
**Perception du télépéage —
Définition d'interface pour compte
de bord utilisant une carte à circuit
intégré (ICC)**

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

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



iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 25110:2017

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



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2017, Publié en Suisse

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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

Sommaire

Page

Avant-propos	iv
Introduction	v
1 Domaine d'application	1
2 Références normatives	2
3 Termes et définitions	2
4 Abréviations	4
5 Modèles de transfert de données	5
5.1 Généralités.....	5
5.1.1 Type transparent.....	5
5.1.2 Type «mise en mémoire cache».....	5
5.1.3 Type «mise en mémoire tampon».....	5
5.2 Symboles.....	5
5.3 Type transparent.....	6
5.3.1 Généralité.....	6
5.3.2 Processus de transfert de données.....	6
5.4 Type «mise en mémoire cache».....	7
5.4.1 Généralité.....	7
5.4.2 Processus de transfert de données.....	7
5.5 Type «mise en mémoire tampon».....	7
5.5.1 Généralité.....	7
5.5.2 Processus de transfert de données.....	8
6 Définition d'interface pour l'accès à l'ICC	8
6.1 Type transparent.....	8
6.1.1 Configuration fonctionnelle.....	8
6.1.2 Commande et réponse entre le RSE et l'OBU.....	9
6.2 Type «mise en mémoire cache».....	9
6.2.1 Configuration fonctionnelle.....	9
6.2.2 Commande et réponse entre le RSE et l'OBU.....	10
6.3 Type «mise en mémoire tampon».....	10
6.3.1 Configuration fonctionnelle.....	10
6.3.2 Commande et réponse entre le RSE et l'OBU.....	11
Annexe A (informative) Exigences relatives au compte de bord	12
Annexe B (informative) Exemple de méthode d'accès à l'ICC	15
Annexe C (informative) Relations d'interopérabilité avec les autres secteurs	32
Bibliographie	34

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/avant-propos.

La norme ISO 25110 a été élaborée par le Comité technique ISO/TC 204, *Systèmes intelligents de transport*.

La présente édition annule et remplace la deuxième édition de l'ISO/TS 25110:2013. Cette édition inclut les principales modifications suivantes, par rapport à la Spécification technique:

- passage d'une Spécification technique au stade de Norme internationale;
- modifications des termes qui traduisent l'harmonisation terminologique des normes relatives à la perception du télépéage (EFC).

Introduction

Contexte et motifs

Il existe deux systèmes de paiement dédiés à la perception du télépéage (EFC). Le premier est un compte centralisé s'appuyant sur une unité embarquée (OBU) monobloc, tandis que le second est un compte de bord employant un moyen de paiement tel qu'une carte à circuit intégré (ICC).

Les ICC sont largement utilisés dans le domaine des transports en commun, en tant que moyens de paiement pour les services de métro et de bus, mais également en tant que cartes monétiques pour les paiements courants, ou en tant que cartes de crédit ou cartes bancaires. L'utilisation des ICC est envisagée en tant que moyen de paiement EFC, en accord avec ces tendances mondiales et dans une optique de commodité et de flexibilité.

Actuellement, les descriptions exposées dans les normes internationales relatives à la perception du télépéage (EFC) sont axées sur le compte centralisé, un système relativement simple permettant une meilleure interopérabilité en matière de télépéage que le compte de bord, système plus complexe exigeant la gestion d'un plus grand nombre d'éléments.

Face à la généralisation des cartes de transport ou des cartes monétiques, une nouvelle Norme internationale traitant du système de compte de bord utilisant ces ICC représente une véritable nécessité, comme l'illustre la [Figure 1](#). En outre, les téléphones mobiles modernes dotés de fonctionnalités ICC, pouvant être désignés sous l'appellation « porte-monnaie électroniques mobiles », sont utilisés dans certains pays en tant que moyens de paiement dans les transports en commun ou dans le domaine de la vente au détail et cet usage se répand si rapidement qu'une normalisation sur ce thème est essentielle afin de prendre également en considération les futurs moyens de paiement EFC.

