

Traffic and Travel Information (TTI) — TTI messages via cellular networks —

Part 5: Internal services

ICS 35.240.60

National foreword

This Draft for Development is the official English language version of CEN/TS 14821-5:2003.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature because technology in this area is rapidly evolving. It should be applied on this provisional basis, so that information and experience of its practical application may be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the European organization responsible for its conversion to a European standard. A review of this publication will be initiated 2 years after its publication by the European organization so that a decision can be taken on its status at the end of its 3-year life. Notification of the start of the review period will be made in an announcement in the appropriate issue of *Update Standards*.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into a European standard, to extend the life of the Technical Specification or to withdraw it. Comments should be sent in writing to the Secretary of BSI Technical Committee EPL/278, Road transport informatics, at British Standards House, 389 Chiswick High Road, London W4 4AL, giving the document reference and clause number and proposing, where possible, an appropriate revision of the text.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement European publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

Summary of pages

This document comprises a front cover, an inside front cover, the CEN/TS title page, pages 2 to 104, an inside back cover and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 8 July 2003

© BSI 8 July 2003

ISBN 0 580 42220 8

Amendments issued since publication

Amd. No.	Date	Comments

English version

**Traffic and Travel Information (TTI) - TTI messages via cellular
networks - Part 5: Internal services**

This Technical Specification (CEN/TS) was approved by CEN on 10 May 2001 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

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



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

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

Table of contents

	PAGE
TABLE OF CONTENTS	2
FOREWORD	3
INTRODUCTION	4
1. SCOPE	5
2. NORMATIVE REFERENCES	6
3. DEFINITIONS AND ABBREVIATIONS	7
3.1 Definitions	7
3.2 Abbreviations	9
4. SPECIFICATION OF INTERNAL SERVICES – CONFIGURATION AND MASTER DATA UPDATE	14
4.1 Goal of the Service	14
4.2 Access Management	14
4.3 Master Data Management	14
4.4 Key Management	14
4.5 Function Contents and Handling of Access Management	15
4.6 General	16
4.7 Configuration Request initiated by the Onboard Equipment	16
4.8 Configuration Update sent by the Service Center	17
4.9 Handling Sequence of Access Management	26
4.10 Requirements for the Onboard Equipment	33
4.11 Function Contents and Handling of Master Data Management	34
5. SPECIFICATION OF KEY MANAGEMENT AND SECURITY	36
5.1 Descriptions for Operators	36
5.2 Roles in Key Management	36
5.3 Encryption of User Data	43
5.4 Key Exchange Procedures	48
5.5 Cryptographic Function in the Onboard Equipment	61
6. ADP FOR CAS FUNCTIONALITY -CONFIGURATION AND KEY MANAGEMENT	65
6.1 General Definitions and Information Elements	65
6.2 Configuration Management	67
6.3 Key Management	73
6.4 ADP for CAS Functionality -Configuration and Key Management - Specification in ASN.1	82
7. SPECIFICATION OF DIAGNOSTIC SERVICES	94
7.1 Goal of the Service	94
7.2 Function Contents and Handling of Diagnosis Functions	94
7.3 Communications Flow between On-Board Equipment and TT Call Office	95
7.4 Requirements for the Onboard Equipment	96
8. ADP FOR DIAGNOSTIC SERVICES - GENERAL DEFINITIONS AND INFORMATION ELEMENTS	97
8.1 General	97
8.2 Diagnostic Request Message	97
8.3 Diagnostic Message	99
8.4 ADP for Diagnostic Services - Specification in ASN.1	101
BIBLIOGRAPHY	104

Foreword

This document (CEN/TS 14821-5:2003) has been prepared by Technical Committee CEN/TC 278 "Road transport and traffic telematics", the secretariat of which is held by NEN, in collaboration with Technical Committee ISO/TC 204 "Transport information and control systems".

This technical specification was prepared by Working Group 7 of CEN TC278. In the field of Traffic and Traveller Information, the innovative rate is high, with many research and development projects under way in many countries, and there is a need to establish prospective standards which allow manufacturers to introduce competitive products to the market in the knowledge that they can accommodate the future issues of the standard(s) without fundamental change to equipment.

In accordance with the CEN/CENELEC "Internal Regulations Part 2: Common Rules for standards work, 04-1996" the original copyright holders on the complete set of documents are Mannesmann Autocom GmbH and TEGARON Telematics GmbH. The original copyright holders hereby grant CEN all necessary rights with regard to said original copyrights to execute the standardisation process as described below.

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

CEN/TS 14821 consists of eight parts; one part describing the framework and seven parts providing detailed specifications of all components, protocols and services that are within the scope of CEN/TS 14821.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this CEN Technical Specification: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and the United Kingdom.

Introduction

Traffic and Traveller Information (TTI) may be disseminated through a number of services or means of communication, covering static displays, portable terminals and in-vehicle equipment.

For all such services, the data to be disseminated, and the message structure involved in the various interfaces, require clear definition and standards formats in order to allow competitive products to operate with any received data.

This technical specification focuses on an application data specification whereby data is produced at a central location and is disseminated via a cellular radio network. It addresses the data specifications for both downlink and uplink existing between a central location and randomly located vehicles. It enables messages to be exchanged between different systems and service providers adopting a variety of applications specifications.

Other technical specifications are being produced by the CEN TC278 Working Group 4 to cover TTI dissemination via other means or services. This set of specifications is named GATS (Global Automotive Telematics Standard). GATS provides the modular framework for implementing such traffic telematics services on an open technology platform and is network - independent. In many details definitions are necessary to ensure interoperability. Therefore, those detailed definitions are given in a network-specific part (CEN/TS 14821-8). With the development of future mobile communication systems towards UMTS / IMT2000 the bottleneck of narrow-band data communication might fade. Due to its modular structure, the GATS framework and applications are prepared for that due to its network-independence. The same holds for emerging technologies for positioning which today is almost exclusively based on GPS.

Other relevant standard developments are, independent from telematics, the application-independent Wireless Application Protocol (WAP), enabling mobile access to the Internet. It is understood that these emerging technologies might fit into the framework of telematics applications in future WAP-versions. For the time being, GATS already today independently from WAP enables access to telematics services. Utilisation of GATS on a WAP protocol stack and identifying necessary adaptation of WAP specifications (if any) is currently under investigation of the appropriate groups within WAP-Forum and GATS-Forum.

1. Scope

This CEN/TS defines the specific interfaces and functionality of traffic telematics (TT) services based on the use of cellular networks. Device manufacturers are enabled to develop terminal equipment compatible to services based on this technical specification. This will allow for interoperability of different terminal equipment and service providers which allows competition between service providers and terminal manufacturers. Furthermore it sets the scene for international availability of these services.

This technical specification specifies

- TT-specific interfaces between terminal and service centre. This especially incorporates the message sets of the application data protocols and the service-independent communication handling (including conditional access and transport protocols).
- Functionality, procedures and requirements of basic terminal components as well as their interaction with the service centre. This especially comprises conditional access and security mechanisms.
- Service Specifications, which are essential to ensure consistent behaviour of terminal and service centre.

The services incorporated within this issue comprise:

- breakdown and emergency services
- interactive traffic information services
- broadcast traffic information services
- navigation services (route assistance, route advice, homing)
- operator services
- general information services
- floating car data collection

It is envisaged that future research and development will lead to improvements on the services listed above as well as to the creation of new services. Nevertheless this technical specification provides the framework for seamless integration of new features and services into the existing architecture.

