NORME INTERNATIONALE

ISO 14819-6

Première édition
2006-04-15

Informations sur le trafic et le tourisme (TTI) — Messages TTI via le codage de messages sur le trafic —

Partie 6: Accès au cryptage et accès conditionnel pour le système de radiodiffusion de données — Codage ALERT C du canal de messages sur le trafic

Traffic and Traveller Information (TTI) — TTI messages via traffic message coding —

Part 6: Encryption and conditional access for the Radio Data System — Traffic Message Channel ALERT C coding

Numéro de référence
ISO 14819-6:2006(F)

© ISO 2006



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2006, 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 **1**

3 Termes et définitions **2**

4 Symboles et abréviations **3**

5 Notation **4**

6 Description d'application **4**
6.1 Introduction au profil des bits des groupes du RDS et à leur notation 4
6.2 RDS-TMC et Application de données ouverte 5
6.2.1 Variante 0 6
6.2.2 Variante 1 6
6.3 Résumé des éléments de données TMC dans les groupes de type 8A 7

7 Principes de la méthodologie de chiffrement et d'accès conditionnel **8**

8 Chiffrement par le prestataire de services **9**
8.1 Exigences du prestataire de services 9
8.2 Utilisation des groupes de type 8A pour le chiffrement du RDS-TMC 10
8.3 Groupe de gestion de chiffrement 10
8.3.1 SID 11
8.3.2 ENCID 11
8.3.3 LTNBE 12
8.4 Chiffrement des codes de localisation 12
8.4.1 Mode d'essai 13
8.4.2 Fréquence de répétition 13

9 Accès par un terminal à des services chiffrés **14**
9.1 Exigences de base d'un fabricant de terminaux 14
9.2 Activation d'un terminal 14
9.2.1 Numéro de série du terminal 15
9.2.2 Profil d'accès 15
9.2.3 Composition du code PIN 15
9.2.4 Règles de mise en œuvre pour les codes PIN 16
9.3 Identification d'un service RDS-TMC chiffré 16
9.4 Déchiffrement des codes de localisation 16

10 Introduction des services chiffrés **17**
10.1 Réponses des terminaux 17
10.2 Stratégie ***de facto*** valide seulement pour les prestataires de services souhaitant générer des recettes avant la mise à disposition généralisée du chiffrement 18
10.3 Actions pour les prestataires de services TMC déchiffrés 18
10.4 Actions pour les prestataires potentiels de services TMC 19
10.5 Échelles de temps 19

Bibliographie **20**

© ISO 2006 – 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 appelée 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 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'OMC concernant les obstacles techniques au commerce (OTC), voir le lien suivant: Avant-propos — Informations supplémentaires.

L'ISO 14819-6 a été élaborée par le comité technique ISO/TC 204, *Systèmes intelligents de transport*, et par le comité technique CEN/TC 278, *Application télématique pour le transport routier et la circulation routière* en collaboration.

L'ISO 14819 comprend les parties suivantes, présentées sous le titre général *Informations sur le trafic et le tourisme (TTI) — Messages TTI via le codage de messages sur le trafic*:

— *Partie 1: Protocole de codage pour le système de radiodiffusion de données (RDS) — Canal de messages d'informations sur le trafic (RDS-TMC) avec Alert-C;*

— *Partie 2: Codes d'événements et d'informations pour le système de radiodiffusion de données (RDS) — Canal de messages d'informations sur le trafic (RDS-TMC);*

— *Partie 3: Références de localisants pour ALERT-C (Référence d'emplacement pour ALERT-C);*

— *Partie 6: Accès au cryptage et accès conditionnel pour le système de radiodiffusion de données — Codage ALERT C du canal de messages sur le trafic.*

© ISO 2006 – Tous droits réservés

Introduction

L'information aux voyageurs sur la circulation peut être diffusée par l'intermédiaire d'un certain nombre de services ou de moyens de communication, Pour les services de ce type, les données à diffuser et la structure des messages impliqués dans les diverses interfaces nécessitent une définition claire et des formats normalisés, afin de permettre l'existence de produits concurrents, quelles que soient les données reçues.

La spécification de données la plus largement prise en charge pour les messages TTI en Europe et ailleurs est le RDS-TMC, spécifié dans les Parties 1, 2 et 3 de l'ISO 14819. Dans le RDS-TMC, les messages TTI sont acheminés dans des groupes de type 8A avec le Système de radiodiffusion de données (RDS), lui-même spécifié dans l'EN 62106.

La norme RDS-TMC a été développée principalement pour les besoins de diffusion des données TTI «à diffuser en clair», en utilisant un modèle de service public.

