EUROPEAN
TELECOMMUNICATION
STANDARD

FINAL DRAFT
pr **ETS 300 394-5-1**

April 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

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 Standards Making Support Dept." at the address shown on the title page.

Contents

Foreword

This final draft European Telecommunication Standard (ETS) has been produced by the Terrestrial Trunked Radio (TETRA) Project of the European Telecommunications Standards Institute (ETSI), and is now submitted for the Voting phase of the ETSI standards approval procedure.

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".

Proposed transposition dates	
Date of latest announcement of this ETS (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

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:

....

....

Version:

....

A.3 Identification of the protocol

This PICS proforma applies to the following standards:

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

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

Annex B (normative): Protocol ICS tables proforma for TETRA V+D Security

B.1 Global statement of conformance

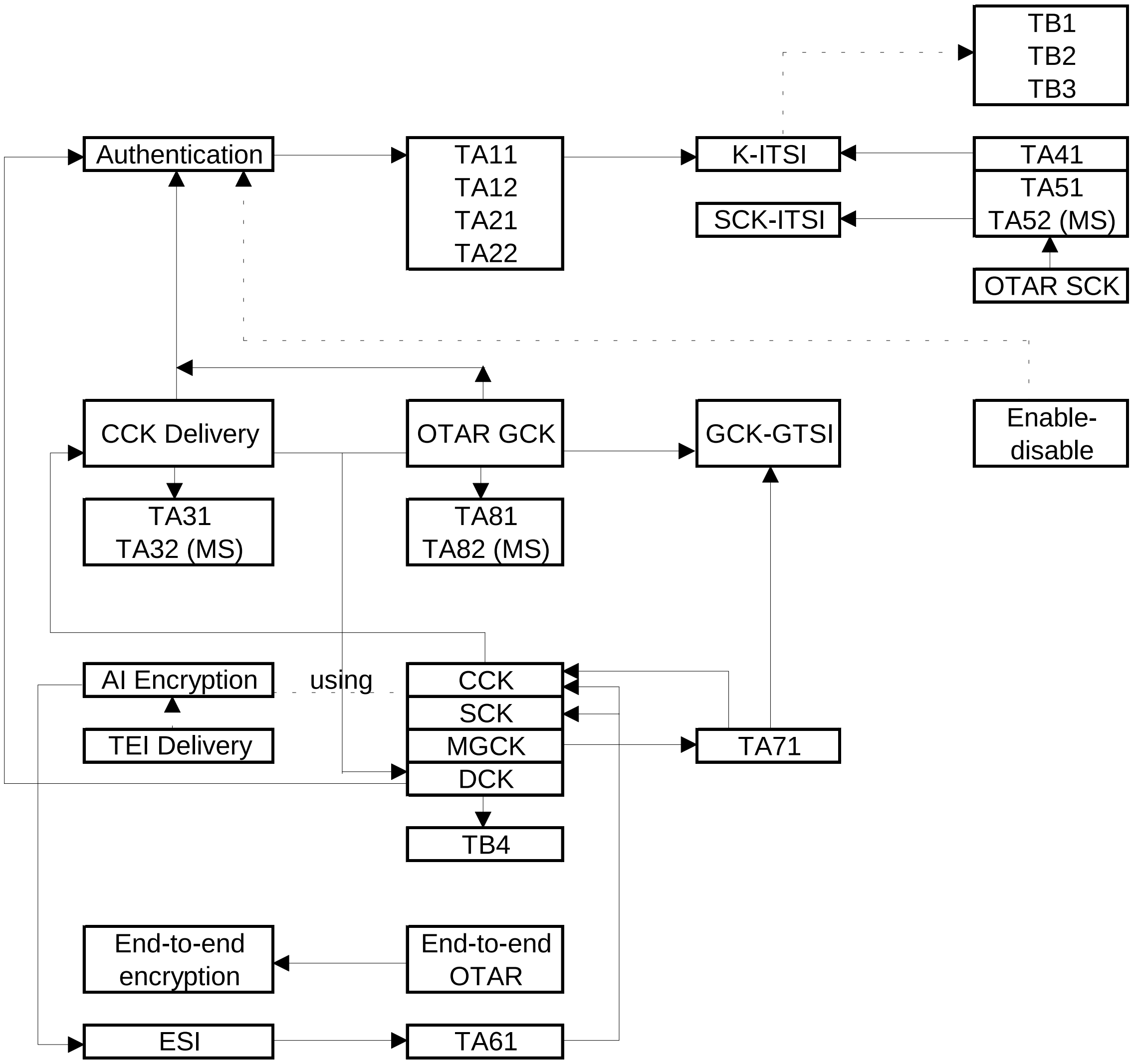
Are all mandatory capabilities implemented? (Yes/No) ....

NOTE: Answering "No" to this question indicates non-conformance to the protocol specification. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming, on pages attached to the PICS proforma.

B.2 Structure of V+D ICS tables

The map below summarizes the general structure of the document and the corresponding tables that shall be completed as a consequence of any entry in any other table. It should be noted that a single PICS may involve traversing this map more than one once.

NOTE: The map below, and similar maps introducing each section, is intended for guidance and is not intended to be treated as normative.



NOTE 1: Arrows on the map indicate the relation "tail" requires "head" (e.g OTAR CCK requires Authentication to be supported).

NOTE 2: The relation from TA61 to CCK and SCK should be interpreted as an either/or relation.

NOTE 3: The link from K-ITSI to TBx is an optional or weak relation.

NOTE 4: The relations from AI Encryption and TA61 to the cipher keys is an either/or relation.

Figure B.1: Overall structure of V+D PICS annex

If the implementation supports authentication this means that as a consequence the implementation shall support TA11, TA12 (and perhaps TA21, TA22) and storage of the ITSI-K relation.

B.3 Major capabilities

Table B.1: V+D Security class supported

Item	Role	Reference	Status	Support
1	Class 1	[1] 6.1.1	o.1	
2	Class 2	[1] 6.1.1	o.1	
3	Class 3	[1] 6.1.1	o.1	

o.1: It is mandatory to support at least one of these items

Table B.2: V+D Security capabilities supported

Item	Security capability	Reference	Status	Support
1	Authentication	[1] 4	c201	
2	OTAR	[1] 4	c201	
3	Enable/disable	[1] 5	m	
4	AI encryption	[1] 6	c202	
5	End-to-end encryption	[1] 7	o	
6	TEI delivery	[1] 4.1.6	m	
7	ESI	[1] 4.2.5	c202	
8	Key change protocol	[1] 4.4.6	c203	

c201: IF B.1/3 - If security class 3 then mandatory else optional
THEN m
ELSE o

c202: IF B.1/3 or B.1/2 - If security class 3, or security class 2 then mandatory
THEN m - else not applicable
ELSE n/a

c203: IF B.1/3 or B.2/2 - If security class 3 or if OTAR supported then mandatory
THEN m - else not applicable
ELSE n/a

B.4 Authentication

NOTE: This clause needs to be completed only if the IUT supports authentication.

Are all mandatory capabilities of authentication implemented? (Yes/No) ....

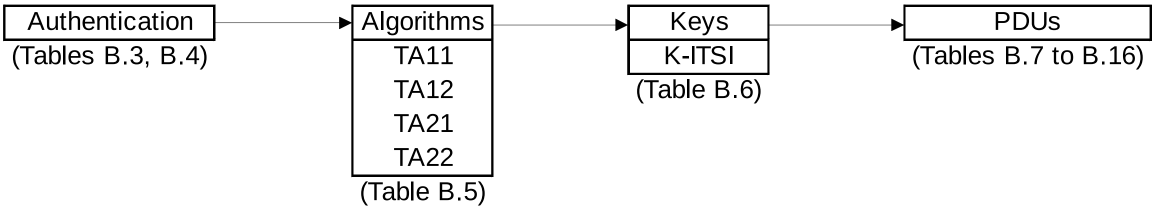


Figure B.2: Authentication PICS table navigation map

Figure B.2 is intended to assist in identifying the tables that should be completed for those implementations purporting to support authentication as defined in ETS 300 392-7 [1], clause 4.

Table B.3: Authentication role

Prerequisite: B.2/1 – IUT supports authentication				
Item	**Authentication role**	**Reference**	**Status**	**Support**
1	MS	[1] 4.4.2.2	o.301	
2	SwMI	[1] 4.4.2.1	o.301	

o.301 It is mandatory to support at least one of these items

Table B.4: Authentication sub-types

Prerequisite: B.2/1 – IUT supports authentication				
Item	**Authentication sub-type**	**Reference**	**Status**	**Support**
1	SwMI initiated authentication	[1] 4.4.2.1	m	
2	MS initiated authentication	[1] 4.4.2.2	m	
3	Authentication initiated by SwMI and made mutual by MS	[1] 4.4.2.3	m	
4	Authentication initiated by MS and made mutual by SwMI	[1] 4.4.2.4	m	
5	SwMI initiated authentication during registration	[1] 4.4.2.5	m	
6	MS initiated authentication during registration	[1] 4.4.2.6	m	
7	Authentication initiated by MS during registration made mutual by SwMI	[1] 4.4.2.7	m	
8	Authentication initiated by SwMI during registration made mutual by MS	[1] 4.4.2.8	m	

Comment: It is stated in ETS 300 392-7ed2 [1], subclause 4.4.2 that if a terminal supports authentication then it shall support all modes. This therefore requires that all entries in table B.4 are mandatory.

B.4.1 Authentication algorithms

The supplier of the implementation shall state the support of each of the AI authentication algorithms.

If the algorithms are not sourced from TAA1 the source of the algorithms shall be specified in subclause A.2.7.

Table B.5: Authentication Algorithms

Prerequisite: B.2/1 – IUT supports authentication				
Item	**Algorithm**	**Reference**	**Status**	**Support**
1	TA11	[1] 4.1.2	m	
2	TA12	[1] 4.1.2	m	
3	TA21	[1] 4.1.3	m	
4	TA22	[1] 4.1.3	m	
NOTE: Support of any of the algorithms (TAxx) requires that the conformance tests defined for the algorithms have been successfully completed.				

