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

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

Reference
REN/TETRA-06181

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

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".

2.2 Informative references

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.

Not applicable.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions 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 EN 300 396-3 [5]).

carrier number: integer, N, used in TETRA to represent the frequency of the RF carrier

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

cipher key: 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]).

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 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: cipher key used as input to the KSG, derived from an address specific cipher key and randomly varied per channel using algorithm TB6

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

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

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

plain text: unencrypted source data

NOTE: The semantic content is available.

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

SCK set: collective term for the group of 32 SCKs associated with each Individual TETRA Subscriber Identity

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

NOTE: Multiple SCK subsets have corresponding SCKs 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

synchronization value: sequence of symbols that is transmitted to the receiving terminal to synchronize the KSG in the receiving terminal with the KSG in the transmitting terminal

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.

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 EN 300 392-2 [1]

3.2 Abbreviations

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

ACK	ACKnowledgement
AI	Air Interface
CK	Cypher Key
CN	Carrier Number
DM	Direct Mode
DMAC	Direct Mode Media Access Control
DMC	A layer 2 Service Access Point (DMC-SAP)
DMCC	Direct Mode Call Control
DMO	Direct Mode Operation
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
GSSI	Group Short Subscriber Identity
GTSI	Group TETRA Subscriber Identity
KAG	Key Association Group
KSG	Key Stream Generator
KSS	Key Stream Segment
MAC	Medium Access Control
MDE	Message Dependent Elements
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
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
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 Media Access
TMO	Trunked Mode Operation
TN	Timeslot Number
TSI	TETRA Subscriber Entity
TVP	Time Variant Parameter
U-PLANE	User-PLANE
URT	Usage Restriction Type
URTC	Usage Restriction Type Confidentiality
V+D	Voice + Data
XOR	eXclusive OR

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 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 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

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, as identified by SCKN, for transmission;
- valid SCKs, 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 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 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.

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

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).

5.2.3.3 Behaviour post call-setup

Once an SCK has been established for a call transaction the master shall make no changes to the ciphering parameters (key, algorithm, class) within that call transaction. If the slave DM-MS perceives that such a change is being attempted the slave DM-MS (receiver) shall ignore the change and maintain the original parameters for the remainder of that call transaction.

5.3 Security class on call follow-on

5.3.1 General

NOTE 1: The mechanisms in this clause apply to security classes 2A, 2B and 2C for slave, DM-GATE and idle MSs.

The slave or idle DM-MS shall have a method of determining the preferred security class to be applied to calls for transmission (see clause 5.1.1). The MS shall use this preferred security class when the MS becomes the call master in the follow on case.

If the follow on transaction is sent to the same address, the new call master shall select the SCKN from KAG associated with that address that it considers to be the current key (which may be different to the SCKN used by the previous call master).

NOTE 2: The new call master may be either a DM-MS or a DM-GATE.

Random access requests (e.g. pre-emption, changeover, timing adjust), should be sent in a manner that the current call master can understand but shall not use a lower security class than its minimum security class as defined in the security profile (see clause 5.1.1). If a slave or idle DM-MS uses class 2C security to send a random access request to the master of a call, the requesting DM-MS should encrypt the request using the SCK being used by the current call master or may use the SCK that it considers current in the associated KAG.

NOTE 3: The term "slave or idle DM-MS" includes gateways and repeaters (although it is noted that a DM-REP does not generate random access requests).

If a random access request is received using a different class to that of the call being pre-empted, any response to the pre-emption request shall be sent using the lower of the two security classes.

NOTE 4: A master may ignore a random access request (without sending a response) if the security class used for the random access request is insufficient.

The master shall respond to any random access request using the SCKN that it considers to be the current SCK for the ongoing call (as indicated by the security profile for the ongoing call). This shall be the same SCKN that the master was using for the call transaction prior to receiving the request.

5.3.2 Normal behaviour

When making an attempt to follow on a pre-existing call the new call master shall establish a new independent TVP.

On receipt of call setup the DM-MS shall extract the encryption parameters from the DMAC-SYNC PDU. These parameters shall be compared with the predefined security profile associated with the destination address. If the parameters match in full the call may be accepted (i.e. speech or data path opened).

