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

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

EESTI STANDARDI EESSÕNA **NATIONAL FOREWORD**

Käesolev Eesti standard EVS-EN ISO 14819-6:2006 sisaldab Euroopa standardi EN ISO 14819-6:2006 ingliskeelset teksti. Käesolev dokument on jõustatud 29.05.2006 ja selle kohta on avaldatud teade Eesti standardiorganisatsiooni ametlikus väljaandes. Standard on kättesaadav Eesti standardiorganisatsioonist.	This Estonian standard EVS-EN ISO 14819-6:2006 consists of the English text of the European standard EN ISO 14819-6:2006. This document is endorsed on 29.05.2006 with the notification being published in the official publication of the Estonian national standardisation organisation. The standard is available from Estonian standardisation organisation.

Käsitlusala: This document establishes a method of encrypting certain elements of the ALERT-C coded data carried in the RDS-TMC type 8A data group, such that without application by a terminal or receiver of an appropriate key, the information conveyed is virtually worthless.	**Scope:** This document establishes a method of encrypting certain elements of the ALERT-C coded data carried in the RDS-TMC type 8A data group, such that without application by a terminal or receiver of an appropriate key, the information conveyed is virtually worthless.

ICS 03.220.20, 35.240.60

Võtmesõnad:

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 14819-6

April 2006

ICS 03.220.20; 35.240.60

English Version

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 (ISO 14819-6:2006)

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 (ISO 14819-6:2006)

Verkehrs- und Reiseinformationen-TTI - Meldungen über Verkehrsmeldungscodierung - Teil 6: Verschlüsselung und Zugangsbedingungen für das Radio Datensystem - Verkehrsmeldungskanal ALERT C Kodierung (ISO 14819-6:2006)

This European Standard was approved by CEN on 20 March 2006.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the Central Secretariat has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No. EN ISO 14819-6:2006: E

Foreword

This document (EN ISO 14819-6:2006) has been prepared by Technical Committee CEN/TC 278 "Road transport and traffic telematics", the secretariat of which is held by NEN, in collaboration with Technical Committee ISO/TC 204 "Transport information and control systems".

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by October 2006, and conflicting national standards shall be withdrawn at the latest by October 2006.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

INTERNATIONAL STANDARD

ISO 14819-6

First edition
2006-04-15

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

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

Reference number
ISO 14819-6:2006(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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.

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 14819-6 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*, in collaboration with CEN Technical Committee CEN/TC 278, *Road transport and traffic telematics*, the secretariat of which is held by NEN.

ISO 14819 consists of the following parts, under the general title *Traffic and Traveller Information (TTI) — TTI messages via traffic message coding*:

— *Part 1: Coding protocol for Radio Data System — Traffic Message Channel (RDS-TMC) using ALERT-C*

— *Part 2: Event and information codes for Radio Data System — Traffic Message Channel (RDS-TMC)*

— *Part 3: Location referencing for ALERT-C*

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

Introduction

Traffic and traveller information may be disseminated through a number of services or means of communication. For such services, the data to be disseminated and the message structure involved in the various interfaces require clear definition and standard formats, in order to allow competitive products to exist with any received data.

The most widely supported data specification for TTI messages within Europe and elsewhere is RDS-TMC, specified in Parts 1, 2 and 3 of EN ISO 14819. In RDS-TMC, TTI messages are conveyed using type 8A groups with the Radio Data System, itself specified in EN 62106.

The RDS-TMC standard was developed principally for the purposes of disseminating TTI data 'free-to-air', using a public-service model.

However, in many countries, the adoption and continuance of TTI services requires a business model based on commercial principals whereby the costs for the collection of the data and its dissemination may be recovered by charging end-users or intermediaries to receive and use the data. In this model, a convenient way that this may be achieved is to encrypt the data in some way, the key to decrypt the data being made available on payment of a subscription or fee. In order to avoid a proliferation of different conditional access systems, the European receiver industry asked the TMC Forum to establish a Task Force to recommend a single method of encryption capable of being widely adopted.

The task force established criteria that any encryption method would have to fulfil. These included:

— conformity with the RDS and TMC specifications and guidelines;

— no, or only minimal, overhead in terms of data capacity required for encryption;

— no hardware change to existing terminals required;

— availability for use by service providers and terminal manufacturers "freely" and "equitably", either free-of-charge or on payment of a modest licence fee;

— applicability to both lifetime and term subscription business models;

— ability of terminals to be activated to receive an encrypted service on an individual basis.

After calling for candidate proposals, the submission from Deutsche Telekom was judged by an expert panel to have best met the pre-determined criteria the task force had established. The method encrypts the 16 bits that form the Location element in each RDS-TMC message to render the message virtually useless without decryption. The encryption is only "light" but was adjudged to be adequate to deter all but the most determined hacker. More secure systems were rejected because of the RDS capacity overhead that was required.

After ratification of the decision to adopt the Deutsche Telekom submission by the TMC Forum Business Group and Management Group, a group was appointed and given the remit to elaborate it and present it as a specification to be submitted for standardization. The group was also requested to produce guidelines for service providers and terminal manufacturers to aid implementation of the specification.

This International Standard describes a non-proprietary light encryption and conditional access system that allows commercial models for RDS-TMC to exist. The reader is assumed to have a pre-existing understanding of, and familiarity with, the RDS and RDS-TMC standards and implementation guidelines.

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

1 Scope

This document establishes a method of encrypting certain elements of the ALERT-C coded data carried in the RDS-TMC type 8A data group, such that without application by a terminal or receiver of an appropriate key, the information conveyed is virtually worthless.

Before a terminal is able to decrypt the data, the terminal requires two “keys”. The first is given in confidence by the service provider to terminal manufacturers with whom they have a commercial relationship; the second is broadcast in the “Encryption Administration Group,” which is also a type 8A group. This International Standard explains the purpose of the two keys and how often and when the transmitted key may be changed.

Before an individual terminal may present decrypted messages to the end-user, it must have been activated to do so. Activation requires that a PIN code be entered. The PIN code controls access rights to each service and subscription period, allowing both lifetime and term business models to co-exist.

The International Standard also describes the considerations for service providers wishing to introduce an encrypted RDS-TMC service, migrating from either a “free-to-air” service based on public “Location Tables” or a commercial service based on a proprietary Location Table.

Finally, “hooks” have been left in the bit allocation of the type 8A group to allow extension of encryption to other RDS-TMC services.

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 14819-1, *Traffic and Traveller Information (TTI) — TTI messages via traffic message coding — Part 1: Coding protocol for Radio Data System — Traffic Message Channel (RDS-TMC) using ALERT-C*

ISO 14819-2, *Traffic and Traveller Information (TTI) — TTI messages via traffic message coding — Part 2: Event and information codes for Radio Data System — Traffic Message Channel (RDS-TMC)*

ISO 14819-3, *Traffic and Traveller Information (TTI) — TTI messages via traffic message coding — Part 3: Location referencing for ALERT-C*

EN 62106, *Specification of the radio data system (RDS) for VHF/FM sound broadcasting in the frequency range from 87, 5 to 108, 0 MHz (IEC 62106:2000)*