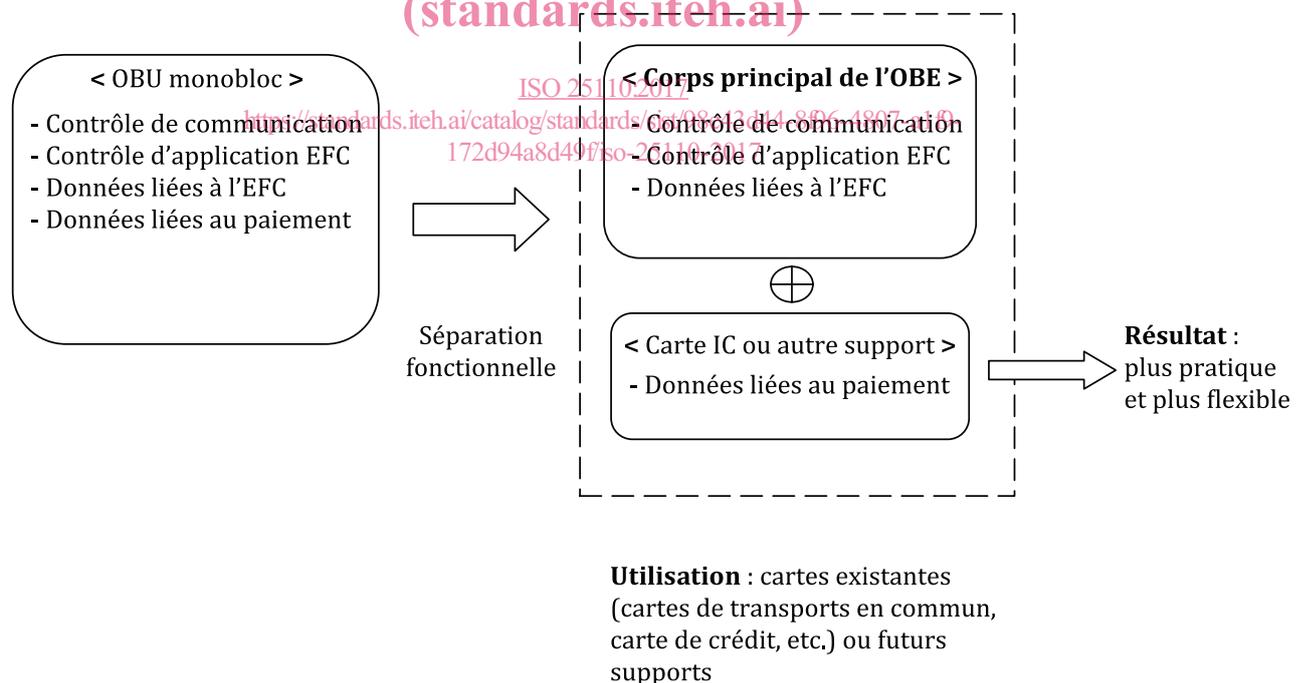


Figure 1 — Motivation en faveur d'un compte de bord s'appuyant sur une carte ICC

La [Figure 2](#) présente le domaine d'application des normes EFC, dans lequel l'OBU est utilisé comme moyen de communication et l'ICC sert de support au moyen de paiement.