5.3.3 Exceptional behaviour

On receipt of call setup the DM-MS shall extract the encryption parameters from the DMAC-SYNC PDU. These parameters shall be compared with the predefined security profile associated with the destination address. If the parameters do not match the security profile (i.e. KSG-id is not identical, SCKN does not belong the KAG specified for the address, or security class is not equal to or greater than the minimum required for the destination address) the call should be rejected (i.e. speech or data path shall be closed) with reason "security parameter mismatch" in call setup with presence check acknowledgement or ignored where no presence check is used.

If the minimum security class required by any subsequent call transaction in the call is not attained the call shall be rejected.

If the minimum security class required by the master to accept any pre-emption request is not attained, or the parameters do not match in full the predefined security profile associated with the destination address of the call, the pre-emption request shall be ignored or rejected. If a pre-emption request is received using a different class to that of the call being pre-empted, the response to the pre-emption request should be sent using the lower of the two security classes. An MS shall use only class 2C to attempt to pre-empt an ongoing class 2C call.

NOTE: A master may ignore a pre-emption request (without sending a response) if the security class used for the pre-emption request is insufficient.

6 Air interface authentication and key management mechanisms

6.1 Authentication

An explicit authentication protocol between mobile terminals in DMO is not provided. The fact that static cipher keys are used (which are generated, controlled and distributed through the DMO system security management which may use the TMO system or may be distributed by a fill gun) provides an implicit authentication between mobile stations as belonging to the same DMO net when successful communication takes place.

In dual-watch mode a DM-MS shall be a valid member of the TETRA TMO network for its TMO operation and when operating in TMO shall operate in accordance with the security class of that network using the procedures defined in EN 300 392-7 [4].

In dual-watch mode a DM-MS operating in DMO shall operate in accordance with the procedures defined in the present document.

6.2 Repeater mode operation

A repeater shall not modify the security class of a call. A repeater shall not modify the KSG-id and SCK applied to the call.

NOTE 1: The DPRES-SYNC signal is not mandatory on a free channel. Where DPRES-SYNC is not broadcast on a free channel there needs to be a prior arrangement to identify the channel, location and other parameters normally present in DPRES-SYNC.

NOTE 2: The DPRES-SYNC signal is sent in clear. Therefore it may be preferable for users who operate in class DM-2-C (or class DM-2-B) to obtain their authorization to use the repeater by prior arrangement so that the repeater does not broadcast their addresses in the DPRES-SYNC signal.

6.3 Gateway mode operation

Calls established through a gateway (i.e. DM-GATE or DM-REP/GATE) shall be considered as multi-hop calls and as such shall use a tandem call setup protocol (i.e. DMO to GATE, GATE to TMO).

In gateway mode the gateway shall be a valid member of the TETRA TMO network and shall operate in accordance with the security class of that network using the procedures defined in EN 300 392-7 [4].

The gateway presence signal (see EN 300 396-5 [8], clauses 13.4.6.2 and 14.1.2) shall indicate the encryption state (encryption applied or clear operation) of the TMO system using the "gateway encryption state on SwMI" information element defined in table 6.1. DMO systems interoperating with TMO systems should use the same encryption state.

EXAMPLE: If TMO encryption state is on, the DMO terminal should communicate in class DM-2-A or DM-2-B or DM-2-C.

Table 6.1: Gateway encryption state on SwMI information element encoding

Information element	Length	Value	Remark
Gateway encryption state on SwMI	1	0_2	The link to the SwMI is not encrypted (Gateway operating in class 1).
		1_2	The link to the SwMI is encrypted (Gateway operating in class 2 or 3).
NOTE 1: The value of the element shall follow the encryption state of the link to the SwMI. NOTE 2: There is no relationship between DMO and TMO encryption states.			

Class 2 TMO systems interworking with DMO systems operating in encrypted mode should not use the same SCK on the TMO side of the gateway as is used on the DMO-net.

The gateway shall be considered as having two synchronized protocol stacks with the TMO network acting as the synchronization master for the call (see figure 6.1).

NOTE 1: The TVP in DMO used for synchronization remains independent of the frame numbering used in TMO.

