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)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

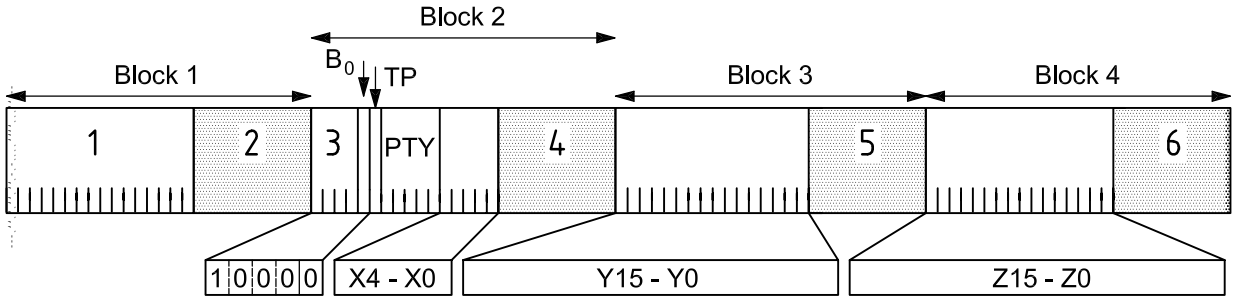
In this International Standard, numbers are DECIMAL, unless specifically indicated otherwise, e.g. 1234 (hex).

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

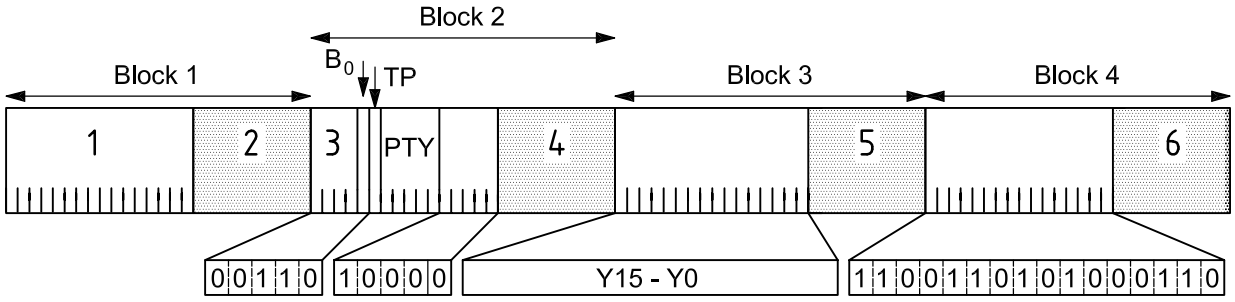
Figure 1 — RDS data group

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.

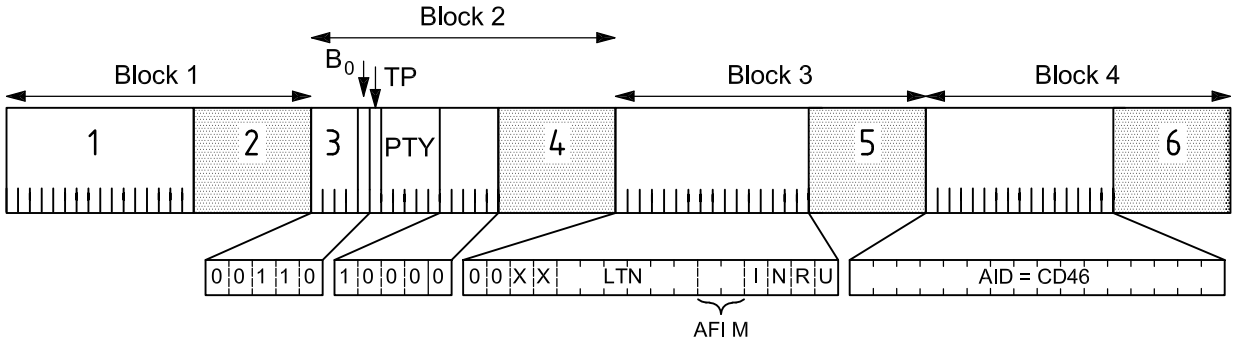
Bits Y11 to Y6 indicate LTN for the service, which in terms of this International Standard which describes encryption, is the most important element. The value of LTN indicates whether or not the location codes (carried in the type 8A groups) are “encrypted”.

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.