Comment: It is stated in ETS 300 392-7ed.2 [1], subclause 4.4.2 that if a terminal supports authentication then it shall support all modes. This therefore requires that all entries in table B.5 are mandatory.

B.4.2 Authentication cipher keys

The supplier of the implementation shall state the support of the store of the cipher key to TETRA address relations.

Table B.6: Authentication cipher key support

Prerequisite: B.2/1 – IUT supports authentication				
Item	**Cipher key**	**Reference**	**Status**	**Support**
1	K-ITSI	[1] 4.2.6	m	

B.4.3 Authentication PDUs

The supplier of the implementation shall state the support in the implementation for each of the authentication PDUs presented in tables B.7. to B.10.

Table B.7: Downlink PDUs for authentication

Prerequisite: B.2/1 – IUT supports authentication				
Item	**Authentication PDUs**	**Reference**	**Status**	**Support**
1	D-AUTHENTICATION DEMAND	[1] 4.4.7.1	m	
2	D-AUTHENTICATION RESPONSE	[1] 4.4.7.3	m	
3	D-AUTHNETICATION RESULT	[1] 4.4.7.4	m	
4	D-AUTHENTICATION REJECT	[1] 4.4.7.2	m	
5	D-LOCATION UPDATE ACCEPT	[1] 4.4.2.5	m	

Comment: D-LOCATION UPDATE ACCEPT contains cipher negotiation parameters and may include the Authentication Downlink type-3 element.

Table B.8: Uplink PDUs for authentication

Prerequisite: B.2/1 – IUT supports authentication				
Item	**Authentication PDUs**	**Reference**	**Status**	**Support**
1	U-AUTHENTICATION DEMAND	[1] 4.4.7.9	m	
2	U-AUTHENTICATION RESPONSE	[1] 4.4.7.11	m	
3	U-AUTHENTICATION RESULT	[1] 4.4.7.12	m	
4	U-AUTHENTICATION REJECT	[1] 4.4.7.10	m	
5	U-LOCATION UPDATE DEMAND	[1] 4.4.2.5	m	

Comment: U-LOCATION UPDATE DEMAND contains cipher negotiation parameters and may include the Authentication Downlink type-3 element.

B.4.4 Authentication PDU elements

The supplier of the implementation shall state the support of the implementation for each of the authentication PDU elements presented in tables B.9 to B.16.

Table B.9: Elements for D-AUTHENTICATION DEMAND PDU

Prerequisite: B.7/1 – IUT supports D-AUTHENTICATION DEMAND				
Item	**Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 4.4.9.21	m	
2	Authentication sub-type	[1] 4.4.7	m	
3	Random challenge [RAND1]	[1] 4.4.9.24	m	
4	Random seed [RS]	[1] 4.4.9.25	m	
5	Proprietary element	[1] 4.4.9.22	o	

Table B.10: Elements for D-AUTHENTICATION RESPONSE PDU

Prerequisite: B.7/2 – IUT supports D-AUTHENTICATION RESPONSE				
Item	**Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 4.4.9.21	m	
2	Authentication sub-type	[1] 4.4.7	m	
3	Random seed [RS]	[1] 4.4.9.25	m	
4	Response value [RES2]	[1] 4.4.9.27	m	
5	Mutual authentication flag	[1] 4.4.9.16	m	
6	Random challenge [RAND1]	[1] 4.4.9.24	m	
7	Proprietary element	[1] 4.4.9.22	o	

Table B.11: Elements for D-AUTHENTICATION RESULT PDU

Prerequisite: B.7/3 – IUT supports D-AUTHENTICATION RESULT				
Item	**Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 4.4.9.21	m	
2	Authentication sub-type	[1] 4.4.7	m	
3	Authentication result [R1]	[1] 4.4.9.3	m	
4	Mutual authentication flag	[1] 4.4.9.16	m	
5	Response value [RES2]	[1] 4.4.9.27	m	
6	Proprietary element	[1] 4.4.9.22	o	

Table B.12: Elements for D-AUTHENTICATION REJECT PDU

Prerequisite: B.7/4 – IUT supports D-AUTHENTICATION REJECT				
Item	**Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 4.4.9.21	m	
2	Authentication sub-type	[1] 4.4.7	m	
3	Authentication reject reason	[1] 4.4.9.2	m	

Table B.13: Elements for U-AUTHENTICATION DEMAND PDU

Prerequisite: B.8/1 – IUT supports U-AUTHENTICATION DEMAND				
Item	**Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 4.4.9.21	m	
2	Authentication sub-type	[1] 4.4.7	m	
3	Random challenge [RAND2]	[1] 4.4.9.24	m	
4	Proprietary element	[1] 4.4.9.22	o	

Table B.14: Elements for U-AUTHENTICATION RESPONSE PDU

Prerequisite: B.8/2 – IUT supports U-AUTHENTICATION RESPONSE				
Item	**Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 4.4.9.21	m	
2	Authentication sub-type	[1] 4.4.7	m	
3	Response value [RES1]	[1] 4.4.9.27	m	
4	Mutual authentication flag	[1] 4.4.9.16	m	
5	Random challenge [RAND2]	[1] 4.4.9.24	m	
6	Proprietary element	[1] 4.4.9.22	o	

Table B.15: Elements for U-AUTHENTICATION RESULT PDU

Prerequisite: B.8/3 – IUT supports U-AUTHENTICATION RESULT				
Item	**Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 4.4.9.21	m	
2	Authentication sub-type	[1] 4.4.7	m	
3	Authentication result [R2]	[1] 4.4.9.3	m	
4	Mutual authentication flag	[1] 4.4.9.16	m	
5	Response value [RES1]	[1] 4.4.9.27	m	
6	Proprietary element	[1] 4.4.9.22	o	

Table B.16: Elements for U-AUTHENTICATION REJECT PDU

Prerequisite: B.8/4 – IUT supports U-AUTHENTICATION REJECT				
Item	**Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 4.4.9.21	m	
2	Authentication sub-type	[1] 4.4.7	m	
3	Authentication reject reason	[1] 4.4.9.2	m	

B.4.5 Registration PDU extended elements

The support of authentication during registration requires that the implementation support the MM PDUs identified by B.7/5 and B.8/5. Support of the MM-registration PDUs shall be declared in the TETRA V+D PICS Proforma ETS 300 392-14. The following "type 3" elements are used to support authentication in these PDUs.

Table B.17: MM Type 3 elements for security enabling at registration

Prerequisite: B.7/5 or B.8/5 – IUT supports U-LOCATION UPDATE COMMAND or D–LOCATION UPDATE ACCEPT PDUs				
Item	**Type 3 element**	**Reference**	**Status**	**Support**
1	Authentication uplink	[1] 4.4.8.2	m	
2	Authentication downlink	[1] 4.4.8.1	m	

Table B.18: Elements for authentication uplink type 3 element

Prerequisite: B.17/1 – IUT supports authentication uplink type 3 element				
Item	**Element**	**Reference**	**Status**	**Support**
1	CCK request flag	[1] 4.4.9.6	m	
2	Random challenge	[1] 4.4.9.24	m	

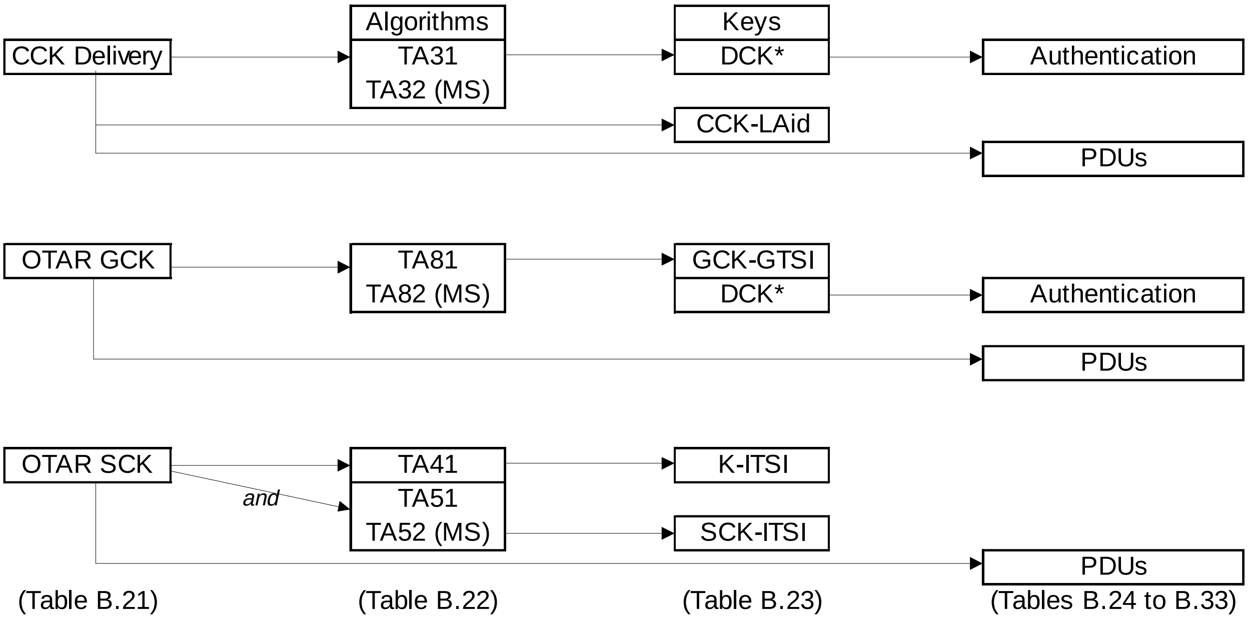
Table B.19: Elements for authentication downlink type 3 element

Prerequisite: B.17/2 – IUT supports authentication downlink type 3 element				
Item	**Element**	**Reference**	**Status**	**Support**
1	Authentication result	[1] 4.4.9.3	m	
2	TEI request flag	[1] 4.4.9.34	m	
3	CCK information flag	[1] 4.4.7.9	m	
4	CCK information	[1] 4.4.9.5	o	

B.5 OTAR

NOTE: This clause needs to be completed only if the IUT supports OTAR.