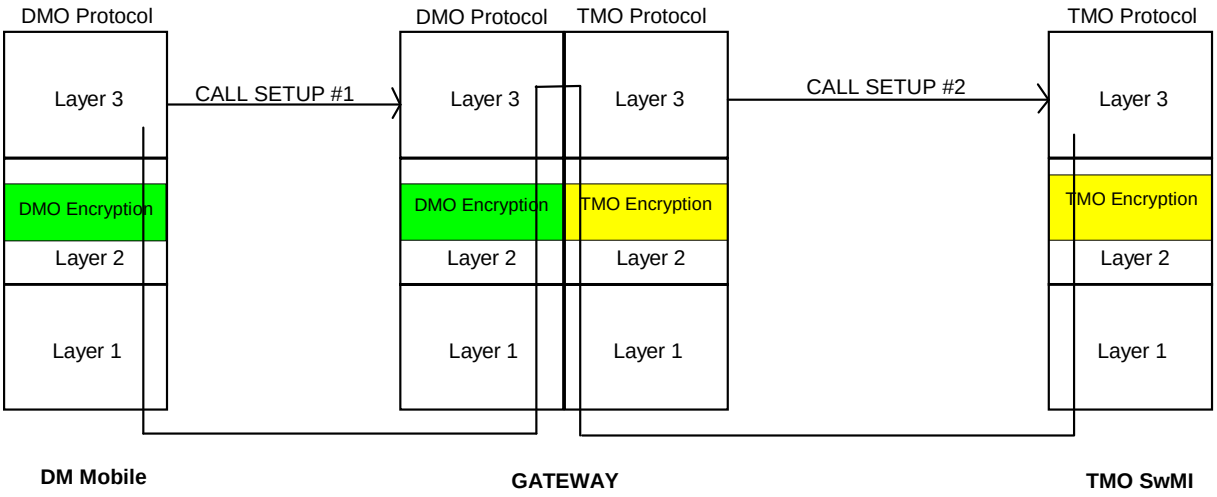


Figure 6.1: TETRA DMO to TETRA TMO gateway

On initial call setup from a DMO-net to a TMO-net the keys in use are as shown in figure 6.2.

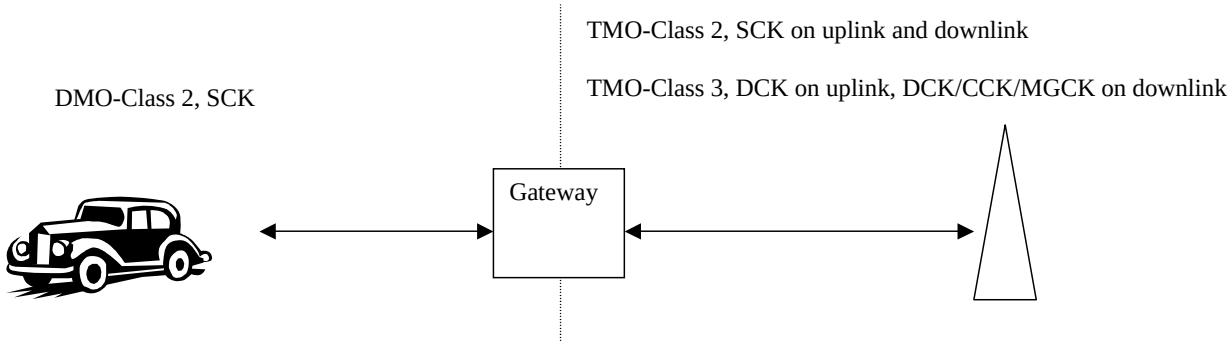


Figure 6.2: Gateway initial key allocations

Throughout an encrypted call (which may include the call setup phase) each layer 2 (i.e. the DMO-protocol layer 2 and the TMO-protocol layer 2) shall decrypt incoming messages and encrypt outgoing messages. This may impose some delay on the end-to-end link. The present document shall not describe methods for correcting this delay.

If the DM-MS is a party to a group call with some members of the group being on the TETRA TMO mode network there may be a delay for any call transaction through the gateway. The present document shall not describe methods for correcting this delay.

