European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

TC 278 *Road Transport and Traffic Telematics* **N1342**

FOR PARALLEL TC REVIEW
DEADLINE: 5 JUNE 2002

Title : Draft prEN ISO CD 14819-6 *Traffic and Travel Information (TTI) - TTI Messages via traffic message coding - Part 6: Encryption and condition access for the Radio Data System - Traffic Message Channel ALERT C coding*

Source : WG 4

Date : 2002-04-03

Status : Draft for TC comments, target date 2002-06-05

Note : The members of CEN/TC 278 and ISO/TC 204 are invited to submit their written comments to the secretariat of CEN/TC 278 (jelte.dijkstra@nen.nl), before 5 June 2002.

Please note that this 6th part in the CEN/ISO 18234 series has not yet been registered as a work item in CEN and ISO. All CEN and ISO members are invited to consider their participation in this new work. A minimum of 5 participating members is required for approval of the work item. CEN members can state their position by submitting the form in document CEN/TC278/N1343.

Secretariat: **Nederlands Normalisatie-instituut (NEN)**
Mr. J.A. Dijkstra
Vlinderweg 6
P.O. box 5059
2600 GB Delft
The Netherlands

Telephone : +31 15 2 690 127
Telefax : +31 15 2 690 242
Telex : 38144 nnni nl
E-mail : jelte.dijkstra@nen.nl
WWW : http://www.nen.nl/cen278

TMC Forum xxx
2002-Jan-28

TMC Forum

Traffic and Travel Information;
RDS-TMC using ALERT-C:
TMC Encryption and Conditional Access 3.0/002

FINAL DRAFT

TRAFFIC MESSAGE CHANNEL

TMC Forum

TMC Forum Secretariat

Project Office

ERTICO

Avenue Louise 326

BRUSSELS

B-1050

Tel.: +32 2 4000 700

Fax: +32 2 4000 701

E-mail: a.gutter@mail.ertico.com

Contents

List of Figures and Tables

Intellectual Property Rights

Attention is drawn to the fact that this specification has been developed under the open publication policy of the TMC Forum. All participants have agreed to work under the project conditions. No IPR, in any aspect of this specification, has been declared before bringing ideas or information to this work and NONE has been registered by any active participant in the TMC Forum, in respect of this specification. Publication of this specification through the usual TMC Forum channels has been undertaken, to ensure that it may already be considered 'prior art'.

Foreword

This document, detailing "TMC Encryption and Conditional Access" has been prepared by a Task Force established by the Business Group and Management Group of the TMC FORUM.

The task force was given the remit to develop a specification, which defined a 'light encryption' method for use with ALERT-C coded RDS-TMC messages, using 3A/8A RDS groups.

The starting point for the specification was the proposals tabled by Deutsche Telekom, submitted in response to a call for proposals during summer 2001. The Deutsche Telekom submission had been chosen by the TMC Forum membership as the proposal most closely meeting the requirements detailed in its call for proposals.

No known national standards (identical or conflicting) exist on this subject.

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 [2], [3], [4] ENV ISO 14819-1,2 and 3. In RDS-TMC, TTI messages are conveyed using type 8A groups with the Radio Data System, itself specified in [1] IEC EN 62106:2000.

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 for 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 sixteen 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 other than the most determined 'hacker'. More secure systems were rejected because of the RDS capacity overhead that was required.

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

This specification 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.

1 Scope

This document establishes a method of encrypting certain of the 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 appropriate keys, the information conveyed is virtually worthless.

Before a terminal is able to decrypt the data, the terminal requires two ‘keys’. The first ‘key’ is given in confidence by the service provider to terminal manufacturers with whom they have a commercial relationship; the second ‘key’ is broadcast in the ‘Encryption Administration group’, which is also a type 8A Group. This specification 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 specification 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 References

2.1 Normative references

[1] IEC EN 62106:2000, Specification of the Radio Data System (RDS) for VHF/FM Sound Broadcasting in the Frequency Range from 87,5 to 108,0 MHz

[2] CEN/ISO ENV ISO 14819-1:1999 – 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.

