SLOVENSKI STANDARD
SIST EN 300 392-7 V2.3.1:2006

01-september-2006

Prizemni snopovni radio (TETRA) – Govor in podatki (V+D) – 7. del: Varnost

Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security

Ta slovenski standard je istoveten z: EN 300 392-7 Version 2.3.1

ICS:

33.070.10	Prizemni snopovni radio (TETRA)	Terrestrial Trunked Radio (TETRA)

SIST EN 300 392-7 V2.3.1:2006 **en**

ETSI EN 300 392-7 V2.3.1 (2006-06)

European Standard (Telecommunications series)

Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security

Reference
REN/TETRA-06160

Keywords
security, TETRA, V+D

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights 9

Foreword 9

Introduction 10

1 Scope 11
1.1 Security classes 11
1.2 Document layout 12

2 References 12

3 Definitions and abbreviations 13
3.1 Definitions 13
3.2 Abbreviations 15

4 Air Interface authentication and key management mechanisms 16
4.1 Air interface authentication mechanisms 16
4.1.1 Overview 16
4.1.2 Authentication of an MS 17
4.1.3 Authentication of the infrastructure 18
4.1.4 Mutual authentication of MS and infrastructure 18
4.1.5 The authentication key 20
4.1.6 Equipment authentication 20
4.2 Air Interface key management mechanisms 21
4.2.1 The DCK 21
4.2.2 The GCK 22
4.2.3 The CCK 23
4.2.4 The SCK 24
4.2.4.1 SCK association for DMO use 25
4.2.4.1.1 DMO SCK subset grouping 25
4.2.5 The GSKO 28
4.2.5.1 SCK distribution to groups with OTAR 28
4.2.5.2 GCK distribution to groups with OTAR 28
4.2.5.3 Rules for MS response to group key distribution 29
4.2.6 Encrypted Short Identity (ESI) mechanism 29
4.2.7 Encryption Cipher Key 30
4.2.8 Summary of AI key management mechanisms 30
4.3 Service description and primitives 31
4.3.1 Authentication primitives 31
4.3.2 SCK transfer primitives 32
4.3.3 GCK transfer primitives 33
4.3.4 GSKO transfer primitives 34
4.4 Authentication protocol 34
4.4.1 Authentication state transitions 34
4.4.2 Authentication protocol sequences and operations 37
4.4.2.1 MSCs for authentication 38
4.4.2.2 MSCs for authentication Type-3 element 44
4.4.2.3 Control of authentication timer T354 at MS 48
4.5 OTAR protocols 48
4.5.1 CCK delivery - protocol functions 48
4.5.1.1 SwMI-initiated CCK provision 49
4.5.1.2 MS-initiated CCK provision with U-OTAR CCK demand 51
4.5.1.3 MS-initiated CCK provision with announced cell reselection 52
4.5.2 OTAR protocol functions - SCK 52
4.5.2.1 MS requests provision of SCK(s) 53
4.5.2.2 SwMI provides SCK(s) to individual MS 54
4.5.2.3 SwMI provides SCK(s) to group of MSs 56
4.5.2.4 SwMI rejects provision of SCK 58

4.5.3 OTAR protocol functions - GCK 58
4.5.3.1 MS requests provision of GCK 58
4.5.3.2 SwMI provides GCK to an individual MS 60
4.5.3.3 SwMI provides GCK to a group of MSs 62
4.5.3.4 SwMI rejects provision of GCK 63
4.5.4 Cipher key association to group address 64
4.5.4.1 SCK association for DMO 65
4.5.4.2 GCK association 68
4.5.5 Notification of key change over the air 70
4.5.5.1 Change of DCK 72
4.5.5.2 Change of CCK 72
4.5.5.3 Change of GCK 72
4.5.5.4 Change of SCK for TMO 72
4.5.5.5 Change of SCK for DMO 73
4.5.5.6 Synchronization of Cipher Key Change 73
4.5.6 Security class change 73
4.5.6.1 Change of security class to security class 1 74
4.5.6.2 Change of security class to security class 2 74
4.5.6.3 Change of security class to security class 3 74
4.5.6.4 Change of security class to security class 3 with GCK 75
4.5.7 Notification of key in use 75
4.5.8 Notification of GCK Activation/Deactivation 75
4.5.9 Deletion of SCK, GCK and GSKO 75
4.5.10 Air Interface Key Status Enquiry 77
4.5.11 Crypto management group 79
4.5.12 OTAR retry mechanism 80