Are all mandatory capabilities of OTAR implemented? (Yes/No) ....



*DCK is not referred to by any PICS tables but indicates that authentication is a prerequisite of this process.

Figure B.3: OTAR PICS table navigation map

Figure B.3 is intended to assist in identifying the tables that should be completed for those implementations purporting to support OTAR as defined in ETS 300 392-7 [1], clause 4.

Table B.20: OTAR role

Prerequisite: B.2/2 – IUT supports OTAR				
Item	**OTAR role**	**Reference**	**Status**	**Support**
1	MS	[1] 4.4.2.2	o.2001	
2	SwMI	[1] 4.4.2.1	o.2001	

o.2001 It is mandatory to support at least one of these items

Table B.21: OTAR sub-types

Prerequisite: B.2/2 – IUT supports OTAR				
Item	**OTAR sub-type**	**Reference**	**Status**	**Support**
1	CCK delivery	[1] 4.4.3	c2101	
2	OTAR GCK	[1] 4.4.5	c2102	
3	OTAR SCK	[1] 4.4.4	c2103	
4	CCK delivery at registration	[1] 4.4.7.2	c2101	

c2101: IF B.1/3 - If security class 3 then mandatory else not applicable
THEN m
ELSE n/a

c2102: IF B.1/3 - If security class 3 then optional else not applicable
THEN o
ELSE n/a

c2103: IF B.1/2 - If security class 2 then optional else not applicable
THEN o
ELSE n/a

B.5.1 OTAR algorithms

The supplier of the implementation shall state the support of each algorithm.

If the algorithms are not sourced from TAA1 the source of the algorithms shall be specified in subclause A.2.7.

Table B.22: OTAR algorithms (from TAA1)

Prerequisite: B.21/1 OR B.21/2 OR B.21/3 OR B.21/4 – IUT supports at least one OTAR sub-type				
Item	**OTAR algorithm**	**Reference**	**Status**	**Support**
1	TA31	[1] 4.2.3	c2201	
2	TA32	[1] 4.2.3	c2202	
3	TA41	[1] 4.2.4	c2203	
4	TA51	[1] 4.2.4	c2204	
5	TA52	[1] 4.2.4	c2205	
6	TA81	[1] 4.2.2	c2206	
7	TA82	[1] 4.2.2	c2207	
8	TB4	[1] 4.2.1	c2208	
NOTE: Support of any of the algorithms (TAxx) requires that the conformance tests defined for the algorithms have been successfully completed.				

c2201: IF (B.21/1 OR B.21/4) AND B.20/2 - If type 3 and SwMI then mandatory, else not applicable
THEN m
ELSE n/a

c2202: IF (B.21/1 OR B.21/4) AND B.20/1 - If type 3 and MS then mandatory, else not applicable
THEN m
ELSE n/a

c2203: IF B.21/3 - If type 2 and IUT supports OTAR then mandatory, else not applicable
THEN m
ELSE n/a

c2204: IF B.21/3 AND B.20/2 - If type 2 and SwMI then mandatory, else not applicable
THEN m
ELSE n/a

c2205: IF B.21/3 AND B.20/1 - If type 2 and MS then mandatory, else not applicable
THEN m
ELSE n/a

c2206: IF B.21/2 AND B.20/2
THEN m - If type 3 and SwMI and OTAR GCK then mandatory,
ELSE n/a - else not applicable

c2207: IF B.21/2 AND B.20/1
THEN m - If type 3 and MS and OTAR GCK then mandatory, else not applicable
ELSE n/a

c2208: IF B.1/3 - If type 3 then mandatory, else not applicable
THEN m
ELSE n/a

B.5.2 OTAR cipher keys

The supplier of the implementation shall state the support of the store of the cipher key to TETRA address relations.

Table B.23: Cipher key and address relations

Prerequisite: B.21/1 OR B.21/2 OR B.21/3 OR B.21/4 – IUT supports at least one OTAR sub-type				
Item	**Key-address relation**	**Reference**	**Status**	**Support**
1	SCK-ITSI	[1] 4.2.6	c2301	
2	GCK-GTSI	[1] 4.2.6	c2302	
3	CCK-LAid	[1] 4.2.6	c2303	

c2301: IF B.21/3 - If OTAR SCK then mandatory, else not applicable
THEN m
ELSE n/a

c2302: IF B. 21/2 - If OTAR GCK then mandatory, else not applicable
THEN m
ELSE n/a

c2303: IF B.21/1 OR B.21/4 - If CCK delivery, or CCK delivery at registration then mandatory,
THEN m - else not applicable
ELSE n/a

B.5.3 OTAR PDUs

Table B.24: OTAR PDUs

Prerequisite: B.21/1 OR B.21/2 OR B.21/3 OR B.21/4 – IUT supports at least one OTAR sub-type				
Item	**OTAR PDU**	**Reference**	**Status**	**Support**
1	D-OTAR CCK Provide	[1] 4.4.7.6	c2401	
2	D-OTAR SCK Provide	[1] 4.4.7.8	c2402	
3	D-OTAR GCK Provide	[1] 4.4.7.7	c2403	
4	U-OTAR CCK Demand	[1] 4.4.7.14	c2401	
5	U-OTAR CCK Result	[1] 4.4.7.15	c2401	
6	U-OTAR SCK Demand	[1] 4.4.7.18	c2402	
7	U-OTAR SCK Result	[1] 4.4.7.19	c2402	
8	U-OTAR GCK Demand	[1] 4.4.7.16	c2403	
9	U-OTAR GCK Result	[1] 4.4.7.17	c2403	
10	U-LOCATION UPDATE DEMAND	[1] 4.4.2.5	c2404	
11	D-LOCATION UPDATE ACCEPT	[1] 4.4.2.5	c2404	

c2401: IF B.21/1 - If class 3 then mandatory, else not applicable
THEN m
ELSE n/a

c2402: IF B.21/3 - If class 2 and OTAR SCK then mandatory, else not applicable
THEN m
ELSE n/a

c2403: IF B.21/2 - If class 3 and OTAR GCK then mandatory, else not applicable
THEN m
ELSE n/a

c2404: IF B.21/4 - If class 3 then mandatory, else not applicable
THEN m
ELSE n/a

B.5.4 OTAR PDU elements

Table B.25: Elements for D-OTAR CCK Provide PDU

Prerequisite: B.24/1						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	PDU Type	[1] 4.4.9.21	m		0000_2	
2	OTAR sub-type	[1] 4.4.9.20	m		000_2	
3	CCK Provision flag	[1] 4.4.9	m			
4	CCK information	[1] 4.4.9.5	m			
5	Proprietary element	[1] 4.4.9.22	o			

Table B.26: Elements for D-OTAR SCK Provide PDU

Prerequisite: B.24/2						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	PDU Type	[1] 4.4.9.21	m		0000_2	
2	OTAR sub-type	[1] 4.4.9.20	m		010_2	
3	Random seed	[1] 4.4.9.25	m			
4	Number of SCKs provided	[1] 4.4.9.18	m		000_2 to 100_2	
5	SCK key and identifier	[1] 4.4.9.28	m			
6	Proprietary element	[1] 4.4.9.22	o			

Table B.27: Elements for D-OTAR GCK Provide PDU

Prerequisite: B.24/3						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	PDU Type	[1] 4.4.9.21	m		0000_2	
2	OTAR sub-type	[1] 4.4.9.20	m		100_2	
3	GSSI	[1] 4.4.9.9	m			
4	Address extension	[1] 4.4.9.1	m			
5	GCK and Identifier	[1] 4.4.9.7	m			
6	Proprietary element	[1] 4.4.9.22	o			

Table B.28: Elements for U-OTAR CCK Demand PDU

Prerequisite: B.24/4						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	PDU Type	[1] 4.4.9.21	m		0101_2	
2	OTAR sub-type	[1] 4.4.9.20	m		000_2	
3	Location area	[1] 4.4.9.10	m			
4	Proprietary element	[1] 4.4.9.22	o			

Table B.29: Elements for U-OTAR CCK Result PDU

Prerequisite: B.24/5						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	PDU Type	[1] 4.4.9.21	m		0101_2	
2	OTAR sub-type	[1] 4.4.9.20	m		001_2	
3	Provision result	[1] 4.4.9.23	m			
4	Future key flag	[1] 4.4.9	m			
5	Future key provision result	[1] 4.4.9.23	m			
6	Proprietary element	[1] 4.4.9.22	o			

Table B.30: Elements for U-OTAR SCK Demand PDU

Prerequisite: B.24/6						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	PDU Type	[1] 4.4.9.21	m		0101_2	
2	OTAR sub-type	[1] 4.4.9.20	m		010_2	
3	Number of SCKs requested	[1] 4.4.9.19	m		00_2 to 11_2	
4	SCK number (SCKN)	[1] 4.4.9.29	m			
5	Proprietary element	[1] 4.4.9.22	o			

Table B.31: Elements for U-OTAR SCK Result PDU

Prerequisite: B.24/7						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	PDU Type	[1] 4.4.9.21	m		0101_2	
2	OTAR sub-type	[1] 4.4.9.20	m		011_2	
3	Number of SCKs requested	[1] 4.4.9.19	m		00_2 to 11_2	
4	SCK number and result	[1] 4.4.9.30	m			
5	Proprietary element	[1] 4.4.9.22	o			

Table B.32: Elements for U-OTAR GCK Demand PDU

Prerequisite: B.24/8						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	PDU Type	[1] 4.4.9.21	m		0101_2	
2	OTAR sub-type	[1] 4.4.9.20	m		100_2	
3	GSSI	[1] 4.4.9.9	m			
4	Address Extension	[1] 4.4.9.1	o			
5	Proprietary element	[1] 4.4.9.22	o			

Table B.33: Elements for U-OTAR GCK Result PDU

Prerequisite: B.24/9						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	PDU Type	[1] 4.4.9.21	m		0101_2	
2	OTAR sub-type	[1] 4.4.9.20	m		101_2	
3	GCK Version Number	[1] 4.4.9.8	m			
4	Provision result (GCK)	[1] 4.4.9.23	m			
5	GSSI	[1] 4.4.9.9	m			
6	Address Extension	[1] 4.4.9.1	m			
7	Proprietary element	[1] 4.4.9.22	o			

B.5.5 Registration PDU extended elements

The support of OTAR CCK Delivery during registration requires that the implementation support the MM PDUs identified by tables B.24/10 and B.24/11. Support of the MM-registration PDUs shall be declared in the TETRA V+D PICS Proforma ETS 300 392-14. The following "type 3" elements are used to support CCK Delivery in these PDUs.

