ETSI TS 100 396-6 V2.1.1 (2022-10)

TECHNICAL SPECIFICATION

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

Reference

RTS/TCCE-06209

Keywords

air 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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 https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**$^{®}$ and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee TETRA and Critical Communications Evolution (TCCE).

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 1: 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.

NOTE 2: Some parts are also published as Technical Specifications such as ETSI TS 100 396-6 (the present document) and those may be the latest version of the document.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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, user speech and data at the AI, using encryption algorithms from two different air interface encryption algorithm sets. 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

2.1 Normative 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 referenced document (including any amendments) applies.

NOTE 1: Some referenced ENs are also published as Technical Specifications. In all cases, the latest version of such a document, either EN or TS, should be taken as the referenced document.

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

NOTE 2: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

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".

2.2 Informative 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 referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 101 053-1: "Rules for the management of the TETRA standard encryption algorithms; Part 1: TEA1".

[i.2] ETSI TS 101 053-2: "Rules for the management of the TETRA standard encryption algorithms; Part 2: TEA2".

[i.3] ETSI TS 101 053-3: "Rules for the management of the TETRA standard encryption algorithms; Part 3: TEA3".

[i.4] ETSI TS 101 053-4: "Rules for the management of the TETRA standard encryption algorithms; Part 4: TEA4".

[i.5] ETSI TS 101 052-1: "Rules for the management of the TETRA standard authentication and key management algorithm set TAA1".

[i.6] ETSI TS 101 053-5: "TCCE Security (TCCE); Rules for the management of the TETRA standard encryption algorithms; Part 5: TEA5".

[i.7] ETSI TS 101 053-6: "TCCE Security (TCCE); Rules for the management of the TETRA standard encryption algorithms; Part 6: TEA6".

[i.8] ETSI TS 101 053-7: "TCCE Security (TCCE); Rules for the management of the TETRA standard encryption algorithms; Part 7: TEA7".

[i.9] ETSI EN 300 396-1: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 1: General network design".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

air interface encryption state: status of encryption in a call (on or off)

call transaction: all of the functions associated with a complete unidirectional transmission of information during a call

NOTE: A call is made up of one or more call transactions. In a simplex call these call transactions are sequential. See ETSI EN 300 396-3 [5].

Carrier Number (CN): integer, N, used in TETRA to represent the frequency of the RF carrier

NOTE: See ETSI TS 100 392-15 [6].

Cipher Key (CK): value that is used to determine the transformation of plain text to cipher text in a cryptographic algorithm

cipher text: data produced through the use of encipherment

NOTE: The semantic content of the resulting data is not available (ISO 7498-2 [2]).

crypto period: the length of time during which a specific key is in use

decipherment: reversal of a corresponding reversible encipherment

NOTE: See ISO 7498-2 [2].

Direct Mode Operation (DMO): mode of simplex operation where mobile subscriber radio units may communicate using radio frequencies which may be monitored by, but which are outside the control of, the TETRA TMO network

NOTE: DM operation is performed without intervention of any base station. See ETSI EN 300 396-3 [5].

DMO-net: number of DMO MSs communicating together and using common cryptographic parameters

encipherment: cryptographic transformation of data to produce cipher text

NOTE: See ISO 7498-2 [2].

Encryption Cipher Key (ECK): cipher key used as input to the KSG, derived from an address specific cipher key and randomly varied per channel using algorithm TB6 where a KSG from TEA set A is in use

end-to-end encryption: encryption within or at the source end system, with the corresponding decryption occurring only within or at the destination end system

explicit authentication: transaction initiated and completed specifically to demonstrate knowledge of a shared secret where the secret is not revealed

Extended Cipher Key (CKX): value that is used to determine the transformation of plain text to cipher text in a cryptographic algorithm where an air interface encryption algorithm from TEA set B is in use

Extended Static Cipher Key (SCKX): predetermined cipher key that may be used to provide confidentiality in class DM-2-A, DM-2-B and DM-2-C systems where an air interface encryption algorithm from TEA set B is in use

implicit authentication: authenticity demonstrated by proof of knowledge of a shared secret where that demonstration is a by-product of another function

Initial Value (IV): sequence of symbols that randomize the KSG inside the encryption unit

Key Association Group (KAG): set of keys associated with one or more GSSIs at different periods of time

key stream: pseudo random stream of symbols that is generated by a KSG for encipherment and decipherment

Key Stream Generator (KSG): cryptographic algorithm which produces a stream of binary digits which can be used for encipherment and decipherment

NOTE: The initial state of the KSG is determined by the initialization value.

