

**DIN EN ISO 25110**

ICS 03.220.01; 35.240.60

**Entwurf**

Einsprüche bis 2017-05-03  
 Vorgesehen als Ersatz für  
 DIN CEN ISO/TS 25110  
 (DIN SPEC 70658):2013-09

**Elektronische Gebührenerhebung –  
 Schnittstellendefinition für die fahrzeugseitige bordeigene  
 Datenverwaltung mit Chipkarte (ICC) (ISO/DIS 25110:2017);  
 Englische Fassung prEN ISO 25110:2017**

Electronic fee collection –

Interface definition for on-board account using integrated circuit card (ICC)  
 (ISO/DIS 25110:2017);

English version prEN ISO 25110:2017

Perception du télépéage –

Définition d'interface pour compte de bord utilisant une carte à circuit intégré (ICC)  
 (ISO/DIS 25110:2017);

Version anglaise prEN ISO 25110:2017

**Anwendungswarnvermerk**

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-03-03 wird der Öffentlichkeit zur Prüfung und  
 Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs  
 besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter [www.din.de/go/entwuerfe](http://www.din.de/go/entwuerfe) bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter [www.entwuerfe.normenbibliothek.de](http://www.entwuerfe.normenbibliothek.de), sofern dort wiedergegeben;
- oder als Datei per E-Mail an [naautomobil@din.de](mailto:naautomobil@din.de) möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter [www.din.de/go/stellungnahmen-norm-entwuerfe](http://www.din.de/go/stellungnahmen-norm-entwuerfe) oder für Stellungnahmen zu Norm-Entwürfen der DKE unter [www.dke.de/stellungnahme](http://www.dke.de/stellungnahme) abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Automobiltechnik (NAAutomobil), 10004 Berlin, Postfach 8 04 62, Behrenstr. 35, 10117 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten  
 Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 49 Seiten

DIN-Normenausschuss Automobiltechnik (NAAutomobil)  
 DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

## **Nationales Vorwort**

Dieses Dokument (prEN ISO 25110:2017) wurde vom Technischen Komitee CEN/TC 278 „Intelligente Verkehrssysteme“, dessen Sekretariat vom NEN (Niederlande) gehalten wird in Zusammenarbeit mit dem Technischen Komitee ISO/TC 204 „Intelligent transport systems“ ausgearbeitet.

Das zuständige deutsche Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 052-02-71 GA „Intelligente Verkehrssysteme“ des Normenausschusses Automobiltechnik.

Der Entwurf ist derzeit zur parallelen Umfrage vorgelegt.

Diese Norm beschreibt Gebührenerhebungssysteme mit integrierten Chipkarten (ICC) als Erweiterung zu den bereits bestehenden Normen, welche sich ausschließlich mit zentralen Gebührenerhebungssystemen beschäftigen. Die Nutzung von integrierten Chipkarten ist gegenwärtig weit verbreitet. Ziel dieser Norm ist es eine Klassifizierung von Datentransfermodellen, basierend auf funktionsfähigen Anforderungen, sowie die Beschreibung einer spezifischen ICC-Zugriffsschnittstelle für fahrzeugseitige Konten. Außerdem beinhaltet diese Norm praktische Transaktionsbeispiele zur Berücksichtigung und einfache Anpassungen bei Straßenmaut Anbietern.

## **Änderungen**

Gegenüber DIN CEN ISO/TS 25110 (DIN SPEC 70658):2013-09 wurden folgende Änderungen vorgenommen:

- a) Überführung in eine Europäische Norm;
- b) Ergänzung, bzw. Harmonisierung von Begriffen im Umfeld der Standardisierung im Bereich Elektronische Gebührenerhebung;
- c) redaktionelle und formelle Anpassungen.

## Nationaler Anhang NA (informativ)

### Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe:

#### 3.1

##### **Zugriffsbeglaubigung**

(en: access credentials)

vertrauenswürdiger Nachweis oder Sicherheitsmodul, das die beanspruchte Identität eines Objekts oder einer Anwendung nachweist

[EN 15509:2014, Definition 3.1]

**ANMERKUNG** Zugriffsbeglaubigungen transportieren Informationen, welche die Zugriffsbedingungen regeln um die entsprechende Operation im adressierten Element in der OBE durchführen zu können. Diese Zugriffsbeglaubigungen können sowohl Passwörter als auch kryptografische Informationen wie Authentifikatoren enthalten.