5 Enable and disable mechanism 80
5.1 General relationships 80
5.2 Enable/disable state transitions 81
5.3 Mechanisms 81
5.3.1 Disable of MS equipment 82
5.3.2 Disable of an subscription 82
5.3.3 Disable of subscription and equipment 82
5.3.4 Enable an MS equipment 82
5.3.5 Enable an MS subscription 82
5.3.6 Enable an MS equipment and subscription 82
5.4 Enable/disable protocol 83
5.4.1 General case 83
5.4.2 Status of cipher key material 83
5.4.2.1 Permanently disabled state 83
5.4.2.2 Temporarily disabled state 84
5.4.3 Specific protocol exchanges 84
5.4.3.1 Disabling an MS with mutual authentication 84
5.4.3.2 Enabling an MS with mutual authentication 85
5.4.3.3 Enabling an MS with non-mutual authentication 86
5.4.3.4 Disabling an MS with non-mutual authentication 88
5.4.4 Enabling an MS without authentication 89
5.4.5 Disabling an MS without authentication 90
5.4.6 Rejection of enable or disable command 90
5.4.7 MM service primitives 91
5.4.7.1 TNMM-DISABLING primitive 91
5.4.7.2 TNMM-ENABLING primitive 92

6 Air Interface (AI) encryption 92
6.1 General principles 92
6.2 Security class 93
6.2.0 Notification of security class 94
6.2.0.1 Security Class of Neighbouring Cells 94
6.2.0.2 Identification of MS security capabilities 95
6.2.1 Constraints on LA arising from cell class 95
6.3 Key Stream Generator (KSG) 95

6.3.1 KSG numbering and selection 95
6.3.2 Interface parameters....96
6.3.2.1 Initial Value (IV)....96
6.3.2.2 Cipher Key 96
6.4 Encryption mechanism 97
6.4.1 Allocation of KSS to logical channels 97
6.4.2 Allocation of KSS to logical channels with PDU association 98
6.4.3 Synchronization of data calls where data is multi-slot interleaved....99
6.4.4 Recovery of stolen frames from interleaved data 100
6.5 Use of cipher keys 100
6.5.1 Identification of encryption state of downlink MAC PDUs 101
6.5.1.1 Class 1 cells....101
6.5.1.2 Class 2 cells....102
6.5.1.3 Class 3 cells....102
6.5.2 Identification of encryption state of uplink MAC PDUs 102
6.6 Mobility procedures 103
6.6.1 General requirements....103
6.6.1.1 Additional requirements for class 3 systems....103
6.6.2 Protocol description....103
6.6.2.1 Negotiation of cipher parameters 103
6.6.2.1.1 Class 1 cells....104
6.6.2.1.2 Class 2 cells....104
6.6.2.1.3 Class 3 cells....104
6.6.2.2 Initial and undeclared cell re-selection....104
6.6.2.3 Unannounced cell re-selection 105
6.6.2.4 Announced cell re-selection type-3....106
6.6.2.5 Announced cell re-selection type-2....106
6.6.2.6 Announced cell re-selection type-1....106
6.6.2.7 Key forwarding 106
6.7 Encryption control....108
6.7.1 Data to be encrypted 108
6.7.1.1 Downlink control channel requirements....108
6.7.1.2 Encryption of MAC header elements....108
6.7.1.3 Traffic channel encryption control....108
6.7.1.4 Handling of PDUs that do not conform to negotiated ciphering mode 109
6.7.2 Service description and primitives....109
6.7.2.1 Mobility Management (MM) 110
6.7.2.2 Mobile Link Entity (MLE)....110
6.7.2.3 Layer 2 112
6.7.3 Protocol functions....112
6.7.3.1 MM 112
6.7.3.2 MLE 112
6.7.3.3 LLC....112
6.7.3.4 MAC 113
6.7.4 PDUs for cipher negotiation 113