Table B.34: MM Type 3 elements for security enabling at registration

Prerequisite: B.24/10 AND B.24/11				
Item	**Type 3 element**	**Reference**	**Status**	**Support**
1	Authentication uplink	[1] 4.4.8.2	m	
2	Authentication downlink	[1] 4.4.8.1	m	

Table B.35: Elements for authentication uplink type 3 element

Prerequisite: B.34/1				
Item	**Element**	**Reference**	**Status**	**Support**
1	CCK request flag	[1] 4.4.9.6	m	
2	Random challenge	[1] 4.4.9.24	o	

Table B.36: Elements for authentication downlink type 3 element

Prerequisite: B.34/2				
Item	**Element**	**Reference**	**Status**	**Support**
1	Authentication result	[1] 4.4.9.3	m	
2	TEI request flag	[1] 4.4.9.34	m	
3	CCK information flag	[1] 4.4.7.2	m	
4	CCK information	[1] 4.4.9.5	m	

B.6 Enable/disable

NOTE: This clause needs to be completed only if the IUT supports enable/disable.

Are all mandatory capabilities of enable/disable implemented? (Yes/No) ....

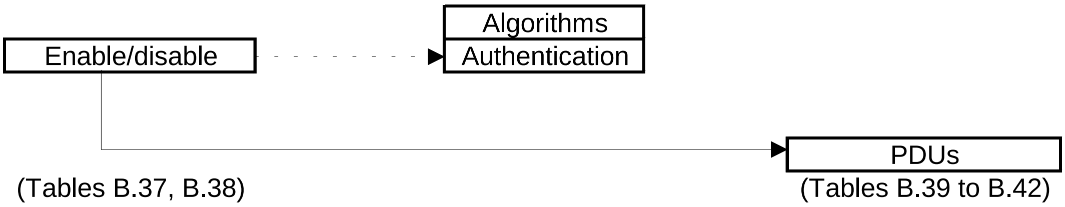


Figure B.4: Enable/disable PICS tables navigation map

Figure B.4 is intended to assist in identifying the tables that should be completed for those implementations purporting to support enable/disable as defined in ETS 300 392-7 [1], clause 5.

Table B.37: Enable/disable modes

Prerequisite: B.2/3 – IUT supports enable/disable				
Item	**Enable/disable sub-type**	**Reference**	**Status**	**Support**
1	Without embedded authentication	[1] 5.3.2	m	
2	With embedded authentication	[1] 5.3.2	c3701	

c3701: IF B.2/1 - If IUT supports authentication then mandatory, else not applicable
THEN m
ELSE n/a

Table B.38: Enable/disable sub-types

Prerequisite: B.37/1 OR B.37/2 – IUT supports one of the enable/disable modes				
Item	**Enable/disable sub-type**	**Reference**	**Status**	**Support**
1	Disable ITSI temporarily	[1] 5.3.2	m	
2	Disable ITSI permanently	[1] 5.3.2	c3801	
3	Enable ITSI	[1] 5.3.5	m	
4	Disable TEI temporarily	[1] 5.3.1	m	
5	Disable TEI permanently	[1] 5.3.1	c3801	
6	Enable TEI	[1] 5.3.4	m	

c3801: IF B.37/1 - If IUT supports enable disable with embedded authentication then mandatory,
THEN m - else not applicable
ELSE n/a

B.6.1 Enable Disable PDUs

Table B.39: Enable/disable PDUs

Prerequisite: B.2/3				
Item	**Enable/disable PDU**	**Reference**	**Status**	**Support**
1	D-DISABLE	[1] 5.4.7.1	m	
2	D-ENABLE	[1] 5.4.7.2	m	
3	U-DISABLE STATUS	[1] 5.4.7.3	m	

B.6.2 Secure Enable Disable PDU elements

Table B.40: Elements for D-DISABLE PDU

Prerequisite: B.39/1 – IUT supports enable/disable				
Item	**Information Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 5.4.8.9	m	
2	Intent/Confirm	[1] 5.4.8.8	m	
3	Disabling type	[1] 5.4.8.3	m	
4	Equipment disable	[1] 5.4.8.5	m	
5	TETRA Equipment Identity	[1] 5.4.8.14	m	
6	Subscription disable	[1] 5.4.8.11	m	
7	Address Extension	[1] 5.4.8.1	m	
8	SSI		m	
9	Authentication challenge	[1] 5.4.8.2	c4001	
10	Proprietary	[1] 5.4.8.10	o	

c4001: IF B.37/2 - If IUT supports enable/disable with embedded authentication then mandatory,
THEN m - else not applicable
ELSE n/a

Table B.41: Elements for D-ENABLE PDU

Prerequisite: B.39/2 – IUT supports enable/disable				
Item	**Information Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 5.4.8.9	m	
2	Intent/Confirm	[1] 5.4.8.8	m	
3	Equipment enable	[1] 5.4.8.6	m	
4	TETRA Equipment Identity	[1] 5.4.8.14	m	
5	Subscription enable	[1] 5.4.8.12	m	
6	Address Extension	[1] 5.4.8.1	m	
7	SSI		m	
8	Authentication challenge	[1] 5.4.8.2	c4101	
9	Proprietary	[1] 5.4.8.10	o	

c4101: IF B.37/2 - If IUT supports enable/disable with embedded authentication then mandatory,
THEN m - else not applicable
ELSE n/a

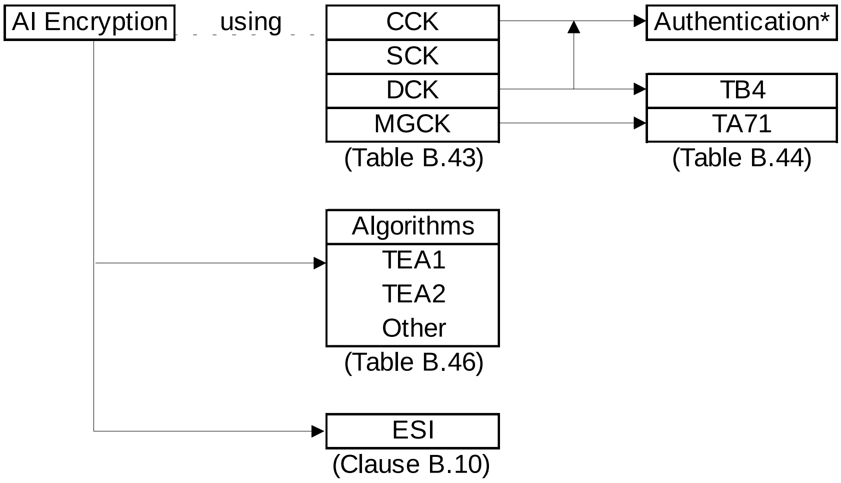
Table B.42: Elements for U-DISABLE STATUS PDU

Prerequisite: B.39/3 – IUT supports enable/disable				
Item	**Information Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 5.4.8.9	m	
2	Equipment status	[1] 5.4.8.7	m	
3	Subscription status	[1] 5.4.8.13	m	
4	Enable/Disable result	[1] 5.4.8.4	m	
5	Address Extension	[1] 5.4.8.1	m	
6	SSI		m	
7	TETRA Equipment Identity	[1] 5.4.8.14	m	
8	Proprietary	[1] 5.4.8.10	o	

B.7 AI encryption

NOTE: This clause needs to be completed only if the IUT supports AI encryption.

Are all mandatory capabilities of AI encryption implemented? (Yes/No) ....



*Authentication and DCK are prerequisites of using CCK.

Figure B.5: AI encryption PICS tables navigation map

Figure B.5 is intended to assist in identifying the tables that should be completed for those implementations purporting to support air interface encryption as defined in ETS 300 392-7 [1], clause 6.

Table B.43: AI encryption with key type

Prerequisite: B.2/4 – IUT supports AI encryption				
Item	**Encryption type**	**Reference**	**Status**	**Support**
1	DCK AI encryption	[1] 6.1.2	c4301	
2	SCK AI encryption	[1] 6.1.2	c4302	
3	CCK AI encryption	[1] 6.1.2	c4301	
4	MGCK AI encryption	[1] 6.1.2	c4303	

c4301: B.1/3 - If IUT is of class 3 then mandatory, else not applicable
THEN m
ELSE n/a

c4302: B.1/2 - If IUT is of class 2 then mandatory, else not applicable
THEN m
ELSE n/a

c4303: B.1/3 - If IUT is of class 3 then optional, else not applicable
THEN o
ELSE n/a

B.7.1 AI encryption algorithms and keys

The supplier of the implementation shall state the support of each algorithm.

If the algorithms are not sourced from TAA1 the source of the algorithms shall be specified in subclause A.2.7.

