NORME INTERNATIONALE

ISO 14906

Troisième édition
2018-10

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

Electronic fee collection — Application interface definition for dedicated short-range communication

Numéro de référence
ISO 14906:2018(F)

© ISO 2018



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2018

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, 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, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **v**

Introduction ..... **vi**

1 Domaine d'application **1**

2 Références normatives **2**

3 Termes et définitions **2**

4 Abréviations **4**

5 Architecture d'interface d'application EFC **5**
5.1 Relation avec l'architecture de communication de DSRC 5
5.2 Utilisation de la couche application de DSRC par l'interface d'application de l'EFC 7
5.3 Adressage des attributs d'EFC 7
5.3.1 Mécanisme de base 7
5.3.2 Rôle de l'EID 8
5.3.3 Instances multiples d'attributs 8
5.4 Adressage des composants 9

6 Modèle de transaction d'EFC **10**
6.1 Généralités 10
6.2 Phase d'initialisation 10
6.2.1 Vue d'ensemble 10
6.2.2 Contenu du BST spécifique à une application d'EFC 11
6.2.3 Contenu du VST spécifique à une application d'EFC 12
6.3 Phase de transaction 13

7 Fonctions d'EFC **15**
7.1 Vue d'ensemble et concepts généraux 15
7.1.1 Fonctions d'EFC et primitives de service 15
7.1.2 Vue d'ensemble des fonctions d'EFC 16
7.1.3 Traitement d'instances multiples 17
7.1.4 Sécurité 18
7.2 Fonctions d'EFC 22
7.2.1 Généralités 22
7.2.2 GET_STAMPED 22
7.2.3 SET_STAMPED 23
7.2.4 GET_SECURE 23
7.2.5 SET_SECURE 24
7.2.6 GET_INSTANCE 25
7.2.7 SET_INSTANCE 26
7.2.8 GET_NONCE 26
7.2.9 SET_NONCE 27
7.2.10 TRANSFER_CHANNEL 28
7.2.11 COPY 29
7.2.12 SET_MMI 29
7.2.13 SUBTRACT 30
7.2.14 ADD 31
7.2.15 DEBIT 31
7.2.16 CREDIT 32
7.2.17 ECHO 33

8 Attributs d'EFC **34**
8.1 Généralités 34
8.2 Groupe de données CONTRACT 35
8.3 Groupe de données RECEIPT 38
8.4 Groupe de données VEHICLE 44
8.5 Groupe de données EQUIPMENT 51

© ISO 2018 – Tous droits réservés

8.6 Groupe de données DRIVER 53
8.7 Groupe de données PAYMENT 55
Annexe A (normative) **Spécifications de type de données d'EFC** **57**
Annexe B (informative) **Transaction CARDME** **58**
Annexe C (informative) **Exemples de types de transaction EFC** **90**
Annexe D (normative) **Tableau de mappage de LatinAlphabetNo2 et 5 à LatinAlphabetNo1** **101**
Annexe E (informative) **Tableau de mappage entre l'attribut Vehicledata d'EFC et le certificat d'immatriculation européen** **102**
Annexe F (normative) **Calculs de sécurité pour DES** **105**
Annexe G (informative) **Exemples de calculs de sécurité pour DES** **110**
Annexe H (normative) **Calculs de sécurité pour AES** **113**
Annexe I (informative) **Exemples de calculs de sécurité pour AES** **118**
Bibliographie **120**

 © ISO 2018 – Tous droits réservés

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/iso/fr/avant-propos.

La norme ISO 14906 a été élaborée par le Comité technique ISO/TC 204, *Systèmes de transport intelligent.*

Cette troisième édition annule et remplace la deuxième édition (ISO 14906:2011), qui a fait l'objet d'une révision technique. Elle prend en compte les rectificatifs ISO 14906:2011/Cor 1:2013 et l'amendement ISO 14906:2011/Amd 1:2015.

Les principaux changements par rapport à l'édition précédente sont les suivants:

— Prise en compte des calculs de sécurité conformément à la norme de chiffrement avancé, comme recommandé dans la norme CEN/TR 16968 sur les mécanismes de sécurité (révision de l'Article 7 et nouvelles Annexes F, G, H et I);

— Mise à jour des articles références normatives, termes et définitions, abréviations et de la Bibliographie;

— Conversion du module ASN.1 en insert électronique;

— Révision de l'Annexe C;

— Suppression de l'Annexe D (informative) sur les exignces fonctionnelles.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

© ISO 2018 – Tous droits réservés

Introduction

Le présent document spécifie une interface d'application relative aux installations de perception du télépéage (EFC) reposant sur des systèmes de communication dédiés à courte portée (DSRC). Il permet l'interopérabilité entre installations EFC à un niveau donné d'interface d'application EFC-DSRC. Ce document est destiné aux applications de facturation par DSRC, mais de façon spécifique la validité de la définition des éléments de données EFC dépasse l'utilisation d'une interface de facturation par DSRC et peut être utilisée pour d'autres applications de DSRC (par exemple une communication de contrôle de conformité) et/ou sur d'autres interfaces (par exemple l'interface d'application de systèmes autonomes).