Cependant, dans un grand nombre de pays, l'adoption et la durée des services TTI requièrent un modèle commercial fondé sur des principes commerciaux permettant de couvrir les coûts de collecte des données et de leur diffusion en faisant payer aux utilisateurs finals ou aux intermédiaires la réception et l'utilisation des données. Dans ce modèle, un moyen commode pour ce faire est de coder les données d'une certaine façon, la clé de déchiffrement des données étant disponible sur paiement d'un abonnement ou d'une redevance. Afin d'éviter la prolifération de différents systèmes d'accès conditionnel, l'industrie européenne des récepteurs a demandé au Forum TMC de recommander une méthode unique de chiffrement capable d'être adoptée dans une large mesure.

Le groupe de travail a établi les critères auxquels toute méthode de chiffrement doit satisfaire. Ces critères sont notamment:

— conformité aux directives et spécifications du RDS et du TMC;

— surcharge nulle, ou seulement minimale, en termes de capacité de données requise pour le chiffrement;

— aucune modification du matériel requise pour les terminaux existants;

— disponibilité pour une utilisation par les prestataires de services et les fabricants de terminaux, de manière libre et équitable, soit gratuitement, soit contre paiement d'une modique redevance de licence;

— applicabilité de modèles commerciaux d'abonnement tant à terme qu'à vie;

— aptitude des terminaux à être activés pour recevoir le service chiffré, sur une base individuelle.

Après l'appel d'offres, un jury d'experts a jugé la soumission de Deutsche Telekom comme étant celle qui a le mieux satisfait aux critères prédéfinis par le groupe de travail La méthode chiffre les 16 bits qui forment l'élément «Localisation» dans chaque message RDS-TMC afin de rendre le message virtuellement inutile en l'absence de déchiffrement. Le chiffrement n'est que «léger» mais il a été jugé adéquat pour dissuader tous les hackers sauf celui le plus déterminé. Des systèmes plus sécurisés ont été rejetés en raison de la surcharge de capacité du RDS qu'ils exigeaient.

Après ratification de la décision d'adopter la soumission de Deutsche Telekom par le groupe Forum Business et le groupe Management TMC, un groupe a été désigné et chargé de l'élaborer et de la présenter sous forme de spécification à soumettre à la normalisation. Il a également été demandé au groupe de produire des lignes directrices pour les prestataires de services et les fabricants de terminaux afin d'aider à la mise en œuvre de la spécification.

La présente Norme internationale décrit un système de chiffrement léger non propriétaire et d'accès conditionnel qui permet l'existence de modèles commerciaux pour le RDS-TMC. Le lecteur est supposé avoir une compréhension préalable et une certaine familiarité des normes du RDS et du RDS-TMC et de leurs lignes directrices de mise en œuvre.

© ISO 2006 – Tous droits réservés

Informations sur le trafic et le tourisme (TTI) — Messages TTI via le codage de messages sur le trafic —

Partie 6:
Accès au cryptage et accès conditionnel pour le système de radiodiffusion de données — Codage ALERT C du canal de messages sur le trafic

1 Domaine d'application

Le présent document établit une méthode de chiffrement de certains éléments de données codées en ALERT-C transportés dans le groupe de données RDS-TMC du type 8A afin que les informations acheminées n'aient virtuellement aucune valeur sans l'application par un terminal ou récepteur d'une clé adéquate.

Avant qu'un terminal ne puisse déchiffrer les données, il lui faut deux «clés». La première est donnée en toute confiance par le prestataire de services aux fabricants de terminaux avec lesquels il entretient une relation commerciale; la seconde est diffusée dans le «Groupe de gestion du chiffrement», qui est aussi un groupe de type 8A. La présente Norme internationale explique le but des deux clés ainsi que la fréquence et le moment auxquels il est permis de changer la clé émise.

Avant qu'un terminal individuel ne puisse présenter des messages déchiffrés à l'utilisateur final, il faut l'activer à cet effet. L'activation requiert la saisie d'un code PIN. Le code PIN commande les droits d'accès à chaque service et la période d'abonnement, permettant la coexistence de modèles commerciaux tant à terme qu'à vie.

La présente Norme internationale décrit aussi les considérations pour les prestataires de services souhaitant introduire un service RDS-TMC chiffré, en migrant d'un service «à diffuser en clair» basé sur des «Tables de localisants» publiques ou d'un service commercial basé sur une «Table de localisants» propriétaire.

Finalement, des «crochets» ont été laissés dans l'allocation des bits du groupe de type 8A pour permettre l'extension du chiffrement à d'autres services du RDS-TMC.