Table B.44: AI key management algorithms

Prerequisite: B.43/1 OR B.43/4 – IUT supports DCK or MGCK encryption				
Item	**Algorithm**	**Reference**	**Status**	**Support**
1	TA71	[1] 4.2.2	c4401	
2	TB4	[1] 4.2.1	c4402	
NOTE: Support of any of the algorithms (TAxx) requires that the conformance tests defined for the algorithms have been successfully completed.				

c4401: IF B.43/4 - If MGCK is used then mandatory, else not applicable
THEN m
ELSE n/a

c4402: IF B.43/1 - If IUT supports DCK AI encryption then mandatory, else not applicable
THEN m
ELSE n/a

Table B.45: AI encryption key and address relations

Prerequisite: B.43/1 OR B.43/2 OR B.43/3 OR B.43/4 – IUT supports AI encryption				
Item	**Algorithm**	**Reference**	**Status**	**Support**
1	K-ITSI	[1] 4.2.6	c4501	
2	SCK-ITSI	[1] 4.2.6	c4502	
3	GCK-GTSI	[1] 4.2.6	c4503	
4	CCK-CCKid-LAid	[1] 4.2.6	c4504	

c4501: IF B.43/1 - If IUT supports DCK AI encryption then mandatory, else optional
THEN m
ELSE o

NOTE: For DCK AI encryption DCK is supported through authentication, table 45 does not address this relation.

c4502: IF B.43/2 - If IUT supports SCK AI encryption then mandatory, else optional
THEN m
ELSE o

c4503: IF B.43/4 - If IUT supports MGCK AI encryption then mandatory, else optional
THEN m
ELSE o

c4504: IF B.43/3 OR B.43/4
THEN m - If IUT supports CCK or MGCK AI encryption then mandatory, else optional
ELSE o

B.7.2 AI encryption algorithms (KSG)

The supplier of the implementation shall state the support of encryption algorithms.

Table B.46: Encryption algorithm (KSG)

Prerequisite: B.43/1 OR B.43/2 OR B.43/3 OR B.43/4 – IUT supports AI encryption					
Item	**Algorithm**	**Reference**	**Status**	**Values**	
				Allowed	**Supported**
1	TEA1	[1] 6.1.3	o.4601	0000_2	
2	TEA2	[1] 6.1.3	o.4601	0001_2	
3	TEA3	[1] 6.1.3	o.4601	0010_2	
4	TEA4	[1] 6.1.3	o.4601	0011_2	
5	Other	[1] 6.1.3	o.4601	0100_2 to 1111_2	
NOTE: Support of the algorithms (TEA1 or TEA2) requires that the conformance tests defined for the algorithm have been successfully completed.					

o.4601: It is mandatory to support at least one of these items

B.8 Key change protocol

NOTE: This clause needs to be completed only if the IUT supports the key change protocol.

Are all mandatory capabilities of the key change protocol implemented? (Yes/No) ....

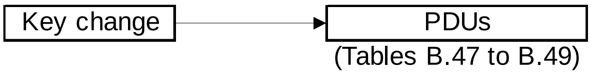


Figure B.6: Key change protocol PICS tables navigation map

Figure B.6 is intended to assist in identifying the tables that should be completed for those implementations purporting to support the key change protocol as defined in ETS 300 392-7 [1], clause 4.

Table B.47: Key change PDUs

Prerequisite: B.2/8 – IUT supports key change protocol				
Item	**Information Element**	**Reference**	**Status**	**Support**
1	D-CK-CHANGE DEMAND	[1] 4.4.7.5	m	
2	U-CK CHANGE RESULT	[1] 4.4.7.13	m	

Table B.48: Elements for D-CK CHANGE DEMAND PDU

Prerequisite: B.47/1 – IUT supports D-CK CHANGE DEMAND PDU				
Item	**Information Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 4.4.7.19	m	
2	Acknowledgement flag	[1] 4.4.7.19	m	
3	Key type	[1] 4.4.7.19	m	
4	SCKN	[1] 4.4.9.29	c4801	
5	SCK-VN	[1] 4.4.9.31	c4801	
6	CCK-id	[1] 4.4.9.4	c4802	
7	GCK-VN	[1] 4.4.9.8	c4803	
8	Time type	[1] 4.4.7.19	m	
9	IV	[1] 4.4.7.19	m	
10	System time	[1] 4.4.7.19	m	

c4801: IF B.21/3 - If SCK OTAR then mandatory, else not applicable
THEN m
ELSE n/a

c4802: IF B.21/1 or B.21/4 - If CCK delivery or CCK deliver at registration then mandatory,

THEN m - else not applicable
ELSE n/a

c4803: IF B.21/2 - If OTAR GCK then mandatory, else not applicable
THEN m
ELSE n/a

Table B.49: Elements for U-CK CHANGE RESULT PDU

Prerequisite: B.47/2 – IUT supports U-CK CHANGE RESULT PDU				
Item	**Information Element**	**Reference**	**Status**	**Support**
1	PDU Type	[1] 4.4.7.20	m	
2	Result	[1] 4.4.7.20	m	

B.9 End-to-end encryption

NOTE: This clause needs to be completed only if the IUT supports end-to end encryption.

There are no mandatory capabilities of end-to-end encryption. Support is only visible by use of the encrypted call type in CMCE.

Are all mandatory capabilities of end-to-end encryption implemented? (Yes/No) ....

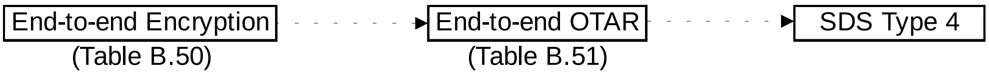


Figure B.7: End-to-end encryption PICS tables navigation map

Figure B.7 is intended to assist in identifying the tables that should be completed for those implementations purporting to support end-to-end encryption as defined in ETS 300 392-7 [1], clause 7.

Table B.50: End-to-end encryption

Prerequisite: B.2/5 – IUT supports end-to-end encryption				
Item	**End-to-end encryption facilities**	**Reference**	**Status**	**Support**
1	End-to-end OTAR	[1] 7	o	

End to end encryption is supported by allowing the encrypted call type element in the U-SETUP PDU (defined in ETS 300 392-2 [4]) to be set to TRUE.

Table B.51: End-to-end OTAR PDUs

Prerequisite: B.50/1 – IUT supports end-to-end OTAR				
Item	**OTAR sub-type**	**Reference**	**Status**	**Support**
1	U-SDS-DATA	[1] 7.6	m	
2	D-SDS-DATA	[1] 7.6	m	
NOTE 1: Only SDS-Type 4 applies for End-to-end OTAR, i.e. element short data type identifier of each of the SDS-DATA PDUs is set to 11_2 and the first byte of the data content is set to 01_{16}. NOTE 2: U-SDS DATA and D-SDS DATA are defined in ETS 300 392-2 [4].				

Table B.52: Elements for U-SDS-DATA as applied to end-to-end OTAR

Prerequisite: B.51/1 – IUT supports U-SDS-DATA PDU						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	PDU Type		m		01111_2	
2	Area selection		m			
3	Called party type identifier		m			
4	Called party short number address		m			
5	Called party SSI		m			
6	Called party extension		m			
7	Short data type identifier		m		11_2	
8	User defined data-1		o			
9	User defined data-2		o			
10	User defined data-3		o			
11	Length indicator		m			
12	User defined data-4		m			
13	External subscriber number		o			
14	Proprietary element		o			

Table B.53: Elements for D-SDS-DATA as applied to end-to-end OTAR

Prerequisite: B.51/2 – IUT supports D-SDS-DATA PDU						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	PDU Type		m		01111_2	
2	Calling party type identifier		m			
3	Calling party SSI		m			
4	Calling party extension		m			
5	Short data type identifier		m		11_2	
6	User defined data-1		o			
7	User defined data-2		o			
8	User defined data-3		o			
9	Length indicator		m			
10	User defined data-4		m			
11	Proprietary element		o			

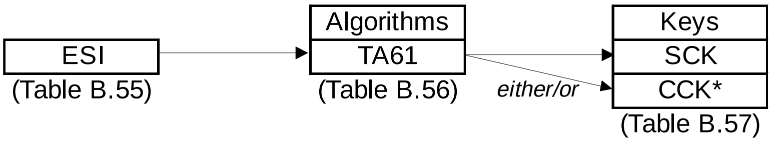
Table B.54: Encoding of SDS User defined data-4 element

Prerequisite: B.51/1 OR B.51/2 – IUT supports D-SDS DATA or U-SDS DATA PDUs					
Item	**Information Element**	**Reference**	**Status**	**Value**	**Support**
1	SDS Type 4 header	[1] 7.6	m	00000001_2	
2	Data	[1] 7.6	m		

B.10 Encrypted short identities

NOTE: This clause needs to be completed only if the IUT supports AI encryption.

Are all mandatory capabilities of ESI implemented? (Yes/No) ....



*Authentication and DCK are prerequisites for use of CCK.

Figure B.8: ESI PICS table navigation map

Figure B.8 is intended to assist in identifying the tables that should be completed for those implementations purporting to support ESI as defined in ETS 300 392-7 [1], clause 6.

Table B.55: ESI sub-types

Prerequisite: B.2/7 – IUT supports ESI				
Item	**ESI sub-type**	**Reference**	**Status**	**Support**
1	CCK address encryption	[1] 4.2.5	c5501	
2	SCK address encryption	[1] 4.2.5	c5502	

c5501: IF B.1/3 - If class 3 then CCK address encryption is mandatory, else not applicable
THEN m
ELSE n/a

c5502: IF B.1/2 - If class 2 then SCK address encryption is mandatory, else not applicable
THEN m
ELSE n/a

B.10.1 ESI algorithms

The supplier of the implementation shall state the support of the ESI authentication algorithm.

If the algorithms are not sourced from TAA1 the source of the algorithms shall be specified in subclause A.2.7.

Table B.56: ESI algorithms

Prerequisite: B.55/1 OR B.55/2 – IUT supports ESI with SCK or CCK				
Item	**Algorithm**	**Reference**	**Status**	**Support**
1	TA61	[1] 4.2.5	m	
NOTE: Support of any of the algorithms (TAxx) requires that the conformance tests defined for the algorithms have been successfully completed.				

B.10.2 ESI keys

The supplier of the implementation shall state the support of the cipher keys required for ESI.