Le présent document définit les spécifications du modèle de transaction EFC, des éléments de données EFC (appelés attributs) ainsi que des fonctions EFC sur lesquels peut se construire une transaction EFC. Le modèle de transaction EFC fournit un mécanisme qui permet de traiter différentes versions de transactions EFC ainsi que les contrats associés. Une transaction EFC donnée comporte un certain nombre des attributs et des fonctions EFC qui sont définis dans le présent document. Il n'est pas envisagé d'introduire l'ensemble complet des attributs et fonctions EFC dans chaque élément d'installation EFC, qu'il s'agisse d'équipements embarqués (OBE) ou d'infrastructures routières (RSE).

Le présent document fournit, à l'intention des opérateurs, une base d'accord indispensable pour assurer l'interopérabilité. Les outils spécifiés dans le document permettent d'assurer cette interopérabilité entre opérateurs pourvu que chacun reconnaisse les transactions EFC des autres (y compris l'échange des algorithmes et des clés de sécurité) et les mette en œuvre dans ses infrastructures comme dans celles des autres ou bien que les opérateurs s'accordent pour définir une nouvelle transaction (et un nouveau contrat) qui leur soient communs. Il convient également que chaque opérateur examine si son infrastructure routière possède les ressources nécessaires pour mettre en œuvre les transactions EFC supplémentaires du type défini.

Pour assurer l'interopérabilité, il convient que les opérateurs se mettent d'accord sur des points tels que:

— les aspects facultatifs à mettre effectivement en œuvre et à utiliser;

— les droits d'accès et la propriété des données de l'application EFC dans l'OBE;

— la politique de sécurité (y compris les algorithmes de chiffrement et la gestion des clés, le cas échéant);

— les questions opérationnelles, comme le nombre de reçus pouvant être conservés pour des raisons de confidentialité, le nombre de reçus nécessaires pour des raisons opérationnelles (tickets d'entrée ou preuves de paiement par exemple);

— les accords entre opérateurs nécessaires pour réglementer les différentes transactions EFC.

Dans cette édition, les utilisateurs sont confrontés à des problèmes de compatibilité ascendante. Ce problème peut être traité en utilisant les éléments suivants:

— Module EfcModule ASN.1, qui comprend un numéro de version;

— Efc-ContextMark (y compris ContextVersion), représentant la version de mise en œuvre, fournit un moyen pour garantir la coexistence de différentes versions de mise en œuvre au moyen d'un tableau de correspondance et du traitement de transactions appropriées associé. Cela permet au logiciel du RSE de déterminer la version de l'OBE et sa capacité à prendre en charge les nouvelles fonctions introduites par cette édition de l'ISO 14906.

L'Annexe A comporte les spécifications normatives ASN.1 des types de données utilisés (paramètres et attributs de l'action EFC).

L'Annexe B donne un exemple de transaction reposant sur la spécification CARDME, avec la spécification du niveau des éléments binaires.

 © ISO 2018 – Tous droits réservés

L'Annexe C donne des exemples informatifs de types de transaction EFC avec les fonctions et attributs EFC spécifiés.

L'Annexe D présente un tableau informatif de mappage des alphabets LatinAlphabetNo2 et 5 sur l'alphabet LatinAlphabetNo1 pour faciliter à un fournisseur de service l'utilisation de l'alphabet LatinAlphabetNo1 pour coder un OBE pour des données disponibles écrites avec des caractères non-Latin1.

L'Annexe E présente un tableau informatif de mappage entre les attributs de données de véhicule EFC et les certificats d'immatriculation européens, destiné à faciliter la tâche d'un fournisseur de service pour la personnalisation d'un OBE avec des données de véhicule.

L'Annexe F présente les calculs de sécurité selon la norme de chiffrement des données (DES). Cette annexe se base sur l'Annexe B de l'EN 15509:2014.

L'Annexe G présente les exemples de calculs de sécurité pour DES. Cette annexe se base sur l'Annexe E de l'EN 15509:2014.

L'Annexe H présente les calculs de sécurité selon la norme de chiffrement avancée (AES). Cette annexe est l'adaptation de l'Annexe B de l'EN 15509:2014 pour AES.