Block 4 (Bits Z15 to Z0) will always be set to the value CD46, which is the AID identifying an RDS-TMC service.



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 3 — Type 3A group, RDS-TMC variant 0, carrying system information

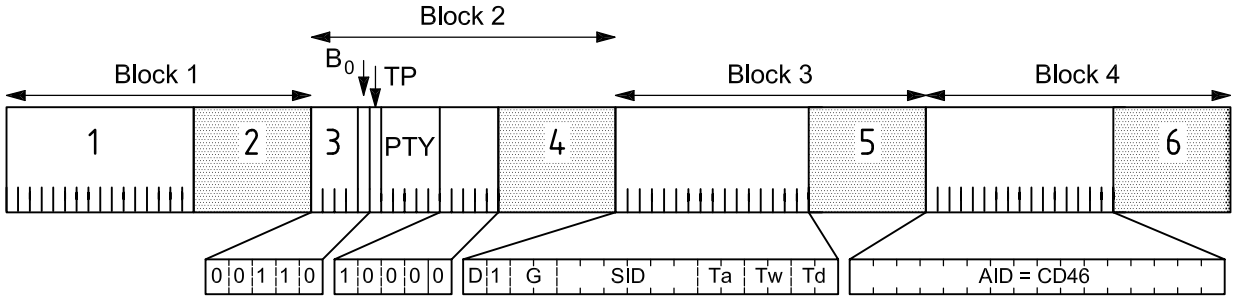
A type 3A group variant 0 shall be transmitted at least once every 5 s.

6.2.2 Variant 1

In variant 1, bits Y11 to Y6 indicate the SID.

Bits Y13 to Y12, Y5 to Y4, Y3 to Y2 and Y1 to Y0 are used to detail respectively the values of Gap (G), activity time (Ta), window time (Tw) and delay time (Td) when the “Spinning Wheel” mode of transmission is used. This is fully specified in ISO 14819-1.

Block 4 (Bits Z15 to Z0) will always be set to the value CD46, which is the AID identifying an ALERT-C RDS-TMC service.



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 4 — Type 3A group, RDS-TMC variant 1, carrying system information

A type 3A group variant 1 shall be transmitted at least once every 10 s, as defined in ISO 14819-1.

Using the SID which is also included within the Encryption Administration group (see 8.3 below) may help terminals to increase the search process for encrypted services.

6.3 Summary of TMC data elements in type 8A groups

Details of particular traffic situations are carried in the RDS-TMC user messages, transmitted as type 8A groups. They provide the following six basic items of information:

— **Event Description** — giving details of the traffic situation, or other factor (e.g. weather) affecting or potentially affecting traffic. An 11-bit number represents the event description, a common table being used by all service providers. The list of numbers and associated descriptions are in ISO 14819-2.

— **Location** — indicating the area, highway segment or point of the source of the traffic situation. The location is indicated by a 16-bit code. Obviously, the table of locations is country- (and maybe service provider-) specific. In order for a terminal to be able to use the location information, it must have a copy of the location table used by the service provider. Each Location Table is referred to by an LTN.

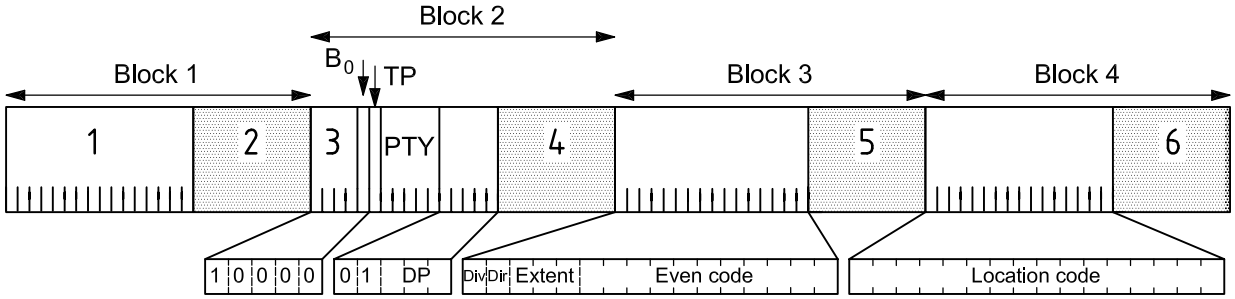
— **Direction** and **Extent** — indicating the number of segments, adjacent to the location indicated affected by the situation, and where appropriate, the direction concerned.