Table B.57: ESI keys

Prerequisite: B.55/1 OR B.55/2 – IUT supports ESI with SCK or CCK				
Item	**Key**	**Reference**	**Status**	**Support**
1	SCK	[1] 4.2.5	c5701	
2	CCK	[1] 4.2.5	c5702	

c5701: B.55/2 - If class 2 then mandatory, else not applicable
THEN m
ELSE n/a

c5702: B.55/1 - If class 3 then mandatory, else not applicable

THEN m
ELSE n/a

B.11 TEI delivery

NOTE: This clause needs to be completed only if the IUT supports TEI delivery.

Are all mandatory capabilities of TEI delivery implemented? (Yes/No) ....

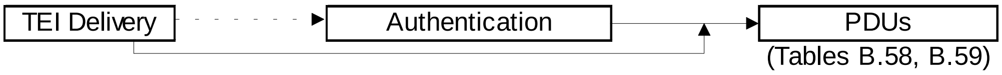


Figure B.9: TEI PICS table navigation map

Figure B.9 is intended to assist in identifying the tables that should be completed for those implementations purporting to support TEI delivery as defined in ETS 300 392-7 [1], clause 6.

B.11.1 TEI delivery PDU

Table B.58: TEI delivery PDUs

Prerequisite: B.2/6 – TEI delivery supported				
Item	**TEI delivery PDU**	**Reference**	**Status**	**Support**
1	U-TEI PROVIDE	[1] 4.4.6.18	m	
2	D-LOCATION UPDATE ACCEPT	[1] 4.4.2.5	m	

B.11.2 TEI delivery PDU elements

Table B.59: Elements for U-TEI PROVIDE PDU

Prerequisite: B.58/1						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	PDU Type	[1] 4.4.8.21	m		1001_2	
2	TEI	[1] 4.4.8.33	m			
3	SSI	[1]	m			
4	Address extension	[1] 4.4.8.1	m			
5	Proprietary element	[1] 4.4.8.22	o			

B.11.3 Registration PDU extended elements

The support of TEI Delivery requires that the implementation supports the MM PDU identified by A.51/2. Support of the MM-registration PDUs shall be declared in the TETRA V+D PICS Proforma ETS 300 392–xx. The following "type 3" elements are used to support CCK Delivery in these PDUs.

Table B.60: MM Type 3 elements for security enabling at registration

Prerequisite: B.58/2				
Item	**Type 3 element**	**Reference**	**Status**	**Support**
1	Authentication downlink	[1] 4.4.8.1	m	

Table B.61: Elements for authentication downlink type 3 element

Prerequisite: B.60/1				
Item	**Element**	**Reference**	**Status**	**Support**
1	Authentication result	[1] 4.4.9.3	m	
2	TEI request flag	[1] 4.4.9.35	m	
3	CCK provision flag	[1] 4.4.8.1	m	
4	CCK information	[1] 4.4.9.5	o	

B.12 PDU support

Are all mandatory capabilities of PDU support implemented? (Yes/No) ....

It is mandatory to support the encoding and decoding of PDUs used in any TETRA layer 3 service.

Table B.62: PDU en/decoding

Prerequisite: B.1/1 OR B.1/2 OR B.1/3				
Item	**Description**	**Reference**	**Status**	**Support**
1	PDU encoding	[1] 4.4.6	m	
2	PDU decoding	[1] 4.4.6	m	

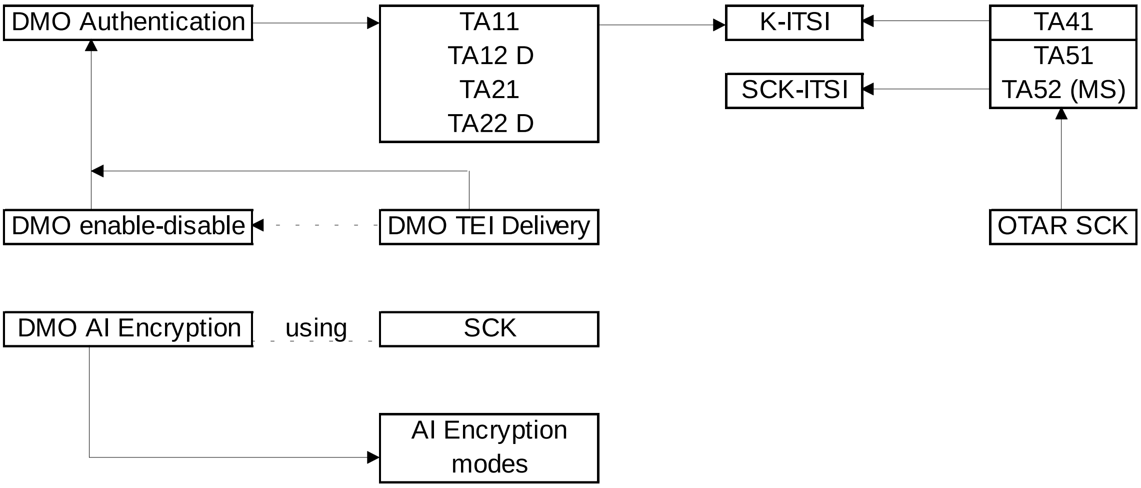
Annex C (normative): Protocol ICS tables proforma for TETRA DMO Security

C.1 Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No) ....

NOTE: Answering "No" to this question indicates non-conformance to the protocol specification. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming, on pages attached to the PICS proforma.

The figure below gives an overview of the structure of the DMO PICS tables:



NOTE: Authentication in DMO is embedded in Secure Enable/Disable

Figure C.1: Overall structure of DMO PICS annex

Table C.1: DMO Entities supported

Item	Entity	Reference	Status	Support
1	DMO-OTAR	2	o	
2	DMO-Secure enable/disable	2	o	
3	DMO-AI encryption	2	o	
4	DMO-End-to-end encryption	2	o	

C.2 OTAR in DMO

NOTE: Support of this facility requires that the OTAR facility of DMO is supported.

Are all mandatory capabilities of DMO OTAR operation implemented? (Yes/No) ....

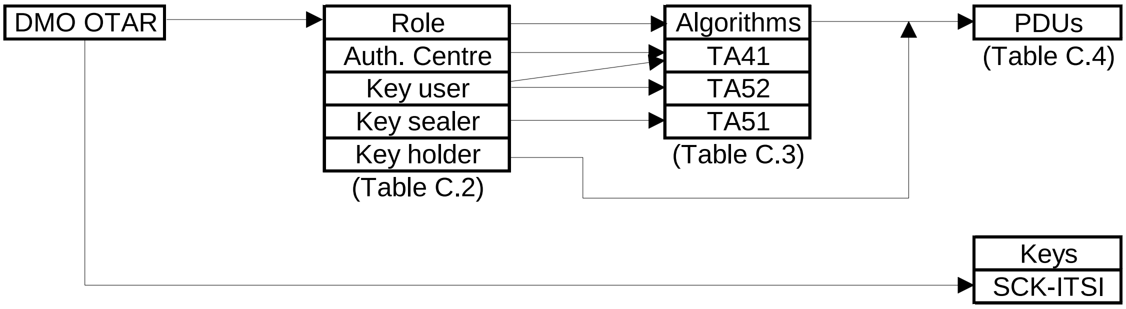


Figure C.2: DMO OTAR PICS table navigation map

Figure C.2 is intended to assist in identifying the tables that should be completed for those implementations purporting to support OTAR in DMO as defined in ETS 300 396-6 [2], clause 7.

For TETRA Direct Mode the implementor should indicate the support of roles.

Table C.2: DMO OTAR roles

Prerequisite: C.1/1 – IUT supports DMO OTAR				
Item	**OTAR role**	**Reference**	**Status**	**Support**
1	Key Sealer	[2] 7.4	o.201	
2	Key User	[2] 7.4	o.201	
3	Key Holder	[2] 7.4	o.201	

o.201 It is mandatory to support at least one of these items

NOTE: An implementation may support more than one role.

C.2.1 DMO OTAR algorithms

The supplier of the implementation shall state the support of the OTAR-SCK algorithms.

If the algorithms are not sourced from TAA1 the source of the algorithms shall be specified in subclause A.2.7.

Table C.3: DMO OTAR algorithms

Prerequisite: C.2/1 OR C.2/2 – IUT supports Key sealer or Key user role				
Item	**Capability**	**Reference**	**Status**	**Support**
1	TA41	[2] 7.2	c301	
2	TA51	[2] 7.2	c302	
3	TA52	[2] 7.2	c301	

c301: IF C.2/2 - If Key user then mandatory, else not applicable
THEN m
ELSE n/a

c302: IF C.2/1 - If key sealer then mandatory, else not applicable
THEN m
ELSE n/a

NOTE: Support of any of the algorithms (TAxx) requires that the conformance tests defined for the algorithms have been successfully completed.

C.2.2 OTAR DMO PDUs

Table C.4: DMO OTAR PDUs

Prerequisite: C.2/1 OR C.2/2 OR C.2/3 – IUT supports any DMO OTAR role				
Item	**Authentication sub-type**	**Reference**	**Status**	**Support**
1	OTAR SCK Provide	[2] 7.6.1	m	
2	OTAR SCK Demand	[2] 7.6.2	m	
3	OTAR SCK Result	[2] 7.6.3	m	

C.2.3 OTAR DMO PDU elements

Table C.5: Elements for OTAR SCK Provide PDU

Prerequisite: C.4/1 – IUT supports OTAR SCK Provide PDU						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	OTAR SCK sub-Type	[2] 7.7.8	m			
2	Random seed	[2] 7.7.11	m			
3	Number of SCKs provided	[2] 7.7.6	m		000_2 to 100_2	
4	ITSI Flag	[2] 7.7.3	m			
5	ITSI	[2] 7.7.2	c501			
6	SCK and identifier	[2] 7.7.12	m			
7	Provision result	[2] 7.7.10	m		100_2	
8	Proprietary	[2] 7.7.9	o			

c501: IF C.2/1 OR C.2/3 - If key sealer or key holder role then mandatory, else not applicable
THEN m
ELSE n/a

Table C.6: Elements of OTAR SCK Demand PDU

Prerequisite: C.4/2 – IUT supports OTAR SCK Demand PDU						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	OTAR SCK sub-Type	[2] 7.7.8	m			
2	ITSI flag	[2] 7.7.3	m			
3	ITSI	[2] 7.7.2	c601			
4	Number of SCKs requested	[2] 7.7.7	m		001_2 to 100_2	
5	SCK number (SCKN)	[2] 7.7.13	m			
6	Proprietary	[2] 7.7.9	o			

c601: IF C.2/1 OR C.2/3 - If key sealer or key holder role then mandatory, else not applicable
THEN m
ELSE n/a

Table C.7: Elements of OTAR SCK Result PDU

Prerequisite: C.4/3 – IUT supports OTAR SCK Result PDU						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	OTAR SCK sub-Type	[2] 7.7.8	m			
2	ITSI flag	[2] 7.7.3	m			
3	ITSI	[2] 7.7.2	m			
4	Number of SCKs requested	[2] 7.7.7	m		001_2 to 100_2	
5	SCK number and result	[2] 7.7.14	m			
6	Proprietary	[2] 7.7.9	o			

C.2.4 SDS Element encoding for carriage of OTAR PDUs

NOTE: Each OTAR PDU is carried using the SDS mechanism of DMO. The SDS PDUs are defined in ETS 300 396-3 [5] and the encoding of the SDTI element is given below.

