TECHNICAL SPECIFICATION

ISO/TS 25110

First edition
2008-11-15

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 25110:2008(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 iv

0 Introduction v
0.1 Background and motivation v
0.2 Objective vi
0.3 Use vi

1 Scope 1

2 Normative references 2

3 Terms and definitions 2

4 Abbreviations 5

5 Data transfer model 6
5.1 Overview 6
5.2 Symbols 7
5.3 Transparent type 7
5.4 Caching type 8
5.5 Buffering type 9

6 Interface definition for ICC access 10
6.1 Transparent type 10
6.2 Caching type 11
6.3 Buffering type 13

Annex A (informative) On-board account requirements 15

Annex B (informative) Example of an ICC access method 18

Annex C (informative) Interoperability relation with other sectors 32

Bibliography 34

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*.

0 Introduction

0.1 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.

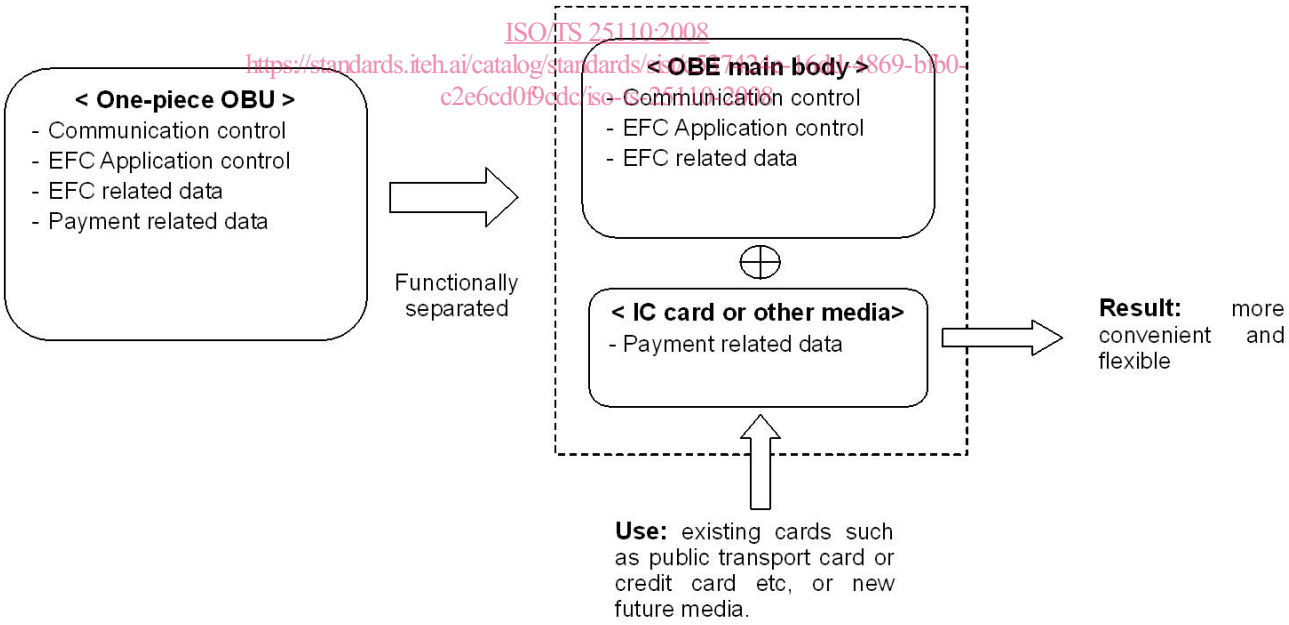

Figure 1 — Motivation for on-board account using ICC

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

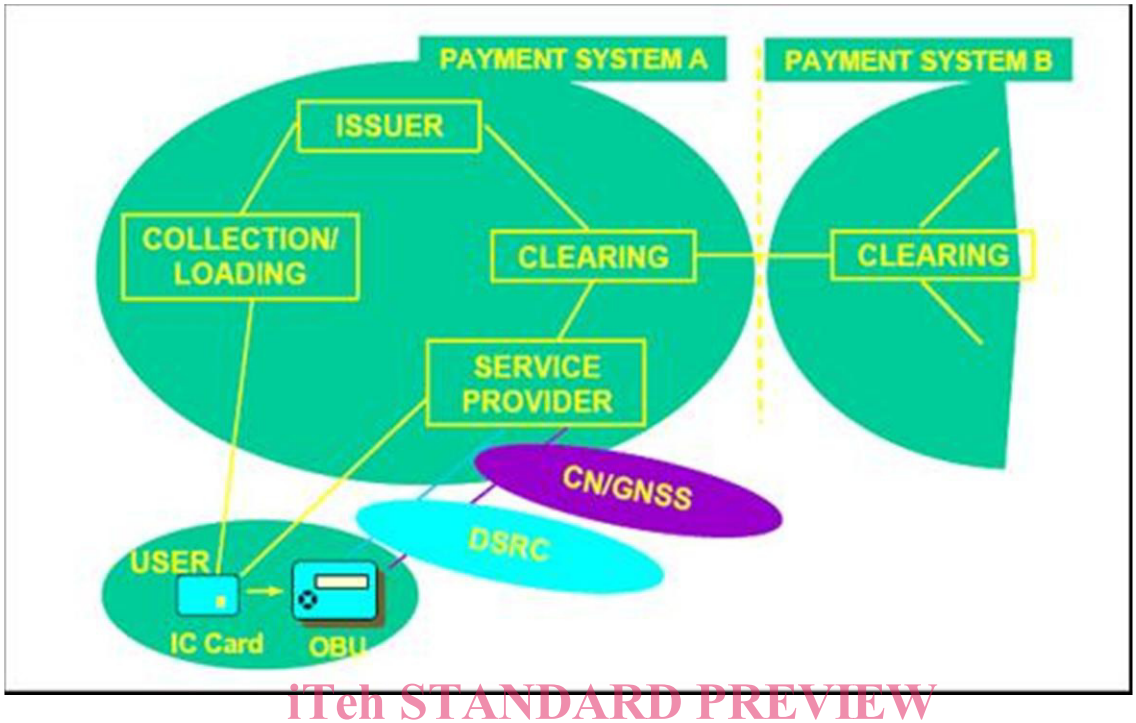