NOTE 2: The DPRES-SYNC signal is not mandatory on a free channel. Where DPRES-SYNC is not broadcast on a free channel there needs to be a prior arrangement to identify the channel, location and other parameters normally present in DPRES-SYNC.

NOTE 3: The DPRES-SYNC signal is sent in clear. Therefore it may be preferable for users who operate in class DM-2-C (or class DM-2-B) to obtain their authorization to use the gateway by prior arrangement so that the gateway does not broadcast their addresses in the DPRES-SYNC signal.

6.4 Air Interface (AI) key management mechanisms

In Direct Mode only one type of cipher key is defined:

- the Static Cipher Key (SCK).

The SCK can be chosen by the system manager and may be distributed from the TMO SwMI using the Over The Air Rekeying (OTAR) mechanism described in EN 300 392-7 [4] or be manually entered in MS. The initial allocation of SCK shall be carried out in advance of communication.

The SCKs should be distributed from the system manager in a secure manner.

NOTE 1: The choice and lifetime of the SCK is outside the scope of the present document and is a matter of network security policy.

The SCK can be considered a binary vector of 80 bits, labelled SCK(0) to SCK(79).

The SCK shall be a member of an SCK set containing up to 32 keys, and each key shall be identified by its position in the SCK set (SCK number). One SCK set is valid for use with one MNI. An MS may store more than one SCK set, and shall reference each SCK set to the MNI of the DMO net to which the SCK applies. The MNI may be the 'Open MNI', in which case the SCK set shall only be used with GTSIs containing the 'Open MNI'.

Members of an SCK set may be shared amongst different DMO nets. They may be allocated in either the home V+D network of the MS or by an external body.

For use in Direct Mode SCKs exist in groups of 30. The convention SCKN, $1 \leq N \leq 30$, shall be used to refer to specific members of this set, labelled SCKN(0) to SCKN(29).

NOTE 2: SCKN-31 and SCKN-32 (labelled SCKN(30) and SCKN(31)) are reserved for use in TETRA Trunked Mode Operation.

NOTE 3: The content of each SCK set and the initial distribution of this set is not covered by the present document.

6.4.1 Key grouping

NOTE 1: The text of EN 300 392-7 [4], clause 4.2.4.1.1 describes a means of managing DMO key grouping across the Air Interface when the MS is registered to the managing SwMI.

For each DMO group call where encryption is to be applied, the MS should have a means to associate one or more SCKs identified by SCKN with the GTSI to be called. The means of associating SCKs with GTSIs is outside the scope of the present document. However this may be achieved using air interface signalling in TMO as specified in EN 300 392-7 [4].

An SCK should have a defined lifetime or crypto period. At the end of this crypto period, it should be replaced. Replacement is achieved when the MS selects a different SCK for transmission. However, as DMO is an uncontrolled environment, different MSs may change their SCK selection at different times. To overcome the possibilities for communication failure, SCKs may be grouped into one or more subsets to facilitate the key management process. The SCKs within a subset shall all be taken from the same SCK set, and therefore shall all be associated with the same MNI.

Keys in different subsets associated with the same GTSI(s) are referred to by the term Key Association Group (KAG). The MS shall consider one SCK of the KAG as current and shall use this SCK as the key for transmission. Any SCK of the KAG may be used for reception. The SCKs within a KAG shall all be taken from the same SCK set, and therefore shall all be associated with the same MNI.

The SCKs within the subsets can be activated separately or together. If an entire subset of SCKs is to be activated together, the crypto periods of all SCKs in the subset shall be the same, and the SCK-VNs of all SCKs in a subset shall also be the same.

Where a group of MSs wish to communicate with each other in class 2, they shall have at least one common SCK in their respective SCK sets, where common SCK shall indicate the same key material identified by common SCKN and SCK-VN.

NOTE 2: Where KAGs of SCKs are used, the MSs should have the entire KAG of SCKs in common.

Where a group of MSs wish to communicate with each other using a repeater in class 2B using address checking or class 2C all devices shall have at least one common SCK (or KAG of SCKs) in their respective SCK sets.

Where a group of MSs wish to communicate with each other using a gateway in class 2 all devices shall have at least one common SCK (or KAG of SCKs) in their respective SCK sets.