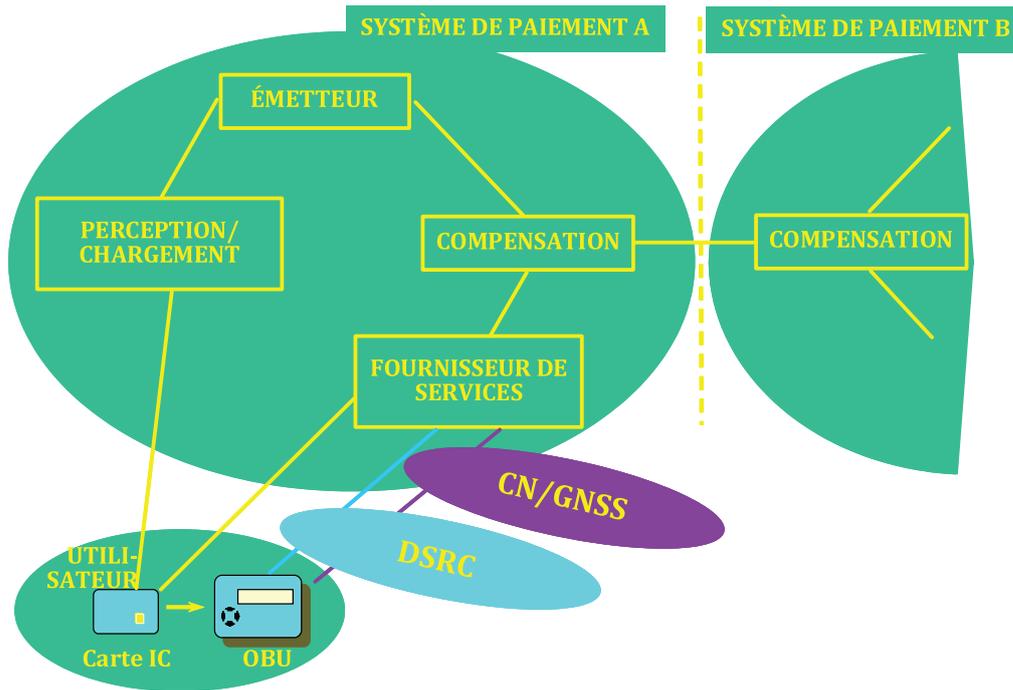


Figure 2 — Illustration du domaine d'application des normes EFC

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Objectif

Ce document a pour objectif de classer les modèles de transfert de données en fonction des exigences opérationnelles, et de définir une interface d'accès à l'ICC spécifique aux comptes de bord utilisant une carte ICC pour chaque modèle. En outre, ce document fournit des exemples pratiques de transactions en [Annexe B](#), à l'attention des opérateurs de routes à péage, permettant d'en faciliter l'adoption.

Usage

Ce document fournit une plateforme technique commune pour les comptes de bord s'appuyant sur des ICC pour répondre à diverses exigences opérationnelles ainsi que des exemples pratiques de comptes de bord en exploitation ou prévus dans plusieurs pays.

Chaque opérateur de route à péage peut établir ses propres spécifications en sélectionnant un modèle parmi les exemples présentés dans ce document (de manière semblable à une boîte à outils) afin de satisfaire ses exigences.

Perception du télépéage — Définition d'interface pour compte de bord utilisant une carte à circuit intégré (ICC)

1 Domaine d'application

Le présent document définit les modèles de transfert de données entre les équipements routiers (RSE) et les cartes à circuit intégré (ICC), et décrit les interfaces entre les RSE et l'équipement embarqué (OBE) pour le compte de bord s'appuyant sur l'ICC. Il fournit également des exemples de définitions d'interfaces et de transactions déployées dans plusieurs pays.

Ce document couvre les aspects suivants:

- modèles de transfert de données entre les RSE et les ICC correspondant aux exigences opérationnelles catégorisées, et le mécanisme de transfert des données pour chaque modèle,
- définition d'interface entre RSE et OBE en fonction de chaque modèle de transfert de données,
- définition d'interface pour chaque modèle,
- configuration fonctionnelle,
- définition des commandes RSE pour l'accès à l'ICC,
- format des données et définition des éléments de données pour les commandes RSE, et
- un exemple de transaction pour chaque modèle en [Annexe B](#).

La [Figure 3](#) présente la configuration du compte de bord et le domaine d'application de ce document. Les descriptions exposées dans ce document sont axées sur l'interface entre les RSE et les OBU pour l'accès à l'ICC.

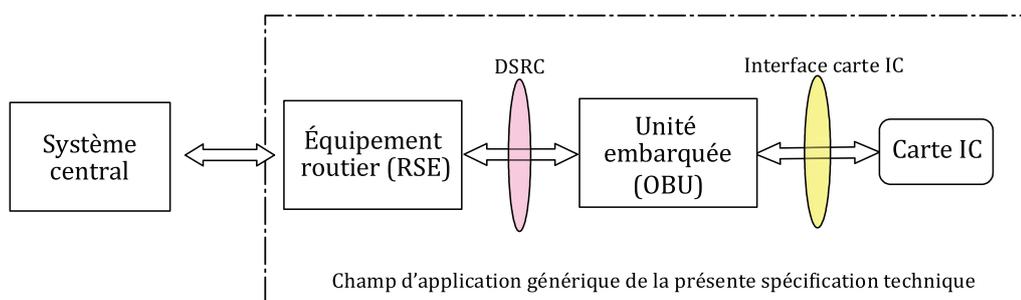


Figure 3 — Configuration du compte de bord et domaine d'application général de l'ISO 25110

La [Figure 4](#) présente la structure en couches des RSE, OBU et ICC, dans laquelle la couche intermédiaire des interfaces d'applications représente le domaine d'application pratique de ce document.