2. Normative references

This Technical Specification incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this Technical Specification only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

ISO/IEC 9797-1	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
ISO/IEC 9797-2:2002	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 10116	<i>Information technology – Security techniques - Modes of operation for an n-bit block cipher</i>
ISO/IEC 10118-1:2000	<i>Information technology - Security techniques – Hash-functions – Part 1: General</i>
ISO/IEC 10118-2	<i>Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher</i>
ISO 11568-3:	<i>Banking - Key management (retail) - Part 3: Key life cycle for symmetric ciphers</i>
PKCS#1: RSA Encryption Standard, RSA Labs Technical Notes, Version 1.5, Nov. 1993	
CCITT, Annex A to CCITT Blue Book Rec. E212	

3. Definitions and abbreviations

3.1 Definitions

For the purposes of this CEN/TS, the following terms and definitions apply:

3.1.1 Attribute (of a Traffic Information Message)

A Traffic Information Message is made up of separate parts that can be called attributes. This includes, for example, an item of information and a length of validity.

3.1.2 Authorisation

Reciprocal proof that the identity provided by the communications partner is valid

3.1.3 Broadcast Service

Data service within a cellular wireless network that allows for mono-directional dissemination of data from a service centre to multiple users in the area of signal reception

3.1.4 Bypass Description

Representation of a Bypass, consisting of a Bypass Hint and/or a Bypass Route.

3.1.5 Bypass Hint

Representation of a hint for a Bypass

3.1.6 Bypass Link

Prominent waypoints on a Bypass Route

3.1.7 Bypass Route

Representation of the route for a Bypass

3.1.8 Cell Broadcast

Broadcast service of the GSM network

3.1.9 Data telegram

Digital message exchanged between two systems

3.1.10 Delivery Notification

Network acknowledgement for successful/ unsuccessful delivery of a message to the mobile device

3.1.11 Functional Road Class

A classification based on the importance of the road element in the connectivity of the total road network

3.1.12 Functional Road Class 0

Motorways

3.1.13 Functional Road Class 1

All non-Motorways that are part of a connection used for nation wide traffic and transport

3.1.14 Geocode

Geocodes are unique identifiers unmistakably defining important points on road networks. Geocodes can be derived from / converted into WGS84 co-ordinates by the algorithm described in CEN/TS 14821-3.

3.1.15 Hardware service agents

Partner companies of the traffic telematics service providers who are authorised to install onboard equipment into vehicles and to maintain it

3.1.16 Homing

Simple form of guidance to destination, in which the direction and straight-line distance of the destination are indicated

3.1.17 Information Element

Information unit of a message

3.1.18 Intersection

Junction of two or more roads

3.1.19 Length of a Speech Report

Length of a Speech Report, including pauses, in tenths of a second

3.1.20 Mobile Originated

Data telegram sent from the onboard equipment to the Service Centre.

3.1.21 Mobile Terminated

Data telegram sent by the Service Centre to the onboard equipment.

3.1.22 Onboard equipment

A system, generally mobile, interacting with the service centre to handle traffic telematics services

3.1.23 Road Junction

Intersection of two or more roads

3.1.24 Route description

Description of a route showing the geometry of street intersections, manoeuvre instructions, street and place names, and geographical co-ordinates

3.1.25 Service centre

System produced by the traffic telematics operators / service providers to handle traffic telematics services

3.1.26 Short Message Service

Packet-based form of data transfer within the GSM network

3.1.27 Speech connection

Communications channel between two systems for the bi-directional transmission of speech

3.1.28 Speech Report

Traffic Information Report transmitted by a speech system

3.1.29 Terminal Device

Generally mobile system interacting with the service centre for implementation of telematics services

3.1.30 TINFO

Traffic Information Report

3.1.31 TINFO Version

Unique identification of a Traffic Message, consisting of a number and a time stamp

3.1.32 Traffic Data

Data for qualification of Traffic Events. This includes:

- Values: speed, traffic flow, traffic density
- Places: position, place designation
- Facts: description of situation

3.1.33 Traffic Event

An occurrence on a road or in an area that is worthy of reporting, such as a traffic jam, wrong-way driver, or fog.

3.1.34 Traffic Information

Technical representation of a Traffic Situation within the onboard equipment, accomplished by a number of Traffic Information Reports.

This Traffic Information can be displayed to the customer via suitable terminals.

3.1.35 Traffic Information Report

Technical representation of a Traffic Event produced by processing traffic data.

Each Traffic Reports uniquely identified by a number, the TINFO ID, a time stamp, the TINFO version.

Note: If the Traffic Event changes, the time stamp changes, but the TINFO ID number does not.

3.1.36 Traffic Situation

The total number of all Traffic Events taking place that deserve reporting within an area. The Traffic Situation is always linked to an area. Thus, for example, an areas could be a conurbation or a geometrically demarcated area; an example is the radius around a point.

3.1.37 Voice connection

Circuit-switched channel between two systems for bi-directional voice transmission

3.1.38 Waypoint

Significant points on the route

3.2 Abbreviations

For the purposes of this CEN/TS, the following abbreviations apply:

3.2.1 % ott

percent of the time

3.2.2 ADP

Application Data Protocol, i.e. a message set for a telematics service

3.2.3 AM

Acknowledge Message

3.2.4 ASN.1

Abstract Syntax Notation

3.2.5 BC

Broadcast

3.2.6 BCS

Broadcast Service

3.2.7 CA

Conditional Access

3.2.8 CAS

Conditional Access and Security

3.2.9 CB

Cellular Broadcast

3.2.10 CBC

Cipher Block Chaining

3.2.11 CLI

Calling Line Identification

3.2.12 CRM

Calling Request Message

3.2.13 CSD

Circuit Switched Data

3.2.14 DES

Data Encryption Standard: symmetrical encryption procedure

3.2.15 DRM

Digital Road Map

3.2.16 DSC

Data Service Centre: depending on the mobile communication network

3.2.17 ELB

Extended Location Block

3.2.18 FCD

Floating Car Data

3.2.19 FCDGM

FCD General Message

3.2.20 FCDPM

FCD Parameter Message

3.2.21 FCDNSM

FCD Notification Set-up Message

3.2.22 FCDRM

FCD Revoke Message

3.2.23 FCDVDSUM

FCD Virtual Detection Site Update Message

3.2.24 GATS

Global Automotive Telematics Standard

3.2.25 GEM

General Error Message

3.2.26 GPS

Global Positioning System NAVSTAR GPS

3.2.27 GSM

Global System for Mobile Communication

3.2.28 IE

Information Element

3.2.29 ICV

Initial Chaining Value

3.2.30 L_max

Max. length of transferable data in **one** data transaction

3.2.31 MAC

Message Authentication Code

3.2.32 MNA

Mobile Network Address

3.2.33 MF

Mandatory Fixed format

3.2.34 MO

Mobile Originated Message

3.2.35 MT

Mobile Terminated Message

3.2.36 MV

Mandatory Variable format

3.2.37 N_min

Minimum number of ELB waypoints

3.2.38 OBU

Onboard Unit, synonymously used telematics device, telematics terminal

CEN/TS 14821-5:2003 (E)

3.2.39 OF

Optional Fixed format

3.2.40 OV

Optional Variable format

3.2.41 PDU

Protocol Data Unit

3.2.42 PFA

Probability of false alarm (i.e. estimated error is too large)

3.2.43 PMD

Probability of missed detection (i.e. estimated error is too small)

3.2.44 RSA

Asymmetrical encryption procedure by Rivest, Shamir and Adleman

3.2.45 SAE

Society of Automotive Engineers, Inc.