[3] CEN/ISO ENV ISO 14819-2:1999 – 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).

[4] CEN/ISO ENV ISO 14819-3:1999 – Traffic and Traveller Information (TTI), TTI Messages via Traffic Message Coding, Part 3: Location referencing for Radio Data System-Traffic Message Channel (RDS-TMC).

2.2 Informative reference

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

3 Abbreviations

For the purposes of this document, the following abbreviations apply:

ACP	Access Profile
AID	Application IDentification
CC	Country Code
ENCID	ENCryption IDentifier
LTN	Location Table Number
LTNBE	Location Table Number Before Encryption
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	Universal Co-ordinated Time

4 Notation

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

5 Definitions

5.1 General to RDS-TMC

5.1.1 Country Code (CC)

The code assigned to a country to be transmitted as the 1st four bits of the transmitted PI code in a broadcast RDS service (see [1] IEC EN 62106:2000).

5.1.2 Event Description

The 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.

5.1.3 Location

An area, highways segment or point location where the source of the problem is situated.

5.1.4 Location Code

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

5.1.5 Location Table Number (LTN)

A number with the value 0 – 63 used to identify the Location Table used by the service provider. 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.

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 specification.

5.1.6 Other Network (ON)

The notation (ON) is 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. Data about the Other Network(s) can hence be pre-stored in terminal equipment, before tuning to it.

5.1.7 Service Identifier (SID)

Code uniquely identifying a TMC service provided by a service provider.

5.1.8 Service Provider

An organisation that manages any data service, by gathering data, processing data, and selling the data service. The service provider then negotiates for the use of the necessary data bandwidth for transmission with a Broadcaster or Transmission Operator.

5.2 Specific to RDS-TMC Encryption and Conditional Access

5.2.1 Access Profile (ACP)

An Access Profile uniquely describes a particular service and subscription period.

5.2.2 Encryption Identifier (ENCID)

The Encryption Identifier is a value indicating which line in the Service Key table of parameters the service provider is using in the encryption process that day. ENCID is transmitted in type 8A groups.

5.2.3 Expiry Date

The 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).

5.2.4 Location Table Number Before Encryption (LTNBE)

A number with the value 1 – 63 used to identify the Location Table used by the service provider prior to the codes within the table being encrypted for transmission. LTNBE is transmitted in type 8A groups.

5.2.5 'PIN' code

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

5.2.6 Serial Number

An alphanumeric identifier, unique to a terminal (or group of terminals), determined by the manufacturer.

5.2.7 Service Key (SVK)

A 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. The Service Key is NOT transmitted.

6 Application Description

In the sections 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 specification.

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.

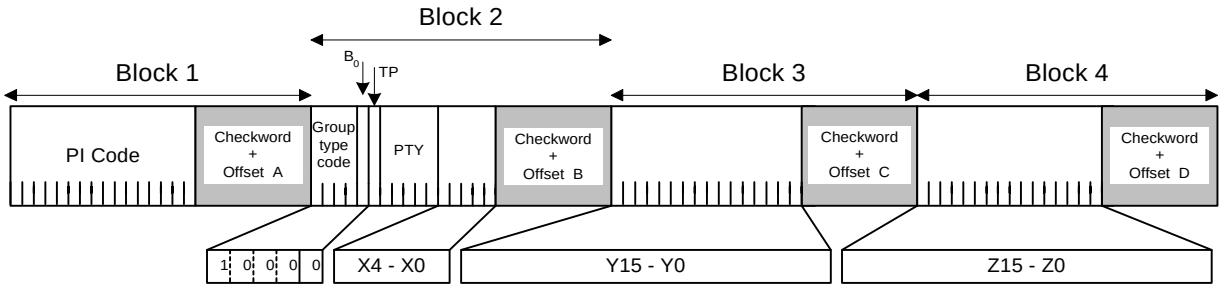

Figure 1: RDS data group

6.2 RDS-TMC and Open Data Application

RDS-TMC using the ALERT-C protocol is defined in [2] ENV ISO 14819-1.