#### 3.2

##### **Attribut**

(en: attribute)

adressierbares Datenpaket, welches aus einem einzelnen Datenelement oder einer strukturierten Sequenz von Datenelementen besteht

[ISO 17575-1:2016, Definition 3.2]

#### 3.3

##### **Authentifikator**

(en: authenticator)

Daten, wenn möglich verschlüsselt, die zur Authentifizierung verwendet werden

[EN 15509:2014, Definition 3.3]

#### 3.4

##### **Kanal**

(en: channel)

Informationsübertragungsweg

[ISO 7498-2:1989, Definition 3.3.13]

#### 3.5

##### **Kryptographie**

(en: cryptography)

Disziplin, welche Prinzipien, Absichten und Methoden zur Datentransformation umfasst, um den Dateninhalt zu verstecken bzw. unentdeckte Veränderungen und/oder unautorisierte Nutzung zu verhindern

[EN 15509:2014, Definition 3.6]

### 3.6

#### **Datengruppe**

(en: data group)

Klasse von verwandten Attributen

[ISO 17575-1:2016, Definition 3.10]

### 3.7

#### **Datenintegrität**

(en: data integrity)

Eigenschaft, dass Daten nicht in unautorisierter Art und Weise verändert oder vernichtet wurden

[ISO 7498-2:1989, Definition 3.3.21, und ISO 14906, Definition 3.10]

### 3.8

#### **Element**

(en: element)

<DRSC> Verzeichnis, welches Anwendungsinformation in Form von Attributen beinhaltet

[ISO 14906:2011, Definition 3.11]

### 3.9

#### **Aussteller**

(en: issuer)

Einrichtung, die für die Ausstellung der Bezahlungsmittel für den Nutzer verantwortlich ist

[ISO/TS 16785:2014, Definition 3.9]

### 3.10

#### **fahrzeuginterne Einrichtung**

##### **OBE**

(en: on-board equipment)

#### **fahrzeuginterne Einrichtung**

(en: on-board equipment)

alle erforderlichen Einrichtungen im Fahrzeug zur Durchführung notwendiger Funktionen der elektronischen Gebührenerhebung (EFC, en: electronic fee collection) und von Kommunikationsdiensten

### 3.11

#### **fahrzeuginterne Einheit**

(en: on-board unit)

einzelne elektronische fahrzeuginterne Einheit zur Durchführung spezifischer Funktionen zur elektronischen Gebührenerhebung und zur Kommunikation mit externen Systemen

### 3.12

#### **Straßenrand-Einrichtung**

(en: roadside equipment)

feste oder mobile Einrichtung entlang einer Straße

### 3.13

#### **Sicherheitsanwendungsmodul**

##### **SAM**

(en: secure application module)

physikalisches Modul, das in sicherer Art und Weise kryptografische Funktionen ausführt und Schlüssel speichert

[ISO/TS 19299:2015, Definition 3.35]

**3.14**

**Dienstelement**

**Service Primitive**

(en: service primitive)

<Kommunikation> elementarer Kommunikationsdienst welcher von Anwendungsprotokoll für den Anwendungsprozess zur Verfügung gestellt wird

[ISO 14906, Definition 3.18]

**3.15**

**Transaktion**

(en: transaction)

gesamter Austausch von Informationen zwischen zwei, physisch getrennten Kommunikationseinrichtungen

[ISO 17575-1:2016, Definition 3.21]

**3.16**

**Transaktionsmodell**

(en: transaction model)

funktionelles Modell, welches die generelle Struktur einer elektronischen Gebührenerhebungstransaktion beschreibt

[ISO 14906, Definition 3.25]

**3.17**

**Transportdienstanbieter**

(en: transport service provider)

Einrichtung, die einen transportrelevanten Dienst anbietet, wie z. B. die Bereitstellung von Straßen