L'Annexe I présente les exemples de calculs de sécurité pour AES. Cette annexe est l'adaptation de l'Annexe E de l'EN 15509:2014 pour AES.

Cette définition d'interface d'application peut également être utilisée avec d'autres supports de DSRC qui n'utilisent pas la couche 7 selon l'ISO 15628/l'EN 12834. Tout support de DSRC fournissant des services de lecture et d'écriture de données pour initialiser une communication et pour exécuter des actions convient pour être utilisé comme base pour cette interface d'application. Les adaptations sont spécifiques au support et ne sont pas traitées ici. L'Annexe B décrit en détail une transaction pour un système de comptabilité centralisé. Le présent document peut également être utilisé pour des systèmes de comptabilité embarquée, conjointement à l'ISO 25110, qui donne des exemples de systèmes basés sur une comptabilité embarquée.

© ISO 2018 – Tous droits réservés

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

1 Domaine d'application

Le présent document spécifie l'interface d'application dans le contexte des installations de perception du télépéage (EFC) utilisant des communications dédiées à courte portée (DSRC).

Cette interface d'application EFC est l'interface du processus d'application EFC avec la couche d'application DSRC, comme le montre la Figure 1 ci-dessous. Le présent document spécifie les éléments suivants:

— les attributs EFC (c'est-à-dire les informations sur l'application EFC) pouvant également être utilisés pour d'autres applications et/ou interfaces;

— les procédures d'adressage des attributs EFC et des composants (matériels) (par exemple ICC et MMI);

— les fonctions de l'application EFC, c'est-à-dire la qualification ultérieure des actions par la définition des services concernés, l'attribution des valeurs ActionType associées ainsi que le contenu et la signification des paramètres des actions;

— le modèle de transaction EFC, qui définit les éléments et les étapes que toutes les transactions ont en commun;

— le comportement de l'interface qui doit assurer l'interopérabilité à un niveau donné d'interface d'application EFC-DSRC.

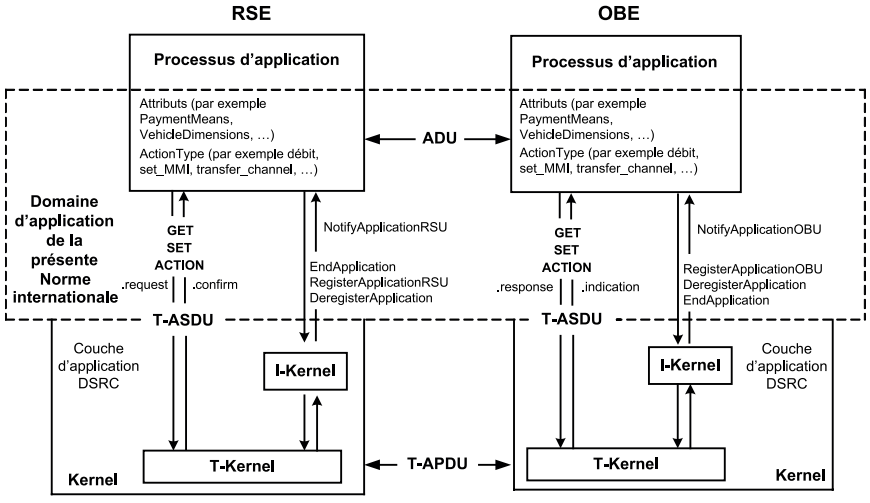


Figure 1 — Interface d'application EFC

Il s'agit d'une interface normalisée répondant à la philosophie de l'interconnexion des systèmes ouverts (OSI) (voir l'ISO/CEI 7498-1) et qui, en tant que telle, ne dépend pas essentiellement des choix de mise en œuvre réalisés de part et d'autre de l'interface.

Le présent document définit en termes de paramètres fictifs (données et fonctions) la fonctionnalité spécifique permettant d'assurer la sécurité de mise en œuvre des transactions EFC. La spécification de la politique de sécurité (y compris les algorithmes de sécurité particuliers et la gestion des clés)

© ISO 2018 – Tous droits réservés

demeure toutefois de la responsabilité de l'opérateur EFC et ne relève donc pas du domaine d'application du présent document.

