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)*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
Access Profile
ACP
a particular service and subscription period

3.2
Country Code
CC
code assigned to a country to be transmitted as the first four bits of the transmitted PI code in a broadcast RDS service

[EN 62106]

3.3
Encryption Identifier
ENCID
value indicating which line in the Service Key table of parameters the service provider is using in the encryption process that day

NOTE ENCID is transmitted in type 8A groups.

3.4
Event Description
details of the road situation, general or specific traffic problems, and other factors (e.g. weather) affecting or potentially affecting the passage of vehicles on the roads and highways network

3.5
Expiry Date
date determined by the service provider on which a particular terminal's ability to decrypt an encrypted service should cease (i.e. end of the paid subscription period)

3.6
Location
area, highway segment or point location where the source of the problem is situated

3.7
Location Code
numeric or alphanumeric representation of a location according to a pre-determined database, known as a Location Table

3.8
Location Table Number
LTN
number with the value 0 to 63 used to identify the Location Table used by the service provider.

NOTE 1 The LTN is generally allocated to each service provider in a country by the relevant government or roads authority from a range assigned to that country. It is transmitted in type 3A groups.

NOTE 2 Value 0, when transmitted in type 3A groups, shows that the service provider is encrypting the location codes transmitted in the manner described in this International Standard.

3.9
Location Table Number Before Encryption
LTNBE
number with the value 1 to 63 used to identify the Location Table used by the service provider prior to the codes within the table being encrypted for transmission

NOTE LTNBE is transmitted in type 8A groups.

3.10
Other Network
ON
notation appended in drawings, where necessary, to indicate that the code being transmitted [e.g. SID (ON)] relates not to the Tuned Service, but to a referenced Other Network

NOTE Data about the Other Network(s) can be pre-stored in terminal equipment.

3.11
PIN code
numeric or alphanumeric code required to be entered into a terminal before that terminal is permitted to present decrypted RDS-TMC messages

NOTE The value of the PIN code is calculated by the terminal manufacturer from an algorithm using terminal serial number and one or more application profiles as factors.

3.12
Serial Number
alphanumeric identifier, unique to a terminal (or group of terminals), determined by the manufacturer

3.13
Service Identifier
SID
Code uniquely identifying a TMC service provided by a service provider

3.14
Service Key
SVK
number given in confidence by a service provider to a terminal manufacturer, identifying which one of eight possible encryption tables the service is using for encryption

NOTE The Service Key is NOT transmitted.

3.15
Service Provider
organization that manages any data service, by gathering data, processing data, and selling the data service

NOTE The service provider negotiates for the use of the necessary data bandwidth for transmission with a Broadcaster or Transmission Operator.

4 Symbols and abbreviations

ACP Access Profile

AID Application IDentification

CC Country Code

ENCID ENCryption IDentifier

LTN Location Table Number

LTNBE Location Table Number Before Encryption

MGS Message Geographical Scope

ODA Open Data Application

ON Other Network

PI Programme Identification

RDS Radio Data System

rfu reserved for future use

SID Service IDentifier

SVK Service Key

TMC Traffic Message Channel

UTC Coordinated Universal Time

5 Notation

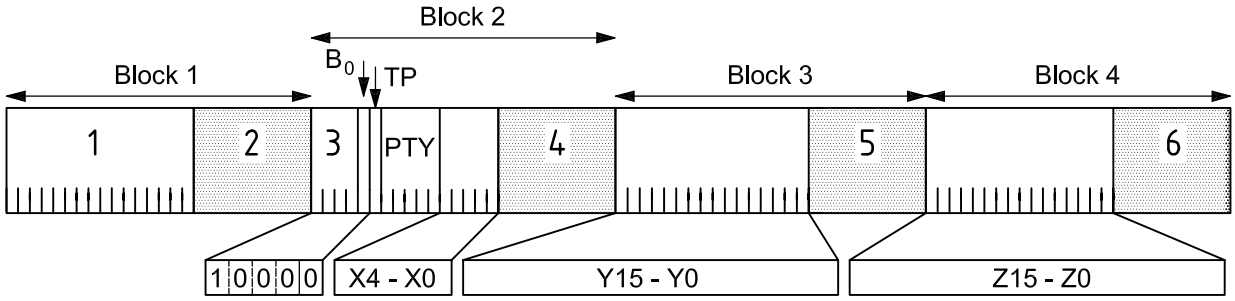
In this International Standard, numbers are DECIMAL, unless specifically indicated otherwise, e.g. 1234 (hex).