Key Stream Segment (KSS): key stream of arbitrary length

Open MNI: network address used in conjunction with an open group address, which allows communication with any users who have selected the same DMO frequency

NOTE 1: The open MNI is encoded as all binary ones ($11…11_2$).

NOTE 2: The open MNI is described in ETSI EN 300 396-1 [i.9].

plain text: unencrypted source data

NOTE: The semantic content is available.

proprietary algorithm: algorithm which is the intellectual property of a legal entity

rep-gate: MS acting as a repeater and gateway

NOTE: For further descriptions of repeaters and gateways, refer to ETSI EN 300 396-1 [i.9].

SCK set: collective term for the group of 32 SCKs and/or SCKXs

NOTE: An SCK set may contain SCKs or SCKXs or both SCKs and SCKXs.

SCK-subset: collection of SCKs and/or SCKXs from an SCK set, with SCKNs in numerical sequence, where every SCK or SCKX in the subset is associated with one or more different GSSIs

NOTE: Multiple SCK subsets have corresponding SCKs or SCKXs associated with the same GSSIs.

Static Cipher Key (SCK): predetermined cipher key that may be used to provide confidentiality in class DM-2-A, DM-2-B and DM-2-C systems with a corresponding algorithm from TEA set A

synchronous stream cipher: encryption method in which a cipher text symbol completely represents the corresponding plain text symbol

NOTE: The encryption is based on a key stream that is independent of the cipher text. In order to synchronize the KSGs in the transmitting and the receiving terminal synchronization data is transmitted separately.

TEA set A: set of air interface encryption algorithms comprising TEA1, TEA2, TEA3 and TEA4

TEA set B: set of air interface encryption algorithms comprising TEA5, TEA6 and TEA7

TETRA algorithm: mathematical description of a cryptographic process used for either of the security processes authentication or encryption

Trunked Mode Operation (TMO): operations of TETRA specified in ETSI EN 300 392-2 [1]

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACK	ACKnowledgement
AI	Air Interface
CK	Cipher Key
CKX	Extended Cipher Key
CN	Carrier Number
DM	Direct Mode
DMAC	Direct Mode Medium Access Control
DMC	A layer 2 Service Access Point (DMC-SAP)
DMCC	Direct Mode Call Control
DMO	Direct Mode Operation
DPRES	DMO PREScence
DSB	Direct mode Synchronisation Burst
ECK	Encryption Cipher Key
EDSI	Encrypted Direct-mode Short Identity
EDSI-URTC	Encrypted DMO Short Identity-Usage Restriction Type Confidentiality
EUIV	EDSI-URTC Initialisation Vector
FN	Frame Number
FRAG	FRAGmented
GATE	GATEway
GSSI	Group Short Subscriber Identity
GTSI	Group TETRA Subscriber Identity
GTX	Gateway Transmit
IV	Initial Value
KAG	Key Association Group
KSG	Key Stream Generator
KSS	Key Stream Segment
MAC	Medium Access Control

MDE	Message Dependent Elements
M-DMO	Managed DMO
MNC	Mobile Network Code
MNI	Mobile Network Identity
MS	Mobile Station
OTAR	Over The Air Rekeying
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
REP	REPeater
RF	Radio Frequency
RG_Add	Repeater or Gateway Address
RX	Receive
SAP	Service Access Point
SCH	Signalling CHannel
SCH/F	Full SCH
SCH/H	Half SCH
SCH/S	Synchronization SCH
SCK	Static Cipher Key
SCKN	Static Cipher Key Number
SCK-VN	SCK-Version Number
SCKX	Extended Static Cipher Key
SDS	Short Data Service
SDU	Service Data Unit
SSI	Short Subscriber Identity
STCH	STolen CHannel
SwMI	Switching and Management Infrastructure
SYNC	SYNChronization
TCH	Traffic CHannel
TCH/S	Speech Traffic CHannel
TDMA	Time Division Multiple Access
TEA	TETRA Encryption Algorithm
TMO	Trunked Mode Operation
TN	Timeslot Number
TSI	TETRA Subscriber Entity
TVP	Time Variant Parameter
TX	Transmit
U-PLANE	User-PLANE
URT	Usage Restriction Type
URTC	Usage Restriction Type Confidentiality
V+D	Voice + Data
VN	Version Number
XOR	eXclusive OR
xSI	Short Identity (of various types)

