SLOVENSKI STANDARD
SIST ETS 300 394-5-1 E1:2003

01-december-2003

Prizemni snopovni radio (TETRA) – Specifikacija za preskušanje skladnosti – 5. del: Varnost – 1. poddel: Izjava o skladnosti izvedbe protokola (PICS) – Proforma specifikacija

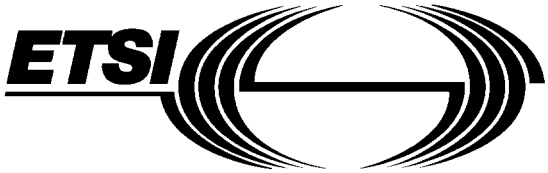
Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 5: Security; Sub-part 1: Protocol Implementation Conformance Statement (PICS) proforma specification

Ta slovenski standard je istoveten z: **ETS 300 394-5-1 Edition 1**

ICS:

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

SIST ETS 300 394-5-1 E1:2003 **en**



EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 394-5-1

July 1999

Source: TETRA

Reference: DE/TETRA-06025

ICS: 33.020

Key words: PICS, TETRA, security, V+D, voice, data

Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 5: Security; Sub-part 1: Protocol Implementation Conformance Statement (PICS) proforma specification

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 - http://www.etsi.org

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 Terrestrial Trunked Radio (TETRA) Project of the European Telecommunications Standards Institute (ETSI).

Every ETS prepared by ETSI is a voluntary standard. This ETS contains text concerning conformance testing of the equipment to which it relates. This text should be considered only as guidance and does not make this ETS mandatory.

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

Part 1: "Radio";

Part 2: "Protocol testing specification for Voice plus Data (V+D)";

Part 4: "Protocol testing specification for Direct Mode Operation (DMO)";

Part 5: "Security".

Transposition dates	
Date of adoption of this ETS:	25 June 1999
Date of latest announcement of this ETS (doa):	30 September 1999
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 March 2000
Date of withdrawal of any conflicting National Standard (dow):	31 March 2000

Blank page

1 Scope

This European Telecommunication Standard (ETS) provides the Protocol Implementation Conformance Statement (PICS) proforma in compliance with the relevant requirements, and in accordance with the relevant guidance given in ISO/IEC 9646-7 [8], ETS 300 406 [3], and in ETR 212 [9] for the following standards:

TETRA; Voice plus Data (V+D); Part 7: Security defined in ETS 300 392-7 [1];

TETRA; Direct Mode; Part 6: Security defined in ETS 300 396-6 [2].

The PICS draft has acted as a fair and independent review of the above standards. The above standards may therefore be subject to modification or extension as a result of this PICS proforma.

The role of the PICS is to enable selection of test cases from ETS 300 394-5-2 for the MS. In the case of the SwMI the PICS is a tool to guide procurement of TETRA systems. This ETS acts as a complement to the PICS for TETRA V+D, ETS 300 392-14.

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 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

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

[3] ETS 300 406 : "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

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

[5] ETS 300 396-3: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 3: Mobile Station to Mobile Station (MS-MS) Air Interface (AI) protocol".

[6] ETS 300 393-7: "Terrestrial Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 7: Security".

[7] ISO/IEC 9646-1 (1994): "Information technology - Open systems interconnection - Conformance testing methodology and framework - Part 1: General concepts".

[8] ISO/IEC 9646-7 (1995): "Information technology - Open systems interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[9] ETR 212: "Methods for testing and Specification (MTS); Implementation Conformance Statement (ICS) proforma style guide".

[10] ISO 8208 (1995): "Information technology - Data communications - X.25 Packet Layer Protocol for Data Terminal Equipment".

[11] ISO/IEC 8348 (1996): "Information technology - Open Systems Interconnection - Network Service Definition".

3 Definitions and abbreviations

3.1 Definitions

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

- Terms defined in ETS 300 392-7 [1];
- Terms defined in ETS 300 396-6 [2];
- Terms defined in ISO/IEC 9646-1 [7] and in ISO/IEC 9646-7 [8].