Figure 2 — Illustration of the scope of the EFC standards

0.2 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.

0.3 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 the standard (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 ICC, and the interface descriptions between RSE and 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 the standard. The descriptions in this Technical Specification focus on the interface between RSE and OBU to access ICC.

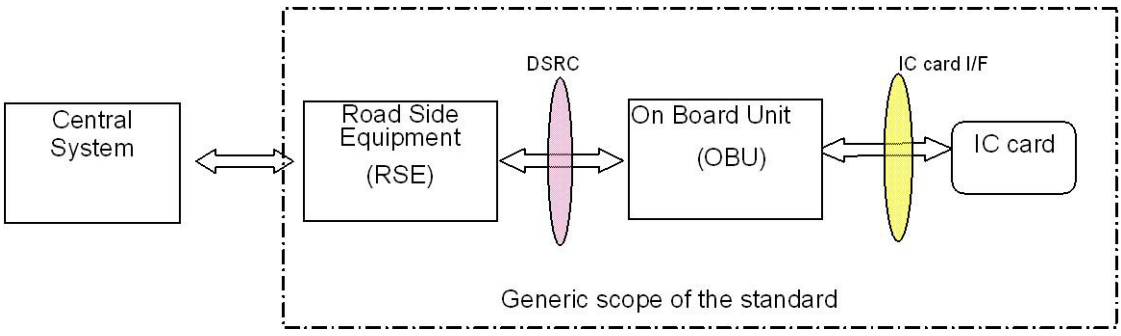

Figure 3 — Configuration of on-board account and generic scope of ISO/TS 25110

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 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 standard, whereas Bridge-2 corresponds to the cashing type.

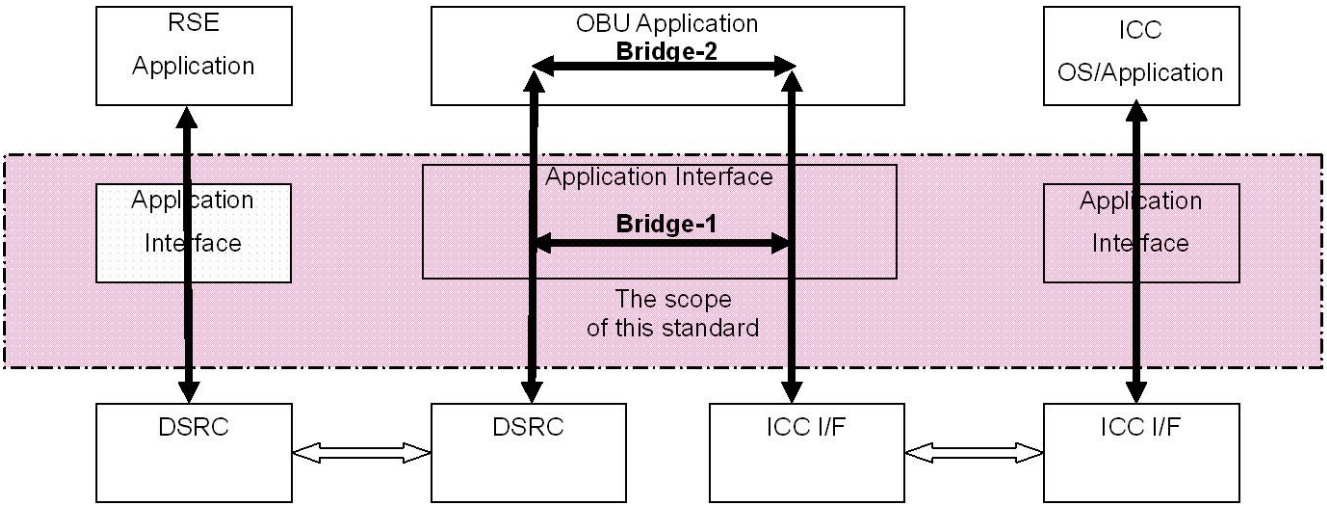

Figure 4 — Scope of ISO/TS 25110

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 14906:2004, *Road transport and traffic telematics — 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**, in order to establish the claimed identity of a roadside equipment (RSE) application process entity