3.2.46 SMS

Short Message Service

3.2.47 SMSC

SMS Centre

3.2.48 SV

Space Vehicle

3.2.49 TEG

Telematics Expert Group – Group within the WAP-Forum Ltd.

3.2.50 TINFO

Traffic Information Report

3.2.51 TOC

Telematics Operator Code

3.2.52 TRP

Transport Protocol

3.2.53 TT

Traffic telematics

3.2.54 TTI

Traffic and Traveller Information

3.2.55 TTFF

Time to First Fix

3.2.56 UTC

Universal Time Co-ordinated

3.2.57 VDS

Virtual Detection Site

3.2.58 vel, V

Velocity

3.2.59 VIN

Vehicle Identification Number

3.2.60 WAP

Wireless Application Protocol

3.2.61 WGS84

World Geodetic System

4. Specification of internal services – configuration and master data update

4.1 Goal of the Service

The task of the internal services is

- the administration and diagnosis of functions and parameters for all services,
- the administration of parameters specific to a particular service, and also
- to check onboard equipment basic functionality.

The separate internal services can be summarised in the areas of access management (4.2), in master data management (4.3), and diagnosis (see 8) for onboard equipment basic functionality. The description of the cryptographic procedures required to meet the security requirements and the associated management of cryptographic keys is done within the framework of the Service „Specification of Key Management and Security“ (see 5), a short overview over this topic and its interaction with the internal services is given in 4.4.

4.2 Access Management

The following belong to the functions and parameters covering all services within the framework of access management:

- Management of communication addresses (Short Message and call addresses),
- Conditional Access management
The concept of Conditional Access (CA) means access control management for telematics services. It primarily includes activation/deactivation of individual services or service groups and the assignment of cryptographic methods and keys to the services.
- Service-specific parameter management,
- Management of service language,
- Management of service availability in the case of roaming.

4.3 Master Data Management

This internal service includes the updating of vehicle-related master data for items that were not known at the time of production of the onboard equipment, or which can change during the lifetime of the onboard equipment.

4.4 Key Management

The „Specification of Key Management and Security“ (see 5) covers the security mechanisms for the traffic telematics services between the onboard equipment and the service center. This therefore touches on the application-independent aspects of the use of cryptographic procedures in carrying out the services at the transport level and CAS layer, the associated key allocation is described within the application Key Management (description and ADP). The application-specific parameterization of key use and the management of service-specific authorization profiles can be found in this specification for Internal Services.

The following function areas are looked at in the „Specification of Key Management and Security“:

- Application of cryptographic methods to provide the security of messages, particularly with respect to:
- Message confidentiality
- Message integrity
- Sender identity / authenticity
- Retaining sender anonymity
- Non-Repudiation

For the individual services, differentiated encryption of the application-dependent data for the individual services is used for the various interactive point-to-point and broadcast data messages services.

The security concept is based on the following properties of the onboard equipment:

The keys required to encode or decode the ADP contents are made accessible to the onboard equipment via point to point data message requests within the framework of the „Specifications of Key Management and Security“ (Key Update) in encrypted form.

The keys are stored in a secured environment in the onboard equipment (1st generation without chip card), or in an encryption module (2nd generation with chip card).

Each key can be allocated to one or more applications for use so that each operator can decide independently if he wishes to secure various services with a single unified key or multiple different keys.

4.5 Function Contents and Handling of Access Management

Access management makes available to the onboard equipment all the necessary information within the onboard equipment to process the services properly.

As a rule access management is initiated by the onboard equipment by an request (Configuration Request Message) and acknowledged by an update message (Configuration Update Message) from the service center.

In addition the service center may send Configuration Update Messages without any initiation from the onboard equipment. These messages may be transmitted individually via point-to-point messages or non-individually via broadcast messages.

The internal service access management (Configuration Update) includes the address-related, authorization-related and also parameter-related updates (Address Update, Access Update and Parameter Update respectively) by the onboard equipment via the data communications media. Additional information transmitted refer to the service availability in case of roaming (using telematics services within other countries and/or networks). Figure 1 gives an overview over the configuration information sent by the service center to the onboard equipment. The individual elements and the context of their application are given in the following sections.

The configuration elements shall be stored in the onboard equipment (with equipment of the first generation without chip card) or in the encryption module (in the case of equipment of the second generation with chip card), so that they can be changed only by the traffic telematics service operator.

Individual situations and the data contents that are consequently transmitted are explained in 4.9.2 to 4.9.7. The following describes the contents of the messages.

The access management specified in this and the following parts of CEN/TS 14821 enable telematics service roaming and interoperability, however, it is not within the scope of this GATS-specifications to define the link between the service operators itself.

4.6 General

The service described below is based on the interface specification

ADP-Version = 2

and shall be signaled at the transport layer as:

Application ID = „Configuration Update“

The following parameter timers are relevant for the process control of Access Management Services itself. The depositing and updating of the timers in the terminal device will be handled according to the following specification as well as the initialization process defined in this CEN/TS. The usage of the different timers is explained within the context of the communication procedures.

Table 4-1 : Parameters

Parameter ID	Identifier	Description	Unit	Range	Scale	Default
1	KM_Ctrl	Control parameter for Key Management, not used in this version of GATS	-	0-65535	1	0
2	IS_Ctrl	Control parameter for Access Management, not used in this version of GATS	-		1	0
3	IS_Twait	Timer between a configuration request message and the configuration update message	s	3600	1	240

All parameter will be transmitted from the service center to the onboard unit as absolute values, without any scaling or offset. In the table the given scaling factors, min. and max. values might be used in the onboard unit for compressed data storage, since the parameter update will be carried out with fixed IE-lengths for each parameter.

4.7 Configuration Request initiated by the Onboard Equipment

The onboard equipment's request for parameters is typically made through the Configuration Request Message. The following information shall be included:

- Identification of the country and mobile network the Configuration Update is requested for.
- The desired type of information (addresses and/or CA information and/or parameters).
- Identification of all applications supported by the terminal, including the ADP Version and the most recent address and parameter update states of the onboard equipment, marked on the basis of the update version number. If currently no address / parameter updates are stored in the terminal the corresponding version number shall be set to zero.

Note: In the case of signaling parameter version number 0 for any application the terminal shall apply the default parameter settings defined by the services specification of consideration.

If, in case of a manually triggered Configuration Request, the terminal does not receive a Configuration Update within the waiting period IS_TWwait, the request has to be cancelled. The parameter IS_TWwait itself can be set by a Configuration Update.

4.8 Configuration Update sent by the Service Center

4.8.1 General

The general structure of the Configuration Update Message sent by the service center via point-to-point or broadcast data messages is given in figure 1. It contains the following information elements:

- a variable number of Configuration Blocks (0...255) and
- Each Configuration Block may contain any combination of the following information elements, which can be used by the service center according to the situation:
 - Application Flag: to flag the application-related validity of the following information, optionally service-related or not service-specific.
 - Address Flag: address information included / not included. Transmitted addresses are always related to applications, i.e. the address flag can only be set in combination with the application flag.
 - Access Flag: authorization information included / not included
 - Parameter Flag: parameters included / not included. Transmitted parameters are always related to applications, i.e. the parameter flag can only be set in combination with the application flag.