— Leerseite —

| <b>Contents</b>                                                    | <b>Page</b> |
|--------------------------------------------------------------------|-------------|
| <b>Foreword .....</b>                                              | <b>5</b>    |
| <b>Introduction .....</b>                                          | <b>6</b>    |
| <b>1 Scope.....</b>                                                | <b>1</b>    |
| <b>2 Normative references .....</b>                                | <b>2</b>    |
| <b>3 Terms and definitions .....</b>                               | <b>2</b>    |
| <b>4 Abbreviations .....</b>                                       | <b>5</b>    |
| <b>5 Data transfer model.....</b>                                  | <b>5</b>    |
| <b>5.1 Overview .....</b>                                          | <b>5</b>    |
| <b>5.1.1 Transparent type .....</b>                                | <b>5</b>    |
| <b>5.1.2 Caching type .....</b>                                    | <b>6</b>    |
| <b>5.1.3 Buffering type .....</b>                                  | <b>6</b>    |
| <b>5.2 Symbols .....</b>                                           | <b>6</b>    |
| <b>5.3 Transparent type .....</b>                                  | <b>7</b>    |
| <b>5.3.1 General description .....</b>                             | <b>7</b>    |
| <b>5.3.2 Data transfer process.....</b>                            | <b>7</b>    |
| <b>5.4 Caching type .....</b>                                      | <b>8</b>    |
| <b>5.4.1 General description .....</b>                             | <b>8</b>    |
| <b>5.4.2 Data transfer process.....</b>                            | <b>8</b>    |
| <b>5.5 Buffering type .....</b>                                    | <b>9</b>    |
| <b>5.5.1 General description .....</b>                             | <b>9</b>    |
| <b>5.5.2 Data transfer process.....</b>                            | <b>9</b>    |
| <b>6 Interface definition for ICC access.....</b>                  | <b>9</b>    |
| <b>6.1 Transparent type .....</b>                                  | <b>9</b>    |
| <b>6.1.1 Functional configuration.....</b>                         | <b>9</b>    |
| <b>6.1.2 Command and response between RSE and OBU .....</b>        | <b>10</b>   |
| <b>6.2 Caching type .....</b>                                      | <b>11</b>   |
| <b>6.2.1 Functional configuration.....</b>                         | <b>11</b>   |
| <b>6.2.2 Command and response between RSE and OBU .....</b>        | <b>11</b>   |
| <b>6.3 Buffering type .....</b>                                    | <b>12</b>   |
| <b>6.3.1 Functional configuration.....</b>                         | <b>12</b>   |
| <b>6.3.2 Command and response between RSE and OBU .....</b>        | <b>12</b>   |
| <b>Annex A (informative) On-board account requirements .....</b>   | <b>14</b>   |
| <b>A.1 Operational requirements for on-board account .....</b>     | <b>14</b>   |
| <b>A.2 Type of ICC .....</b>                                       | <b>14</b>   |
| <b>A.3 Interoperability requirements for ICC.....</b>              | <b>15</b>   |
| <b>A.4 Performance of each transfer model .....</b>                | <b>15</b>   |
| <b>Annex B (informative) Example of an ICC access method .....</b> | <b>17</b>   |
| <b>B.1 Transparent type model.....</b>                             | <b>17</b>   |
| <b>B.1.1 Transparent type model-1 (for prepaid payment) .....</b>  | <b>17</b>   |
| <b>B.1.1.1 General .....</b>                                       | <b>17</b>   |
| <b>B.1.1.2 Data type definition .....</b>                          | <b>17</b>   |

|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| B.1.1.3 Transaction .....                                                   | 17 |
| B.1.1.3.1 ..... ETC Distance based charging (closed system) .....           | 17 |
| B.1.2 Transparent type model-2 (for post payment) .....                     | 20 |
| B.1.2.1 General.....                                                        | 21 |
| B.1.2.2 Data type definition .....                                          | 21 |
| B.1.2.3 Transaction .....                                                   | 22 |
| B.1.2.3.1 ..... Parking system .....                                        | 22 |
| B.2 Caching type model .....                                                | 25 |
| B.2.1 General.....                                                          | 25 |
| B.2.2 Data type definition .....                                            | 25 |
| B.2.3 Transaction example .....                                             | 27 |
| B.2.3.1 ETC flat rate charging (open system) and credit payment .....       | 27 |
| B.2.3.2 ETC distance rate charging (closed system) and credit payment ..... | 29 |
| B.3 Buffering type model .....                                              | 32 |
| B.3.1 General.....                                                          | 32 |
| B.3.2 RSE Command definition .....                                          | 32 |
| B.3.2.1 Debit command .....                                                 | 32 |
| B.3.3 Transaction .....                                                     | 32 |
| Annex C (informative) Interoperability relation with other sectors.....     | 34 |
| Bibliography .....                                                          | 36 |

## 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 25110 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

This edition cancels and replaces the second edition of ISO/TS 25110:2013. This edition incorporates the following main modifications compared to the Technical Specification

- conversion from a Technical Specification to an International Standard;
- amendment of terms, in order to reflect harmonization of terms across electronic fee collection (EFC) standards.

## Introduction

### Background and motivation

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

ICCs have been widely used for public transport cards such as subway and bus payment means, and electronic money cards for general purpose payments, as well as for credit cards and banking cards. 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.