4 DMO security class

4.1 General

TETRA security is defined in terms of class. DMO security offers 4 classes defined in table 4.1.

NOTE: DMO offers equivalence to TMO security class 1 (no encryption enabled) and to TMO security class 2 (SCK and SCKX encryption supported).

Table 4.1: Direct Mode security class

DMO security class	Remark
DM-1	No encryption applied.
DM-2-A	The DM-SDU and any related traffic is AI encrypted. Addresses are not encrypted.
DM-2-B	The destination address (SSI), DM-SDU and any related traffic are AI encrypted.
DM-2-C	In the DMAC-SYNC PDU, the PDU is encrypted from destination address element and onwards except for source address type element, and any related traffic is AI encrypted. In the DMAC-DATA PDU, the PDU is encrypted from the destination address type element and onwards.
NOTE 1: Except in DMAC-DATA PDUs for class DM-2-C the destination and source address type elements are never encrypted. NOTE 2: DM-1 is considered the lowest level of security. NOTE 3: DM-2-A through DM-2-B to DM-2-C provide progressively increased levels of security by encrypting more of the signalling content.	

The security class is identified in DMAC-SYNC PDUs by the AI encryption state element (see table 4.2).

Table 4.2: AI encryption state element encoding

Information element	Length	Value	Class
Air Interface encryption state	2	00_2	DM-1
		10_2	DM-2-A
		11_2	DM-2-B
		01_2	DM-2-C

On establishing a call the first master shall establish the security class of the call. The security class should be maintained for the duration of the call.

4.2 DM-2-A

The purpose of security class DM-2-A is to provide confidentiality of user traffic and signalling in applications where it is not necessary to hide the addressing information.

In addition security class DM-2-A allows calls to be made through a repeater where the repeater is not provided with the capability to encrypt or decrypt messages by maintaining the layer 2 (MAC) elements of any signalling in clear.

Addresses identified by the Usage Restriction Type (URT) field in repeaters, gateways and combined repeater-gateways, shall be in clear (i.e. the Encrypted DMO Short Identity-Usage Restriction Type Confidentiality (EDSI-URTC) shall not apply).

4.3 DM-2-B

The purpose of security class DM-2-B is to provide confidentiality of user traffic and signalling.

Security class DM-2-B extends the confidentiality applied to signalling over that provided in class DM-2-A to encrypt parts of the MAC header. The encryption allows repeater operation to be made without requiring the repeater to be able to encrypt and decrypt transmissions unless it wishes to check the validity of the destination address. In class DM-2-B because the source address is in clear, a pre-emptor can identify the pre-emption slots and hence the call can be pre-empted even if the pre-emptor does not have the encryption key being used by the call master.

Addresses identified by the URT field in repeaters, gateways and combined repeater-gateways, should be encrypted (i.e. EDSI-URTC should apply).

4.4 DM-2-C

The purpose of security class DM-2-C is to provide confidentiality of user traffic and signalling including all identities other than those of repeaters and gateways.

In addition in class DM-2-C the bulk of the MAC header elements are encrypted. Where repeaters are used, the repeater requires the ability to encrypt and decrypt all transmissions. In class DM-2-C calls can only be pre-empted by an MS which has the SCK or SCKX in use by the call master.

Addresses identified by the URT field in repeaters, gateways and combined repeater-gateways, should be encrypted (i.e. EDSI-URTC should apply).