The information containers hold the following according to the setting of the above-mentioned flags:

- If the Application Flag is set to service-specific, then the Application Container follows with a number of services for which the following information has validity. It includes for each application the Application ID and additional information on the usability of these services abroad.
- If the Address Flag has been set, then the Address Container follows with a number of Address Blocks which include communication addresses and related control information.
- If the Access Flag has been set, then the Access Container follows with authorization and cipher control information.
- If the Parameter Flag has been set, then the Parameter Container follows with service-specific parameters.

Note: optionally a free text for display within the terminal after successful processing of the message. Each Configuration Update Message shall only contain one text element. If more than one is included the last one shall be displayed with the highest priority.

The terminal shall only accept Configuration Update Messages sent by the domestic (master) operator as defined within the initial activation procedure (Key Control Message with Admin_Command = Assign_Operator or Assign_and_Load_Keys). If the terminal receives a Configuration Update Message which changes any of the current service permission (Access Update) or service availability (Address Update) it should actively give a notification to the user (beep, display a popup or so on). A service shall only be marked as available if it is allowed by Access Update and all types of communication addresses necessary for this service are loaded.

If the terminal receives a General Error Message instead of the Configuration Update Message expected (using the same transport context as of the Configuration Request Message) or if the configuration update procedure is terminated without receiving any response (time out) this may cause services to be not available. In the first case the terminal should display the content of the General Error Message, in the second case it should actively give a notification to the user, too.

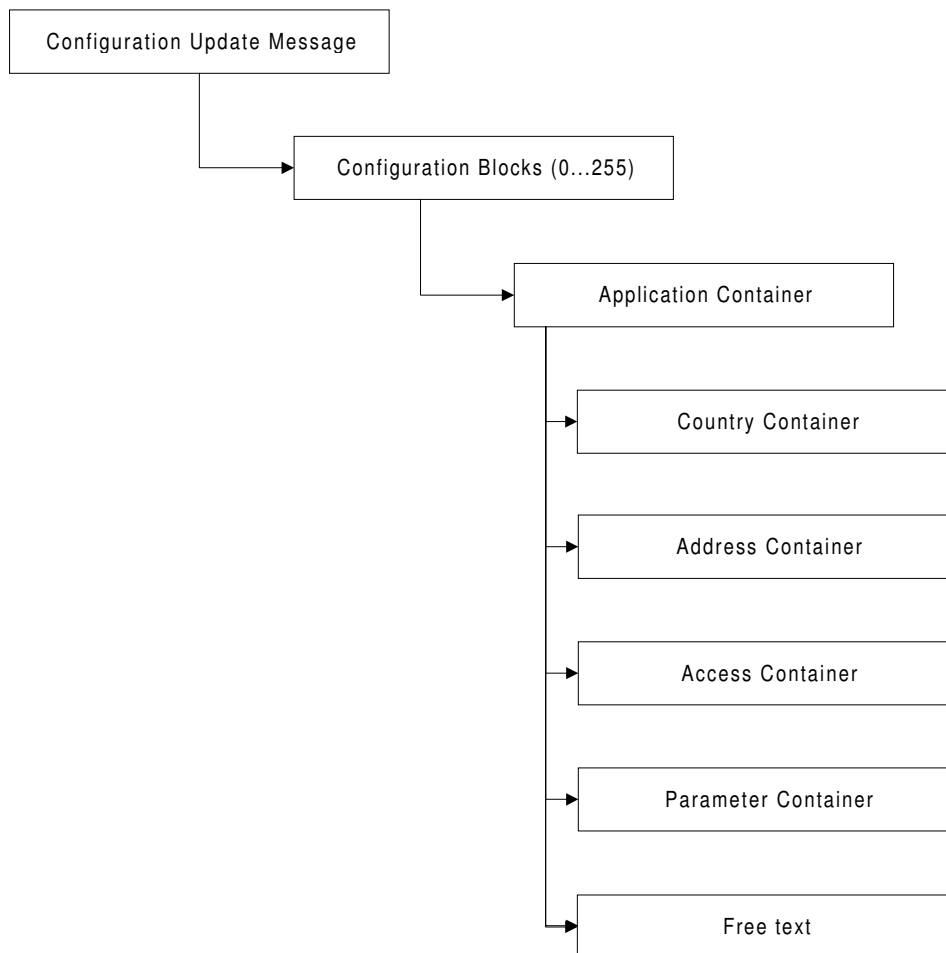


Figure 4-1: General structure of a configuration update message

4.8.2 Application-related and country-related Update validity

The access management for the various services can be identical. Thus an update is described for the service-specific areas of validity. In order to make it possible to use this abroad as well, the relevant neighbouring countries in which a service or a group of services are offered are named as well.

The application elements given in an update message are listed as follows:

- Number of applications for which the following message is valid
- for each Application:
 - Application ID
 - Number of adjacent countries to the location in which TT roaming is possible with the home-based TT operator for the service in question
 - Mobile Country Code / Mobile Network Code

As a rule the terminal shall provide separate configuration table entries (address, access, parameter, language) for all applications supported. Deviations may be defined within the services specification of consideration, e.g. two or more Application IDs may use the same parameter data set and address data set but different access data sets if specified.

4.8.3 Address Management

All the services available within the traffic telematics onboard equipment shall be allocated to addresses by which the communications unit can make queries from the onboard equipment to the service provider or receive messages from the service provider. Over the course of time, the addresses established at the beginning of the introduction of the service may lose their validity. The reasons for this can be, for example, changing structures by the mobile network operator, by the fixed network connections or by the service vendor. It is not possible to make a prediction about any changes to be expected in the addresses.

It cannot be assumed in the case of Mobile Originated queries from the onboard equipment that the recipient address is identical to the sender address in the case of Mobile Terminated replies from the service center. Plausibility checks are made for this reason, and are entered on the base of the address masks for the relevant communications network.

In this case it is necessary that the communications interface of the onboard equipment compares to the sender address in the case of MT messages with the relevant addresses. This check is done specifically to the particular service, this concerns the service Configuration Update itself as well as the services Key Management. Upon receipt of an MT-Message both the primary address as well as the backup address of the corresponding address type (Mobile Network Address, Fixed Network Destination or Call) have to be checked. Hence, an MT-Message has to be accepted if either the primary or the backup address fulfils the check criterion. This is independent of the address used for a preceding MO-Message. Furthermore, in the case of TT Roaming, an MT Message has to be accepted if either the domestic or foreign address fulfils the check criterion.

The Configuration Update service provides mechanisms which allow the service provider to initiate address changes without requiring the customer to take any action on the onboard equipment. These addresses are updated by the Configuration Update service and stored in the onboard equipment in non-volatile memory.

The Configuration Update service also provides additional options to make changes of address for service providers outside one's own country. This will make it possible to make use of traffic telematics services not only within one's own country but also in other countries.

4.8.3.1 Address Types

Multiple addresses with various meanings for service handling are required both in terms of the network and the services offered. Thus when sending data telegrams, alternatively a Mobile Network Address is required in connection with a Large Account (destination) address or only an Mobile Network Address is required when using a virtual Mobile Network Address. In the case of operator-supported services a call number is required in addition. Backup addresses are required for some services which are to be used in the case of particular communication errors. The following address types are therefore defined for use in the onboard equipment:

Table 4-2: Address types

	MNA	MNA-Backup	Destination	Destination-Backup	Call	Call Backup
Meaning	MNA or virtual MNA	MNA or virtual MNA	e.g. Large Account / X.25	e.g. Large Account / X.25	Voice	Voice

Note: In case of emergency services the terminal shall use the standardized emergency number as a hard-coded fall back number in those case where neither Call Address nor the Call Backup Address could be used for a successful setup of a voice connection.