It is an example of a RDS Open Data Application (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 Application IDentification (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 Application IDentification (AID) code for ALERT-C coded RDS-TMC messages is CD46 (hex), indicated in Block 4, bits Z15-Z0. The group type carrying the RDS-TMC data – which by convention is a type 8A group – is given by bits X4 – X0.

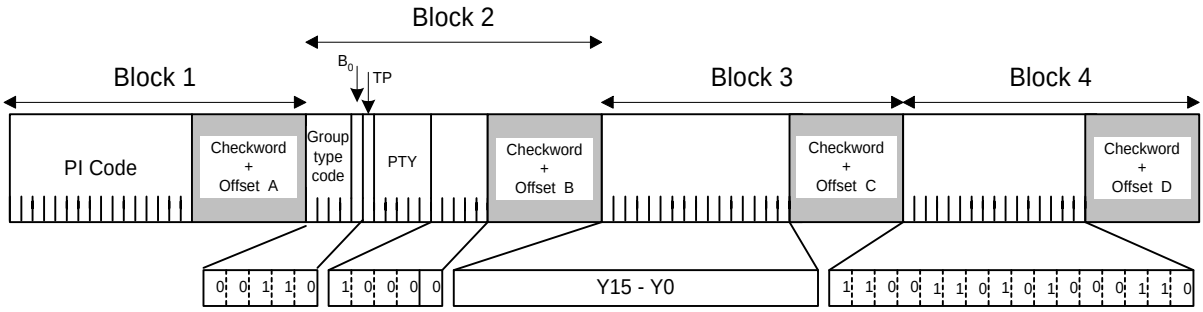

Figure 2: Type 3A group (ODA) – indicating RDS-TMC (CD46 (hex)) carried in group 8A

The bits in Y15 – 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 [2] ENV ISO 14819-1; they are summarised as follows:

6.2.1 Variant 0

In variant 0, bits Y5 –Y0 indicate the Alternative Frequency Indicator (AFI), the Mode of Transmission Indicator (M) and Message Geographical Scope (MGS) elements.

Bits Y11 – Y6 indicate the Location Table Number (LTN) for the service, which in terms of this specification 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 [2] ENV ISO 14819-1, LTN = 0 was an excluded value, and only values 1 – 63 were permitted. This specification 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 a LTN with value '0' in the type 3A group. The Location Table Number used by the service provider, the codes of which are now to be encrypted, is given by the element Location Table Number Before Encryption (LTNBE), transmitted in the Encryption Administration Group, described in 7.2 below.

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

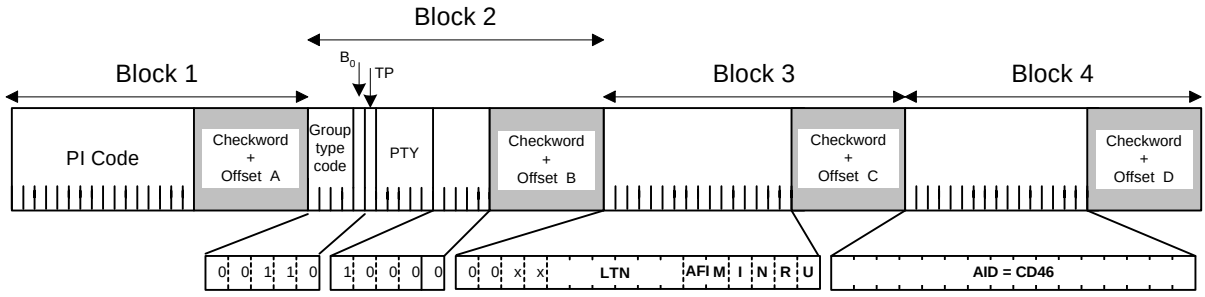

Figure 3: Type 3A group, RDS-TMC variant 0, carrying system information

6.2.1.1 Repetition rate

A type 3A group variant 0 shall be transmitted at least once every five seconds.