5 DMO call procedures

5.1 General

5.1.1 Security profile

5.1.1.0 General

An MS should maintain a security profile for each destination address. The security profile should contain at least the following for each destination address:

- KSG, as identified by its KSG-identifier;
- current SCK or SCKX, as identified by SCKN, for transmission;
- valid SCKs or SCKXs, as identified by SCKN, for reception;
- the preferred, and minimum, security class to be applied to calls for transmission;
- the minimum security class to be applied to calls for reception; and
- the minimum security class that a master will accept in a pre-emption request.

The preferred security class is the security class to be used for transmission when the MS is acting as a call master. The minimum security class for transmission is the lowest security class that the MS shall use to transmit responses to other signalling.

NOTE 1: Minimum may be the same as preferred.

NOTE 2: A default profile may be maintained in addition to a profile for specific addresses.

NOTE 3: A profile should exist for received individual calls (i.e. for calls where destination address is that of the receiving MS).

NOTE 4: If the preferred security class to be applied to calls for transmission is DM-2-C the minimum security class that a master will accept in a pre-emption request should be set to class DM-2-C MS.

5.1.1.1 Indication of security parameters

In call setup procedures the DMAC-SYNC PDU found in logical channel SCH/S shall contain the parameters required to identify the security class of the call, the encryption algorithm and the identity of the key in use, in addition to the current value of the Time Variant Parameter used to synchronize the encryption devices (see also annex A).

The DMAC-SYNC PDU is defined in clause 9 of ETSI EN 300 396-3 [5] and contains the security elements identified in table 5.1.

Table 5.1: Security elements of DMAC-SYNC PDU contents in SCH/S

Information element	Length	Value	Remark
Air interface encryption state	2		Security class (see note 1)
Time Variant Parameter	29	Any	
Reserved	1	0	Default value is 0
KSG number	4		
Encryption key number	5		Identifies SCKN (see note 2)
NOTE 1: If set to DM-1 the other security elements shall not be present. NOTE 2: The encoding is such that 00000_2 indicates SCKN = 1, 11111_2 indicates SCKN = 32.			

5.2 Security class on call setup

5.2.1 General

On establishing a call the first master shall establish the security class of the call by setting the Air Interface (AI) encryption state element of DMAC-SYNC PDU using data contained in the master's security profile.

Once an SCK or SCKX has been established for a call transaction the master shall make no changes to the ciphering parameters (key, algorithm, class) within that call transaction.The security class and algorithm should be maintained for the duration of the call. The key may be different in different transactions because each MS may have a different definition of which SCKN is current.

NOTE: In exceptional conditions such as during the process of transitioning from use of an algorithm in TEA set A to an algorithm in TEA set B, the algorithm in use in different call transactions may be different, for example if one MS is using SCK with an algorithm in TEA set A, and another MS is using SCKX with an algorithm in TEA set B. ETSI EN 300 392-7 [4], annex D describes principles that would allow an MS to transition from use of a KSG from TEA set A to use of a KSG from TEA set B.

5.2.2 Normal behaviour

On receipt of call setup the DM-MS shall extract the ciphering parameters from the DMAC-SYNC PDU. These parameters shall be compared with the DM-MS's predefined security profile associated with the destination address. If the parameters match the security profile (i.e. KSG-id identical, SCKN belongs to the KAG specified for the address, security class is equal to or greater than the minimum required for the destination address) the call may be accepted (i.e. speech or data path opened).

5.2.3 Exceptional behaviour

5.2.3.0 General

On receipt of call setup the slave DM-MS shall extract the ciphering parameters from the DMAC-SYNC PDU. These parameters shall be compared with the DM-MS's predefined security profile associated with the destination address.

5.2.3.1 Call-setup with presence check

If the parameters do not match the security profile (i.e. KSG-id is not identical, or SCKN does not belong to the KAG specified for the address, or security class is not equal to or greater than the minimum required for the destination address) the slave should ignore or reject the call (i.e. speech or data path closed) with reason "security parameter mismatch".

5.2.3.2 Call-setup without presence check

If the parameters do not match the security profile (i.e. KSG-id is not identical, or SCKN does not belong to the KAG specified for the address, or security class is not equal to or greater than the minimum required for the destination address), the slave should ignore the call (i.e. speech or data path closed).