Addresses will be transmitted to the terminal according to data type specification „Address Coding“. This information has to be interpreted as follows:

- If the information element „Validity range of Address“ is set to „unknown“, the following address in the information element „address“ is to be interpreted transparently, i.e. it is to be used for communication without any prefixes. National addresses like „0802 1234567“ as well as international addresses like „+448021234567“ can be used. Hereby, in the case of roaming the terminal cannot check if an address can correctly be used in the current country/net.
- If the information element „Validity range of Address“ is set to „international address“, the following address in the information element „address“ is to be prefixed by „+“. A typical case would be an international address like „44821234567“, where the terminal has to prefix a „+“. International addresses can be used in the domestic as well as in a foreign country.
- If the information element „Validity range of Address“ is set to „national address“, the following address in the information element „address“ is to be interpreted transparently, i.e. it is to be used for communication without any prefixes. A typical case would be a national address like „0821234567“. The international address format „+44821234567“ may be used as well. National addresses can only be used in their country of origin, i.e. the Mobile Country Code and Mobile Network Code as indicated by the module (if available) have to be in accordance with the corresponding values in the address block.

Special conversions of address formats, if required by specific mobile phones at their interface to the telematics onboard equipment, have to be provided by the terminal and are outside the scope of this specification.

4.8.3.2 Comparison Masks for MO and MT Addresses

Since it cannot be assumed that the sender address in the case of mobile terminated messages from the service center is identical to the receiver address in the case of mobile originated messages, masks are used to permit a comparison between these addresses. In this way it is possible to ensure that MT replies are only processed by the onboard equipment if they come from the correct service center, and messages from other origin are ignored by the onboard equipment.

The masks depend on the numbering plan of the network operator, so their parameters depend on the address type.

Table 4-3: Comparison masks for MO and MT addresses

	Address type reference					
	MNA	MNA Backup	Dest.	Dest. Backup	Call Ref.	Call Backup
Mask for MT messages	A	a'	B	b'	C	c'

Various masks can be used (options a, b, c) to check the liability of an MT message by comparison with the sender address stored in the onboard equipment for MO messages for the various address types (MNA, destination, call or their backups):

Example:	MO Mobile Network Address:	„+44821234567“
	MT Mobile Network Address:	„+44821231566“
	Mask:	***DDDDDDDD*DD*
	D	Direct match required
	*	Wildcard

The fixed length address mask bit string is applied to the variable length address string flush right.

For MT-voice calls the address mask is irrelevant since the information will not be routed forward to the telematics unit, nevertheless for extended data services it might be used.

4.8.3.3 Elements of Address Management

An update message includes the address elements listed below:

- Type of address allocation:
New allocation, i.e., all other service-related entries will be deleted or only certain address entries will be replaced
- The version of the overall address update:
this address number will be transferred with each address request message to the service center in order to carry out a comparison with the current address configuration. The version number 0 will not be used by the service center.
- A variable number of address entries with the following layout
 - Type of address entry, optionally
 - Absolute address with additional Address ID by which access is made by the onboard equipment for the service-specific configuration of the address allocation. Thus it is possible to use addresses for multiple services.
 - The Address ID alone as a reference to existing absolute addresses.
 - Comparison mask in the case of absolute address entries.
 - Primary Message Identifier.
 - A code (Network Type) which defines the address to be used as an MNA, Destination or Call address.
 - A code (Backup Flag) which shows whether the following address is to be used as a standard or as a backup.
 - Address data corresponding to the type of entry (Address ID / address and comparison mask in the case of absolute address entries / Primary Message ID and range).

All absolute addresses referenced within a Configuration Update Message shall be transmitted within the same message, because it is impossible to detect which absolute addresses are stored within the onboard unit.

4.8.3.4 Address Organisation in the Onboard Equipment

Since the allocation of individual addresses to the services is not unique, the addresses are referenced in the Configuration Update message (for example, a MNA or Voice Call address can be used for several different services). Thus it is possible to reference a specific address multiple without having to duplicate the transmission. This means that it is necessary to enter so-called address tables in the onboard equipment so that the allocation of the absolute address is given from the combination of the Address ID and network type of the Address Block.

The 6 different address types can thus be organised in the onboard equipment in user tables in such a way that their elements can be referenced several times and their contents, in other words, the numbers, can be changed independently of each other, as seen in the address table shown below:

Example:

Table 4-4: Example of address table

Network Type	Address ID (as reference number)							
	1	2	3	4	5	6	7	8
MNA	No. 1	No. 2	No. 3	No. 4	No. 5	No. 6	No. 7	No. 8
Dest.	No. 1	No. 2	No. 3	No. 4	No. 5	No. 6	No. 7	No. 8
Call	No. 1	No. 2	No. 3	No. 4	No. 5	No. 6	No. 7	No. 8

Each entry no. x indicates an absolute address and the assigned address mask.

Note: Address management in the onboard equipment may be done by a reference table which establishes the context between the services and the absolute addresses. The reference table has a pointer which is service-specific, to the contents of the address tables (see 4.8.3.1). It is thus stored in the onboard equipment or in the encryption module as the case may be (if one exists) in non-volatile memory and is updated by the Configuration Update.

Example: the following table gives a sample layout of an address reference table.

Table 4-5: Example of layout of an address reference table

Application ID	Address type reference					
	MNA	MNA Backup	Dest.	Dest. Backup	Call	Call Backup
TINFO	3	0	0	0	4	5
Breakdown	2	2	1	0	2	3
Emergency call	1	2	1	1	1	3
FCD	4	0	0	0	0	0

Meaning of the fields:

Application ID: Service code

Address types: Reference to the service address (see 4.8.3.1)

If the Address ID equals to zero no absolute address is referred to. The service centre may send an Address Update with Address ID = 0 for a specific service to indicate that the service is currently not available in the network of consideration, regardless of other address sets (see 6.1.1).

Absolute address tables and address reference tables are both managed by the terminal with respect to their validity for different countries, mobile networks and operators (see 6.1.1).

4.8.4 Authorization (Access) Management

The Configuration Update service also includes the management of service authorization and encryption. The authorization required for service use and, if necessary, access to keys for encryption or decryption of the message is transmitted to the onboard equipment via Access Update.

The keys are entered within the framework of the Key Update (see 5 „Specification of Key Management and Security“).

Authorization provides access to the traffic telematics services, insofar as the participant is entitled to use them. It can be understood as a status in which it is possible to handle and bill for a service on a technical and administrative level. The status of the authorization is attained through an activation process which is started from the service center. The result is sent to the onboard equipment in the form of a authorization profile via an encrypted access update message. It is not therefore absolutely essential for the service center to explicitly initiate deactivation within the onboard equipment, since a service will be deactivated at the onboard equipment on exceeding an authorization expiration date. The onboard equipment shall however be in a position to correctly process instructions from the service center to deactivate services.

In addition, in the Access Update the information is supplied as to whether the MO and/or MT communications paths are to be secured. In detail, these are the functions of encryption, signature and identification via the unique Equipment ID. The latter is used in particular to check the access authorisation in the central service administration.