Table C.8: DM SDS PDUs

Prerequisite: C.1/1 – IUT supports DMO OTAR				
Item	**OTAR sub-type**	**Reference**	**Status**	**Support**
1	DM-SDS-UDATA	[1] 7.6	m	
2	DM-SDS-DATA	[1] 7.6	m	
3	DM-SDS ACK	[1] 7.6	m	

Table C.9: Elements for DM-SDS-UDATA as applied to OTAR

Prerequisite: C.8/1 – IUT supports DM-SDS-UDATA for OTAR in DMO						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	SDS time remaining		m			
2	SDS transaction type		m			
3	Priority level		m			
4	FCS flag		m			
5	Additional addressing flag		m			
6	Additional addressing type(s)		m			
7	Calling party TSI		m			
8	Short data type identifier		m		0101_2	
9	User defined data-1		o			
10	User defined data-2		o			
11	User defined data-3		o			
12	Length indicator		m			
13	User defined data-4		o			
14	Precoded status		o			
15	OTAR information		m			
16	Enable/disable information		o			
17	FCS		m			

Table C.10: Elements for DM-SDS-DATA as applied to OTAR

Prerequisite: C.8/2 – IUT supports DM-SDS-DATA for OTAR in DMO						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	SDS time remaining		m			
2	SDS transaction type		m			
3	Priority level		m			
4	FCS flag		m			
5	Additional addressing flag		m			
6	Additional addressing type(s)		m			
7	Calling party TSI		m			
8	Short data type identifier		m		0101_2	
9	User defined data-1		o			
10	User defined data-2		o			
11	User defined data-3		o			
12	Length indicator		m			
13	User defined data-4		o			
14	Precoded status		o			
15	OTAR information		m			
16	Enable/disable information		o			
17	FCS		m			

Table C.11: Elements for DM-SDS-ACK as applied to OTAR

Prerequisite: C.8/3 – IUT supports DM-SDS-ACK for OTAR in DMO						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	FCS flag		m			
2	Acknowledgement type		m			
3	Short data type identifier		m		0101_2	
4	User defined data-1		o			
5	User defined data-2		o			
6	User defined data-3		o			
7	Length indicator		m			
8	User defined data-4		o			
9	Precoded status		o			
10	OTAR information		m			
11	Enable/disable information		o			
12	FCS		m			

C.3 Secure enable/disable in DMO

NOTE: Support of this facility requires that the Secure enable disable facility of DMO is supported.

Are all mandatory capabilities of DMO Enable/disable operation implemented? (Yes/No) ....

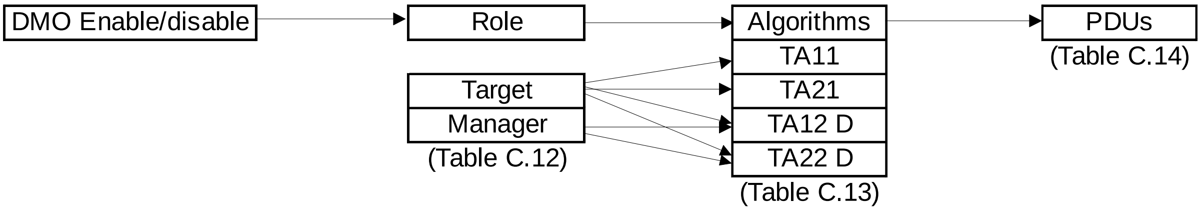


Figure C.3: DMO secure enable/disable PICS table navigation map

Figure C.3 is intended to assist in identifying the tables that should be completed for those implementations purporting to support secure enable/disable in DMO as defined in ETS 300 396-6 [2], clause 8.

For TETRA Direct Mode the implementer should indicate the support of roles.

Table C.12: DMO Enable/disable roles

Prerequisite: C.1/2 – IUT supports enable/disable in DMO				
Item	**Secure enable/disable sub-type**	**Reference**	**Status**	**Support**
1	Manager	[2] 8.5	o.1201	
2	Target	[2] 8.5	o.1201	

o.1201 It is mandatory to support at least one of these items

NOTE: An implementation may support more than one role.

C.3.1 DMO Secure enable/disable algorithms

The supplier of the implementation shall state the support of the enable/disable authentication algorithms

If the algorithms are not sourced from TAA1 the source of the algorithms shall be specified in subclause A.2.7.

Table C.13: DMO secure enable/disable authentication algorithms

Prerequisite: C.12/1 OR C.12/2 – IUT supports manager or target role				
Item	**Capability**	**Reference**	**Status**	**Support**
1	TA11	[2] 8.5	c1301	
2	TA21	[2] 8.5	c1301	
3	TA12 D	[2] 8.5	m	
4	TA22 D	[2] 8.5	m	

c1301: IF C.12/2 - If IUT supports the target role then mandatory, else not applicable
THEN m
ELSE n/a

NOTE: Support of any of the algorithms (TAxx) requires that the conformance tests defined for the algorithms have been successfully completed.

C.3.2 DMO secure enable/disable PDUs

Table C.14: DMO secure enable/disable PDUs

Prerequisite: C.12/1 OR C.12/2 – IUT supports manager or target role				
Item	**Authentication sub-type**	**Reference**	**Status**	**Support**
1	ENDIS COMMAND	[2] 8.7.4.1	m	
2	ENDIS AUTHENTICATE	[2] 8.7.4.2	m	
3	ENDIS COMMAND CONFIRM	[2] 8.7.4.3	m	
4	ENDIS RESULT	[2] 8.7.4.4	m	
5	ENDIS TEI PROVIDE	[2] 8.7.4.5	m	
6	ENDIS REJECT	[2] 8.7.4.6	m	

C.3.3 ENDIS PDU elements

Table C.15: Elements of ENDIS COMMAND PDU

Prerequisite: C.14/1 – IUT supports ENDIS COMMAND PDU				
Item	**Information Element**	**Reference**	**Status**	**Support**
1	ENDIS PDU type	[2] 8.7.5.7	m	
2	Command	[2] 8.7.5.5	m	
3	Random seed (RS)	[2] 8.7.5.13	m	
4	Authentication challenge (RAND1)	[2] 8.7.5.2	m	
5	ITSI	[2] 8.7.5.9	m	
6	TEI	[2] 8.7.5.18	m	
7	Proprietary	[2] 8.7.5.12	o	

Table C.16: Elements of ENDIS AUTHENTICATE PDU

Prerequisite: C.14/2 – IUT supports ENDIS AUTHENTICATE PDU				
Item	**Information Element**	**Reference**	**Status**	**Support**
1	ENDIS PDU type	[2] 8.7.5.7	m	
2	Authentication challenge (RAND1)	[2] 8.7.5.2	m	
3	Authentication response (RES1)	[2] 8.7.5.3	m	
4	Proprietary	[2] 8.7.5.12	o	

Table C.17: Elements of ENDIS COMMAND CONFIRM PDU

Prerequisite: C.14/3 – IUT supports ENDIS COMMAND CONFIRM PDU				
Item	**Information Element**	**Reference**	**Status**	**Support**
1	ENDIS PDU type	[2] 8.7.5.7	m	
2	Command	[2] 8.7.5.5	m	
3	Authentication response (RES2)	[2] 8.7.5.3	m	
4	Authentication result (R1)	[2] 8.7.5.4	m	
5	Proprietary	[2] 8.7.5.12	o	

Table C.18: Elements of ENDIS RESULT PDU

Prerequisite: C.14/4 – IUT supports ENDIS RESULT PDU				
Item	**Information Element**	**Reference**	**Status**	**Support**
1	ENDIS PDU type	[2] 8.7.5.7	m	
2	Authentication result (R2)	[2] 8.7.5.4	m	
3	Equipment status	[2] 8.7.5.8	m	
4	Subscription status	[2] 8.7.5.17	m	
5	Enable/Disable result	[2] 8.7.5.6	m	
6	Reject reason	[2] 8.7.5.14	m	
7	Proprietary	[2] 8.7.5.12	o	

Table C.19: Elements of ENDIS TEI PROVIDE PDU

Prerequisite: C.14/5 – IUT supports ENDIS TEI PROVIDE PDU				
Item	**Information Element**	**Reference**	**Status**	**Support**
1	ENDIS PDU type	[2] 8.7.5.7	m	
2	Authentication result (R2)	[2] 8.7.5.4	m	
3	TETRA Equipment identity	[2] 8.7.5.18	m	
4	Proprietary	[2] 8.7.5.12	o	

Table C.20: Elements of ENDIS REJECT PDU

Prerequisite: C.14/6 – IUT supports ENDIS REJECT PDU				
Item	**Information Element**	**Reference**	**Status**	**Support**
1	ENDIS PDU type	[2] 8.7.5.7	m	
2	Reject reason	[2] 8.7.5.14	m	
3	ITSI	[2] 8.7.5.9	m	
4	TEI	[2] 8.7.5.18	m	
5	Proprietary	[2] 8.7.5.12	o	

C.3.4 SDS Element encoding for carriage of ENDIS PDUs

NOTE: Each ENDIS PDU is carried using the SDS mechanism of DMO. The SDS PDUs are defined in ETS 300 396-3 [5] and the encoding of the SDTI element is given below.