NOTE Les normes existantes applicables aux couches physiques et autres couches de protocoles, à la fois entre RSE et OBE et entre OBE et ICC, n'entrent pas dans le domaine d'application de ce document. Par exemple, les éléments relatifs à la communication dédiée à courte portée (DSRC) (L-1, L-2, et L-7) et les éléments relatifs à l'ICC (commandes ICC, définition des données, etc.) n'entrent pas dans le domaine d'application de ce document.

Un OBU contient deux types de ponts virtuels. Le premier type est Bridge-1 sur lequel une commande RSE envoyée depuis le RSE est décomposée et la commande d'accès ICC contenue dans une unité de données de protocole d'application (APDU) faisant partie de la commande RSE est transférée à l'interface de l'ICC en vue d'accéder à l'ICC. Le second type est Bridge-2 sur lequel une commande RSE

envoyée depuis le RSU est convertie en commande d'accès ICC et transférée à l'interface de l'ICC en vue d'accéder à l'ICC.

Bridge-1 correspond au type transparent et au type «mise en mémoire tampon» défini dans le présent document, tandis que Bridge-2 correspond au type «mise en mémoire cache».

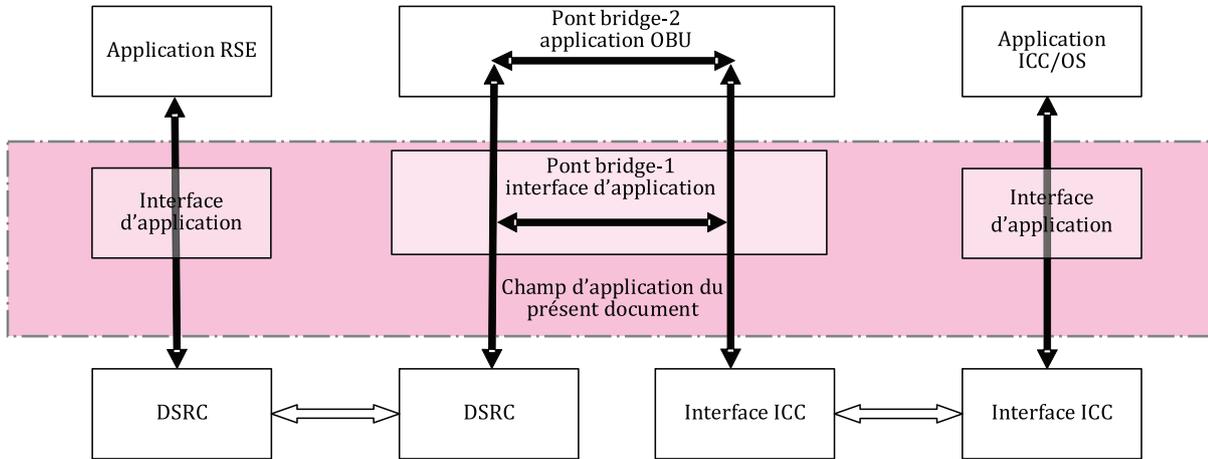


Figure 4 — Domaine d'application de l'ISO 25110

2 Références normatives

Les documents suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 14906, Perception du télépéage — Définition de l'interface d'application relative aux communications dédiées à courte portée

ISO 15628, Systèmes de transport intelligents — Communication dédiée à courte portée (DSRC) — Couches d'applications DSRC

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1 droits d'accès

attestation de confiance ou module sécurisé qui établit l'identité revendiquée d'un objet ou d'une application

[SOURCE: EN 15509:2014, 3.1]

Note 1 à l'article: Les justificatifs d'accès comportent les informations nécessaires pour satisfaire aux conditions d'accès afin d'exécuter l'opération sur l'élément adressé dans l'OBE. Les justificatifs d'accès peuvent comporter des mots de passe ainsi que des informations cryptographiques, par exemple des authentifiants.