The service authorization profile and the security functions to be used are stored in non-volatile memory in the onboard equipment in the reference tables and specific to the service, but in a way that cannot be manipulated. In detail, the following elements are transferred in encrypted form within the framework of the configuration update per subscribed or freely accessible service:

Access Status: The Access Status has the following allocations:

Table 4-6: Access status

ID	Description	Access	Expiration	Charging Models
0	Default service can be used by any user (MID) without any time limit	yes	date: no SIM: no	undefined
1	Opened service can be used by any user (MID) for a limited subscription time	yes	date: yes SIM: no	undefined
2	Deactivated service status at the terminal after the expiration date has been passed; not set by the service center	no (Configuration Request to be sent)	--	--
3	Denied service blocked by the service center	no	date: yes SIM: no	--

Note 1: The reentering of a SIM-card into the terminal device / mobile device previously used has not to be interpreted as an change of SIM-card.

Note 2: The type of charging should be used by the terminal for customer information, especially in the case of roaming.

The following authorisation combinations are to be provided as factory default settings for the authorisation tables:

Table 4-7: Authorisation combinations

Service	Status
Internal services	Default
Key Management	Default
All other services	Denied

Priority: The service prioritisation is split into

CEN/TS 14821-5:2003 (E)

1. Top priority:
Services of this priority interrupt all other services (e.g., emergency call service)
2. Normal priority:
Service handling is done according to the FIFO principle

The following settings are to be provided as factory defaults for service priority:

Table 4-8: Default service priority

Service	Priority
Internal services	normal
Key Management	normal
Emergency call	top
All other services	Normal

CA expiration date:

The expiration date is to be checked by the terminal for all access status values except Default and Deactivated. The initial value for expiration dates should be set to max. values, i.e. 2053-12-31 23:59:59 (YYYY-MM-DD HH:MM:SS)

Cipher Control Block:

defines the ciphering parameters if the Key Flag is set. It includes:

Key Generation Number:

References the basic key to be used to generate transaction keys

Key Flag:

States whether MO data telegrams between the onboard equipment and the service center are to be encrypted.

Triple DES Flag:

States whether encryption is to be done with a simple DES process and single key length or with a triple DES process with doubled key length. If the Triple DES Flag is set to 1 but if only a single DES key is available, then the Triple DES Flag is set to 0. Consequently encryption will only be done with single DES.

Triple MAC Flag:

States whether the Message Authorization Codes is to be made up with a simple DES process and single key length or with a triple DES process with doubled key length. If the Triple MAC Flag is set to 1 but only a single DES key is available to create the MAC, then the Triple MAC Flag is set to 0. Consequently, the MAC Flag will only be created with a single DES procedure.

MAC Length Flag:

States whether 1 byte or 4 bytes of the Message Authentication Code (MAC) is to be transferred in the case of MO messages.

Equipment ID Flag:

Defines whether data telegrams from the onboard equipment to the service center shall include the Equipment ID. The Equipment ID is given in the CAS layer as needed. In the case of encryption of MO messages (see also Key Flag), the following is done

- if the Equipment ID Flag is set, then an individualised key derivation,
- if the Equipment ID Flag is not set, no individualised key derivation (see also 5: Specification of Key Management and Security).

Padding Flag:

States whether the last bytes of an MO message which does not fill a complete DES block is to be sent unencrypted, or whether this data is to be padded with random data in order to form an additional complete data block for encryption.

The terminal may receive access updates requiring one or more applications to be processed using DES keys which are currently not known by the terminal. In this case the terminal shall send a Key Request Message immediately to make the applications available without error handling during service access.

4.8.5 Parameter Management

Parameters are used in each service which determine the time behaviour or the handling of the service. These can be, for example:

- Limiting values for timers
- Repeating numbers for service inquiries in the case of communication with problems
- Other parameters like switches for control of service procedures

Over the course of time, the timing parameters established in the beginning of the service introduction may lose their validity, since it is possible that there will be changes in the overall system operating times. In such cases the timing parameters shall be adapted. The reasons for changes in the timing parameters of the services could be changes in the transfer times of the Short Messages (depending on the network operator) or changed reaction times of the traffic telematics service center (depending on the server load). It is not possible at this time to predict such changes in the overall system operating times.

All parameters are defined in the relevant service specifications, but the transmission of these parameters is done, however, within the framework of the internal services, since it would be inefficient to do this separately for each service.

The service parameters mentioned above are equipment- and operator-related. In addition, the internal services also include master data maintenance. This covers in contrast individual parameters, which are currently only car-related parameters required by the security services (see 4.11).

4.8.5.1 Parameter Tables

Parameter update is done specifically for each service within the framework of the Configuration Update messages from the service center to the onboard equipment. The parameter sections sent within them consist of the following elements:

- Parameter version number, identifying the parameter set (unique for this service/these services)
- Number of parameters
- Parameter IDs
- Parameter Values

The default values for the service-specific parameters as defined within service specifications shall be set at the factory by the manufacturer of the onboard equipment so that only changes need to be transmitted by Configuration Update.

4.8.6 Language Management

A terminal may support multiple languages for user input and output. In this case it should provide an interface to the user for preferred language selection.

A service center may support multiple languages as well. But there is no guarantee that the preferred language of any user is supported by a specific service center.

The language selection is done by the service center as indicated by the language and indicated in the ADP message header (see CEN/TS 14821-2).

4.8.7 Service-Roaming availability

In order to make it possible to use services abroad conveniently, the relevant countries in which any telematics services are offered are named along with the available TT service providers. This includes preferably but not exclusively the adjacent countries.

- Number of countries in which TT roaming is possible with the home-based TT operator for the service in question. To delete all entries an empty country container is transmitted (number of entries = 0).

- TT Service Provider Mobile Country Code / Mobile Network Code

For all countries service roaming is offered this way the terminal shall enable an automated, but user confirmed configuration update. For countries without explicit roaming support the terminal may offer a user interface to trigger a configuration request manually. This only affects the configuration update service, therefore the handling of roaming availability is not application specific (in contrast to address, access, parameter and language handling).

4.9 Handling Sequence of Access Management

4.9.1 General

Access management (Configuration Update) can be initiated as follows:

1. Initiation by the onboard equipment via Point to Point data message through the Configuration Request Message or Key Confirm Message including a Configuration Request Block.
2. Initiation from the service center, e.g., within the services / customer administration of the traffic telematics operator and transmission of a Configuration Update message via Point to Point data message.
This includes an optional initiation by the user via a speech connection to service center.
3. Sending of Configuration Update messages via broadcast data messages without explicit initiation.

4.9.2 Address-related Configuration Update = Address Update

Efforts are to be made to broadcast the address-related Configuration Update via broadcast data messages so as to minimise communication costs. As well various triggers relating to the onboard equipment and the service center are possible to initiate an individual update through explicit queries. The handling of the Configuration Update service varies according to whether the mobile telephone is subscribed to within the domestic network or within another telephone network. If the mobile telephone is within its domestic network, all address accesses relate to the reference table for the domestic network. If the mobile telephone is subscribed to another network, then all address accesses for Configuration Update relate to the reference tables of the guest network(s).

4.9.2.1 Configuration Update National (domestic networks)

The onboard equipment receives from the service provider a Configuration Update message (via broadcast or point-to-point data messages MT) with address contents. This message contains address modifications for one or more services. The message includes the elements described in 4.8.3.3.