— **Duration and Persistence** — giving an indication of how long the situation/problem is expected to last.

— **Diversion Advice** — indicating whether drivers are advised to find and follow an alternative route.

NOTE These are fully described in ISO 14819-1 and the ALERT-C Coding Handbook, the summary above is included to aid understanding the encryption principles adopted in this International Standard.

Figure 5 indicates where these elements are coded in a type 8A TMC single group message.



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 5 — RDS-TMC single group message

Although most traffic situations can be described using a single group message, the provision exists within the RDS-TMC specification to use up to five RDS-TMC groups to more fully describe a particular problem, including for example, detailed diversion advice.

The first group of multi-group messages contains the Direction, Extent, Event code and the Location code, which occupy the same bit-positions as in a single group message.

Subsequent groups can include the Duration and Persistence element, quantifiers, qualifiers, and specific advice (e.g. maximum recommended speed limit). Location codes may be also be included within these subsequent message groups to indicate diversionary routes that should (or may) be followed.

7 Principles of the Encryption and Conditional Access methodology

The principle adopted in this International Standard for TMC Encryption and Conditional Access can be described by the following:

— The service provider uses a bit-manipulation technique to encrypt the 16 bits forming all location codes transmitted in every TMC message, which renders the information worthless. The primary location element is transmitted both in single group messages and in the first group of multi-group messages; other location codes, which are used to describe diversions, may be included in other than the first group of multi-group messages.

— The location code is encrypted according to certain pre-defined parameters of an encryption algorithm. Each combination of parameters is referred to by two values, the “Service Key” and the “Encryption Identifier”. As the combination of parameters are pre-defined and stored within each terminal, provided the terminal is advised which combination of Service Key and Encryption Identifier is in use, it is able to decrypt the location code.

— The service provider, under commercial arrangements with the terminal manufacturer, advises which “Service Key” their service will use; the “Service Key” is NOT transmitted information.

— The service provider transmits an “Encryption Identifier” that identifies the values of the parameters used to encrypt messages on that particular day.

— Before a message is allowed to be decrypted, the individual terminal must have been activated for that particular RDS-TMC service.

— Activation of a particular terminal is allowed for a particular service, and until a certain date. These are determined according to the business model and agreements between the service provider and terminal manufacturer. The combination of service and time period is referred to as the “Access Profile”.

— The terminal manufacturer determines the PIN code required to be entered to activate a particular terminal for a particular Access Profile, or combination of Access Profiles. Different PIN codes will hence activate the terminal for different combinations of services, or periods of time. The PIN to activate a particular terminal is either input by the manufacturer, or communicated to the service provider or other party responsible for providing customer support.

— Once activated, the terminal uses a bit-manipulation technique to decrypt the transmitted location code, hence recovering the original location code, and making the message valid.

The encryption/decryption methodology used is based on some elementary bit-level functions available for all high-level language compilers. The functions require the introduction of parameters to control the bit manipulation process. The encryption/decryption process is symmetrical: the parameters used by both the service provider for encryption, and by the terminal equipment for decryption, are derived from the same Service Key tables.

8 Encryption by the service provider

8.1 Service provider's requirements

In addition to the requirements that a service provider already has to enable a "free-to-air" RDS-TMC service, the following shall be able to offer an encrypted TMC service as specified:

— a copy of one of the eight Service Key Tables, each of which details 32 different sets of parameters and values which can be used to encrypt the location codes.

NOTE A Service Key table (and its reference number) is obtained from the TMC Forum office at ERTICO;

— software to encrypt location codes using the sets of parameters and values in the Service Key table used;

— the ability to transmit and set appropriate values for the parameters in the Encryption Administration group to describe the service and the encryption parameters in use. The Encryption Administration group is a type 8A group with bits X4-X0 = 00000 and bits Y15-Y13 = 000;

— an arrangement with terminal equipment suppliers, which allows their terminals to be activated to receive the service provider's encrypted service. As part of this arrangement, the service provider advises the terminal manufacturer which Service Key they will use, and whether the agreement is a "lifetime" one, or for a particular period only. The parameters which identify the service (i.e. Country Code, Service Identifier and Location Table Number Before Encryption), the Service Key and the expiry date together form the Access Profile for that service;

— if the service provider also has entered into an alliance with other service providers (to collectively offer, for example, a pan-European TMC service), the Access Profiles of the other alliance partners as well.