3.2 attribut

information d'application constituée d'un élément de données ou d'une séquence structurée de tels éléments

[SOURCE: ISO 17575-1:2016, 3.2]

3.3**authentifiant**

Des données, possiblement cryptées, qui sont utilisées pour l'authentification

[SOURCE: EN 15509:2014, définition 3.3]

3.4**canal chemin de transfert de l'information**

[SOURCE: ISO 74982:1989, 3.3.13]

3.5**cryptographie**

principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée

[SOURCE: EN 15509:2014, 3.6]

3.6**groupe de données**

collection d'attributs étroitement liés (3.2)

[SOURCE: ISO 17575-1:2016, 3.10]

3.7**intégrité des données**

propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée

[SOURCE: ISO 14906:2011, 3.10-modifié]

3.8**élément**

Répertoire <DSRC> contenant des informations d'application sous la forme d'attributs (3.2)

[SOURCE: ISO 14906:2011, 3.11]

3.9**émetteur**

entité chargée de délivrer le moyen de paiement à l'utilisateur

[SOURCE: ISO/TS 16785:2014, 3.9]

3.10**équipement embarqué****OBE**

tous les équipements nécessaires à bord d'un véhicule pour effectuer les fonctions et les services de communication nécessaires pour le télépéage

3.11**unité embarquée**

unité électronique unique à bord d'un véhicule pour effectuer des fonctions spécifiques de télépéage et pour la communication avec des systèmes externes

3.12**équipement en bord de route**

équipement fixe ou mobile installé le long de la route

3.13**module d'application sécurisé****SAM**

module physique qui exécute en toute sécurité des fonctions cryptographiques, et stocke les clés

[SOURCE: ISO/TS 19299:2015, 3.35]

3.14

primitive de service

<communication> service de communication élémentaire fourni par le protocole de la couche application aux processus d'application

[SOURCE: ISO 14906:2011,3.18]

3.15

transaction

ensemble de l'échange d'informations entre deux moyens de communication physiquement séparés

[SOURCE: ISO 17575-1:2016, 3.21]

3.16

modèle de transaction

modèle fonctionnel décrivant la structure générale des transactions de collecte de péage par paiement électronique

[SOURCE: ISO 14906:2011, 3.25]

3.17

fournisseur de service de transport

entité fournissant un service lié au transport tels que les liaisons routières

4 Abréviations

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Pour les besoins du présent document, les abréviations suivantes s'appliquent à l'ensemble du document, sauf mention contraire.

AID	Application Identifier (identifiant d'application) https://standards.iteh.ai/catalog/standards/sist/98e43d44-896-4807-a19-11d4-455c30880193
APDU	Application Protocol Data Unit (unité de données de protocole d'application)
ASN.1	Abstract Syntax Notation One (notation de syntaxe abstraite un) (voir ISO/IEC 88241)
ATR	Answer to Reset (réponse à la réinitialisation)
ATS	Answer to Select (réponse à la sélection)
BST	Beacon Service Table (tableau de service de balises)
DSRC	Dedicated Short-Range Communications (communications dédiées à courte portée)
EAL	Evaluation Assurance Level (niveau d'assurance d'évaluation)
EFC	Electronic Fee Collection (perception du télépéage)
EID	Element Identifier (identifiant d'élément)
ERP	Electronic Road Pricing (tarification électronique)
EVENT-RT	Rapport EVENT (voir ISO 15628)
MAC	Medium Access Control (contrôle d'accès au support)
ICC	Integrated Circuit(s) Card (carte à circuit(s) intégré(s))
IFMS	Interoperable Fare Management System (système de gestion tarifaire interopérable)
OBE	On-Board Equipment (équipement embarqué)

5 Modèles de transfert de données

5.1 Généralités

Trois types de modèles de transfert de données existent pour le compte de bord s'appuyant sur une ICC pour répondre aux exigences opérationnelles décrites à l'[Annexe A](#).