The addresses are allocated to a specific service by an application identifier. The number of service addresses depends on the relevant service, a maximum of 6 different addresses per service are possible (see 4.8.3). After receiving the Configuration Update message, the onboard equipment compares the received Application ID with the one stored in the onboard equipment. If the received Configuration Update message includes an application ID for which authorization has been entered within the onboard equipment, the service address to be changed is overwritten. If the authorization for this service is neither available within the onboard equipment nor granted by the current message, the address change shall be ignored.

The onboard equipment can initiate an Address Update through the Configuration Request Message by inputting the service-specific address version number transmitted within the Address Update. The onboard equipment subsequently receives a valid Configuration Update message via a Point to Point connection from the service provider. This message includes all the addresses for the services referenced in the message; this can apply to all the services subscribed to by the customer or freely accessible services or any desired selection. If the onboard equipment has previously not had any Address Update for a service, then the address version number is pre-initialised with 0. Otherwise, the last stored address version number will be sent along with the queries.

If the terminal receives an Address Update with an Address Version Number changed and not all applications are updated, then the terminal shall clear the relevant entries within the Address Reference Table and block the services missing current addresses.

A terminal may support multiple domestic networks giving the user the opportunity to change the mobile network (by change of SIM card) very flexible. In this case the terminal shall be able to keep at least two

sets of address tables for domestic networks (or more according to the number of networks to be supported). Furthermore it shall check after initial activation (see 4.9.5) which of the required address sets are present and which are left to further updates. All network-specific address sets not transmitted automatically by the service center are to be requested explicitly by the terminal to keep compatibility to terminals without multiple network support.

4.9.2.2 Configuration Update international (guest networks)

In order to be able to use the onboard equipment outside one's own country as well, the above mentioned configuration elements to access the foreign service providers shall also be stored in the onboard equipment. Thus it is essential to keep at least two sets of tables for addresses, access data, service parameters and language information

1. The first set is to be used for the services of the service provider(s) within the domestic network. Additionally it may be used within other networks if applicable (see 6.1.1). If the terminal supports multiple domestic networks this set exists multiple.
2. The second set is to be used for the services of a service provider within a guest network. To avoid toggling the configuration between two or three networks within a country and between two or three countries near the border line (causing extensive communication cost and poor service availability during toggling) it is recommended to provide storage capacity for 10 networks. Table space should be managed by a Last-Recently-Used-Strategy based on countries.

If a mobile telephone registers to an international mobile network, a customer can receive upon making explicit request from the onboard equipment a chargeable Configuration Update (if applicable) for a service provider in this network, insofar as there is information in the onboard equipment on the availability of the services in question for the location at that time (Country Container, see 4.8.7). This procedure is also valid for countries/networks abroad for which no preconfiguration via Country Container has been performed for the terminal device. In both cases a Point to Point Configuration Request Message will be sent (automatically triggered if an appropriate Country Container is available, otherwise manually triggered) to the service center of the domestic service provider. This Configuration Request requires the explicit approval of the user. This message includes the Mobile Country Code (mandatory) and the Mobile Network Code (mandatory) of the network that the mobile phone is currently registered to. The service center then checks which service provider is available for this customer within this network. As a result of this, the onboard equipment receives a Point to Point Configuration Update message. This includes the address and, if applicable, the authorization profile and/or special parameters for access to the international service provider.

The inquiry in the domestic network for the address for a Configuration Update of the international service provider is only required if the telephone is subscribed to a network in which there is no address for an international Configuration Update service.

If the onboard equipment only receives an address for a local Configuration Update, but not for user services, then the onboard equipment will carry out an additional Configuration Update via the local address.

If a customer does not want an international Configuration Update, no request (Configuration Update request) is made to the domestic service provider.

Security-related functions such as, for example, emergency call, shall always use a valid address entry for the country in question. This entry may be the address of the home service provider.

If the terminal receives a Configuration Update with no service permission for a specific country (empty Country Container or Access = Denied) then all address and parameter entries related to that country are deleted.

4.9.3 Authorization-related Configuration Update = Access Update

4.9.3.1 Adaptation to changed service subscriptions

Changes in the access authorisation for the user are administered centrally and a difference notation is made within in the centrally held authorization profile to note that the profile stored within the onboard equipment has not been updated yet. In the case of a Configuration Request Message (or optionally other inquiry) by the corresponding telephone number of the Customer (MID) and/or Equipment ID, a comparison will be made for the onboard equipment used to that moment (Equipment ID) with the authorization profile stored within the service administration. If a difference is found for the current

existing combination of MSISDN and Equipment ID, then a Configuration Update with the changed authorization profile is carried out. Finally, the difference notation is deleted at the service center as long as a network-related N/ACK indicates that a successful transmission has been made.

If the terminal receives a new access profile whilst processing a high priority service (e.g. Emergency Call) it shall be ensured that the activation of the new access profile does not interrupt the high priority service procedure within the terminal.

In the same way it is also possible to initiate a key transfer from the service center, see also the „Specification of Key Management and Security (5).

There is also the option for the customer to examine the profile stored within his onboard equipment. If in his opinion this does not match with the profile subscribed by him then he can query his current profile at the traffic telematics operator by the configuration update via an input at the onboard equipment (see also initialisation). The user shall confirm this process, since he may be liable to extra charges.

4.9.3.2 Handling of service authorization after automatic deactivation in the onboard equipment

If a portion of the authorization profile stored within the onboard equipment ceases to be valid as a result of passing the corresponding expiration date (on the onboard equipment itself the status "Deactivated" is reached), then the onboard equipment automatically requests a current authorization profile from the service center via a Configuration Update Request Message.

If no valid combination of MSISDN and Equipment ID is available for the Access Update, then the access status is set to "Denied" in the update message. Consequently further automatic configuration requests from this onboard equipment will be suppressed until the access status changes to „Deactivated“ again.

Note: The access states "Denied" and "Denied_MSISDN" have got an assigned expiration date too.

If the access status is "Denied" and the onboard equipment has access to Mobile Network-specific data (IMSI, serial number of the SIM card), then a change of the SIM card will change the access status to „Deactivated“ and end the blocking of Configuration Update Requests within the onboard equipment.

If there has been further subscription to the service, then the configuration update message for this service receives a new expiration date.

If the service remains blocked on the basis of the entries in the central customer data base, then the onboard equipment takes one of the access states „Denied“ on the basis of the Configuration Update Message sent back to the equipment depending on the service characteristics. This means that this service can no longer be requested directly from the user within the onboard equipment (e.g., deletion of all service addresses including CA and, if applicable, encryption entries). In this case the terminal should actively give a notification to the user (beep, display a popup or so on).

4.9.4 Parameter-related Configuration Update = Parameter Update

The Parameter Update is used for optimum setting of the service handling in the onboard equipment. The update is carried out as follows:

The onboard equipment receives a Configuration Update Message from the traffic telematics service center with service-specific parameter contents (parameter update). A comparison is made within the onboard equipment with the usable applications. The old parameter set will be overwritten, if applicable. If the service is not authorized in the onboard equipment, the parameter message is ignored.

Apart from the Configuration Update sent out by the traffic telematics service center, the onboard equipment can also send a configuration request message with input of the parameter version number stored within the onboard equipment to the service center. The onboard equipment subsequently receives a valid parameter update message from the service center, and in this case exclusively by point to point data message.

Parameters that are not transmitted remain unchanged. Reset of single parameters to default values has to be done explicitly. If the onboard equipment had not received any parameter update previously, the parameter version shall be pre-initialised with 0 for all services.

