



**SLOVENSKI STANDARD**  
**DSIST ETS 300 396-6:1999**  
**01-1 1999**

---

Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security

Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security

**Ta slovenski standard je istoveten z: ETS 300 396-6 Edition 1**

---

**ICS:**

33.020	Telekomunikacije na splošno	Telecommunications in general
33.070.10	Prizemni snopovni radio (TETRA)	Terrestrial Trunked Radio (TETRA)

**DSIST ETS 300 396-6:1999** en





**E**UROPEAN  
**T**ELECOMMUNICATION  
**S**TANDARD

**ETS 300 396-6**

April 1998

---

Source: TETRA

Reference: DE/RES-06007-6

ICS: 33.020

**Key words:** Direct Mode, security, TETRA

**Terrestrial Trunked Radio (TETRA);  
Direct Mode Operation (DMO);  
Part 6: 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

**Internet:** [secretariat@etsi.fr](mailto:secretariat@etsi.fr) - <http://www.etsi.fr> - <http://www.etsi.org>

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 1998. All rights reserved.



## Contents

Foreword .....	7
1 Scope .....	9
2 Normative references .....	9
3 Definitions and abbreviations .....	10
3.1 Definitions .....	10
3.2 Abbreviations .....	11
4 Operational Security .....	12
4.1 Single-Hop Calls .....	12
4.2 Multi-Hop Calls .....	13
4.3 Call Synchronization .....	15
4.3.1 Synchronization of calls through a repeater .....	15
4.3.2 Synchronization of data calls where data is multi-slot interleaved .....	16
4.3.2.1 Recovery of stolen frames from interleaved data .....	17
5 Authentication Mechanisms .....	17
5.1 Mobile to mobile operation .....	17
5.2 Dual Watch Operation .....	17
5.3 Gateway mode operation .....	17
6 Air Interface (AI) encryption .....	19
6.1 General principles .....	19
6.2 Key Stream Generator (KSG) .....	19
6.2.1 KSG numbering and selection .....	19
6.3 Encryption mechanism .....	20
6.3.1 Interface parameters .....	20
6.3.1.1 Time Variant Parameter (TVP) .....	20
6.3.1.2 Cipher Key .....	21
6.3.1.3 Identification of cipher keys .....	21
6.3.2 Data to be encrypted .....	21
6.3.2.1 Encryption of MAC header elements .....	21
6.3.2.1.1 DMAC-SYNC PDU encryption .....	23
6.3.2.1.2 DMAC-DATA PDU encryption .....	24
6.3.2.2 Traffic channel encryption control .....	24
6.4 AI encryption protocol .....	24
6.4.1 General .....	24
6.4.1.1 Positioning of encryption process .....	25
6.4.2 Service description and primitives .....	25
6.4.2.1 DMCC-ENCRYPT primitive .....	27
6.4.2.2 DMC-ENCRYPTION primitive .....	28
6.4.3 Protocol Functions .....	28
7 Air Interface (AI) key management mechanisms .....	29
7.1 Key numbering and storage .....	29
7.2 Over The Air Rekeying .....	29
7.3 OTAR service description and primitives .....	30
7.3.1 SCK transfer primitives .....	30
7.4 OTAR SCK protocol functions .....	30
7.4.1 OTAR protocol models .....	32
7.5 OTAR Protocol MSCs .....	33
7.5.1 Case 1: KU requests key from KH .....	33
7.5.2 Case 2: KU requests key from KH acting as a relay for KSL .....	34
7.5.3 Case 3: KH distributing SCK unsolicited .....	35
7.5.4 Case 4: Error scenarios with SDS timeout from KU or KH .....	36