8.2 Use of type 8A groups for RDS-TMC encryption

RDS-TMC data is carried within a type 8A group. Bits X4 – X0 indicate the usage of the remaining bits, Y15 to Y0 and Z15 to Z0.

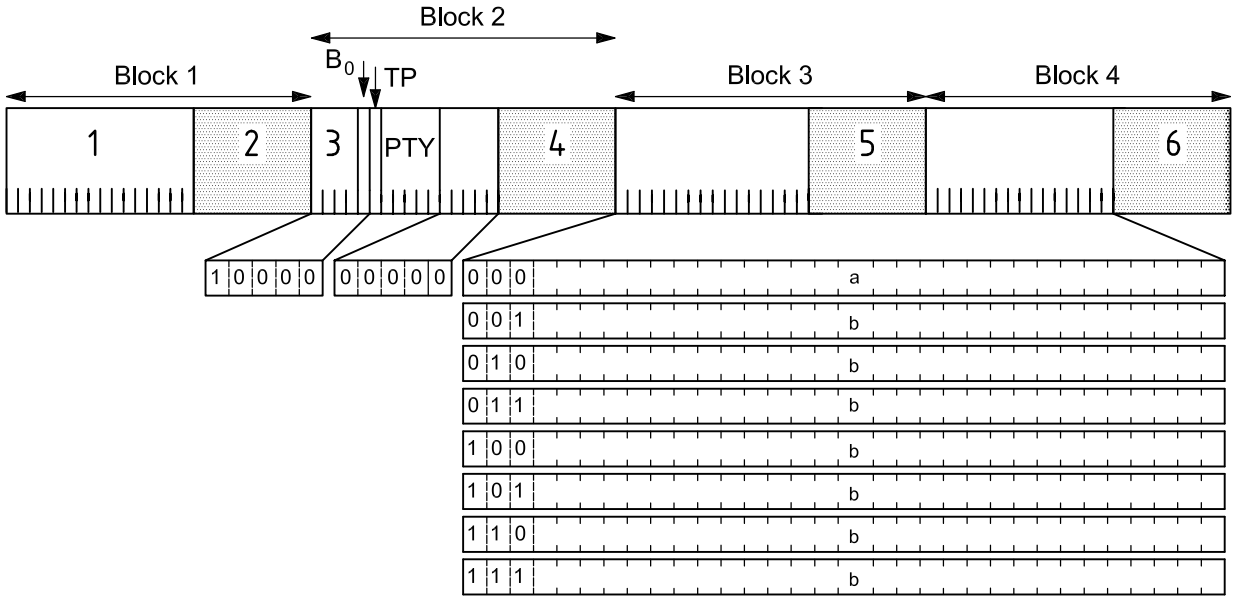
In older versions of ISO 14819-1, X4 – X0 = 00000 was an unused bit combination.

This International Standard for an encrypted RDS-TMC service now uses this bit pattern to provide to the terminal details of the encryption parameters. When bits X4 – X0 = 00000 and hence indicate an encrypted service, bits Y15 – Y13 are used to indicate variants.

Variant 0 indicates the Encryption Administration group, which is used to detail the encryption parameters.

Variants 1 to 7 are currently undefined, and may later be assigned for use for other RDS-TMC encrypted services.

Figure 6 illustrates the usage of these variants.



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

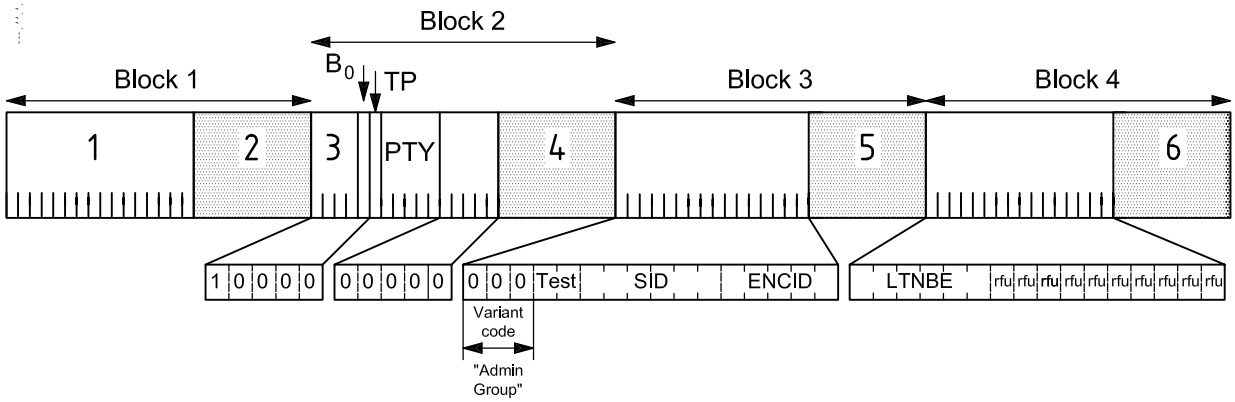
a Encryption Administration group.

b Reserved for future use.