6.2.2 Variant 1

In variant 1, bits Y11-Y6 indicate the Service Identifier (SID).

Bits Y13 – Y12, Y5 – Y4, Y3 – Y2 and Y1 – 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 [2] ENV ISO 14819-1.

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

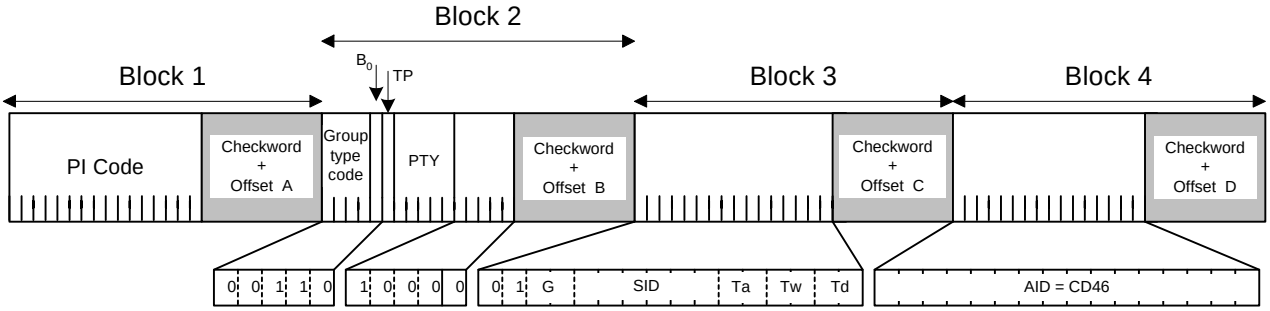

Figure 4: Type 3A group, RDS-TMC variant 1, carrying system information

6.2.2.1 Repetition rate

A type 3A group variant 1 shall be transmitted at least once every ten seconds, as defined in [2] ENV ISO 14819-1.

Using the Service Identifier (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 eleven-bit number represents the event description, a common table being used by all service providers. The list of numbers and associated descriptions are in [3] CEN/ISO ENV ISO 14819-2
- **Location** – indicating the area, highway segment or point of the source of the traffic situation. The location is indicated by a sixteen-bit code. Obviously, the table of locations is country (and may be service provider) specific. In order for a terminal to be able to use the location information, it requires to have a copy of the location table used by the service provider. Each Location Table is referred to by a Location Table Number (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 & 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.

These are fully described in [2] CEN/ISO ENV ISO 14819-1: 1999, and [5] The ALERT-C Coding Handbook, the summary above is included to aid understanding the encryption principles adopted in this specification.

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

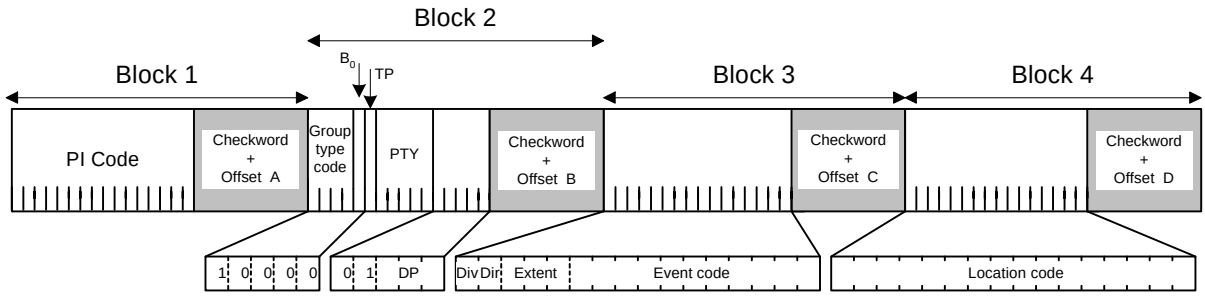

Figure 5: RDS-TMC single group message

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 specification for TMC Encryption and Conditional Access can be described simply as:

- The service provider uses a bit-manipulation technique to encrypt the sixteen 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. 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: a) for a particular service, and b) 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, viz. the parameters use 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, additionally the following are required to be able to offer an encrypted TMC service as specified:

- a copy of one of the eight Service Key Tables, each of which details thirty-two different sets of parameters and values which can be used to encrypt the location codes. 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 – Y0 and Z15 – Z0.

