SLOVENSKI STANDARD
SIST ETS 300 393-7:1999

01-julij-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 Edition 1

ICS:

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

SIST ETS 300 393-7:1999 **en**

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

Contents

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

Blank page

1 Scope

This European Telecommunication Standard (ETS) describes the security mechanisms in the Trans-European Trunked Radio (TETRA) Packet Data Optimized (PDO) standard. It provides mechanisms for authentication and key management mechanisms for the air interface.

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 [3], based on a threat analysis:

- authentication of a user by the RPDI;

- authentication of the RPDI by a user.

The use of encryption is not described in this ETS but may be provided by the application using TETRA PDO as a transport and network service.

2 Normative references

This ETS incorporates by dated and 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 ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETS 300 393-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 1: General network design".

[2] ETS 300 393-2: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 2: Air Interface (AI)".

[3] ETR 086-3: "Radio Equipment and Systems (RES); Trans European Trunked Radio (TETRA) systems; Technical requirements specification; Part 3: Security aspects".

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

[5] ETS 300 392-7: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice and Data (V+D); Part 7: Security".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this ETS, the following definitions apply:

Authentication Code (AC): A (short) key to be entered by the user into the terminal.

Authentication Key (K): The primary secret, the knowledge of which has to be demonstrated for authentication. On the infrastructure side, it is stored in a secure place of the home network. In the terminal it is generated in one of three ways: 1) the authentication key may be generated from an authentication code AC that is manually entered by the user; 2) the authentication key may be generated from a user authentication key UAK stored in a module (detachable or not); 3) the authentication key may be generated from both the UAK stored in a module and the PIN entered by the user.

Personal Identification Number (PIN): Entered by the user into the terminal and used to generate the authentication Key (K)together with the User Authentication Key (UAK).

Proprietary Algorithm: An algorithm which is the intellectual property of a legal entity.

Random challenge (RAND1, RAND2): A random value generated by the infrastructure to authenticate a user or in a terminal to authenticate the infrastructure, respectively.

Random Seed (RS): A random value used to derive a session authentication key from the authentication key.

Response (RES1, RES2): A value calculated in the terminal from RAND1 and the KS to prove the authenticity of a user to the infrastructure or by the infrastructure from RAND2 and the KS' to prove its authenticity to a user, respectively.

Session Authentication Key (KS, KS'): Generated from the authentication key and a random seed for the authentication of a user. It has a more limited lifetime than the authentication key and can be stored in less secure places and forwarded to visited networks.

Spoofer: An entity attempting to obtain service from or interfere with the operation of the system by impersonation of an authorized system user or system component.

User Authentication Key (UAK): Stored in a (possibly detachable) module within the terminal and used to derive the authentication key (with or without a PIN as an additional parameter).

3.2 Abbreviations

For the purposes of this ETS, the following abbreviations apply.

AC	Authentication code
AI	Air Interface
BS	Base Station
ITSI	Individual TETRA Subscriber Identity
K	Authentication Key
KS	Session authentication Key
LLC	Logical Link Control
MAC	Medium Access Control
MLE	Mobile Link Entity
MM	Mobility Management
MS	Mobile Station
PDU	Protocol Data Unit
PIN	Personal Identification Number
RAND1	Random challenge 1
RAND2	Random challenge 2
RES1	Response 1
RES2	Response 2
RPDI	Radio Packet Data Infrastructure
RS	Random Seed
SAP	Service Access Point
SDU	Service Data Unit
TA	TETRA Algorithm
UAK	User authentication key
XRES1	Expected response 1
XRES2	Expected response 2

4 Air Interface authentication and key management mechanisms

NOTE: The algorithms referred to in this clause may be the same as those defined in ETS 300 392-7 [5] with some outputs ignored.

4.1 Air interface authentication mechanisms

4.1.1 Overview

Authentication is optional, however if it is used it shall be as described in this clause.

The authentication method described is a symmetric secret key type. In this method one secret, the authentication key, shall be shared by each of the authenticating parties, and there should be strictly two parties with knowledge of the secret. Authentication shall be achieved by the parties proving to each other knowledge of the shared secret.