Annex A (normative): PDU and element definitions 114

A.1 Authentication PDUs....114
A.1.1 D- AUTHENTICATION demand....114
A.1.2 D- AUTHENTICATION reject....114
A.1.3 D- AUTHENTICATION response....115
A.1.4 D- AUTHENTICATION result....115
A.1.5 U- AUTHENTICATION demand....115
A.1.6 U-AUTHENTICATION reject....116
A.1.7 U-AUTHENTICATION response....116
A.1.8 U-AUTHENTICATION result....117

A.2 OTAR PDUs 117
A.2.1 D-OTAR CCK Provide 117
A.2.2 U-OTAR CCK Demand 117
A.2.3 U-OTAR CCK Result 118
A.2.4 D-OTAR GCK Provide....118

A.2.5 U-OTAR GCK Demand 119
A.2.6 U-OTAR GCK Result 120
A.2.6a D-OTAR GCK Reject 120
A.2.7 D-OTAR SCK Provide 121
A.2.8 U-OTAR SCK Demand 122
A.2.9 U-OTAR SCK Result 122
A.2.9a D-OTAR SCK Reject 122
A.2.10 D-OTAR GSKO Provide 123
A.2.11 U-OTAR GSKO Demand 123
A.2.12 U-OTAR GSKO Result 124
A.2.12a D-OTAR GSKO Reject 124

A.3 PDUs for key association to GTSI 125
A.3.1 D-OTAR KEY ASSOCIATE demand 125
A.3.2 U-OTAR KEY ASSOCIATE status 125

A.4 PDUs to synchronize key or security class change 126
A.4.1 D-CK CHANGE demand 126
A.4.2 U-CK CHANGE result 127

A.4a PDUs to delete air interface keys in MS 128
A.4a.1 D-OTAR KEY DELETE demand 128
A.4a.2 U-OTAR KEY DELETE result 128

A.4b PDUs to obtain Air Interface Key Status 129
A.4b.1 D-OTAR KEY STATUS demand 129
A.4b.2 U-OTAR KEY STATUS response 130

A.5 Other security domain PDUs 130
A.5.1 U-TEI PROVIDE 130
A.5.2 U-OTAR PREPARE 131
A.5.3 D-OTAR NEWCELL 131
A.5.4 D-OTAR CMG GTSI PROVIDE 132
A.5.5 U-OTAR CMG GTSI RESULT 132

A.6 PDUs for Enable and Disable 133
A.6.1 D-DISABLE 133
A.6.2 D-ENABLE 133
A.6.3 U-DISABLE STATUS 134

A.7 MM PDU type 3 information elements coding 134
A.7.1 Authentication downlink 134
A.7.2 Authentication uplink 135

A.8 PDU Information elements coding 135
A.8.1 Acknowledgement flag 135
A.8.2 Address extension 135
A.8.3 Authentication challenge 135
A.8.4 Authentication reject reason 136
A.8.5 Authentication result 136
A.8.6 Authentication sub-type 136
A.8.7 CCK identifier 136
A.8.8 CCK information 136
A.8.9 CCK Location area information 137
A.8.10 CCK request flag 137
A.8.11 Change of security class 137
A.8.12 Cipher parameters 138
A.8.13 CK provision flag 138
A.8.14 CK provisioning information 138
A.8.15 CK request flag 138
A.8.16 Class Change flag 139
A.8.17 DCK forwarding result 139
A.8.18 Disabling type 139
A.8.19 Enable/Disable result 139
A.8.20 Encryption mode 140