In [2] CEN/ISO ENV ISO14819-1:1999, X4 – X0 = 00000 was an unused bit combination.

This specification 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 – 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.

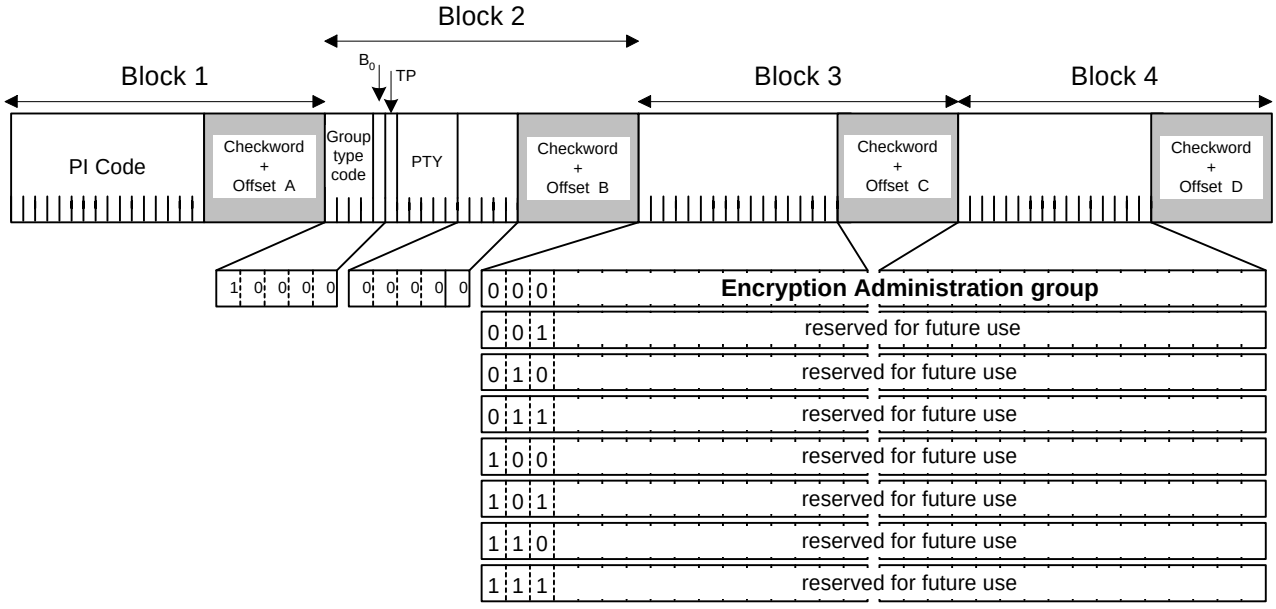

Figure 6: Type 8A group, used for encrypted RDS-TMC, showing variant usage.

8.3 Encryption Administration group

The Encryption Administration group (figure 7) comprises the Service Identifier (SID), the ENCryption Identifier (ENCID) and the Location Table Number Before Encryption (LTNBE). Also included are two test bits.