2 Références normatives

Les documents suivants sont mentionnés dans le texte de sorte qu'une partie ou la totalité de leur contenu constitue les exigences 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 612, *Véhicules routiers — Dimensions des automobiles et véhicules tractés — Dénominations et définitions*

ISO 1176, *Véhicules routiers — Masses — Vocabulaire et codes*

ISO 3166-1, *Codes pour la représentation des noms de pays et de leurs subdivisions — Partie 1: Codes de pays*

ISO 3779, *Véhicules routiers — Numéro d'identification des véhicules (VIN) — Contenu et structure*

ISO 4217, *Codes pour la représentation des monnaies*

ISO/IEC 7812-1, *Cartes d'identification — Identification des émetteurs — Partie 1: Système de numérotation*

ISO/IEC 8825-2, *Technologies de l'information — Règles de codage ASN.1: Spécification des règles de codage compact (PER) — Partie 2*

ISO/IEC 9797-1:2011, *Technologies de l'information — Techniques de sécurité — Codes d'authentification de message (MAC) — Partie 1: Mécanismes utilisant un chiffrement par blocs*

ISO 14816:2005, *Télématique du transport routier et de la circulation routière — Identification automatique des véhicules et des équipements — Codification et structure des données*

ISO 15628:2013, *Systèmes intelligents de transport — Communications spécialisées à courte portée (DSRC) — Couche d'application DSRC*

ISO/IEC 18033-3:2010, *Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement — Partie 3: Chiffrement par blocs*

EN 12834:2003, *Télématique de la circulation et du transport routier — Communication dédiée à courte portée — Couche application*

3 Termes et définitions

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

L'ISO et la CEI tiennent à jour des bases de données terminologiques destinées à la normalisation aux adresses suivantes:

— IEC Electropedia: disponible sur http://www.electropedia.org/

— Plate-forme de navigation en ligne de l'ISO: disponible à l'adresse http://www.iso.org/obp

3.1
justificatifs d'accès
attestation de confiance ou module sécurisé établissant l'identité déclarée d'un objet ou d'une application

© ISO 2018 – Tous droits réservés

3.2
attribut
paquet de données adressables consistant en un élément de données unique ou des séquences structurées d'éléments de données

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

3.3
authentifiant
données (pouvant être chiffrées) utilisées à des fins d'authentification

3.4
voie
chemin de transfert des informations

[SOURCE: ISO 7498-2:1989, définition 3.3.13]

3.5
cryptographie
discipline incluant les 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, définition 3.6]

3.6
groupe de données
classe d'attributs étroitement liés

[SOURCE: ISO 17575-1:2016, définition 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/TS 19299:2015, définition 3.28]

3.8
élément
répertoire DSRC contenant des informations d'application sous la forme d'attributs

3.9
équipement embarqué
tout équipement nécessaire à bord d'un véhicule pour l'exécution des fonctions requises de collecte du télépéage et des services de communication

3.10
unité embarquée
appareil électronique simple installé à bord d'un véhicule servant à l'exécution des fonctions requises de collecte du télépéage et à la communication avec les systèmes externes

3.11
équipement routier
équipement fixe ou mobile installé le long de la route

3.12
percepteur de péage
entité juridique qui collecte le péage dû pour la circulation des véhicules dans un secteur à péage

[SOURCE: ISO 17573:2010, définition 3.16]

© ISO 2018 – Tous droits réservés

3.13
secteur à péage
domaine ou partie d'un réseau routier où est appliqué un régime de péage

[SOURCE: ISO 17573:2010, définition 3.18]

3.14
service de perception du télépéage
service permettant aux utilisateurs de régler le péage

3.15
fournisseur de services de télépéage
entité juridique assurant des services de télépéage dans un ou plusieurs secteurs à péage

[SOURCE: ISO 17573:2010, définition 3.23 modifiée]

3.16
transaction
ensemble des échanges d'informations entre deux installations de communication physiquement séparées

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

3.17
modèle de transaction
modèle fonctionnel décrivant la structure des transactions de paiement électronique

4 Abréviations

Pour les besoins du présent document, les termes abrégés suivants s'appliquent, sauf indication contraire.

AP	Processus d'application (Application Process)
APDU	Unité de données de protocole d'application (Application Protocol Data Unit)
ASN.1	Notation de syntaxe abstraite un (Abstract Syntax Notation One) (ISO/IEC 8824-1)
BST	Tableau de service de balises (Beacon Service Table)
CCC	Communication de contrôle de conformité
cf	Confirmer
DSRC	Communication dédiée à courte portée (Dedicated Short-Range Communication)
EFC	Perception du télépéage (Electronic Fee Collection)
EID	Identifiant d'élément (Element Identifier)
GNSS	Géolocalisation et navigation par un système de satellites
ICC	Carte à circuit(s) intégré(s) (Integrated Circuit(s) Card)
IID	Identifiant du demandeur (Invoker Identifier)
I-Kernel	Noyau d'initialisation (Initialisation Kernel)
ind	Indication

© ISO 2018 – Tous droits réservés