SLOVENSKI STANDARD

PSIST ETS 300 392-7:1999

01-maj-1999

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: **ETS 300 392-7 E1:1996-12**

ICS:

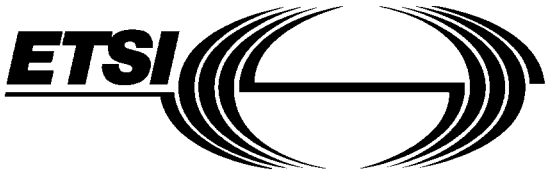
33.070.10	Prizemni snopovni radio (TETRA)	Terrestrial Trunked Radio (TETRA)

PSIST ETS 300 392-7:1999 **en**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST ETS 300 392-7:1999

SIST ETS 300 392-7:1999



EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 392-7

December 1996

Source: ETSI TC-RES

Reference: DE/RES-06001-7

ICS: 33.060, 33.060.50

Key words: TETRA, V+D, security

Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

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

Copyright Notification: No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1996. All rights reserved.

SIST ETS 300 392-7:1999

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

SIST ETS 300 392-7:1999

Contents

Foreword 7

1 Scope 9

2 Normative references 9

3 Definitions and abbreviations 10
3.1 Definitions 10
3.2 Abbreviations 12

4 Air Interface authentication and key management mechanisms 13
4.1 Air interface authentication mechanisms 13
4.1.1 Overview 13
4.1.2 Authentication of a user 13
4.1.3 Authentication of the infrastructure 14
4.1.4 Mutual authentication of user and infrastructure 15
4.1.5 The authentication key 17
4.1.5.1 Generation of K 18
4.1.6 Equipment authentication 18
4.2 Air Interface key management mechanisms 18
4.2.1 The DCK 18
4.2.2 The GCK 19
4.2.3 The CCK 20
4.2.4 The SCK 21
4.2.5 Encrypted Short Identity (ESI) mechanism 22
4.2.6 Summary of AI key management mechanisms 23
4.3 Service description and primitives 24
4.3.1 Authentication primitives 24
4.3.2 SCK transfer primitives 24
4.3.3 GCK transfer primitives 25
4.4 Definition of protocols 26
4.4.1 Authentication state transitions 26
4.4.2 Overview of authentication protocol 27
4.4.2.1 Case 1: SwMI authenticates MS 27
4.4.2.2 Case 2: MS authenticates SwMI 29
4.4.2.3 Case 3: Mutual authentication initiated by SwMI 31
4.4.2.4 Case 4: Mutual authentication initiated by MS 33
4.4.2.5 Case 5: SwMI authenticates MS during registration 35
4.4.2.6 Case 6: MS authenticates SwMI during registration 38
4.4.2.7 Case 7: Mutual authentication initiated by MS during registration 40
4.4.2.8 Case 8: SwMI rejects authentication demand from MS 42
4.4.2.9 Case 9: MS rejects authentication demand from SwMI 42
4.4.3 OTAR protocol functions - CCK 43
4.4.3.1 SwMI-initiated OTAR CCK provision and subsequent SYSINFO-initiated CCK change 43
4.4.3.2 SYSINFO-initiated CCK change and MS-initiated OTAR CCK provision 45
4.4.3.3 MS-initiated OTAR CCK provision during cell re-selection announcement signalling 46
4.4.4 OTAR protocol functions - SCK 47
4.4.4.1 MS requests provision of SCK(s) 47
4.4.4.2 SwMI provides SCK(s) to MS 48
4.4.5 OTAR protocol functions - GCK 49
4.4.5.1 MS requests provision of GCK 49
4.4.5.2 SwMI provides GCK to MS 50
4.4.6 PDU descriptions 51

SIST ETS 300 392-7:1999

4.4.6.1 D-AUTHENTICATION DEMAND 54
4.4.6.2 D-AUTHENTICATION RESPONSE 54
4.4.6.3 D-AUTHENTICATION RESULT 55
4.4.6.4 D-AUTHENTICATION REJECT 55
4.4.6.5 U-AUTHENTICATION DEMAND 55
4.4.6.6 U-AUTHENTICATION RESPONSE 56
4.4.6.7 U-AUTHENTICATION RESULT 56
4.4.6.8 U-AUTHENTICATION REJECT 56
4.4.6.9 D-OTAR CCK Provide 57
4.4.6.10 D-OTAR SCK Provide 57
4.4.6.11 D-OTAR GCK Provide 57
4.4.6.12 U-OTAR CCK Demand 58
4.4.6.13 U-OTAR CCK Result 58
4.4.6.14 U-OTAR SCK Demand 58
4.4.6.15 U-OTAR SCK Result 59
4.4.6.16 U-OTAR GCK Demand 59
4.4.6.17 U-OTAR GCK Result 59
4.4.6.18 U-TEI PROVIDE 60
4.4.7 MM PDU type 3 information elements coding 60
4.4.7.1 Authentication uplink 60
4.4.7.2 Authentication downlink 60
4.4.8 PDU Information elements coding 61
4.4.8.1 Address extension 61
4.4.8.2 Authentication result 61
4.4.8.3 Authentication reject reason 61
4.4.8.4 CCK identifier 61
4.4.8.5 CCK key and identifier 62
4.4.8.6 CCK information for current LA 62
4.4.8.7 CCK provision indicator 62
4.4.8.8 CCK request flag 62
4.4.8.9 GCK key and identifier 63
4.4.8.10 GCK version number 63
4.4.8.11 GSSI 63
4.4.8.12 Location area list 63
4.4.8.13 Location area 63
4.4.8.14 Mobile country code 63
4.4.8.15 Mobile network code 64
4.4.8.16 Mutual authentication flag 64
4.4.8.17 Number of location areas 64
4.4.8.18 Number of SCKs provided 64
4.4.8.19 Number of SCKs requested 65
4.4.8.20 OTAR sub-type 65
4.4.8.21 PDU type 65
4.4.8.22 Proprietary 66
4.4.8.23 Provision result 66
4.4.8.24 Random challenge 66
4.4.8.25 Reject cause 67
4.4.8.26 Random seed 67
4.4.8.27 Response value 67
4.4.8.28 SCK version number 67
4.4.8.29 SCK key and identifier 67
4.4.8.30 SCK number 68
4.4.8.31 SCK number and result 68
4.4.8.32 Sealed Key 68
4.4.8.33 TEI 68
4.4.8.34 TEI information 69
4.4.8.35 TEI request flag 69
4.4.8.36 Type 3 element identifier 69
4.5 Boundary conditions for the cryptographic algorithms and procedures 69
4.6 Dimensioning of the cryptographic parameters 73
4.7 Summary of the cryptographic processes 74