In particular, the following terms defined in ISO/IEC 9646-1 [7] apply:

Implementation Conformance Statement (ICS): statement made by the supplier of an implementation or system claimed to conform to a given specification, stating which capabilities have been implemented. The ICS can take several forms: protocol ICS, profile ICS, profile specific ICS, information object ICS, etc.

ICS proforma: document, in the form of a questionnaire, which when completed for an implementation or system becomes an ICS

Protocol ICS (PICS): ICS for an implementation or system claimed to conform to a given protocol specification

3.2 Abbreviations

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

BS	Base Station
CC	Call Control sub entity within CMCE
CMCE	Circuit Mode Control Entity
CONP	Connection Oriented Network Protocol
DTMF	Dual Tone Multi Frequency
ETS	European Telecommunication Standard
ICS	Implementation Conformance Statement
ITSI	Individual TETRA Subscriber Identity
IUT	Implementation Under Test
LLC	Logical Link Control
LLME	Lower Layer Management Entity
MAC	Medium Access Control
MCC	Mobile Country Code
MM	Mobility Management
MNC	Mobile Network Code
MS	Mobile Station
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
RPDI	Radio Packet Data Infrastructure
SCLNP	Specific Connectionless Network Protocol
SAP	Service Access Point
SCS	System Conformance Statement
SDU	Service Data Unit
SP	Service Primitive
SS	Supplementary Service sub entity within CMCE
SUT	System Under Test
SwMI	Switching and Management Infrastructure

4 Conformance to this PICS proforma specification

If it claims to conform to this ETS the actual PICS proforma to be filled in by a supplier shall be technically equivalent to the text of the PICS proforma given in annex A, and shall preserve the numbering/naming and ordering of the proforma items.

A PICS which conforms to this ETS shall be a conforming PICS proforma completed in accordance with the guidance for completion given in clause A.1.

Annex A (normative): Protocol ICS proforma for TETRA Security

A.1 Guidance for completing the PICS proforma

A.1.1 Purposes and structure

The purpose of this PICS proforma is to provide a mechanism whereby a supplier of an implementation of the requirements defined in ETS 300 392-7, or ETS 300 396-6, may provide information about the implementation in a standardized manner.

The PICS proforma is subdivided into subclauses for the following categories of information with some of these subclauses also included in a set of separate annexes covering V+D and DMO specific aspects:

- Guidance for completing the PICS proforma (annex A)
  - Identification of the implementation;
  - Identification of the protocol;
- V+D Specific Aspects (annex B)
  - Global statement of conformance;
  - Authentication;
  - Over The Air Rekeying (OTAR);
  - Enable/disable;
  - Air Interface encryption;
  - Key change protocol;
  - End-to-end encryption.
  - Encrypted short identities;
  - TEI delivery;
  - PDU support.
- DMO specific aspects (annex C)
  - OTAR in DMO;
  - Enable/Disable in DMO (ENDIS);
  - Air Interface encryption;
  - End-to-end encryption.

A.1.2 Abbreviations and conventions

The PICS proforma contained in this annex is comprised of information in tabular form in accordance with the guide-lines presented in ISO/IEC 9646-7.

Item column

The item column contains a number which identifies the item in the table.

Item description column

The item description column describes in free text each respective item (e.g. elements, timers, etc.). It implicitly means "is <item description> supported by the implementation?".

Status column

The following notations, defined in ISO/IEC 9646-7, are used for the status column:

m	mandatory - the capability is required to be supported.
o	optional - the capability may be supported or not.
n/a	not applicable - in the given context, it is impossible to use the capability.

x — prohibited (excluded) - there is a requirement not to use this capability in the given context.

oi — qualified optional - for mutually exclusive or selectable options from a set. "i" is an integer which identifies a unique group of related optional items and the logic of their selection which is defined immediately following the table.

ci — conditional - the requirement on the capability ("m", "o", "x" or "n/a") depends on the support of other optional or conditional items. "i" is an integer identifying a unique conditional status expression which is defined immediately following the table.