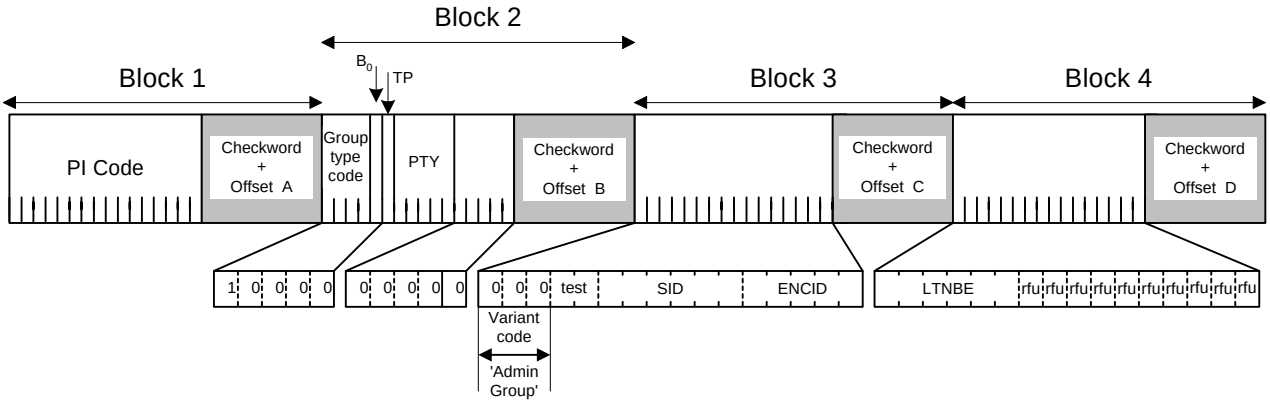

Figure 7: Type 8A group, RDS-TMC Encryption Administration group

8.3.1 Service Identifier (SID)

The **SID** is a six-bit number transmitted in bits Y10 – Y5. The assignment of SID is described in the Annex to [4] CEN/ISO ENV 14819-3:1999, 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 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 Encryption Identifier (ENCID)

To minimise 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 thirty-two 'lines'. Each 'line' gives the values of three parameters used to encrypt the sixteen bits of the location code.

The service provider decides which set of parameters values will be used to encrypt the location codes used for messages transmitted on that particular day. The 'line' in the Service Key table used, is advised to the terminal by the value of variable **ENCID**, transmitted as bits Y4 - 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 specification. Section 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 resultant value is the encrypted location code that is transmitted.

8.3.3 Location Table Number Before Encryption (LTNBE)

In order to provide any RDS-TMC service, non-encrypted or encrypted, it is required that the terminal equipment has a copy of the Location codes used by the service provider. The service provider must transmit the Location Table Number (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 is 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, is indicated indirectly using bits Z15 – Z10, **LTNBE**, in the Encryption Administration group. The value of LTN (in type 3A groups) must be set to '0', to indicate that the service is encrypted.

The **LTNBE** has the range 1 – 63, and the value transmitted identifies the number of the Location Table the service provider is using. Consequently, the value of LTNBE used on any service is Country, and additionally may be service provider, specific. The assignment of LTN (and hence LTNBE) is described in the Annex to [4] CEN/ISO ENV 14819-3:1999, 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 contain thirty-two 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.

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

Table 1: Example Service Key table showing Encryption Parameter Values

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 above, reproduced again here.

ENCID	Rotate right (hex)	Start Bit	XOR value (hex)
4	**2**	**7**	**39**

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**	0**001**	**1100**	**1**000	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**			

Table 2: Showing encryption of Location code 1234 (hex) using ENCID 4 parameter values

8.4.1.1 Changes to the Encryption parameters

The service provider must 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.

It is a requirement that transmitters on which an RDS-TMC service is provided transmit RDS CT (Clock Time) groups (type 4A groups). The time is transmitted as UTC ± Local offset.

8.4.2 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:

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 specification.

Table 3: Use of test bits

8.4.3 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 must 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 8.4.1.1 above).

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

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 must 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 must 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 requires:

- 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;
- to be able 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 specification 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 requires to 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 authorised to decode;
- the electronic serial number of the terminal;
- together with any other manufacturer-required access codes (e.g. theft security code).