Figure 6 — Type 8A group, used for encrypted RDS-TMC, showing variant usage

8.3 Encryption Administration group

The Encryption Administration group (Figure 7) comprises the SID, the ENCID and the LTNBE. Also included are two test bits.



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 7 — Type 8A group, RDS-TMC Encryption Administration group

8.3.1 SID

The SID is a six-bit number transmitted in bits Y10 to Y5. The assignment of SID is described in the Annex to ISO 14819-3, and generally is allocated to a service provider by the relevant Government or roads authority in each country.

Providing RDS-TMC as an encrypted service, rather than non-encrypted, does not affect the value of the SID transmitted.

The SID transmitted in this group must be the same as that transmitted in variant 1 of the type 3A group if that variant is used. SID is included in the Encryption Administration group for completeness, such that all the elements required by a terminal to determine whether a TMC service may be offered are included within a single group.

8.3.2 ENCID

To minimize the overhead potentially required when encrypting data, the parameters used to encrypt the location codes are stored in eight Service Key tables in the terminal equipment. Each of the eight Service Key tables has 32 “lines”. Each line gives the values of three parameters used to encrypt the 16 bits of the location code.

The service provider decides which set of parameter values will be used to encrypt the location codes used for messages transmitted on that particular day. The line that is used in the Service Key table is advised to the terminal by the value of the variable ENCID, transmitted as bits Y4 to Y0 in the Encryption Administration group.

The Service Key tables are not publicly available, but are made available to service providers and terminal manufacturers under confidentiality agreements by the TMC Forum. For reasons of secrecy, therefore, actual Service Key tables are not published in this International Standard. 8.4 below, however, provides part of a fictitious Service Key table to illustrate the principle of encryption, which is based on elementary bit-level functions available for all high-level language compilers.

The functions are:

— Bit-wise Rotate Right the original location code expressed in binary, by a given number of bits,

— Position a given binary value at a given Start Bit,

— Apply an XOR operation between the given value and the rotated location code.

The resulting value is the encrypted location code that is transmitted.

8.3.3 LTNBE

In order to provide any RDS-TMC service, non-encrypted or encrypted, the terminal equipment shall have a copy of the Location codes used by the service provider. The service provider shall transmit the LTN to identify which particular table of codes is used on his service.

When the service is being offered non-encrypted, the Location Table Number used shall be transmitted directly in the type 3A group, variant 0, as described in 6.2.1 above.

Where the service is encrypted as described in the specification, the source Location Table Number, which contains the codes which were subsequently encrypted, shall be indicated indirectly using bits Z15 to Z10, LTNBE, in the Encryption Administration group. The value of LTN (in type 3A groups) shall be set to 0, to indicate that the service is encrypted.

The LTNBE shall have the range 1 to 63, and the value transmitted shall identify the number of the Location Table the service provider is using. Consequently, the value of LTNBE used on any service shall be country-specific, and additionally may be service provider-specific. The assignment of LTN (and hence

LTNBE) is described in the Annex to ISO 14819-3, and generally is allocated to a service provider by the relevant Government or roads authority in each country.

8.4 Encrypting location codes

Each of the eight Service Key tables contains 32 entries and instructions as to how the original Location code is to be encrypted. The service provider's TMC server applies the instructions according to the table entries for that day's chosen ENCID.

Table 1 — Example Service Key table showing Encryption Parameter Values

ENCID	Rotate right (hex)	Start Bit	XOR value (hex)
0	0	0	0
1	8	1	19
2	4	3	9B
3	C	6	7E
4	2	7	39
...	1	8	4B
31	3	1	AB

As an example of encrypting a location code, Table 2 shows the process of encoding location code 1234 (hex) with the parameters values for ENCID 4 from Table 1.

