

First edition  
2006-04-15

---

---

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

Part 6:

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

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

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



Reference number  
ISO 14819-6:2006(E)

© ISO 2006

This is a preview of "ISO 14819-6:2006". [Click here to purchase the full version from the ANSI store.](#)

**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 2006

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of "ISO 14819-6:2006". Click here to purchase the full version from the ANSI store.

## Contents

Page

Foreword.....	iv
Introduction .....	v
1 Scope .....	1
2 Normative references .....	1
3 Terms and definitions.....	2
4 Symbols and abbreviations .....	3
5 Notation .....	4
6 Application description .....	4
6.1 Introduction to RDS group bit pattern and notation .....	4
6.2 RDS-TMC and Open Data Application .....	5
6.3 Summary of TMC data elements in type 8A groups.....	7
7 Principles of the Encryption and Conditional Access methodology .....	8
8 Encryption by the service provider.....	9
8.1 Service provider's requirements.....	9
8.2 Use of type 8A groups for RDS-TMC encryption.....	9
8.3 Encryption Administration group .....	10
8.4 Encrypting location codes.....	12
9 Access to decrypted services by a terminal.....	13
9.1 Terminal manufacturer's basic requirements.....	13
9.2 Activation of a terminal .....	14
9.3 Identifying an encrypted RDS-TMC service .....	15
9.4 Decrypting location codes.....	15
10 Introduction of Encrypted services .....	16
10.1 Terminal responses .....	17
10.2 De facto strategy valid only for service providers wishing to generate revenue, prior to general availability of encryption.....	17
10.3 Actions for existing providers of unencrypted TMC services .....	17
10.4 Actions for potential providers of TMC services.....	18
10.5 Timescales.....	18
Bibliography .....	19

## 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*

This is a preview of "ISO 14819-6:2006". [Click here to purchase the full version from the ANSI store.](#)

## 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.