Depending on the business model and relationship between business partners, any of the service provider, the terminal manufacturer or the car industry may be responsible for the PIN code generation and distribution. If the PIN code needs to be assigned by the service provider, they must have access to the serial number of the terminal. This can be done by making the serial number available through the end-user or by allowing the service provider to have access to the terminal manufacturers' 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, is terminal and business model specific, but is a value calculated from consideration of the following elements:

9.2.1 Serial Number of terminal

As it is the intent to prohibit widespread unauthorised activation of terminals, it is required that the electronic 'serial number' of each terminal is 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 must 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 (ACP)

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:

- Service Key (SVK)
- Service Identifier (SID)
- Location Table Number Before Encryption (LTNBE)
- Country Code (CC)
- Expiry Date for this particular 'contract'. 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 the parameters for up to 32 Access Profiles in memory. 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:

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

The length and format of the resultant PIN code is entirely for the manufacturer to determine using their own algorithms. Obviously, manufacturers will design algorithms that produce PIN codes that 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 paragraph 9.2.3 above.

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

When a terminal requires to 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 is to 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-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 Location Table Number 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 above.

In order to decrypt the location code, the terminal requires to know which Service Key table the service provider is using; a copy of that Service Key table; and to 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:

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

Table 4: Example Table of Decryption Parameter Values, derived from Encryption table

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

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**	0**001**	**1100**	**1**000	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**

Table 5: Showing decryption of Location code 180D (hex) using ENCID 4 parameter values

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 document. 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, this is before 'encryption-ready' terminals become widely available, which is expected to be in 2003.

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

Para 10.1 below summarises the expected terminal responses, Para 10.2 presents an interim strategy who wish 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 will not recognise a service with LTN = 0, as this value was specifically excluded in [2] CEN/ISO ENV ISO 14819-1:1999. Old terminals will not have been programmed to allow decryption of location codes.

Encryption-ready terminals will be designed to recognise either:

- LTN = n or:
- LTN = 0 (and can read LTNBE = n), which has been introduced in this specification.
- In addition, encryption-ready terminals must fulfil the requirements to achieve decryption of the location codes are described in Section 9 of this specification.

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

	Unencrypted service (LTN ¹ 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)

Table 6: Terminal responses to unencrypted and encrypted services

10.2 De-facto strategy valid only for Service Providers wishing to generate a revenue, prior to general availability of encryption

This case is to be regarded as a de-facto TMC Forum solution valid for a short-term period only until introduction of full encryption, documented in this specification.

Initially service providers transmit an interim Location Table Number, 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:

- 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 will carry on functioning as before. Encryption-ready terminals that come to the market will 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).
- 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 can take place over a wide timescale, as the upgraded terminals will continue to work with the existing un-encrypted service. Upgrading of terminals factory-fitted by the automotive industry could be undertaken at the vehicle's normal (annual) servicing visit.

  Note that not all the installed receiver base may be presented for modification, especially those supplied and fitted as an after-market product. These receivers will fail to work when the service is switched to an encrypted one.

  It may not be possible technically 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:

- To use an interim Location Table Number as described in paragraph 10.2. This short-term 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 implemention of new Location Tables for this short-term period. The implementation of a new Location Table will be completed most likely at the same moment decryption-capable terminals become available.
- 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.
- 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

It is anticipated that upgrading of the existing installed receiver base will take until at least the end of 2003. Consequently it is unlikely that providers of existing unencrypted TMC services will be able to consider switching to an encrypted service until at least then.

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.

Document History

Version	Date	Comment
1.0/001	2001-10-24	Draft for comment produced post Windsor meeting 9th-11th Oct 2001
1.0/002	2001-11-30	Minor editorial alterations as the result of received feedback
2.0/001	2001-12-18	Substantial revisions post meetings on 12th and 17th December
3.0/001	2002-01-21	Substantial revisions post meeting on 11th January 2002 and e-mail comments
3.0/002	2002-01-28	Minor Typographical alterations – status changed to FINAL DRAFT