Reference column

The reference column gives reference to ETS 300 392-7, except where explicitly stated otherwise. In providing the reference the format [x] a.b.c.d is used where [x] is the number of the referenced document from clause 2, and a.b.c.d refers to the specific clause or subclause of the reference document.

Support column

The support column shall be filled in by the supplier of the implementation. The following common notations, defined in ISO/IEC 9646-7, are used for the support column:

Y or y — supported by the implementation

N or n — not supported by the implementation

N/A, n/a or - — no answer required (allowed only if the status is n/a, directly or after evaluation of a conditional status)

It is also possible to provide a comment to an answer in the space provided at the bottom of the table.

NOTE: As stated in ISO/IEC 9646-7, support for a received PDU requires the ability to encode/decode all mandatory elements of that PDU. Supporting a PDU while having no ability to encode/decode a mandatory element is non-conformant. Support for an element of a PDU means that the semantics of that element are supported. It does not mean that the element shall always be present in the PDU.

Values allowed column

The values allowed column contains the type, the list, the range, or the length of values allowed. The following notations are used:

– range of values: <min value> ... <max value>
  EXAMPLE: 5 ... 20

– list of values: <value1>, <value2>, ..., <valueN>
  EXAMPLE: 2, 4, 6, 8, 9
  EXAMPLE: '1101'B, '1011'B, '1111'B
  EXAMPLE: '0A'H, '34'H, '2F'H

– list of named values: <name1>(<val1>), <name2>(<val2>), ..., <nameN>(<valN>)
  EXAMPLE: reject(1), accept(2)

– length: size (<min size> ... <max size>)
  EXAMPLE: size (1 ... 8)

Values supported column

The values supported column shall be filled in by the supplier of the implementation. In this column, the values or the ranges of values supported by the implementation shall be indicated.

References to items

For each possible item answer (answer in the support column) within the PICS proforma exists a unique reference, used, for example, in the conditional expressions. It is defined as the table identifier, followed by a solidus character "/", followed by the item number in the table. If there is more than one support column in a table, the columns are discriminated by letters (a, b, etc.), respectively.

EXAMPLE 1: A.5/4 is the reference to the answer of item 4 in table A.5.

EXAMPLE 2: A.6/3b is the reference to the second answer (i.e. in the second support column) of item 3 in table A.6.

Prerequisite line

A prerequisite line takes the form: Prerequisite: <predicate>.

A prerequisite line in the beginning of a clause or table indicates that the whole clause or the whole table is not required to be completed if the predicate is FALSE.

NOTE: In this PICS proforma, all the tables have a prerequisite independently on the status of the predicate referred to being mandatory or optional. This is done for readability reasons.

A.1.3 Instructions for completing the PICS proforma

The supplier of the implementation shall complete the PICS proforma in each of the spaces provided. In particular, an explicit answer shall be entered, in each of the support or supported column boxes provided, using the notation described in subclause A.1.2.

If necessary, the supplier may provide additional comments in space at the bottom of the tables, or separately on sheets of paper.

More detailed instructions are given at the beginning of the different subclauses of the PICS proforma.

A.2 Identification of the implementation

NOTE: This section is to be completed for each submission of a PICS for V+D and DMO.

Identification of the Implementation Under Test (IUT) and the system in which it resides (the System Under Test (SUT)) should be filled in so as to provide as much detail as possible regarding version numbers and configuration options.

The product supplier information and client information should both be filled in if they are different.

A person who can answer queries regarding information supplied in the PICS should be named as the contact person.

A.2.1 Date of the statement

.....

A.2.2 Implementation Under Test (IUT) identification

IUT name:

.....

.....

IUT version:

.....

A.2.3 System Under Test (SUT) identification

SUT name:

.....

.....

Hardware configuration:

.....

.....

.....

Operating system:

.....

A.2.4 Product supplier

Name:

.....

Address:

.....

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

.....

A.2.5 Client

(If different from product supplier)

Name:

.....

Address:

.....

.....

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

.....

A.2.6 PICS contact person

(A person to contact if there are any queries concerning the content of the PICS)

Name:

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

A.2.7 Authentication algorithm identification

If TAA1 (ETSI) is used then this section can be skipped.

Supplier:

.....