Table 2 — Encryption of Location code 1234 (hex) using ENCID 4 parameter values

Encryption process	**Bits**	15...12	11...8	7...4	3...0
TMC Server applying bit manipulation according to the values for ENCID 4	Original Location code (hex)	1	2	3	4
	Original Location code expressed in Binary	0001	0010	0011	0100
	Rotate right 2 bits	0000	0100	1000	1101
	39 (hex) starting at bit 7	0001	1100	1000	0000
	Result after XOR operation	0001	1000	0000	1101
Values transmitted	Hence transmitted encrypted Location code (hex)	1	8	0	D
	ENCID Value transmitted in Encryption Administration Group	4			

The service provider shall always use the same Service Key table, but may change the encryption parameters and hence the ENCID once per day, if desired. Any change, however, shall be made only at T04:00 Local Time.

If a change to the ENCID is made, then to prevent the possibility of messages being incorrectly decrypted by applying a wrong ENCID, no other traffic message conveying type 8A group (i.e. those with bits X4 – X0 in the range 00001 – 01111) shall be transmitted between T03:58 and T04:02 local time.

Transmitters on which an RDS-TMC service is provided shall transmit RDS CT (Clock Time) groups (type 4A groups). The time shall be transmitted as UTC ± Local offset.

8.4.1 Test mode

Bits Y12 and Y11 are used to allow service providers and terminal manufacturers to test various aspects of the encryption process.

The four possible states of bits Y12 and Y11 are shown in Table 3:

Table 3 — Use of test bits

Y12	Y11	Meaning
0	0	Location code not encrypted, terminal shall ignore ENCID, and instead shall use encryption parameters with values 0,0,0.
0	1	Location code encrypted, but terminal shall ignore ENCID and instead use encryption parameters pre-advised by the service provider (which of course must be 'pre-stored' within the terminal).
1	0	Reserved for future use.
1	1	Full encryption used as described in this International Standard.

8.4.2 Repetition rate

Although the elements within the Encryption Administration group are relatively static, as described above the ENCID value may change on a daily basis. Consequently, before a terminal is able to decrypt any message, it shall have received an Encryption Administration group previously that day and checked the ENCID to determine the encryption parameters being used on this service. (A day is determined to have begun at T04:00 Local Time – see 8.4).

As different terminals are being turned on at different times throughout the day, the service provider shall transmit this group reasonably frequently. This group should preferably be transmitted at least once (with immediate repetitions) every 10 s. The minimum repetition rate shall be once every 20 s.

9 Access to decrypted services by a terminal

9.1 Terminal manufacturer's basic requirements

In order to offer any RDS-TMC service, the manufacturer of the terminal equipment shall be able to decode the type 3A group variant 0 information primarily to ascertain the Location Table Number in use on that service. In order to produce valid messages, the terminal shall have access to the Location Table identified by that number.

To use an encrypted RDS-TMC service, in addition to the requirements needed for a non-encrypted service, the terminal manufacturer shall have:

— notification from the service provider of the Service Key table being used on a particular service;

— a copy of the appropriate Service Key table, available from the TMC Forum office at ERTICO;

— the ability to decode the Encryption Administration group which details the source Location Table (LTNBE) the codes of which have been encrypted, and the particular Encryption parameters in use on any particular day (ENCID).

These are required in order to be able to decrypt and hence recover the location codes transmitted on the services offered by service providers with whom a commercial arrangement exists.

9.2 Activation of a terminal

It is the intent of this International Standard to allow for every terminal to be individually activated to receive encrypted RDS-TMC services. Theoretically, this allows for a service provider to offer an end-user any combination of RDS-TMC services required and subscription periods, thus fulfilling the requirements of different business models.

Each individual terminal shall be activated by its own PIN code, which is either input by the end-user, or may be pre-loaded into the terminal at manufacture, or any point in the commercial chain according to the business model required.

The PIN code is a numeric or alphanumeric value, computed using manufacturer-specific algorithms, representing:

— the combination of services and subscription periods the terminal is authorized to decode;

— the electronic serial number of the terminal;

— any other manufacturer-required access codes (e.g. theft security code).

Depending on the business model and relationship between business partners, any service provider, the terminal manufacturer or the car industry may be responsible for the PIN code generation and distribution. If the PIN code is assigned by the service provider, the provider must have access to the serial number of the terminal. This can be done by making the serial number available to the end-user or by allowing the service provider to have access to the terminal manufacturer's internal database.

Alternatively, the terminal manufacturer may generate a PIN code on behalf of the service provider.