5.1.1 Type transparent

Les données de la commande ICC sont transférées directement du RSE à l'ICC via l'OBU. L'OBU stocke temporairement les données de la commande ICC et les données de réponse dans la mémoire tampon. Voir la [Figure 5](#).

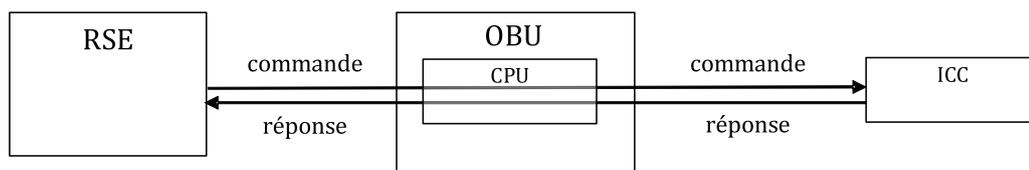


Figure 5 — Structure générique du type transparent

5.1.2 Type «mise en mémoire cache»

Les données EFC sont lues depuis l'ICC lors de la présentation et stockées dans le SAM de l'OBU. Lors de la communication DSRC, les données EFC présentes dans le SAM sont transférées au RSE. Voir la [Figure 6](#).

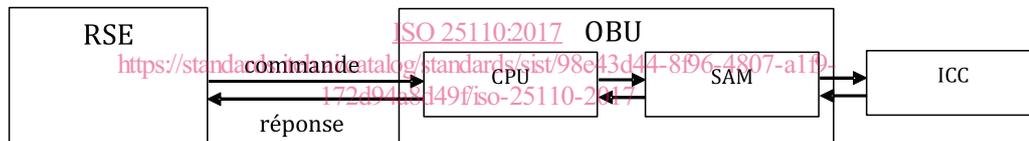


Figure 6 — Structure générique du type «mise en mémoire cache»

5.1.3 Type «mise en mémoire tampon»

Les données EFC non sensibles sont lues depuis l'ICC lors de la présentation et stockées en mémoire tampon dans l'OBU. Lors de la communication DSRC, les données EFC présentes en mémoire tampon sont transférées au RSE. Voir la [Figure 7](#).

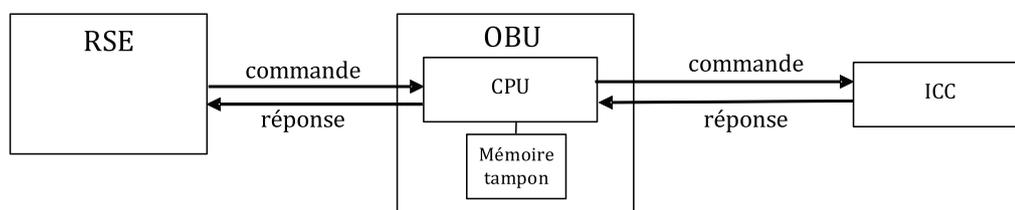


Figure 7 — Structure générique du type «mise en mémoire tampon»

5.2 Symboles

Les symboles représentés à la [Figure 8](#) sont utilisés dans le mécanisme de transfert des données de chaque modèle.