A.8.20.1 Class 1 cells 140
A.8.20.2 Class 2 cells 140
A.8.20.3 Class 3 cells 140
A.8.21 Equipment disable 140
A.8.22 Equipment enable 141
A.8.23 Equipment status 141
A.8.23a Explicit response 141
A.8.24 Frame number 141
A.8.25 Future key flag 141
A.8.26 GCK data 142
A.8.27 GCK key and identifier 142
A.8.28 GCK Number (GCKN) 142
A.8.28a GCK Provision result 142
A.8.28b GCK rejected 143
A.8.29 GCK select number 143
A.8.29a GCK Supported 143
A.8.30 GCK Version Number (GCK-VN) 143
A.8.31 Group association 144
A.8.32 GSKO Version Number (GSKO-VN) 144
A.8.33 GSSI 144
A.8.34 Hyperframe number 144
A.8.35 Intent/confirm 144
A.8.36 Void 144
A.8.37 Key association status 144
A.8.38 Key association type 145
A.8.39 Key change type 145
A.8.39a Key delete type 145
A.8.39b Key status type 146
A.8.40 Key type flag 146
A.8.41 KSG-number 146
A.8.42 Location area 146
A.8.43 Location area bit mask 146
A.8.44 Location area selector 147
A.8.45 Location area list 147
A.8.46 Location area range 147
A.8.46a Max response timer value 147
A.8.47 Mobile country code 147
A.8.48 Mobile network code 147
A.8.49 Multiframe number 148
A.8.50 Mutual authentication flag 148
A.8.51 Network time 148
A.8.52 Number of GCKs changed 148
A.8.52a Number of GCKs deleted 148
A.8.52b Number of GCK status 148
A.8.52c Number of GCKs provided 149
A.8.52d Number of GCKs rejected 149
A.8.52e Number of GCKs requested 149
A.8.53 Number of groups 150
A.8.53a Number of GSKO status 150
A.8.54 Number of location areas 150
A.8.55 Number of SCKs changed 150
A.8.55a Number of SCKs deleted 151
A.8.56 Number of SCKs provided 151
A.8.56a Number of SCKs rejected 151
A.8.57 Number of SCKs requested 151
A.8.57a Number of SCK status 152
A.8.57b OTAR reject reason 152
A.8.57c OTAR retry interval 152
A.8.58 OTAR sub-type 153
A.8.59 PDU type 153
A.8.60 Proprietary 154
A.8.61 Provision result 154

A.8.62 Random challenge 154
A.8.63 Random seed 154
A.8.64 Random seed for OTAR 154
A.8.65 Void 155
A.8.66 Response value 155
A.8.67 SCK data 155
A.8.68 SCK information 155
A.8.69 SCK key and identifier 155
A.8.70 SCK Number (SCKN) 156
A.8.71 SCK number and result 156
A.8.72 SCK provision flag 156
A.8.72a Void 156
A.8.72b SCK rejected 156
A.8.73 SCK select number 157
A.8.73a SCK subset grouping type 157
A.8.73b SCK subset number 157
A.8.74 SCK use 158
A.8.75 SCK version number 158
A.8.76 Sealed Key (Sealed CCK, Sealed SCK, Sealed GCK, Sealed GSKO) 158
A.8.77 Security information element 159
A.8.78 Session key 159
A.8.79 Slot Number 159
A.8.80 SSI 159
A.8.81 Subscription disable 160
A.8.82 Subscription enable 160
A.8.83 Subscription status 160
A.8.84 TEI 160
A.8.85 TEI request flag 161
A.8.85a Timeshare cell and AI encryption information 161
A.8.86 Time type 161
A.8.87 Type 3 element identifier 161

Annex B (normative): Boundary conditions for the cryptographic algorithms and procedures 162

B.1 Dimensioning of the cryptographic parameters 167

B.2 Summary of the cryptographic processes 168

Annex C (normative): Timers 170

C.1 T354, authorization protocol timer 170

C.2 T371, Delay timer for group addressed delivery of SCK and GCK 170

C.3 T372, Key forwarding timer 170

Annex D (informative): Bibliography 171

Annex E (informative): Change request history 172

History 173

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Technical Committee Terrestrial Trunked Radio (TETRA).

