SLOVENSKI STANDARD

PSIST ETS 300 393-7:1999

01-maj-1999

Radijska oprema in sistemi (RES) - Vseevropski sistem snopovnega radia (TETRA) - Optimiran sistem za prenos paketiranih podatkov (PDO) - 7. del: Varnost

Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 7: Security

Ta slovenski standard je istoveten z: ETS 300 393-7 E1:1997-05

ICS:

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

PSIST ETS 300 393-7:1999 en

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

SIST ETS 300 393-7:1999

EUROPEAN
TELECOMMUNICATION
STANDARD

ETS 300 393-7

May 1997

Source: ETSI TC-RES

Reference: DE/RES-06004-7

ICS: 33.020

Key words: TETRA, PDO, SECURITY

Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); 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 1997. All rights reserved.

SIST ETS 300 393-7:1999

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 300 393-7:1999

Contents

Foreword 5

1 Scope 7

2 Normative references..7

3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 8

4 Air Interface authentication and key management mechanisms 8
4.1 Air interface authentication mechanisms..8
4.1.1 Overview...8
4.1.2 Authentication of a user..9
4.1.3 Authentication of the infrastructure...10
4.1.4 Mutual authentication of user and infrastructure 11
4.1.5 The authentication key 13
4.1.5.1 Generation of K...13
4.1.6 Equipment authentication...14
4.2 Service Description and Primitives 14
4.2.1 BS Authentication primitives...14
4.2.2 MS Authentication primitives 15
4.3 Definition of Protocols...16
4.3.1 Authentication State Transitions..16
4.3.2 Overview of authentication protocol 17
4.3.2.1 Case 1: RPDI authenticates MS 17
4.3.2.2 Case 2: MS authenticates RPDI 18
4.3.2.3 Case 3: Mutual authentication initiated by RPDI..18
4.3.2.4 Case 4: Mutual authentication initiated by MS...20
4.3.2.5 Case 5: RPDI authenticates MS during registration 21
4.3.2.6 Case 6: MS authenticates RPDI during registration 22
4.3.2.7 Case 7: Mutual authentication initiated by MS during registration 23
4.3.2.8 Case 8: RPDI rejects authentication demand from MS.......25
4.3.2.9 Case 9: MS rejects authentication demand from RPDI.......26
4.3.3 PDU descriptions..26
4.3.3.1 D-AUTHENTICATION DEMAND..29
4.3.3.2 D-AUTHENTICATION RESPONSE 29
4.3.3.3 D-AUTHENTICATION RESULT 30
4.3.3.4 D-AUTHENTICATION REJECT 30
4.3.3.5 U-AUTHENTICATION DEMAND..30
4.3.3.6 U-AUTHENTICATION RESPONSE 31
4.3.3.7 U-AUTHENTICATION RESULT 31
4.3.3.8 U-AUTHENTICATION REJECT 31
4.3.3.9 U-TEI PROVIDE 32
4.3.4 MM PDU type 3 information elements coding 32
4.3.4.1 Authentication uplink...32
4.3.4.2 Authentication downlink 32
4.3.5 PDU Information elements coding 33
4.3.5.1 Address extension 33
4.3.5.2 Authentication result 33
4.3.5.3 Authentication reject reason 33
4.3.5.4 Mobile country code..33
4.3.5.5 Mobile network code...33
4.3.5.6 Mutual authentication flag...34
4.3.5.7 PDU type 34
4.3.5.8 Proprietary 34

SIST ETS 300 393-7:1999

4.3.5.9 Random challenge 34
4.3.5.10 Reject cause 35
4.3.5.11 Random seed 35
4.3.5.12 Response value 35
4.3.5.13 TEI 35
4.3.5.14 TEI information 35
4.3.5.15 TEI request flag 36
4.3.5.16 Type 3 element identifier 36
4.4 Boundary conditions for the cryptographic algorithms and procedures 36
4.5 Dimensioning of the cryptographic parameters 38
4.6 Summary of the cryptographic processes 39

5 Secure Enable and Disable mechanism 39
5.1 General relationships 39
5.2 Mechanisms 40
5.3 Service description and primitives 40
5.4 Definition of enable-disable protocol 41
5.4.1 Enable/Disable state transitions 41
5.4.2 Overview of enable-disable protocol 42
5.4.2.1 Disabling an MS using authentication 43
5.4.2.2 Enabling an MS using authentication 44
5.4.3 MM PDUs structures and contents 45
5.4.3.1 D-DISABLE 46
5.4.3.2 D-ENABLE 46
5.4.3.3 U-DISABLE STATUS 47
5.4.4 MM Information elements coding 47
5.4.4.1 Address extension 47
5.4.4.2 Authentication challenge 47
5.4.4.3 Disabling type 47
5.4.4.4 Enable/disable result 48
5.4.4.5 Equipment disable 48
5.4.4.6 Equipment enable 48
5.4.4.7 Equipment status 48
5.4.4.8 Intent/confirm 49
5.4.4.9 PDU Type 49
5.4.4.10 Proprietary 49
5.4.4.11 Subscription disable 49
5.4.4.12 Subscription enable 49
5.4.4.13 Subscription status 50
5.4.4.14 TETRA equipment identity 50

History 51

SIST ETS 300 393-7:1999

Foreword

This European Telecommunication Standard (ETS) has been produced by the Radio Equipment and Systems (RES) Technical Committee of the European Telecommunications Standards Institute (ETSI).

This ETS is a multi-part standard and will consist of the following parts:

Part 1:	"General network design".
Part 2:	"Air Interface (AI)".
Part 7:	**"Security".**
Part 10:	"SDL Model of Air Interface", (DE/TETRA-04004-10).
Part 11:	"PICS Proforma", (DE/TETRA-04004-11).

Transposition dates	
Date of adoption:	2 May 1997
Date of latest announcement of this ETS (doa):	31 August 1997
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	28 February 1998
Date of withdrawal of any conflicting National Standard (dow):	28 February 1998

SIST ETS 300 393-7:1999

Blank page