

ETSI EN 300 396-6 V1.5.1 (2012-09)



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

(<https://standards.iteh.ai>)
Document Preview

[ETSI EN 300 396-6 V1.5.1 \(2012-09\)](https://standards.iteh.ai/catalog/standards/etsi/eaf4827b-8e5e-46b2-825b-8d5b0cf77643/etsi-en-300-396-6-v1-5-1-2012-09)

<https://standards.iteh.ai/catalog/standards/etsi/eaf4827b-8e5e-46b2-825b-8d5b0cf77643/etsi-en-300-396-6-v1-5-1-2012-09>

Reference

REN/TETRA-06181

Keywordsair interface, data, DMO, security, security mode,
speech, TETRA**ETSI**650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

iteh Standards
(<https://standards.iteh.ai>)
Document Preview

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2012.
All rights reserved.

DECTTM, PLUGTESTSTM, UMTSTM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM and LTETM are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM[®] and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	5
Foreword.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	7
3 Definitions and abbreviations.....	7
3.1 Definitions.....	7
3.2 Abbreviations	8
4 DMO security class	9
4.1 General	9
4.2 DM-2-A.....	10
4.3 DM-2-B.....	10
4.4 DM-2-C.....	10
5 DMO call procedures	11
5.1 General	11
5.1.1 Security profile	11
5.1.1.1 Indication of security parameters	11
5.2 Security class on call setup.....	12
5.2.1 General.....	12
5.2.2 Normal behaviour	12
5.2.3 Exceptional behaviour	12
5.2.3.1 Call-setup with presence check.....	12
5.2.3.2 Call-setup without presence check.....	12
5.2.3.3 Behaviour post call-setup.....	12
5.3 Security class on call follow-on	13
5.3.1 General.....	13
5.3.2 Normal behaviour	13
5.3.3 Exceptional behaviour	13
6 Air interface authentication and key management mechanisms	14
6.1 Authentication	14
6.2 Repeater mode operation.....	14
6.3 Gateway mode operation.....	14
6.4 Air Interface (AI) key management mechanisms	16
6.4.1 Key grouping	16
6.4.2 Identification of cipher keys in signalling.....	19
7 Enable and disable mechanism.....	19
8 Air Interface (AI) encryption	19
8.1 General principles.....	19
8.2 Encryption mechanism	20
8.2.1 Allocation of KSS to logical channels.....	20
8.3 Application of KSS to specific PDUs.....	21
8.3.1 Class DM-1	21
8.3.2 Class DM-2A	21
8.3.2.1 DMAC-SYNC PDU encryption.....	21
8.3.2.2 DMAC-DATA PDU encryption	22
8.3.2.3 DMAC-FRAG PDU encryption.....	22
8.3.2.4 DMAC-END PDU encryption	22
8.3.2.5 DMAC-U-SIGNAL PDU encryption.....	23
8.3.2.6 Traffic channel encryption	23
8.3.3 Class DM-2B	23

8.3.3.1	DMAC-SYNC PDU encryption	24
8.3.3.2	DMAC-DATA PDU encryption	24
8.3.3.3	DMAC-FRAG PDU encryption	24
8.3.3.4	DMAC-END PDU encryption	25
8.3.3.5	DMAC-U-SIGNAL PDU encryption	25
8.3.3.6	Traffic channel encryption	25
8.3.4	Class DM-2C	25
8.3.4.1	DMAC-SYNC PDU encryption	26
8.3.4.2	DMAC-DATA PDU encryption	27
8.3.4.3	DMAC-FRAG PDU encryption	27
8.3.4.4	DMAC-END PDU encryption	27
8.3.4.5	DMAC-U-SIGNAL PDU encryption	27
8.3.4.6	Traffic channel encryption	28
8.4	Encryption of identities in repeater and gateway presence signal	28
9	Encryption synchronization	30
9.1	General	30
9.1.1	Algorithm to establish frame number to increment TVP	31
9.1.1.1	Master DM-MS operation	31
9.1.1.2	Slave DM-MS operation	31
9.2	TVP used for reception of normal bursts	32
9.3	Synchronization of calls through a repeater	32
9.3.1	Algorithm to establish frame number to increment TVP	33
9.3.1.1	Master DM-MS operation	33
9.3.1.2	Slave DM-MS operation	33
9.4	Synchronization of calls through a gateway	33
9.5	Synchronization of data calls where data is multi-slot interleaved	34
9.5.1	Recovery of stolen frames from interleaved data	35
Annex A (normative):	Key Stream Generator (KSG) boundary conditions	36
A.1	Overview	36
A.2	Use	37
A.3	Interfaces to the algorithm	37
A.3.1	ECK	37
A.3.1.1	Use of ECK in class DM-2-A and DM-2-B	37
A.3.1.2	Use of ECK in class DM-2-C	38
A.3.2	Keystream	38
A.3.3	Time Variant Parameter (TVP)	38
Annex B (normative):	Boundary conditions for cryptographic algorithm TB6	39
Annex C (informative):	Encryption control in DM-MS	40
C.1	General	40
C.2	Service description and primitives	40
C.2.1	DMCC-ENCRYPT primitive	41
C.2.2	DMC-ENCRYPTION primitive	43
C.3	Protocol functions	44
Annex D (informative):	Bibliography	45
Annex E (informative):	Change request history	46
History		47

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Terrestrial Trunked Radio (TETRA).

The present document is part 6 of a multi-part deliverable covering Direct Mode Operation, as identified below:

- Part 1: "General network design";
- Part 2: "Radio aspects";
- Part 3: "Mobile Station to Mobile Station (MS-MS) Air Interface (AI) protocol";
- Part 4: "Type 1 repeater air interface";
- Part 5: "Gateway air interface";
- Part 6: "Security";**
- Part 7: "Type 2 repeater air interface";
- Part 8: "Protocol Implementation Conformance Statement (PICS) proforma specification";
- Part 10: "Managed Direct Mode Operation (M-DMO)".

NOTE: Parts 7, 8 and 10 of this multi-part deliverable are of "historical" status and will not be updated according to this version of the standard.

National transposition dates

Date of adoption of this EN:	14 September 2012
Date of latest announcement of this EN (doa):	31 December 2012
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 June 2013
Date of withdrawal of any conflicting National Standard (dow):	30 June 2013

1 Scope

The present document defines the Terrestrial Trunked Radio system (TETRA) Direct Mode of operation. It specifies the basic Air Interface (AI), the interworking between Direct Mode Groups via Repeaters and interworking with the TETRA Trunked system via Gateways. It also specifies the security aspects in TETRA Direct Mode and the intrinsic services that are supported in addition to the basic bearer and teleservices.

The present document describes the security mechanisms in TETRA Direct Mode. It provides mechanisms for confidentiality of control signalling and user speech and data at the AI. It also provided some implicit authentication as a member of a group by knowledge of a shared secret encryption key.

The use of AI encryption gives both confidentiality protection against eavesdropping, and some implicit authentication.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

- [1] ETSI EN 300 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".
- [2] ISO 7498-2: "Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture".
- [3] ETSI EN 300 396-2: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 2: Radio aspects".
- [4] ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- [5] ETSI EN 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] ETSI TS 100 392-15: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 15: TETRA frequency bands, duplex spacings and channel numbering".
- [7] ETSI EN 302 109: "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption".
- [8] ETSI EN 300 396-5: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 5: Gateway air interface".
- [9] ETSI EN 300 396-4: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 4: Type 1 repeater air interface".