The present document is part 7of a multi-part deliverable covering the Voice plus Data (V+D), as identified below:

EN 300 392-1: "General network design";

EN 300 392-2: "Air Interface (AI)";

EN 300 392-3: "Interworking at the Inter-System Interface (ISI)";

ETS 300 392-4: "Gateways basic operation";

EN 300 392-5: "Peripheral Equipment Interface (PEI)";

EN 300 392-7: "Security";

EN 300 392-9: "General requirements for supplementary services";

EN 300 392-10: "Supplementary services stage 1";

EN 300 392-11: "Supplementary services stage 2";

EN 300 392-12: "Supplementary services stage 3";

ETS 300 392-13: "SDL model of the Air Interface (AI)";

ETS 300 392-14: "Protocol Implementation Conformance Statement (PICS) proforma specification";

TS 100 392-15: "TETRA frequency bands, duplex spacings and channel numbering";

TS 100 392-16: "Network Performance Metrics";

TR 100 392-17: "TETRA V+D and DMO specifications";

TS 100 392-18: "Air interface optimized applications".

NOTE: Part 10, sub-part 15 (Transfer of control), part 13 (SDL) and part 14 (PICS) of this multi-part deliverable are in status "historical" and are not maintained.

National transposition dates	
Date of adoption of this EN:	26 May 2006
Date of latest announcement of this EN (doa):	31 August 2006
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	28 February 2007
Date of withdrawal of any conflicting National Standard (dow):	28 February 2007

Introduction

The present document differs from version 2.1.1 of the TMO security specification in the following key areas:

- change requests approved against V2.1.1 of the present document have been included;
- the end-to-end encryption clause has been **deleted** (and is available in EN 302 109 [7]);
- rules for key association have been **added**.

The document clause, figure and table numbering complies with the ETSI drafting rules conventions for continuous numbering in SR 001 262 (see bibliography), clause 5.2.1a.

1 Scope

The present document defines the Terrestrial Trunked Radio system (TETRA) supporting Voice plus Data (V+D). It specifies the air interface, the inter-working between TETRA systems and to other systems via gateways, the terminal equipment interface on the mobile station, the connection of line stations to the infrastructure, the security aspects in TETRA networks, the management services offered to the operator, the performance objectives, and the supplementary services that come in addition to the basic and teleservices.

The present part describes the security mechanisms in TETRA V+D. It provides mechanisms for confidentiality of control signalling and user speech and data at the air interface, authentication and key management mechanisms for the air interface.

1.1 Security classes

TETRA security is defined in terms of class. Each class has associated features that are mandatory or optional and are summarized in table 1.

Table 1: Summary of Security features in TETRA by class

Class	Authentication	OTAR	Encryption	Enable-Disable
	Clause 4	Clause 4	Clause 6	Clause 5
1	O	O (see note 3)	-	O
2	O	O	M	O
3	M (see note 1)	M (see note 2)	M	O†

KEY: M = Mandatory
O = Optional
- = Does not apply
† = Recommended

NOTE 1: Authentication is required for generation of DCK.
NOTE 2: OTAR for CCK is mandatory, other key management OTAR mechanisms are optional.
NOTE 3: Required if key material is either distributed in preparation for security class transition, or during cell reselection to a cell of a different security class.

The present document describes a system in which all signalling and traffic within that system comply with the same security class. However, signalling permits more than one security class to be supported concurrently within a SwMI, and movements between these classes are described in the present document. The SwMI shall control the state of AI encryption.