6 Application description

In 6.1 and 6.2 below, the basics of RDS and RDS-TMC are introduced in order to provide the reader with the framework necessary to understand the method of encryption detailed in this International Standard.

6.1 Introduction to RDS group bit pattern and notation

The general format for all RDS data groups is as shown in Figure 1. Of the sixty-four data bits in each group, the sixteen in Block 1, and the first eleven in Block 2, have specific values essential to the correct operation of the basic RDS system features. The remaining thirty-seven bits, indicated in RDS-TMC with the notation X4-X0, Y15-Y0 and Z15-Z0 have uses specific to the particular RDS feature or application being coded.



Key

1 PI code
2 Checkword and Offset A
3 Group type code
4 Checkword and Offset B
5 Checkword and Offset C
6 Checkword and Offset D

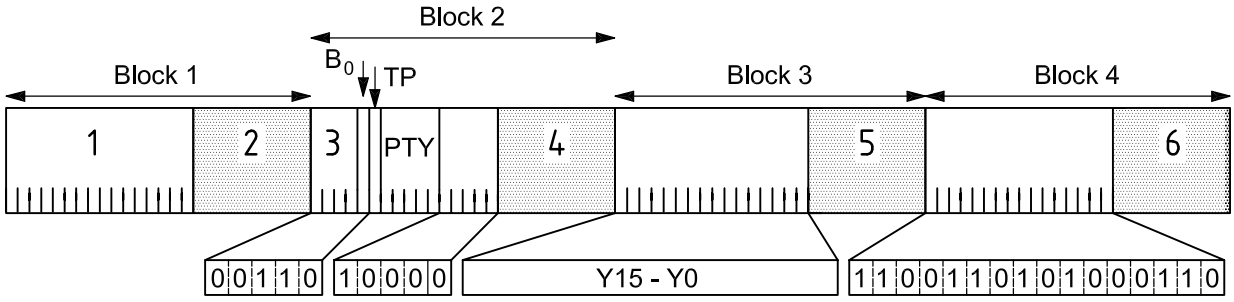
Figure 1 — RDS data group

6.2 RDS-TMC and Open Data Application

RDS-TMC using the ALERT-C protocol is defined in ISO 14819-1.

It is an example of an RDS ODA, which allows the application to be transmitted in any appropriate unused RDS group type in the particular RDS service. The application identified by its AID code, and the group in which it is being transmitted is identified using a type 3A group, which in effect acts as an index for all ODAs.

The structure of an ODA type 3A group is given in Figure 2. The AID code for ALERT-C coded RDS-TMC messages is CD46 (hex), indicated in Block 4, bits Z15 to Z0. The group type carrying the RDS-TMC data – which by convention is a type 8A group – is given by bits X4 to X0.



Key

1 PI code
2 Checkword and Offset A
3 Group type code
4 Checkword and Offset B
5 Checkword and Offset C
6 Checkword and Offset D

Figure 2 — Type 3A group (ODA) indicating RDS-TMC (CD46 (hex)) carried in group 8A

The bits in Y15 to Y0 are used to convey parameters describing the nature and transmission details of the particular RDS-TMC service.

Two variants have been defined, which are fully described in ISO 14819-1; they are summarized as follows:

6.2.1 Variant 0

In variant 0, bits Y5 to Y0 indicate the AFI, the Mode of Transmission Indicator (M) and MGS elements.

Bits Y11 to Y6 indicate LTN for the service, which in terms of this International Standard which describes encryption, is the most important element. The value of LTN indicates whether or not the location codes (carried in the type 8A groups) are “encrypted”.

In older versions of ISO 14819-1, LTN = 0 was an excluded value, and only values of 1 to 63 were permitted. This International Standard now makes use of this previously excluded zero value to indicate an encrypted service.

Non-zero LTN values in a type 3A group indicate **non-encrypted** services; these may be either free-to-air services using a publicly available Location Table, or services which use a proprietary Location Table to restrict use. In either case, in order to produce any valid messages, the terminal must have access to the Location Table identified by the LTN.

An **encrypted** RDS-TMC service is indicated by an LTN with value 0 in the type 3A group. The LTN used by the service provider, the codes of which are now to be encrypted, is given by the element LTNBE, transmitted in the Encryption Administration Group, described in 8.3 below.