2 Références normatives

Les documents de référence 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 14819-1, *Systèmes intelligents de transport — Informations sur le trafic et le tourisme via le codage de messages sur le trafic — Partie 1: Protocole de codage pour le système de radiodiffusion de données (RDS) — Canal de messages d'informations sur le trafic (RDS-TMC) avec ALERT-C*

ISO 14819-2, *Systèmes intelligents de transport — Informations sur le trafic et le tourisme via le codage de messages sur le trafic — Partie 2: Codes d'événements et d'informations pour le système de radiodiffusion de données (RDS) — Canal de messages d'informations sur le trafic (RDS-TMC) avec ALERT-C*

ISO 14819-3, *Systèmes intelligents de transport — Informations sur le trafic et le tourisme via le codage de messages sur le trafic — Partie 3: Références de localisants pour le système de radiodiffusion de données (RDS) — Canal de messages d'informations sur le trafic (RDS-TMC) avec ALERT-C*

© ISO 2006 – Tous droits réservés

EN 62106, *Spécification du système de radiodiffusion de données (RDS) pour la radio à modulation de fréquence dans la bande 87,5 à 108,0 MHz (CEI 62106:2000)*

3 Termes et définitions

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

3.1
profil d'accès
ACP
service et période d'abonnement particuliers

3.2
code de pays
CC
code assigné à un pays devant être émis comme étant les quatre premiers bits du code PI émis dans un service RDS de diffusion

[SOURCE: EN 62106]

3.3
identifiant de chiffrement
ENCID
valeur indiquant quelle ligne dans la table de paramètres Clés de Service le prestataire de services utilise dans son processus de chiffrement le jour en question

Note 1 à l'article: L'ENCID est émis dans des groupes de type 8A.

3.4
description d'événement
indication des détails de la situation routière, des problèmes généraux ou spécifiques de circulation, et autres facteurs (par exemple, météorologiques) affectant ou affectant potentiellement le passage des véhicules sur les réseaux routiers et autoroutiers

3.5
date d'expiration
date fixée par le prestataire de services à laquelle il convient que cesse la capacité d'un terminal particulier à déchiffrer un service chiffré (c'est-à-dire la fin de la période d'abonnement payée)

3.6
localisation
zone, section d'autoroute ou point où est située la source du problème

3.7
code de localisation
représentation numérique ou alphanumérique d'une localisation en fonction d'une base de données prédéfinie, appelée Table de localisants

3.8
numéro de table de localisants
LTN
nombre, ayant une valeur de 0 à 63, servant à identifier la Table de localisants utilisée par le prestataire de services

Note 1 à l'article: Le LTN est en général attribué à chaque prestataire de services dans un pays par les pouvoirs publics habilités ou l'autorité compétente chargée des routes à partir d'une plage affectée au pays en question. Il est émis dans des groupes de type 3A.

Note 2 à l'article: Lorsqu'elle est émise dans des groupes de type 3A, la valeur 0 montre que le prestataire de services chiffre les codes de localisation émis de la manière décrite dans la présente Norme internationale.

© ISO 2006 – Tous droits réservés

3.9
numéro de table de localisants avant chiffrement
LTNBE
nombre, ayant une valeur de 1 à 63, servant à identifier la Table de localisants utilisée par le prestataire de services avant que les codes dans la table ne soient chiffrés en vue de l'émission

Note 1 à l'article: Le LTNBE est émis dans des groupes de type 8A.

3.10
autre réseau
ON
notation jointe en dessins, si cela s'avère nécessaire, pour indiquer que le code émis [par exemple. SID (ON)] se rapporte à un autre réseau référencé et non au Service «reçu»

Note 1 à l'article: Les données relatives à un ou plusieurs autres réseaux peuvent être stockées au préalable dans l'équipement terminal.

3.11
code PIN
code numérique ou alphanumérique qu'il et exigé de saisir dans un terminal avant que ce dernier ne soit autorisé à présenter des messages RDS-TMC déchiffrés

Note 1 à l'article: La valeur du code PIN est calculée par le fabricant du terminal à partir d'un algorithme utilisant comme facteurs le numéro de série du terminal et un ou plusieurs profils d'application.

3.12
numéro de série
identifiant alphanumérique, propre au terminal (ou groupe de terminaux), déterminé par le fabricant

3.13
identifiant de service
SID
code identifiant de façon univoque un service TMC fourni par un prestataire de services

3.14
clé de service
SVK
nombre donné en toute confiance par un prestataire de services à un fabricant de terminaux, identifiant celle des huit tables de chiffrement possibles que le service utilise pour le chiffrement

Note 1 à l'article: La clé de service N'EST PAS émise.

3.15
prestataire de services
organisation qui gère un service de données en recueillant et traitant les données et en commercialisant le service de données

Note 1 à l'article: Le prestataire de services négocie avec un opérateur de diffusion et/ou de transmission l'usage de la largeur de bande de données nécessaire à la transmission.

4 Symboles et abréviations

ACP Profil d'accès (Access Profile)

AID Identification d'application (Application IDentification)

CC Code de pays (Country Code)

ENCID Identifiant de chiffrement (ENCryption IDentifier)

© ISO 2006 – Tous droits réservés