The Parameter Version No. is entered by the traffic telematics service center and gives the number of the parameter set currently used within the onboard equipment. It can be read out by a technician and thus used to help in diagnosis.

4.9.5 Initial activation of new onboard equipment

Onboard equipment requires for its first initialisation the address by which the relevant operator Key Management and Configuration Update is to be handled. The initial address information can be provided as follows:

- By the manufacturer if the service provider is known at production.
- At the Point of Sale by the dealer, this should be done preferably by keyboard and display. In the case of onboard equipment without appropriate input capabilities, it shall at least be possible to input the initial address via a device interface.
- By the customer through manual input after being informed of the initial address of his service provider. This should be done preferably by keyboard and display.
- Optionally, the onboard equipment may be set into a position being able to initiate the activation procedure using a Configuration Update Message with initial address information. This message may be sent anonymously (without any equipment-related information, initial address for application „Key Management“ only) by the service center, if requested by the customer or dealer via a hotline call when the onboard equipment is ready to receive. This requires that the onboard equipment is able to process the initial address update first and then to initiate the activation procedure using the address received.
- As another option a data access mechanism may be defined which allows to fetch the initial address information from the SIM card. Such a mechanism may be subject to mutual agreement between equipment manufacturer and telematics operator.

To initiate the activation procedure the onboard equipment sends a request for operator allocation and transfer of the operator master key (Key_Request_Message, see also ADP Key Management and Security), to this initial address. The service center then sends a Key Control Message (or this is initiated by the service center, see item 4 above) which includes the mandatory calling number(s) for Key Management and Configuration Update in an Address Container as defined in this specification for Internal Services. Both services can optionally be handled by a single unified calling number or by separate calling numbers.

Within the framework of operator allocation, onboard equipment without a hardware encryption module will be specifically allocated an operator-specific Temporary Equipment ID (24 bit) which is required for terminal identification and message encryption. The manufacturer-specific Initial Equipment ID (see 5 „Specification of Key Management and Security“) is not affected by this.

In the case of operator allocation of the onboard equipment, the Temporary Equipment ID is assigned by the service center for the onboard equipment making the query and sent in the reply message within the framework of the Key Control Message (see 5 „Specification of Key Management and Security“) to the onboard equipment. Here this Equipment ID is stored permanently.

The Equipment ID is the card ID in the case of equipment with an encryption module. Personalisation is done before sending out the card to the customer. In this case the card carries all operator-specific information needed and the operator allocation procedure may be omitted.

It remains open for the service center to link the transfer of the master and application keys directly with the operator allocation or to do this separately at a later time.

4.9.6 Deregistration of onboard equipment

4.9.6.1 General

If a user no longer wants to make use of equipment that had been used previously (without a replaceable chip card) and which has been allocated to his contract and MSISDN by the service center, the customer shall inform the service operator of this in his own interests (e.g. at the point of sale or, if applicable, by contacting the service center), in order to retain his user-specific service profile, to be able to transfer to another item of onboard equipment if required and to protect against service charging caused by the new equipment user. The service center enters this deregistration of the previous onboard equipment to the service administration so that it will delete all the user-related service authorization for this onboard equipment. The Equipment ID is retained at the service center for security reasons.

From an Equipment point of view a new user can access the still authorized services of the previous user using this onboard equipment, since there is no direct access by the service center to the authorization profile stored in the onboard equipment:

- In the case of interactive services via Point to Point communication, an access check is made immediately by the service administration based on the contract state and authorization profile for the Equipment ID / MSISDN. If the contract state has changed the service center may send a Configuration Update Message with the valid authorization profile or a Key Control Message for deregistration. A new user may be granted access to Point to Point services which have still been authenticated for the previous owner within the onboard equipment, such as emergency call, one time only at no charge.
- In the case of broadcast services, the user does not come directly in contact with the service center, so that he can make use of this at no cost until the expiration date of the authorization of the broadcast service at the latest.

A new user of the old onboard equipment (in case of buying a car including TT equipment) has the option to delete all the TT operator-specific entries, (all the keys, addresses, access and parameters) in a configuration mode. The equipment is now in a reset mode and will not support any services any longer (see 5 „Specification of Key Management and Security“). The user shall be informed by the terminal that the terminal is in reset state (without operator assignment), especially it shall be clarified that security-relevant services (as emergency call) are not available in this state.

4.9.6.2 Onboard equipment without access to network -specific data

In the case of onboard equipment which has no access to the data listed in 4.10.1 (IMSI and the serial numbers of the SIM card), a new user (a MID unknown to the traffic telematics service center) can request information when first using this onboard equipment of the still authorized service of the previous user, since there is no direct access by the service center to the authorization profile stored in the onboard equipment. In the case of interactive services via Point to Point connections, a check is made immediately by the service administration of the authorization profile on the basis of the Equipment ID identified in the onboard equipment and, insofar as the status of this onboard equipment has changed, the valid authorization profile is sent to the vehicle in an additional Configuration Update Message. In the case of exclusive use of broadcast services, the user does not come directly in contact with the service center, so that he can make use of this at no cost until the expiration date of the authorization of the broadcast service at the latest. A new user can likewise make use one time only at no charge of the Point to Point services to be activated, such as emergency call, which has still been authenticated for the previous owner within the onboard equipment.

4.9.6.3 Onboard equipment with access to network-specific data

In the case of onboard equipment which have available the data required as listed within 4.10.1 or adequate substitute data, the onboard equipment will automatically create a new and empty authorization profile on the first use of a SIM card not known up to that point within the onboard equipment, which exclusively offers the default services previously available to the onboard equipment.

The onboard equipment initiates a Configuration Update (Configuration Request Message) to query the current authorization profile for the user at that time and, if necessary, initiates an access update for the transfer of all the required authorization profiles. The user shall confirm this process, since he may be liable for billing.

4.9.7 Communications Handling Sequences

4.9.7.1 General

The handling sequence between the service center and the onboard equipment consists of a Configuration Request Message (if initiated by the terminal), the Configuration Update Message with situation-related data contents. The Configuration Update initiation procedures and the minimum contents of the Configuration Update Message for typical scenarios are summarised in Table 4-9.

In the case of the initial activation of the onboard equipment, the cryptographic keys are entered within the framework of key management (see 5 „Specification of Key Management and Security“) before.

Table 4-9: Communications handling sequences

Trigger event	Initiation	Address contents	CA contents	Parameter contents
Initial activation (4.9.5)	Configuration Request Message or Key Confirm Message (from Terminal to Service center)	X	X*	X
Authorization expired	Configuration Request Message (automatic) from Terminal to Service center		X*	
Use abroad (4.9.2.2)	Configuration Request Message (user confirmed) from Terminal to Service center	X		
Subscription to a new service	Configuration Request Message (manually initiated by user) or profile difference noted by the Service center	X	X*	X
Introduction of new services	From Service center to Terminal via Broadcast	X	X*	X
Address Update via Broadcast (4.9.2.1)	From Service center to Terminal via Broadcast	X		
Deregistration of terminal	Access check in Service center		X or Key Control Message	

Note: X or Key Control Message with symmetrical encryption process for secured transmission from the service center to the onboard equipment

For all Configuration Updates triggered by a request from the terminal the minimum contents of the update message is defined by the contents (flags) within the request message. Based on centrally detected profile differences the service center may send more information than requested by the terminal.