5 Secure enable and disable mechanism 75

SIST ETS 300 392-7:1999

5.1 General relationships 75
5.2 Enable/disable state transitions 76
5.3 Mechanisms 76
5.3.1 Disable of MS equipment 77
5.3.2 Disable of MS subscription 77
5.3.3 Disable an MS subscription and equipment 77
5.3.4 Enable an MS equipment 77
5.3.5 Enable an MS subscription 77
5.3.6 Enable an MS equipment and subscription 78
5.4 Enable/disable protocol 78
5.4.1 General case 78
5.4.2 Specific protocol exchanges 78
5.4.2.1 Disabling an MS using authentication 78
5.4.2.2 Disable an MS without authentication 80
5.4.2.3 Enable an MS using authentication 81
5.4.2.4 Enable an MS without authentication 83
5.4.3 MM service primitives 84
5.4.3.1 TNMM-DISABLING primitive 84
5.4.3.2 TNMM-ENABLING primitive 84
5.4.4 MM PDUs structures and contents 85
5.4.4.1 D-DISABLE 85
5.4.4.2 D-ENABLE 85
5.4.4.3 U-DISABLE STATUS 86
5.4.5 MM Information elements coding 86
5.4.5.1 Address extension 86
5.4.5.2 Authentication challenge 86
5.4.5.3 Disabling type 87
5.4.5.4 Enable/Disable result 87
5.4.5.5 Equipment disable 87
5.4.5.6 Equipment enable 87
5.4.5.7 Equipment status 87
5.4.5.8 Intent/confirm 88
5.4.5.9 PDU Type 88
5.4.5.10 Proprietary 88
5.4.5.11 Subscription disable 88
5.4.5.12 Subscription enable 88
5.4.5.13 Subscription status 89
5.4.5.14 TETRA equipment identity 89

6 Air Interface (AI) encryption 89
6.1 General principles 89
6.1.1 Key Stream Generator (KSG) 90
6.1.2 Encryption mechanism 90
6.1.3 KSG numbering and selection 92
6.1.4 Interface parameters 93
6.1.4.1 Initial Value (IV) 93
6.1.4.2 Cipher Key 93
6.1.5 Use of cipher keys 93
6.1.5.1 Encrypted SwMI types 94
6.1.5.2 Identification of cipher keys 96
6.1.5.3 Change of CCK in an LA 96
6.1.6 Data to be encrypted 97
6.1.6.1 Downlink control channel requirements 97
6.1.6.2 Encryption of MAC header elements 98
6.1.7 Traffic channel encryption control 98
6.2 Mobility procedures 98
6.2.1 General requirements 98
6.2.2 Mobility within a location area 99
6.2.3 Mobility between location areas 99
6.2.4 Cell change with uninterrupted ciphering 100
6.3 Air interface encryption protocol 101
6.3.1 General 101
6.3.1.1 Positioning of encryption process 101

SIST ETS 300 392-7:1999

6.3.1.2 Operation of encryption process 102
6.3.2 Service description and primitives 103
6.3.2.1 Mobility Management (MM) 103
6.3.2.2 Mobile Link Entity (MLE) 103
6.3.2.3 Layer 2 104
6.3.3 Protocol functions 105
6.3.3.1 MM 105
6.3.3.2 MLE 105
6.3.3.3 LLC 105
6.3.3.4 MAC 105
6.3.4 PDUs for cipher negotiation 105

7 End-to-end encryption 106
7.1 Introduction 106
7.2 Voice encryption and decryption mechanism 106
7.2.1 Protection against replay 107
7.3 Data encryption mechanism 107
7.4 Exchange of information between encryption units 108
7.4.1 Synchronization of encryption units 108
7.4.2 Encrypted information between encryption units 109
7.4.3 Transmission 109
7.4.4 Reception 111
7.4.5 Stolen frame format 112
7.5 Location of security components in the functional architecture 113
7.6 End-to-end key management 114

History 115