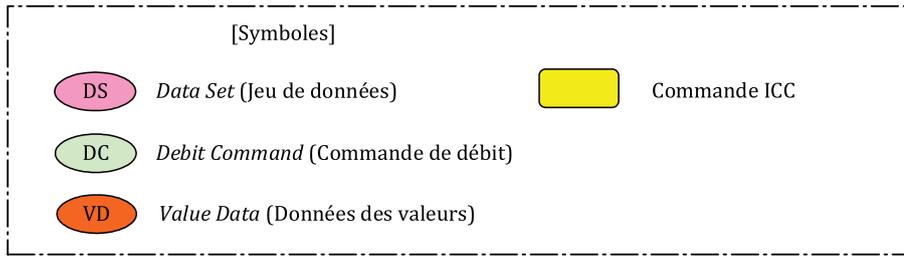


Figure 8 — Définition des symboles

5.3 Type transparent

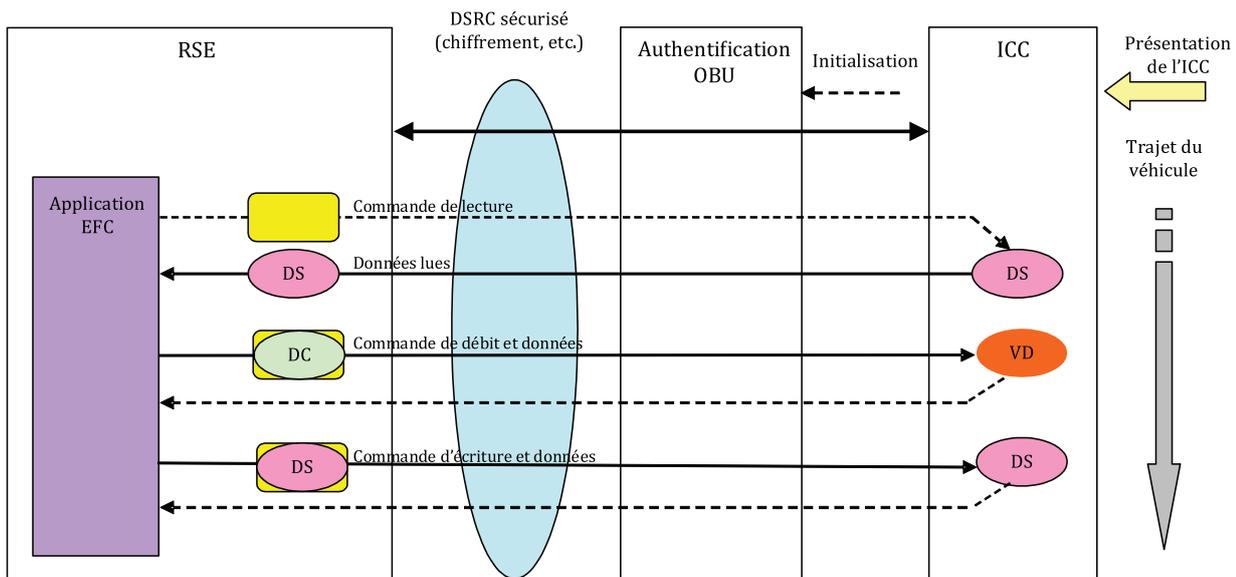
5.3.1 Généralité

Dans ce modèle, la vitesse maximale du véhicule dépend du débit de transfert des données entre l'ICC et l'OBU. Ainsi, le véhicule doit s'arrêter ou avancer au pas sous une antenne RSE lorsqu'un contact ICC conventionnel est utilisé. Le type transparent consiste à simplifier l'OBU en éliminant la mémoire sécurisée contenue dans ce dernier. Les performances seront ainsi améliorées en fonction du développement de l'ICC grâce à un haut débit de données.

5.3.2 Processus de transfert de données

Dans ce modèle, les échanges de données entre RSE et ICC sont traités directement après avoir établi la communication DSRC et une fois l'authentification entre le RSE et l'OBU réalisée. L'authentification mutuelle entre l'ICC et le RSE est traitée directement avant l'échange des données d'application et l'accès aux données des valeurs.

Dans la séquence de lecture, la commande READ est envoyée par le RSE à l'ICC via l'OBU pour lire le jeu de données stocké dans l'ICC. Dans la réponse à la commande READ, les données stockées dans l'ICC sont transférées de l'ICC au RSE via l'OBU. Cette même procédure est suivie dans la séquence d'écriture. Lors d'un paiement prépayé, la commande de débit est envoyée par le RSE et cette même procédure est suivie, comme l'illustre la Figure 9.



NOTE Dans le cas d'un paiement prépayé, la commande de débit est utilisée.

Figure 9 — Processus de transfert de données du type transparent

5.4 Type «mise en mémoire cache»

5.4.1 Généralité

Dans ce modèle, l'OBU lit les jeux de données sur l'ICC et les stocke en mémoire sécurisée à l'intérieur de l'OBU, lors de l'insertion et de la réalisation de l'authentification. Ce type permet un haut débit d'échange de données entre le RSE et l'OBU, même lorsque l'on emploie une ICC caractérisée par un bas débit de données. Avec ce type «mise en mémoire cache», la vitesse maximale du véhicule est revue à la hausse, à concurrence des performances de la communication DSRC, quel que soit le débit de transfert des données de l'ICC.