The authenticating parties shall be the authentication centre of the Radio Packet Data Infrastructure (RPDI) and the Mobile Station (MS). The MS is considered, for the purposes of authentication, to represent the user as defined by the Individual TETRA Subscriber Identity (ITSI). At the air interface the Base Station (BS) is assumed to be trusted by the RPDI and the authentication exchange proves knowledge given to the BS by the authentication centre. This knowledge shall be the session authentication key.

Authentication and provision of keys for use at the air-interface shall be linked by the use of a common algorithm set. This algorithm set shall include a means of providing keys for use in group calls. The controlling party in all authentication exchanges shall be the RPDI.

The authentication process describes a 3-pass challenge-response-result protocol.

It is assumed that the intra-system interface linking the BS to the authentication centre is adequately secure.

4.1.2 Authentication of a user

In this subclause, a mechanism is described that shall be used to achieve the authentication of a user of an MS by the RPDI. This shall be done using a challenge response protocol, with a session authentication key derived from an authentication key that shall be shared by the user and the infrastructure. The session authentication key shall be provided by an authentication centre of the home system.

The computation of the session authentication key shall be carried out by an algorithm, TA11. The computation of the response shall be done by another algorithm, TA12P.

The BS shall generate a random number as a challenge RAND1. The MS shall compute a response, RES1, and the BS shall compute an expected response, XRES1. The BS on receipt of RES1 from the MS shall compare it with XRES1. If the values are equal the result R1 shall be set to TRUE, else the result R1 shall be set to FALSE.

The process is summarized in figure 1.

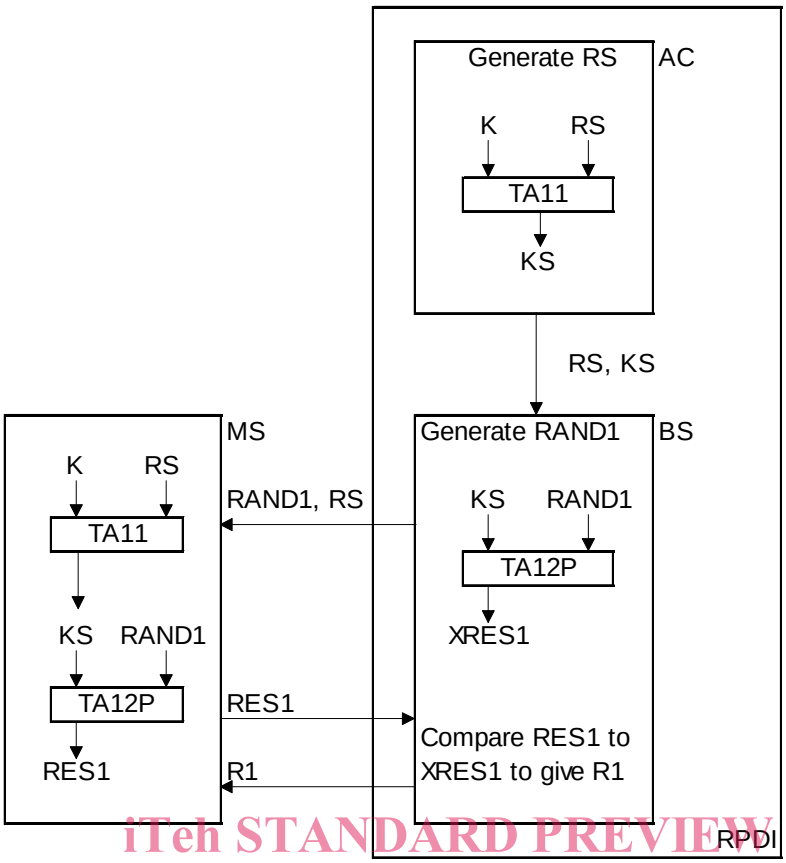

Figure 1: Authentication of a user by the infrastructure

4.1.3 Authentication of the infrastructure

Authentication of the infrastructure by a user shall be carried out in the same way as described in subclause 4.1.2 with the roles of the claimant and verifier reversed. The MS shall generate a challenge, RAND2, the BS shall generate an actual response, RES2, and the MS shall generate an expected response, XRES2. The MS on receipt of RES2 from the BS shall compare it with XRES2. If the values are equal the result R2 shall be set to TRUE, else the result R2 shall be set to FALSE.