An MS may support one, several, or all security classes. Each cell shall support at any one time one of the following options:

- class 1 only;
- class 2 only;
- class 2 and class 1;
- class 3 only; or
- class 3 and class 1.

Class 2 and class 3 are not permitted to be supported at the same time in any cell.

1.2 Document layout

Clause 4 describes the authentication and key management mechanisms for the TETRA air interface. The following two authentication services have been specified for the air-interface in ETR 086-3 (see bibliography), based on a threat analysis:

- authentication of an MS by the TETRA infrastructure;
- authentication of the TETRA infrastructure by an MS.

Clause 5 describes the mechanisms and protocol for enable and disable of both the mobile station equipment and the mobile station user's subscription.

Air interface encryption may be provided as an option in TETRA. Where employed, clause 6 describes the confidentiality mechanisms using encryption on the air interface, for circuit mode speech, circuit mode data, packet data and control information. Clause 6 describes both encryption mechanisms and mobility procedures. It also details the protocol concerning control of encryption at the air interface.

The present document does not address the detail handling of protocol errors or any protocol mechanisms when TETRA is operating in a degraded mode. These issues are implementation specific and therefore fall outside the scope of the TETRA standardization effort.

The detail description of the Authentication Centre is outside the scope of the present document.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI EN 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

[2] ETSI EN 300 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

[3] Void.

[4] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

[5] ETSI EN 300 812: "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 3: Integrated Circuit (IC); Physical, logical and TSIM application characteristics".

[6] ETSI EN 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

[7] ETSI EN 302 109: "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption".

[8] ETSI EN 300 392-12-22: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 12: Supplementary services stage 3; Sub-part 22: Dynamic Group Number Assignment (DGNA)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Authentication Code (AC): (short) sequence to be entered by the user into the MS that may be used in addition to the UAK to generate K with algorithm TB3

authentication Key (K): primary secret, the knowledge of which has to be demonstrated for authentication

authentication session: period between consecutive successful authentication operations

CCK Identity (CCK-id): identification of the key within an LA

cipher key: value that is used to determine the transformation of plain text to cipher text in a cryptographic algorithm

cipher text: data produced through the use of encipherment

NOTE: The semantic content of the resulting data is not available (see ISO 7498-2 [4]).

class: See security class.

Common Cipher Key (CCK): cipher key that is generated by the infrastructure to protect group addressed signalling and traffic

NOTE: CCK is also used to protection of SSI identities (ESI) in layer 2.

Crypto Management Group (CMG): group of MSs with common key material

decipherment: reversal of a corresponding reversible encipherment (see ISO 7498-2)

Derived Cipher Key (DCK): key generated during authentication for use in protection of individually addressed signalling and traffic

encipherment: cryptographic transformation of data to produce cipher text (see ISO 7498-2)

Encryption Cipher Key (ECK): cipher key that is used as input to the encryption algorithm

NOTE: This key is derived from one of SCK, DCK, MGCK or CCK and modified using an algorithm by the broadcast data of the serving cell.

encryption mode: choice between static (SCK) and dynamic (DCK/CCK) encipherment

encryption state: encryption on or off

end-to-end encryption: encryption within or at the source end system, with the corresponding decryption occurring only within or at the destination end system (defined in EN 302 109)

Extended Group Session Key for OTAR (EGSKO): cipher key used for distribution of keys to groups of MSs

fallback SCK: key used by class 3 system when operating in class 2, for example in a fault or fallback situation

Group Cipher Key (GCK): cipher key known by the infrastructure and MS to protect group addressed signalling and traffic

NOTE: Not used directly at the air interface but modified by CCK to give a Modified Group Cipher Key (MGCK).

Group Session Key for OTAR (GSKO): cipher key used to derive EGSKO for the distribution of keys to groups of MSs

Initialization Value (IV): sequence of symbols that randomize the KSG inside the encryption unit

key association group: set of keys associated with one GSSI at different periods of time