The length and format of the PIN code, and the algorithm used to generate it, are terminal- and business-model specific, but are calculated from consideration of the following elements:

9.2.1 Serial Number of terminal

As it is the intent to prohibit widespread unauthorized activation of terminals, the electronic serial number of each terminal shall be a parameter that contributes to the determination of each terminal's activation PIN code.

As terminals may have access rights to more than one service, terminal manufacturers and the car industry may wish to keep the serial number of terminals secret. In this case the industrial partner in the chain shall act as trust agent.

The serial number hence is one element used to generate an appropriate PIN code required to activate the terminal.

9.2.2 Access Profile

Another element used in the generation of the PIN code is the Access Profile for each service. The Access Profile is the combination of the following parameters:

— SVK,

— SID,

— LTNBE,

— CC,

— Expiry Date for this particular contract.

NOTE The expiry date may be any date in the future, and obviously if set in the far distance (e.g. 28th Feb 2100), allows in effect for lifetime activation.

A different Access Profile hence exists for each RDS-TMC service and expiry date.

A terminal should be able to store in its memory the parameters for up to 32 Access Profiles. The value of the PIN code input shall determine the combination of services active within a particular terminal.

9.2.3 PIN Code composition

The PIN code is the algorithmic product of:

Serial Number + Access Profile 1 (+ ACP2…+ ACPn) + other (e.g. theft) access codes

The length and format of the resulting PIN code is entirely for manufacturers to determine using their own algorithms. Obviously, manufacturers will design algorithms that produce PIN codes which allow for easy input into their terminals, taking into account their Man-Machine-Interface.

9.2.4 Implementation rules for PIN codes

The PIN code implementation adopted by terminal manufacturers should fulfil the following requirements.

— The addition and activation of new services.

  This mechanism should allow the addition of new services and the modification of existing services, independent of other processes, and therefore it should support entering a full PIN code including all elements described in 9.2.3.

— The re-activation of services for a new subscription period.

  When a terminal must be re-activated for a new subscription period without changing any other service describing elements, it should be designed that only a short PIN code needs to be re-entered. The reduction in size of the PIN code should be encouraged for a subscription extension where no other change to the service combinations is required.

9.3 Identifying an encrypted RDS-TMC service

A terminal identifies that the TMC service on a particular frequency is encrypted by decoding the type 3A group information. The LTN (bits Y5 to Y0) in variant 0 will be set to 000000 if the service is encrypted.

The terminal must not attempt to present any RDS-TMC messages, even if the terminal had a previous knowledge of the LTN in use for that service, without first having decrypted the transmitted location element.

9.4 Decrypting location codes

The decryption process is the reverse of the encryption process described in 8.4.

In order to decrypt the location code, the terminal shall know which Service Key table the service provider is using; shall have a copy of that Service Key table; and shall have received the ENCID code on that service anytime since T04:00 Local Time that day, to advise the particular values in use within that Service Key table.

The decryption process is a series of bit-manipulation processes, requiring knowledge of:

— a value to be used in an XOR operation,

— the positioning of the Start Bit of the value to be used in the XOR operation, and

— a subsequent Bit-wise Rotate Left, by a given number of bits.

Using as an example the same fictitious Service Key table used to illustrate the encryption process, the equivalent derived decryption table is:

Table 4 — Example of decryption parameter values, derived from Encryption table

ENCID	XOR value (hex)	Start Bit	Rotate left (hex)
0	0	0	0
1	19	1	8
2	9B	3	4
3	7E	6	C
4	39	7	2
...	4B	8	1
31	AB	1	3

The bit-manipulation process the terminal requires to recover the location code using the example values used in 8.4 is illustrated in Table 5:

Table 5 — Decryption of location code 180D (hex) using ENCID 4 parameter values

Decryption process	Bits	15...12	11...8	7...4	3...0
Values received	ENCID value from Encryption Administration Group	**4**			
	Encrypted Location Code (hex) received	**1**	**8**	**0**	**D**
	Encrypted Location Code expressed in Binary	0001	1000	0000	1101
Receiver applying bit manipulation according to the values for ENCID 4	39 (hex) starting at bit 7	0001	1100	1000	0000
	Result after XOR operation	0000	0100	1000	1101
	Result after rotating left 2 bits	0001	0010	0011	0100
	Hence recovered Location Code in clear (hex)	1	2	3	4

10 Introduction of Encrypted services

RDS-TMC terminals currently in use, or already in production, were not designed to handle the encryption method specified in this International Standard. However terminals produced in the near future are expected to be designed to be encryption-ready.