It is only possible for a repeater or gateway to be used by MSs with the same MNI but different SCK sets, if the repeater or gateway contains an SCK set associated with that MNI containing the SCKs (or KAGs of SCKs) needed by both sets of MSs. In this case, the SCK set used by the repeater or gateway with that MNI will be different to the SCK sets used by those groups of MSs.

If the parties to a call load different keys from each other, the receiving party will decode messages incorrectly, thus causing erroneous operation. The result of this, and any corrective action put in place to prevent errors, is outside the scope of the present document.

Subset groups shall be identified by the SCK subset grouping type as shown in table 6.2 and the membership of each resulting subset shall be identified as shown in table 6.3.

The SCK subset numbering shall be determined by the SCK subset grouping type. In all cases, SCK subset number = 1 corresponds to the subset with SCKN = 1 as the first value. Other subset numbers are determined according to table 6.3.

Table 6.2: SCK subset grouping type definitions

SCK subset grouping type	Maximum number of SCK subsets (n)	Maximum number of SCKs per subset (m)	Remarks
0	1	30	No effective subset grouping.
1	2	15	
2	3	10	Suited for past-present-future mode of operation.
3	4	7	Only 28 keys of 30 are associated to groups.
4	5	6	
5	6	5	
6	7	4	Only 28 keys of 30 are associated to groups.
7	10	3	
8	15	2	
9	30	1	30 versions of 1 key.

Table 6.3: Membership by SCKN value of each subset of each subset grouping type

SCK subset number	SCK subset grouping type								
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	1 to 30	1 to 15	1 to 10	1 to 7	1 to 6	1 to 5	1 to 4	1 to 3	1 to 2
2	X	16 to 30	11 to 20	8 to 14	7 to 12	6 to 10	5 to 8	4 to 6	3 to 4
3	X	x	21 to 30	15 to 21	13 to 18	11 to 15	9 to 12	7 to 9	5 to 6
4	X	x	x	22 to 28	19 to 24	16 to 20	13 to 16	10 to 12	7 to 8
5	X	x	x	x	25 to 30	21 to 25	17 to 20	13 to 15	9 to 10
6	X	x	x	x	x	26 to 30	21 to 24	16 to 18	11 to 12
7	X	x	x	x	x	x	25 to 28	19 to 21	13 to 14
8	X	x	x	x	x	x	x	22 to 24	15 to 16
9	X	x	x	x	x	x	x	25 to 27	17 to 18
10	X	x	x	x	x	x	x	28 to 30	19 to 20
11	X	x	x	x	x	x	x	x	21 to 22
12	X	x	x	x	x	x	x	x	23 to 24
13	X	x	x	x	x	x	x	x	25 to 26
14	X	x	x	x	x	x	x	x	27 to 28
15	X	x	x	x	x	x	x	x	29 to 30

NOTE 1: For SCK Subset group number = 9 (not shown), 30 subsets of 1 key each, the SCK subset number is equal to the SCKN, i.e. SCK subset number = 1 signifies SCKN = 1 and so on.
NOTE 2: A table entry given by "x" indicates an illegal value that shall not be used.

All SCKNs in a KAG shall be associated with a GTSI by implication when the SCKN in that KAG that is in subset#1 is associated with that GTSI.

The association of SCKNs within a KAG with any GTSI can also be determined from the following formula:

Where:

SCK(i) are the members of a KAG;

SCK(f) is the associated SCKN in the first subset; and

there are (n) subsets, each containing (m) member SCKs.

Then:

```
For j = 0 to (n - 1)
{
    i = f + m*j
}
```

EXAMPLE 1: Associating GTSI#22 with SCKN#3 in subset group type 2 implies association of SCKN#3, SCKN#13 and SCKN#23 with GTSI#22, i.e. SCKN#3, SCKN#13, SCKN#23 are members of the same KAG.

EXAMPLE 2: Associating GTSI#22 with SCKN#3 in subset group type 4 implies association of SCKN#3, SCKN#9, SCK#15, SCKN#21 and SCKN#27 with GTSI#22, i.e. SCKN#3, SCKN#9, SCKN#15, SCKN#21 and SCKN#27 are members of the same KAG.