The same authentication key K shall be used as in the case of authentication of the user by the infrastructure together with a random seed RS. However, the algorithms shall be different: TA11 shall be replaced by TA21 and TA12P by TA22P. Hence, there should also be a different value for the session authentication key, KS'. The process is summarized in figure 2.

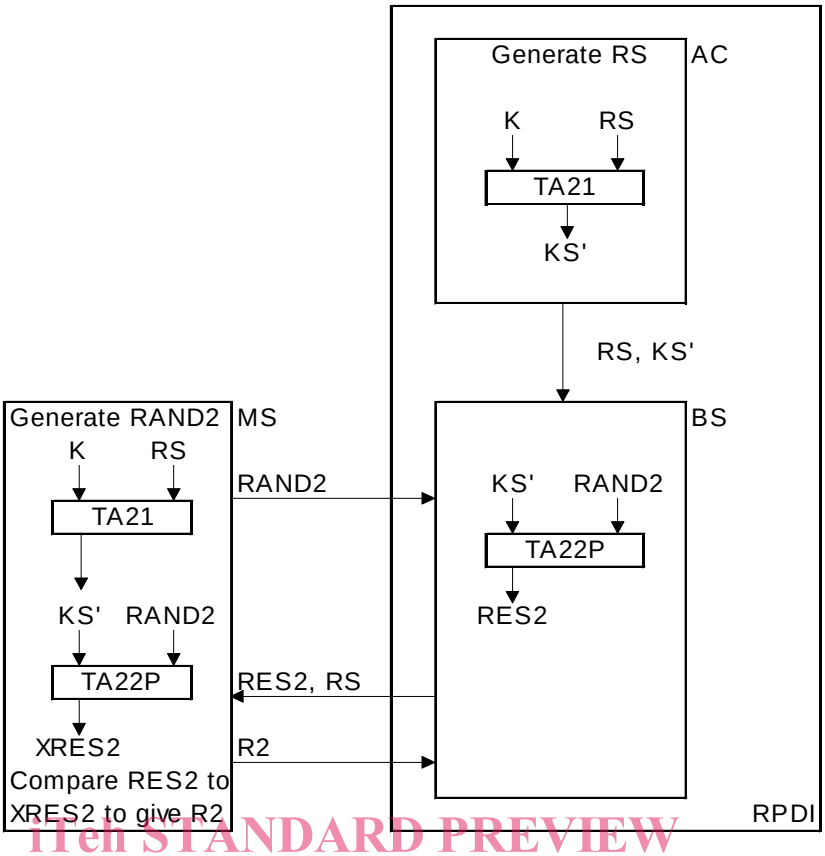

Figure 2: Authentication of the infrastructure by a user

4.1.4 Mutual authentication of user and infrastructure

Mutual authentication of user and infrastructure shall be achieved using a combined three pass mechanism. The algorithms and key K used shall be same as those used in the one way authentication described in the previous subclauses. The decision to make the authentication mutual shall be made by the first party to be challenged, not the initial challenging party. Thus mutual authentication shall be started as a one way authentication by the first challenging party, and shall be made mutual by the responding party.

If the first authentication in such a case fails the second authentication shall be abandoned.

If the authentication was initiated by the RPDI, it shall use K and one random seed RS with algorithms TA11 and TA12P to generate a session key KS. It shall then send random challenge RAND1 to the MS together with random seed RS. The MS shall run TA11 to generate session key KS, and because the authentication is to be made mutual it shall also run algorithm TA12P to generate a second session key KS'. Both MS and RPDI shall run algorithm TA12P; the MS then sends its response RES1 back to the RPDI. However, the MS also sends its mutual challenge RAND2 to the RPDI at the same time. The RPDI shall compare the response from the MS RES1 with its expected response XRES1, and because it has received a mutual challenge, it shall run TA12P to generate session key KS'. The RPDI shall then run TA22P to produce its response to the MS's challenge RES2. RES2 is sent to the MS, which shall also run TA22P to produce expected response XRES2. The MS shall compare RES2 with XRES2; and if the same, mutual authentication will have been achieved.

The process is shown in figure 3.

