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 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

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.

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.

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.