[ISO 14906]

NOTE 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** execute a specific operation during the **transaction**

[ISO 14906]

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

[ISO 14906]

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]

3.5
channel
information transfer path

[ISO 14906]

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

[ISO 14906]

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

[ISO 14906]

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 14906]

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

[ISO 14906]

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

[ISO 14906]

3.11
element
in the context of DSRC, a directory containing application information in form of **attributes**

[ISO 14906]

3.12
on-board equipment
equipment located within the vehicle and supporting the information exchange with the **roadside equipment,** composed of the **on-board unit** and other sub-units whose presence have to be considered optional for the execution of a **transaction**

[ISO 14906]

3.13
on-board unit
minimum component of an **on-board equipment**, whose functionality always includes at least the support of the DSRC interface

[ISO 14906]

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

[ISO 14906]

3.15
service
⟨EFC⟩ road transport related facility provided by a **service provider**; normally a type of infrastructure, the use of which is offered to the **user** for which the **user** may be requested to pay

[ISO 14906]

3.16
service primitive
⟨communication⟩ elementary communication service provided by the application layer protocol to the application processes

[ISO 14906]

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

3.17
service provider
⟨EFC⟩ operator that accepts the user's payment means and in return provides a road-use service to the user

[ISO 14906]

3.18
session
exchange of information and interaction occurring at a specific EFC station between the **roadside equipment** and the user/vehicle

[ISO 14906]

3.19
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]

3.20
transaction model
functional model describing the general structure of electronic payment fee collection transactions

[ISO 14906]

3.21
user
entity that uses transport services provided by the **service provider** according to the terms of a **contract**

3.22
transport service provider
person, company, authority or abstract entity offering a transport service to the user for which the user has to pay a fee (the fee will in some cases be zero, e.g. emergency vehicles)

[ISO/TS 17573]

3.23
issuer
entity responsible for the payment system and responsible for issuing the payment means to the user

[ISO/TS 17573]

4 Abbreviations

For the purpose 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

OBU On-board Unit

RSE Roadside Equipment

SAM Secure Application Module

VST Vehicle Service Table

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

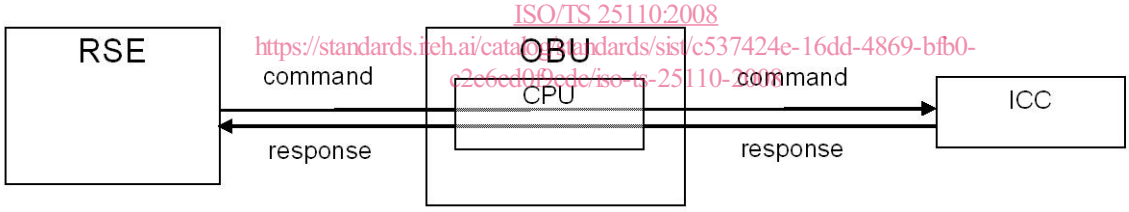

Figure 5 — Generic structure of transparent type

5.1.2 Caching type

The EFC related data is 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.

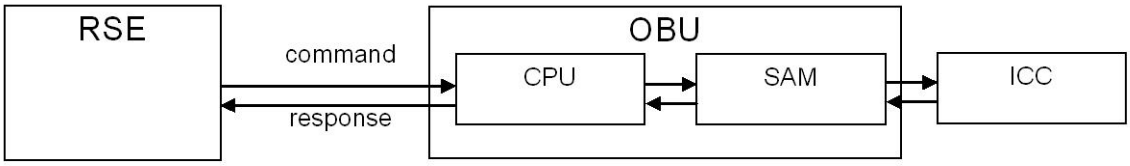

Figure 6 — Generic structure of caching type

5.1.3 Buffering type

The EFC related data which is limited to non-sensitive data is 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.

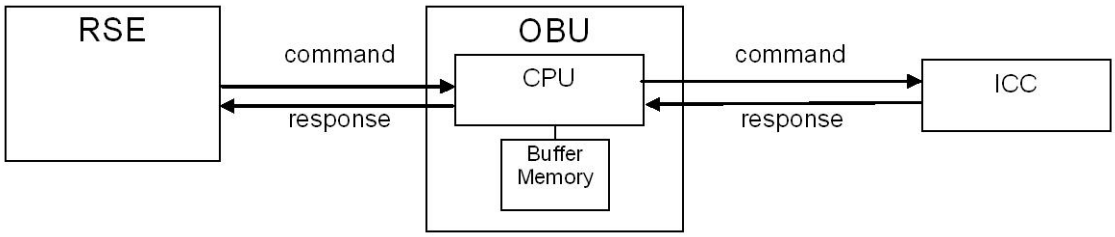

Figure 7 — Generic structure of buffering type

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 is exchanged and value data is 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 same procedure is processed, as shown in Figure 9.