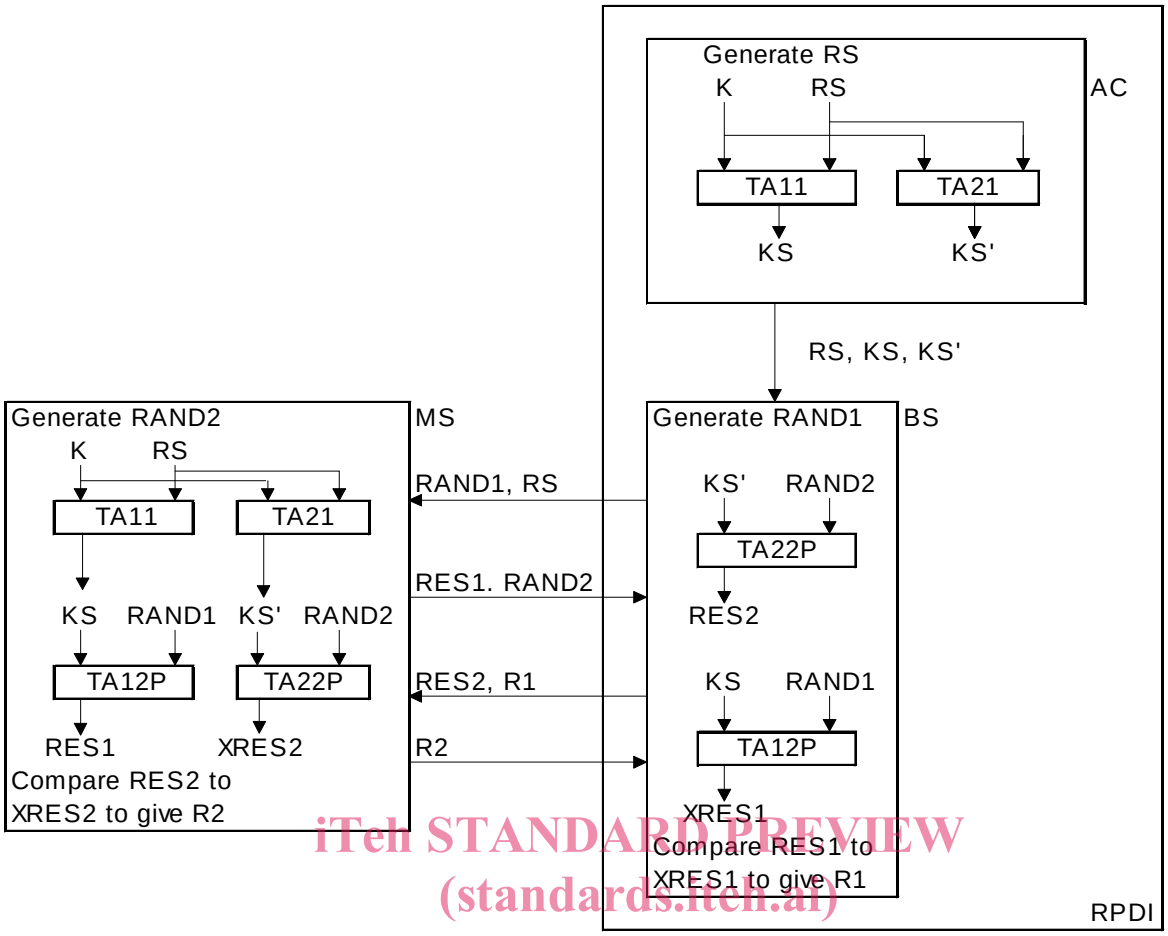

Figure 3: Mutual authentication initiated by RPDI

The mutual authentication process may also occur if a one way authentication is initiated by the MS, and then made mutual by the RPDI. In this case, the algorithms are the same, however the sequence is reversed as shown in figure 4.