EXAMPLE 3: If SCK subset grouping number = 2 (corresponding to 3 subsets of 10 keys), then n = 3, m = 10, and if f = 5, then SCKN = 5, SCKN = 15 and SCKN = 25 shall be associated with the same GTSI and are members of the same KAG.

6.4.2 Identification of cipher keys in signalling

The encryption parameters (KSG number, Encryption key number, Time Variant Parameter) are identified in DMAC-SYNC PDU (EN 300 396-3 [5], clause 9.1.1). The terminal shall have a method of determining the SCKN and KSG to be applied to calls to any address.

NOTE: The selection of SCK and the association of SCK to an address is outside the scope of the present document.

EXAMPLE: The Over The Air Rekeying (OTAR) mechanisms described in EN 300 392-7 [4] may be used to associate keys to addresses. The association mechanisms provide a form of authentication in which by pre-assignment of keys and addresses any received communication matching the stored key-address association will indicate that the transmitter of the communication has a higher probability than not of being associated with the same key management group.

7 Enable and disable mechanism

An enable or disable applied to a subscription or an equipment in TMO as described in EN 300 392-7 [4] shall also apply to DMO.

If an MS is disabled in TMO it shall remain disabled even if the user attempts to switch to DMO.

8 Air Interface (AI) encryption

8.1 General principles

AI encryption provides confidentiality on the radio link between a DM-MS and either a single DM-MS or a group of DM-MSs, and between a DM-MS and repeaters, gateways and rep-gates.

AI encryption operates by combining the output of a Key Stream Generator (KSG), referred to as a Key Stream Segment (KSS), with the contents of messages to be transmitted across the AI. The KSG uses an Encryption Cipher Key (ECK) and a Time Variant Parameter (TVP) as input where the ECK is derived from the SCK required to communicate with the destination and other parameters. The specification of the KSG and its inputs is given in annex A.

Both control and traffic (speech or data) information can be encrypted. The encryption process shall take place in the upper Medium Access Control (MAC) layer of the TETRA protocol stack (see figure 8.1).

NOTE: The encryption method described is a bit replacement type in which each bit of clear text that is to be encrypted is replaced by a bit of cipher text to avoid error propagation.

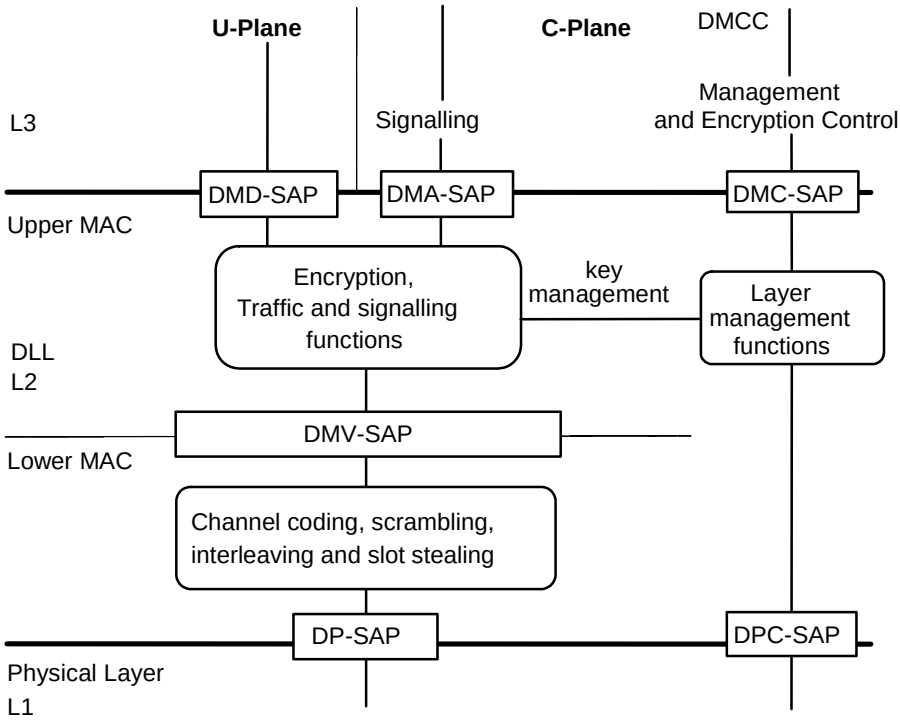


Figure 8.1: Relationship of security functions to layer functions

AI encryption is a separate function to the end-to-end encryption service described in EN 302 109 [7]. Information that has already been encrypted by the end-to-end service may be encrypted again by the AI encryption function. A service invoked without end-to-end encryption may still be encrypted over the AI.

8.2 Encryption mechanism

The key stream bits shall be modulo 2 added (XORed) with plain text bits in data, speech and control channels to obtain encrypted cipher text bits, with the exception of the MAC header bits and fill bits, prior to channel encoding being applied.

EXAMPLE: KSS(0) shall be XORed with the first transmitted bit of a traffic burst (before channel encoding is applied).

If the information in a slot has fewer bits than the length of KSS produced, the last unused bits of KSS shall be discarded. For example, if there are m information bits and n bits of KSS generated, KSS(0) to KSS(m-1) shall be utilized, KSS(m) to KSS(n-1) shall be discarded.

Where a PDU is fragmented over many slots the KSS is restarted on each slot with new TVP.

8.2.1 Allocation of KSS to logical channels

KSS shall be allocated to TETRA logical channels as shown in table 8.1 and the unused bits (also indicated) shall be discarded.

NOTE 1: The allocation of KSS to synchronization channels is described in clause 8.3.

Table 8.1: KSS allocation to logical channels

Logical channel	Bits in channel	KSS assignment
TCH/2,4	144	KSS (124 to 267)
TCH/4,8	288	KSS (124 to 411)
TCH/7,2 (note 1)	432	KSS (0 to 431)
STCH+TCH/2,4	124 + 144	KSS (0 to 123) + KSS (124 to 267)
STCH+TCH/4,8	124 + 288	KSS (0 to 123) + KSS (124 to 411)
STCH+TCH/7,2	124 + 432	KSS (0 to 123) + KSS (0 to 431) (note 1)
TCH/S (full)	274	KSS (0 to 273)
STCH+TCH/S	124 + 137	KSS (0 to 123) + KSS (216 to 352)
SCH/F	268	KSS (0 to 267)
SCH/S+SCH/H (note 2)	60 + 124	KSS (0 to 123)
STCH+STCH	124 + 124	KSS (0 to 123) + KSS (216 to 339)
NOTE 1: Where TCH/7,2 is stolen the first 216 encrypted bits of TCH/7,2 are not transmitted. NOTE 2: SCH/H only follows SCH/S (and SCH/S is not encrypted).		

NOTE 2: KSS repeat is possible only for multi-slot interleaved circuit mode data when both half slots in a single slot are stolen.

The first bit to be encrypted shall be enciphered with the first usable bit of KSS according to table 8.1. Any following bit to be encrypted shall be ciphered with incremental KSS bits. Therefore, when there is a gap in the bit-stream to be encrypted, it is dealt with as shown in table 8.2. This method of KSS assignment is equivalent to the method described in EN 300 392-7 [4].

Table 8.2: KSS allocation

KSS sequence			KSS(0)	KSS(1)	KSS(2)			KSS(3)	KSS(4)		KSS(5)
Bits	C	C	X	X	X	C	C	X	X	C	X
X: bits to be encrypted. C: bits in clear.											

8.3 Application of KSS to specific PDUs

This clause describes the method of applying AI encryption to PDUs in the upper DMAC layer.

The DMAC-SYNC PDU (see EN 300 396-3 [5], clause 9.1.1) and the DMAC-DATA PDU (see EN 300 396-3 [5], clause 9.2.1) contain an AI Encryption State element (see EN 300 396-3 [5], clause 9.3.2) that indicates the security class of the PDU and the succeeding call. See also EN 300 396-3 [5], clause 8.5.3.

8.3.1 Class DM-1

AI Encryption shall not be used in Class DM-1.