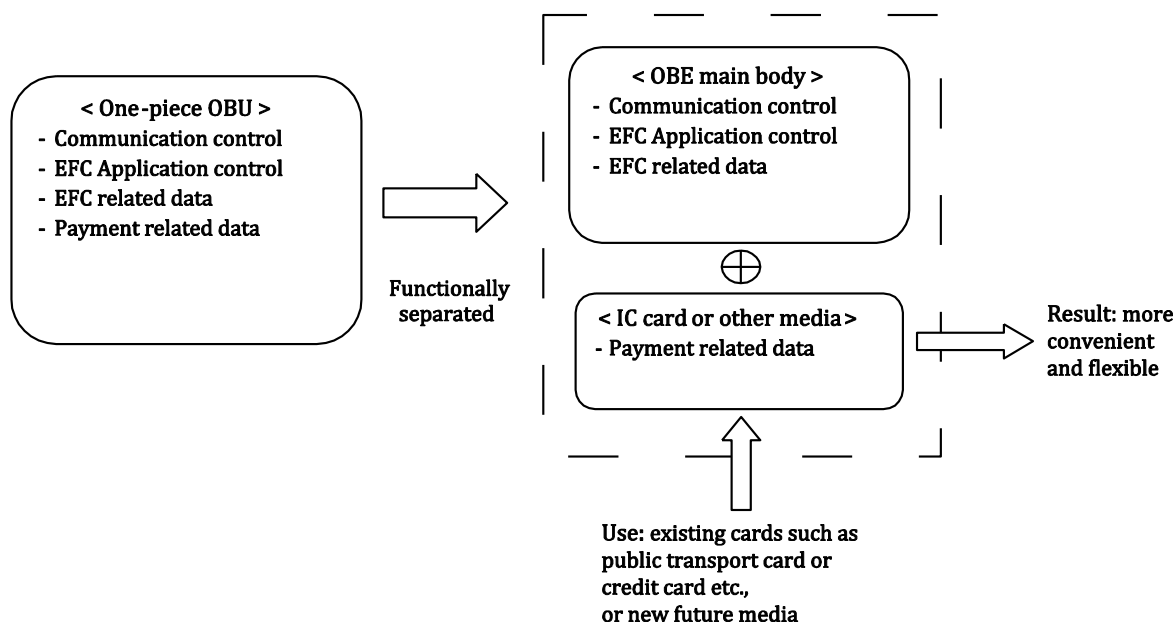


Figure 1 — Motivation for on-board account using ICC

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.