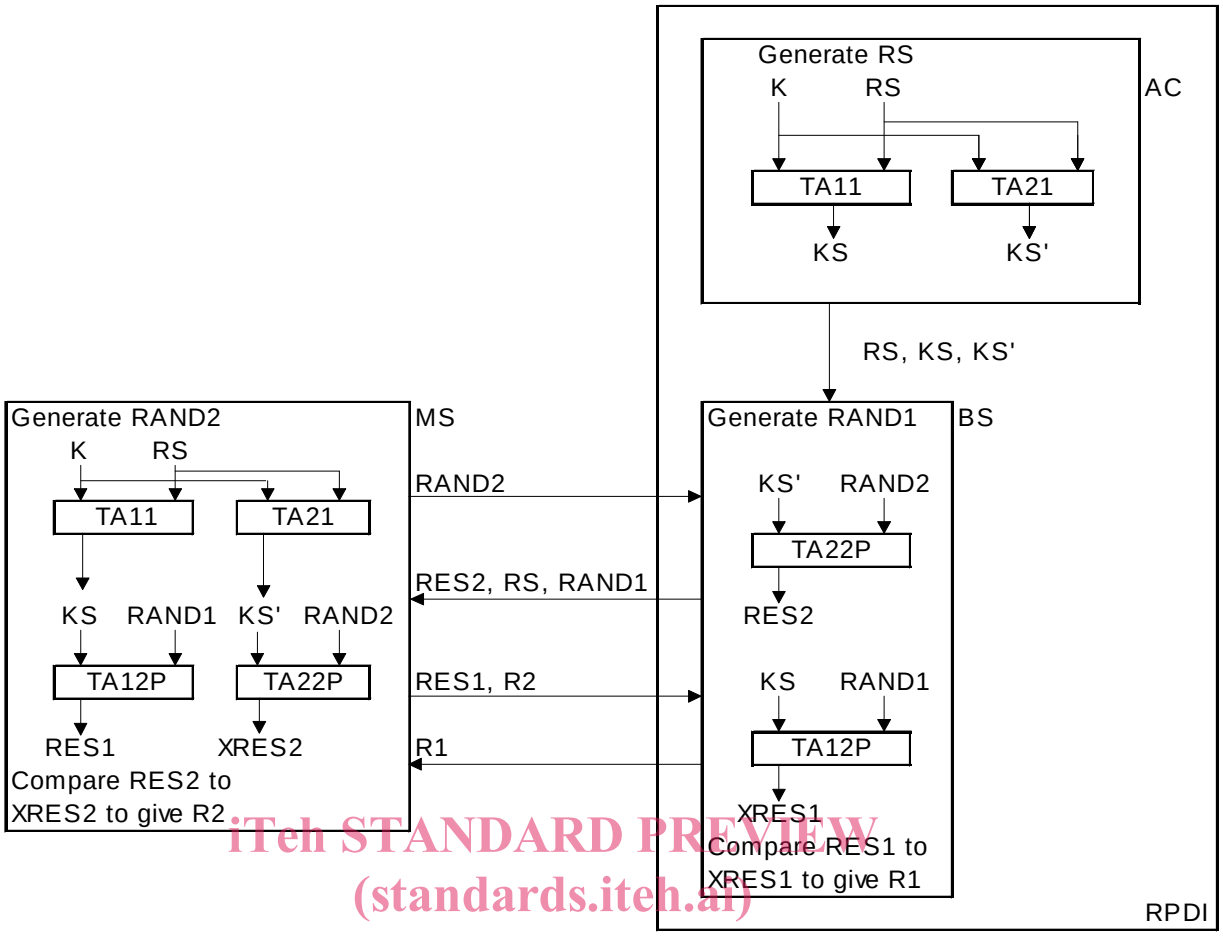

Figure 4: Mutual authentication initiated by MS

4.1.5 The authentication key

Users should be authenticated by a process that is carried out in the MS, as described in subclause 4.1.2. To provide against misuse of lost, or stolen, MS, and to authenticate the user to the MS, the user should be required to make an input before K is available and valid for use. K may be stored in a module, which may or may not be detachable, and the user may be required to make an input to this module, e.g. a personal identification number (PIN).

4.1.5.1 Generation of K

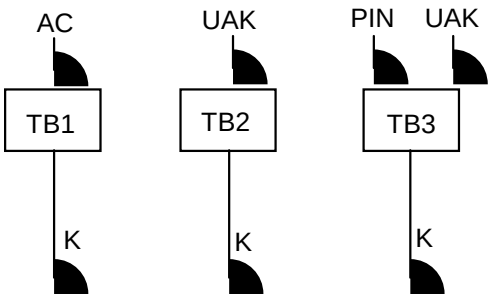

Figure 5: Generation of the authentication key

The generation of K shall be carried out using at least one of the following cases, summarized in figure 5: