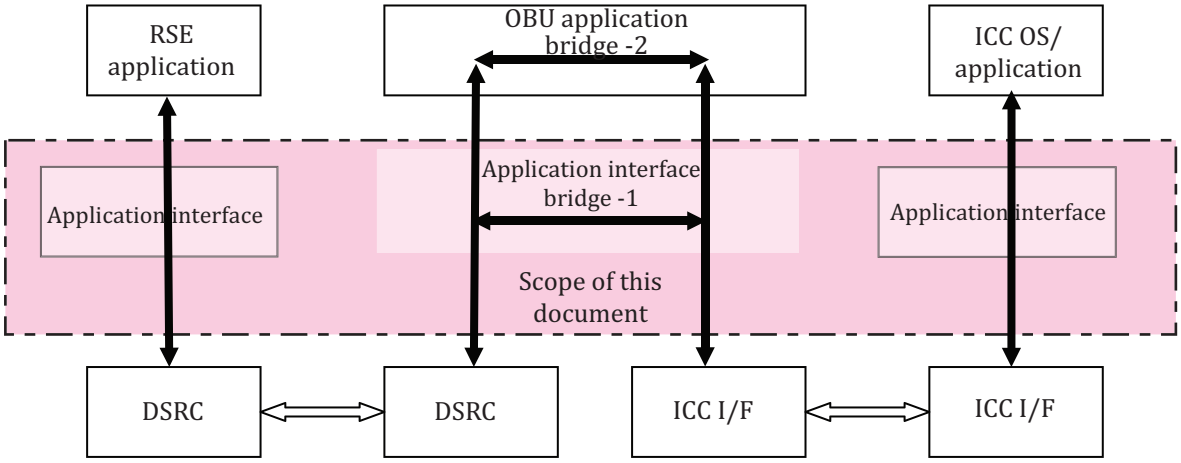


Figure 4 — Application interfaces of RSE, OBU and ISS and the scope of this document

2 Normative references

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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 25110:2017
https://standards.iteh.ai/catalog/standards/sist/98e43d44-8f96-4807-a1f9-172d94a8d49f/iso-25110-2017

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]

© ISO 2017 – All rights reserved

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO 25110:2017
https://standards.iteh.ai/catalog/standards/sist/98e43d44-8f96-4807-a1f9-172d94a8d49f/iso-25110-2017

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

© ISO 2017 – All rights reserved

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 25110:2017
https://standards.iteh.ai/catalog/standards/sist/98e43d44-8f96-4807-a1f9-172d94a8d49f/iso-25110-2017

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

© ISO 2017 – All rights reserved

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

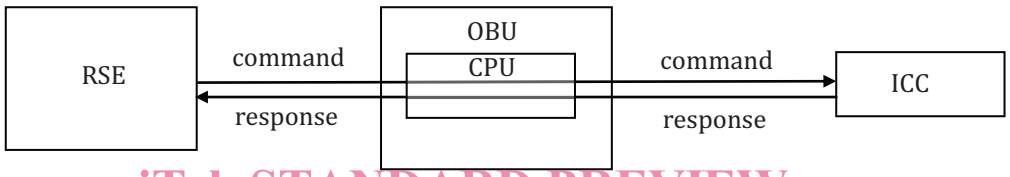
5 Data transfer models

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.



iTeh STANDARD PREVIEW
(standards.iteh.ai)

Figure 5 — Generic structure of transparent type

ISO 25110:2017
https://standards.iteh.ai/catalog/standards/sist/98e43d44-8f96-4807-a1f9-172d94a8d49f/iso-25110-2017

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.

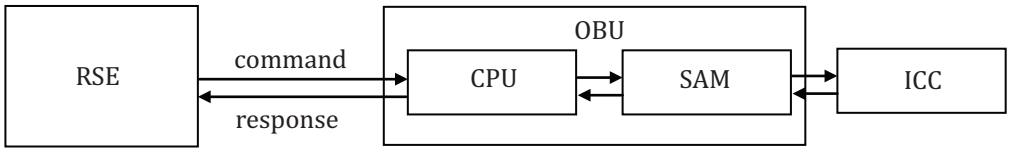


Figure 6 — Generic structure of caching type

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.