	7.5.5	Case 5: Error scenarios where KH provides no keys in response to demand.....	37
7.6		PDU descriptions.....	37
	7.6.1	OTAR SCK Provide .....	38
	7.6.2	OTAR SCK Demand.....	38
	7.6.3	OTAR SCK Result .....	39
7.7		PDU Information elements coding .....	39
	7.7.1	Address extension .....	39
	7.7.2	ITSI .....	39
	7.7.3	ITSI flag .....	40
	7.7.4	Mobile country code.....	40
	7.7.5	Mobile network code.....	40
	7.7.6	Number of SCKs provided.....	40
	7.7.7	Number of SCKs requested.....	41
	7.7.8	OTAR SCK sub-type.....	41
	7.7.9	Proprietary .....	41
	7.7.10	Provision result .....	41
	7.7.11	Random seed (OTAR).....	42
	7.7.12	SCK key and identifier .....	42
	7.7.13	SCK number .....	42
	7.7.14	SCK number and result .....	42
	7.7.15	SCK version number.....	43
	7.7.16	Sealed Key.....	43
	7.7.17	Session key (OTAR).....	43
	7.7.18	Short subscriber identity .....	43
8		Secure Enable and Disable mechanism.....	43
	8.1	Overview .....	43
	8.2	General relationships .....	44
	8.3	Enable/Disable state transitions .....	45
	8.4	Mechanisms.....	45
	8.4.1	Disable of MS equipment.....	46
	8.4.2	Disable of MS subscription .....	46
	8.4.3	Disable an MS subscription and equipment .....	46
	8.4.4	Enable an MS equipment .....	46
	8.4.5	Enable an MS subscription .....	46
	8.4.6	Enable an MS equipment and subscription .....	46
	8.5	Enable/disable authentication mechanism.....	47
	8.6	Enable/Disable service description and primitives .....	47
	8.6.1	Enable/Disable primitives .....	47
	8.7	Enable - disable protocol.....	49
	8.7.1	General Case.....	49
	8.7.2	Enable-Disable protocol models.....	49
	8.7.3	Specific Protocol Exchanges .....	50
	8.7.3.1	Successful disabling of a target with mutual authentication.....	51
	8.7.3.2	Successful enabling of a target with mutual authentication .....	52
	8.7.3.3	Successful delivery of TEI with mutual authentication .....	54
	8.7.3.4	Rejection of ENDIS command .....	55
	8.7.3.5	Authentication failure during ENDIS exchange.....	56
	8.7.4	Protocol messages .....	57
	8.7.4.1	ENDIS COMMAND .....	57
	8.7.4.2	ENDIS AUTHENTICATE .....	57
	8.7.4.3	ENDIS COMMAND CONFIRM .....	57
	8.7.4.4	ENDIS RESULT .....	58
	8.7.4.5	ENDIS TEI PROVIDE .....	58
	8.7.4.6	ENDIS REJECT .....	58
	8.7.5	Information elements coding .....	59
	8.7.5.1	Address extension .....	59
	8.7.5.2	Authentication challenge.....	59
	8.7.5.3	Authentication response.....	59
	8.7.5.4	Authentication result.....	59
	8.7.5.5	Command .....	60

	8.7.5.6	Enable/Disable result.....	60
	8.7.5.7	ENDIS PDU type .....	60
	8.7.5.8	Equipment status.....	61
	8.7.5.9	ITSI .....	61
	8.7.5.10	Mobile country code.....	61
	8.7.5.11	Mobile network code.....	61
	8.7.5.12	Proprietary .....	61
	8.7.5.13	Random seed .....	62
	8.7.5.14	Reject reason .....	62
	8.7.5.15	Session key .....	62
	8.7.5.16	Short subscriber identity .....	62
	8.7.5.17	Subscription status .....	63
	8.7.5.18	TETRA equipment identity.....	63
9		End-to-end encryption .....	63
	9.1	Introduction .....	63
	9.2	Voice encryption and decryption mechanism .....	63
	9.2.1	Protection against replay .....	64
	9.3	Data encryption mechanism .....	65
	9.4	Exchange of information between encryption units .....	65
	9.4.1	Synchronization of encryption units.....	65
	9.4.2	Encrypted information between encryption units.....	66
	9.4.3	Transmission.....	67
	9.4.4	Reception .....	69
	9.4.5	Stolen frame format.....	69
	9.5	Location of security components in the functional architecture .....	70
	9.6	End-to-end Key Management.....	72
	Annex A (normative):	Protocol mapping between V+D and DMO for gateway operations .....	73
	A.1	OTAR mapping .....	73
	A.1.1	DM-GWAY requests provision of SCK(s) from SwMI on behalf of a DM-MS.....	73
	A.2	Enable-Disable mapping .....	75
	A.2.1	DM-GWAY acting as intermediary in Secure enable/disable procedure .....	75
	A.2.1.1	Disable .....	75
	A.2.1.2	Enable .....	77
	History.....		79

Blank page