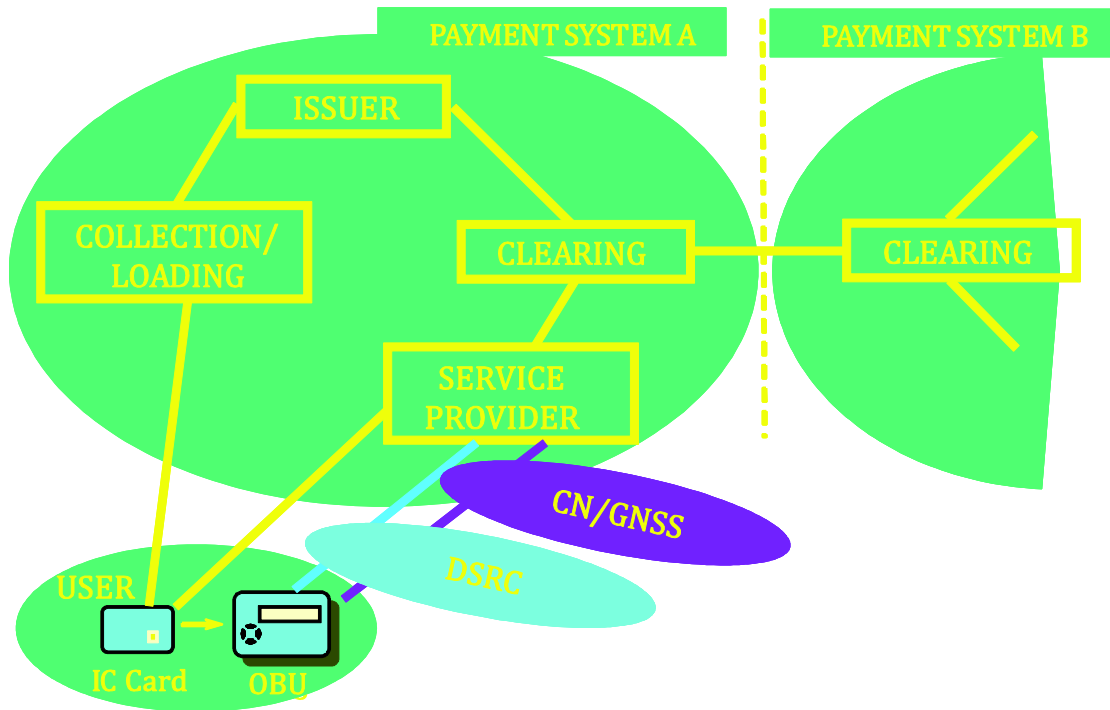


Figure 2 — Illustration of the scope of the EFC standards

### Objective

The objective of this document 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 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.

**- Entwurf -**

# 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 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 document 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 document. The descriptions in this document focus on the interface between RSE and OBU to access ICC.

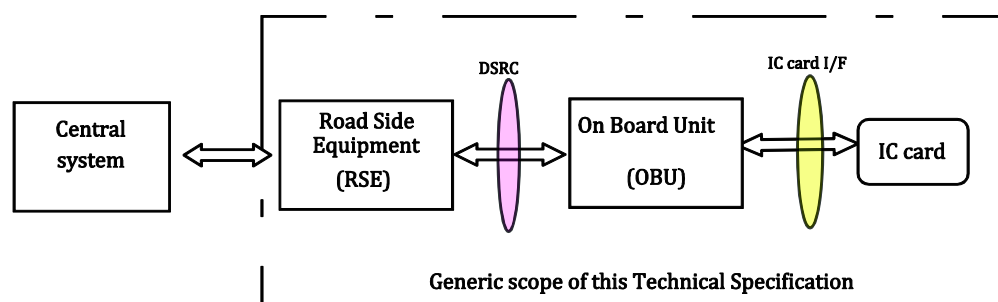


**Figure 3 — Configuration of on-board account and generic scope of ISO 25110**

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 document.

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 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 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 document, whereas Bridge-2 corresponds to the caching type.

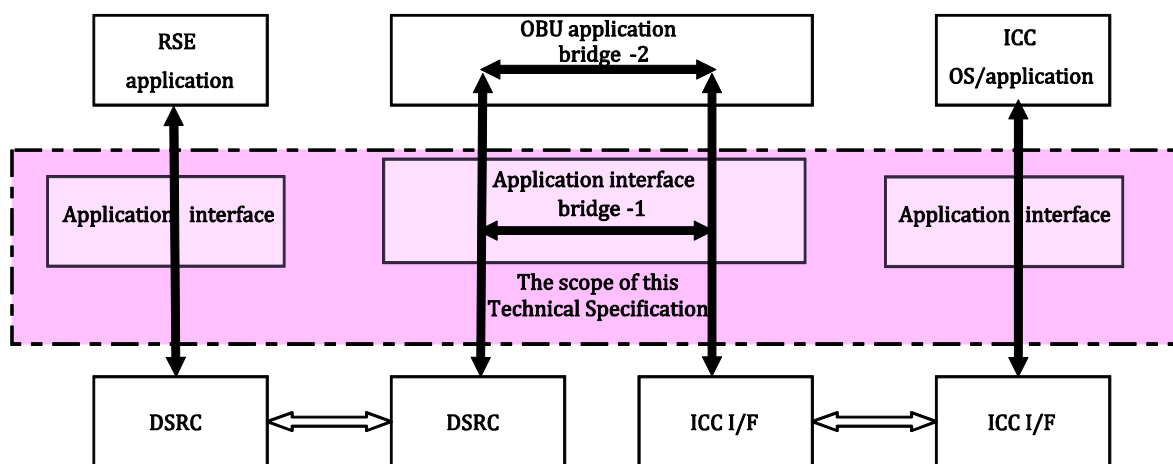


Figure 4 — Scope of ISO 25110

## 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, *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**

trusted attestation or secure module that establishes the claimed identity of an object or application

[EN 15509:2014, definition 3.1]

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

#### **attribute**

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

[ISO 17575-1:2016, definition 3.2]

### 3.3

#### **authenticator**

data, possibly encrypted, that is used for authentication

[EN 15509:2014, definition 3.3]

### 3.4

#### **channel**

information transfer path

[ISO 7498-2:1989, definition 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

[EN 15509:2014, definition 3.6]

### 3.6

#### **data group**

class of closely related attributes

[ISO 17575-1:2016, definition 3.10]

### 3.7

#### **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]

### 3.8

#### **Element**

DSRC directory containing application information in the form of attributes