Table C.21: DM SDS PDUs

Prerequisite: C.1/2 – IUT supports DMO enable/disable				
Item	**OTAR sub-type**	**Reference**	**Status**	**Support**
1	DM-SDS-UDATA	[1] 7.6	m	
2	DM-SDS-DATA	[1] 7.6	m	
3	DM-SDS ACK	[1] 7.6	m	

Table C.22: Elements for DM-SDS-UDATA as applied to ENDIS

Prerequisite: C.21/1 – IUT supports DM-SDS UDATA PDU						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	SDS time remaining		m			
2	SDS transaction type		m			
3	Priority level		m			
4	FCS flag		m			
5	Additional addressing flag		m			
6	Additional addressing type(s)		m			
7	Calling party TSI		m			
8	Short data type identifier		m		0110_2	
9	User defined data-1		o			
10	User defined data-2		o			
11	User defined data-3		o			
12	Length indicator		m			
13	User defined data-4		o			
14	Precoded status		o			
15	OTAR information		o			
16	Enable/disable information		m			
17	FCS		m			

Table C.23: Elements for DM-SDS-DATA as applied to ENDIS

Prerequisite: C.21/2 – IUT supports DM-SDS DATA PDU						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	SDS time remaining		m			
2	SDS transaction type		m			
3	Priority level		m			
4	FCS flag		m			
5	Additional addressing flag		m			
6	Additional addressing type(s)		m			
7	Calling party TSI		m			
8	Short data type identifier		m		0110_2	
9	User defined data-1		o			
10	User defined data-2		o			
11	User defined data-3		o			
12	Length indicator		m			
13	User defined data-4		o			
14	Precoded status		o			
15	OTAR information		o			
16	Enable/disable information		m			
17	FCS		m			

Table C.24: Elements for DM-SDS-ACK as applied to ENDIS

Prerequisite: C.21/3 – IUT supports DM-SDS ACK PDU						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	FCS flag		m			
2	Acknowledgement type		m			
3	Short data type identifier		m		0110_2	
4	User defined data-1		o			
5	User defined data-2		o			
6	User defined data-3		o			
7	Length indicator		m			
8	User defined data-4		o			
9	Precoded status		o			
10	OTAR information		o			
11	Enable/disable information		m			
12	FCS		m			

C.4 DMO AI encryption

NOTE: This clause needs to be completed only if the IUT supports DMO AI encryption.

Are all mandatory capabilities of DMO AI encryption implemented? (Yes/No) ....

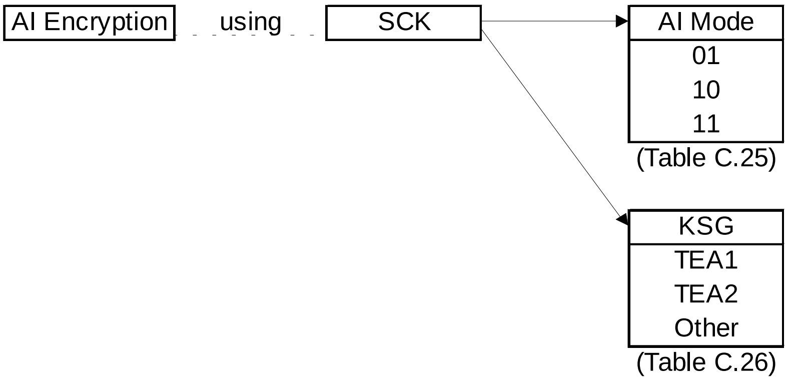


Figure C.4: DMO AI encryption PICS tables navigation map

Figure C.4 is intended to assist in identifying the tables that should be completed for those implementations purporting to support air interface encryption as defined in ETS 300 396-6 [2], clause 6.

Table C.25: DMO AI encryption mode

Prerequisite: C.1/3 – IUT supports AI encryption				
Item	**DMO AI encryption mode**	**Reference**	**Status**	**Support**
1	Encryption mode 00_2 (Clear operation)	[2] 6.3.2.1	m	
2	Encryption mode 01_2	[2] 6.3.2.1	o.2501	
3	Encryption mode 10_2	[2] 6.3.2.1	o.2501	
4	Encryption mode 11_2	[2] 6.3.2.1	o.2501	

o.2501 It is mandatory to support at least one of these items

C.4.1 DMO AI encryption algorithms

The supplier of the implementation shall state the support of encryption algorithms.

Table C.26: Encryption algorithm

Prerequisite: C.25/2 OR C.25/3 OR C.25/4 – IUT supports one of the (non clear) encryption modes					
Item	**Encryption algorithm**	**Reference**	**Status**	**Values**	
				Allowed	**Supported**
1	TEA1	[2] 6.2.1	o.2601	0000_2	
2	TEA2	[2] 6.2.1	o.2601	0001_2	
3	Other	[2] 6.2.1	o.2601	0010_2 to 1111_2	
NOTE:	Support of the algorithms (TEA1 or TEA2) requires that the conformance tests defined for the algorithm have been successfully completed.				

o.2601 It is mandatory to support at least one of these items

C.5 DMO End-to-end encryption

NOTE: This clause needs to be completed only if the IUT supports end-to end encryption.

There are no mandatory capabilities of end-to-end encryption. Support is only visible by use of the encrypted call type in CMCE.

Are all mandatory capabilities of end-to-end encryption implemented? (Yes/No) ....

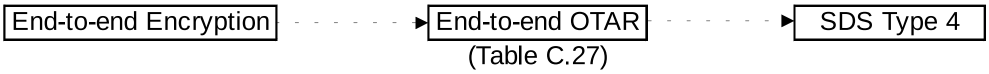


Figure C.5: End-to-end encryption PICS tables navigation map

Figure C.5 is intended to assist in identifying the tables that should be completed for those implementations purporting to support end-to-end encryption as defined in ETS 300 392-7 [1], clause 7, ETS 300 393-7 [6], clause 7 and ETS 300 396-6 [2], clause 9.

Table C.27: End-to-end encryption

Prerequisite: C.1/4 – IUT end-o-end encryption				
Item	**End-to-end encryption facilities**	**Reference**	**Status**	**Support**
1	End-to-end OTAR	[1] 7	o	

End to end encryption is supported by allowing the encrypted call type element in the U-SETUP PDU (defined in ETS 300 396-3 [5]) to be set to TRUE.

Table C.28: End-to-end OTAR PDUs

Prerequisite: C.27/1 – IUT supports DMO end-to-end OTAR				
Item	**OTAR sub-type**	**Reference**	**Status**	**Support**
1	DM-SDS-UDATA	[1] 7.6	m	
2	DM-SDS-DATA	[1] 7.6	m	
3	DM-SDS ACK	[1] 7.6	m	
NOTE 1:	Only SDS-Type 4 applies for End-to-end OTAR, i.e. element short data type identifier is of each of the SDS-DATA PDUs is set to 11_2 and the first byte of the data content is set to 01_{16}.			
NOTE 2:	DM-SDS DATA, DM-SDS U DATA and DM-SDS ACK are defined in ETS 300 396-3 [5].			

Table C.29: Elements for DM-SDS-UDATA as applied to end-to-end OTAR

Prerequisite: C.28/1 – IUT supports DM-SDS-UDATA PDU						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	SDS time remaining		m			
2	SDS transaction type		m			
3	Priority level		m			
4	FCS flag		m			
5	Additional addressing flag		m			
6	Additional addressing type(s)		m			
7	Calling party TSI		m			
8	Short data type identifier		m		0011_2	
9	User defined data-1		o			
10	User defined data-2		o			
11	User defined data-3		o			
12	Length indicator		m			
13	User defined data-4		m			
14	Precoded status		o			
15	OTAR information		o			
16	Enable/disable information		o			
17	FCS		m			

Table C.30: Elements for DM-SDS-DATA as applied to end-to-end OTAR

Prerequisite: C.28/2 – IUT supports DM-SDS-DATA PDU						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	SDS time remaining		m			
2	SDS transaction type		m			
3	Priority level		m			
4	FCS flag		m			
5	Additional addressing flag		m			
6	Additional addressing type(s)		m			
7	Calling party TSI		m			
8	Short data type identifier		m		0011_2	
9	User defined data-1		o			
10	User defined data-2		o			
11	User defined data-3		o			
12	Length indicator		m			
13	User defined data-4		m			
14	Precoded status		o			
15	OTAR information		o			
16	Enable/disable information		o			
17	FCS		m			

Table C.31: Elements for DM-SDS-ACK as applied to end-to-end OTAR

Prerequisite: C.28/3 – IUT supports DM-SDS-ACK PDU						
Item	**Information Element**	**Reference**	**Status**	**Support**	**Values**	
					Allowed	**Supported**
1	FCS flag		m			
2	Acknowledgement type		m			
3	Short data type identifier		m		0011_2	
4	User defined data-1		o			
5	User defined data-2		o			
6	User defined data-3		o			
7	Length indicator		m			
8	User defined data-4		m			
9	Precoded status		o			
10	OTAR information		o			
11	Enable/disable information		o			
12	FCS		m			

Table C.32: Encoding of SDS User defined data-4 element

Prerequisite: C.28/1 OR C.28/2 OR C.28/3 –IUT supports DM-SDS DATA or DM-SDS UDATA or DM-SDS ACK PDUs					
Item	**Information Element**	**Reference**	**Status**	**Value**	**Support**
1	SDS Type 4 header	[1] 7.6	m	00000001_2	
2	Data	[1] 7.6	m		

History

Document history			
January 1998	Public Enquiry	PE 9822:	1998-01-30 to 1998-05-29
April 1999	Vote	V 9925:	1999-04-20 to 1999-06-18