5.4.2 Processus de transfert de données

Dans ce modèle, les données lues à partir de l'ICC sont stockées en mémoire sécurisée telle que le SAM à l'intérieur de l'OBU afin de garantir la sécurité des informations.

Ce type permet de satisfaire les exigences de vitesse élevée du véhicule en traitant un haut débit d'échange de données entre le RSE et l'OBU quel que soit le type d'ICC. Voir la [Figure 10](#).

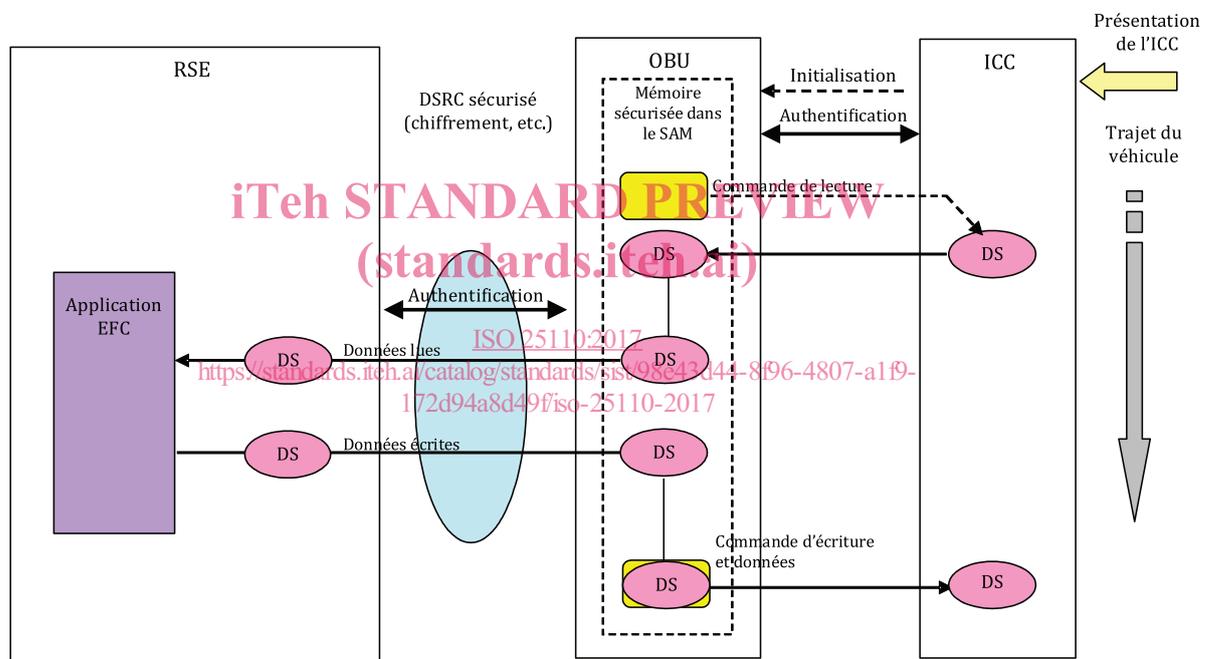


Figure 10 — Processus de transfert de données du type «mise en mémoire cache»

5.5 Type «mise en mémoire tampon»

5.5.1 Généralité

Ce type «mise en mémoire tampon» reprend les fonctionnalités du type transparent et du type «mise en mémoire cache». Toutefois, les jeux de données stockés dans l'ICC sont limités aux données non sensibles qui ne doivent pas être falsifiées ou divulguées. Dans ce type «mise en mémoire tampon», les données sont transférées selon la même méthode que pour le type «mise en mémoire cache», et les jeux de données de l'ICC sont lus et stockés en mémoire tampon à l'intérieur de l'OBU lorsque l'ICC est insérée dans l'OBU. Les jeux de données stockés en mémoire tampon sont transférés au RSE lors de la séquence de lecture DSRC. Lors d'une écriture, les jeux de données du RSE sont transférés à l'OBU et stockés dans la mémoire tampon de l'OBU puis transférés à l'ICC.