Currently, a number of service providers are operating TMC services or intend to do so within the next few months.

Service providers considering adopting the methods of encryption described in this International Standard should be aware of the effect of migrating from a non-encrypted to an encrypted service on the existing installed base, and newly-produced terminals.

10.1 below summarizes the expected terminal responses, and 10.2 presents an interim strategy to introduce a commercial service prior to the general availability of encryption-ready terminals.

10.1 Terminal responses

A distinction can be drawn between “old” terminals (i.e. not encryption-ready) and “new” terminals (i.e. encryption-ready).

Old terminals do not recognize a service with LTN = 0, as this value was specifically excluded in older versions of ISO 14819-1. Old terminals have not been programmed to allow decryption of location codes.

Encryption-ready terminals will be designed to recognize either:

— LTN = n or:

— LTN = 0 (and can read LTNBE = n), which has been introduced in this International Standard.

— In addition, encryption-ready terminals must fulfil the requirements to achieve decryption of the location codes as described in Clause 9 of this International Standard.

Response of both types of terminal to broadcast services can best be summarized by the following truth table:

Table 6 — Terminal responses to unencrypted and encrypted services

	Unencrypted service (LTN ≠ 0)	**Encrypted service (LTN = 0)**
Terminal with no decryption software	Will work as normal for ALERT-C service with no modification needed.	Will not work and “fail silent”. Modification of software needed.
Encryption-ready Terminal	Will work as normal for ALERT-C service with no modification needed.	Will work using encrypted ALERT-C services without further modifications (assuming it has been activated to receive the particular service).

10.2 De facto strategy valid only for service providers wishing to generate revenue, prior to general availability of encryption

This case shall be regarded as a de facto TMC Forum solution valid for an interim period until introduction of full encryption, documented in this International Standard.

Initially, service providers transmit an interim LTN, LTN = n; however another LTN (LTN = m) is used on the CD-ROM within the terminal.

The terminal software program requires a specific line of code to be included such that:

IF CC (Country Code) = z
THEN LTN n = LTN m

The values for z, m and n are service provider-specified.

When the service provider begins encrypted services, transmission becomes LTN = 0 with LTNBE = m.

10.3 Actions for existing providers of unencrypted TMC services

An existing provider of an unencrypted TMC service has two options:

a) To carry on providing unencrypted services (as they already have an existing successful business model). In this case, the installed base of terminals without decryption software shall carry on functioning as before. Encryption-ready terminals that come to the market shall also function correctly and receive the unencrypted services (as long as the SID and LTN in their databases match those of the service, and have been activated for the service).

b) To start a programme of upgrading the existing terminals without decryption software to enable them to receive an encrypted service at a later date. The upgrading of the installed terminals may take place over a wide timescale, as the upgraded terminals shall continue to work with the existing unencrypted service. Upgrading of terminals factory-fitted by the automotive industry could be undertaken at the vehicle's normal (annual) servicing visit.

NOTE Not all the installed receiver base may be presented for modification, especially those supplied and fitted as an after-market product. These receivers fail to work when the service is switched to an encrypted one. It may not be technically possible to upgrade all existing terminals, so obviously these too will fail to work when the service is switched to an encrypted one.

10.4 Actions for potential providers of TMC services

A provider who intends to provide a new TMC service has three options:

a) To use an interim LTN as described in 10.2. This interim solution for early adopters allows generation of revenue without using encryption and new proprietary Location Tables. Decryption-capable terminals will support (in parallel) for a large period interim Location Tables Numbering and decryption. This option avoids the need for implementation of new Location Tables for this interim period. The implementation of a new Location Table will be completed most likely at the same moment decryption-capable terminals become available.

b) To initially provide an unencrypted service. Both terminals without decryption software and those that are encryption-ready can use this. The service provider should plan for, and encourage, the upgrading of receivers without decryption software.

c) To broadcast an encrypted service from day one and appreciate that only encryption-ready receivers will be able to receive the service.

10.5 Timescales

Providers of new TMC services can plan to provide encrypted TMC services as soon as they have been able to secure commercial arrangements with terminal manufacturers to provide sufficient encryption-ready terminals for their service.

Bibliography

[1] TMC FORUM, *TMC Compendium – ALERT-C Coding Handbook F02.1:1999*

ICS 03.220.20; 35.240.60

Price based on 19 pages