© ISO 2017 – All rights reserved

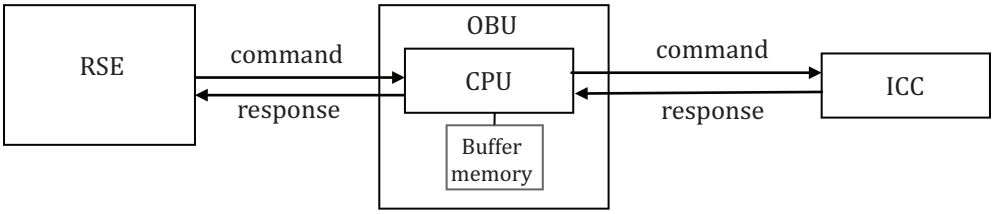
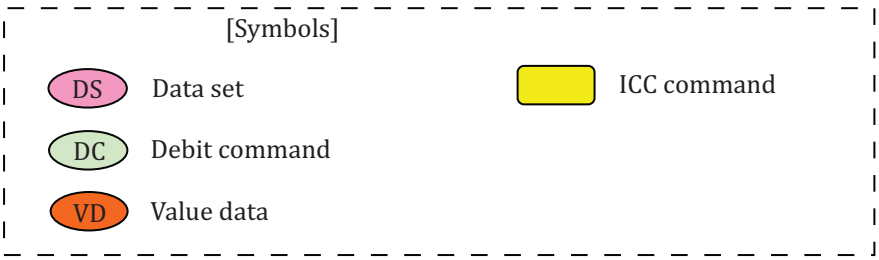


Figure 7 — Generic structure of buffering type

5.2 Symbols

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



iTeh STANDARD PREVIEW
(standards.iteh.ai)

Figure 8 — Definition of symbols

ISO 25110:2017
https://standards.iteh.ai/catalog/standards/sist/98e43d44-8f96-4807-a1f9-172d94a8d49f/iso-25110-2017

5.3 Transparent type

5.3.1 General

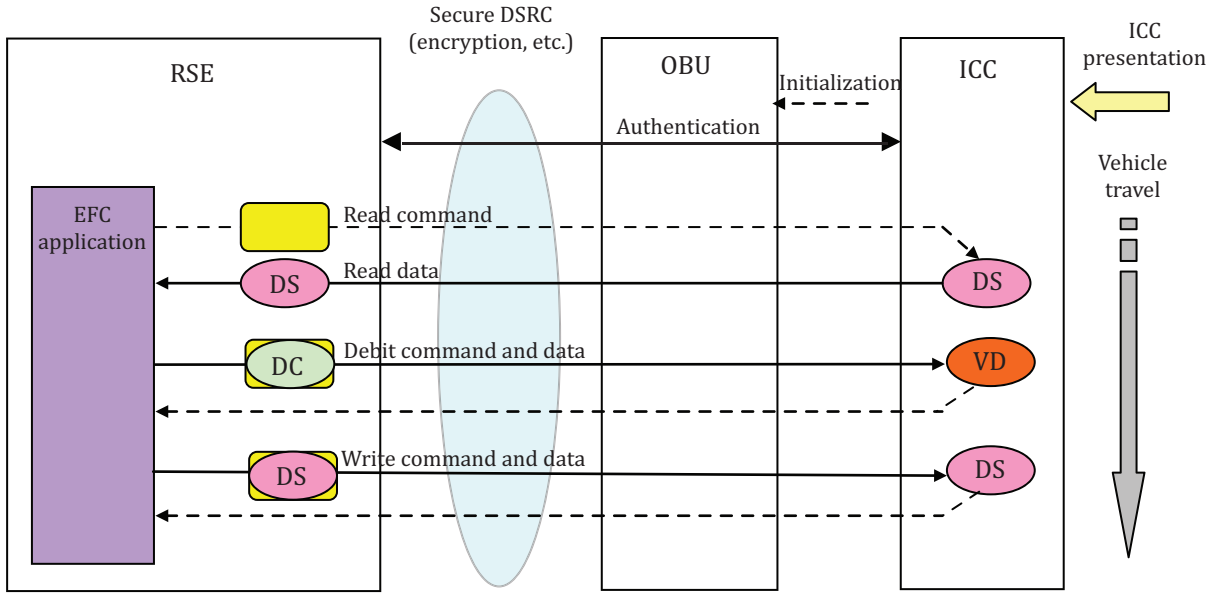
In this model, the maximum vehicle speed depends on the data transfer rate between the ICC and OBU so that the vehicle has to stop or go through slowly under an RSE antenna in case a conventional contact ICC is used. The feature of the transparent type is to make the OBU simple by eliminating the secure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

© ISO 2017 – All rights reserved



NOTE Debit command is used in case of prepaid payment.

Figure 9 — Data transfer process of transparent type

5.4 Caching type

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5.4.1 General

ISO 25110:2017
https://standards.iteh.ai/catalog/standards/sist/98e43d44-8f96-4807-a1f9-172d94a8d49f/iso-25110-2017

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.

© ISO 2017 – All rights reserved