8.3.2 Class DM-2A

In class DM-2A the DM-SDU and any related traffic is AI encrypted. See figure 8.2 in which the data to be encrypted is multiplied one bit at a time by a Key Stream Segment (KSS) generated using a cipher key modified by algorithm TB6 input to the Key Stream Generator (KSG) along with a Time Variant Parameter (TVP) synchronized to the TDMA structure.

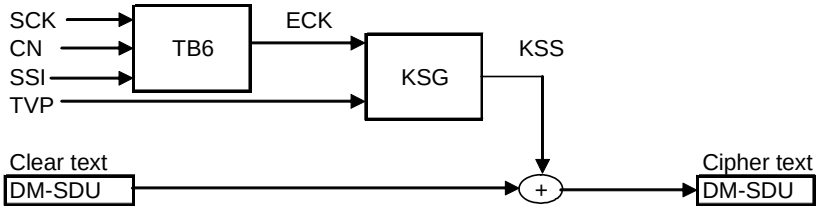
8.3.2.1 DMAC-SYNC PDU encryption

See EN 300 396-3 [5], clause 9.1.1 for a full description of this PDU.

The DMAC-SYNC PDU contained in logical channel SCH/S shall always be in clear.

The DMAC-SYNC PDU contained in logical channel SCH/H shall be encrypted as follows (see figure 8.2):

- Encryption starts at the first bit of the DM-SDU contained in the final element of the PDU. The bit number of the first encrypted bit depends on the length of the preceding parts of the PDU, including whether or not address elements are present.



NOTE: For decryption the input is cipher text and output is clear text.

Figure 8.2: Encryption process as it occurs in TETRA DMO Class DM-2-A

8.3.2.2 DMAC-DATA PDU encryption

The SSI input to TB6 shall be the SSI used in the DMAC-SYNC PDU as described in clause A.3.1.1.

See EN 300 396-3 [5], clause 9.2.1 for a full description of this PDU.

The DMAC-DATA PDU, sent in either a full signal slot (logical channel SCH/F) or using a stolen channel (STCH), shall be encrypted as follows:

- Encryption starts at the first bit of the DM-SDU contained in the final element of the PDU. The bit number of the first encrypted bit depends on the length of the preceding parts of the PDU, including whether or not address elements are present.

EXCEPTION: The first bit of the DM-SDU shall be encrypted with KSS(216) if the PDU is sent on the STCH in the second half slot.

8.3.2.3 DMAC-FRAG PDU encryption

The SSI input to TB6 shall be the SSI used in the DMAC-SYNC PDU as described in clause A.3.1.1.

See EN 300 396-3 [5], clause 9.2.2 for a full description of this PDU.

The DMAC-FRAG PDU shall be encrypted as follows:

- the DMAC-FRAG header, bits 1 to 4, shall be in clear, all other bits shall be encrypted (i.e. DMAC-FRAG[0] DMAC-FRAG[3] shall be in clear);
- the first bit of the SDU fragment shall be encrypted with KSS(0).

8.3.2.4 DMAC-END PDU encryption

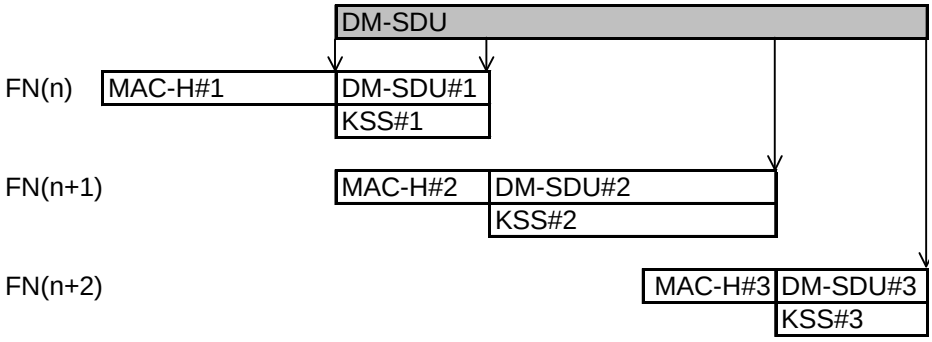
The SSI input to TB6 shall be the SSI used in the DMAC-SYNC PDU as described in clause A.3.1.1.

See EN 300 396-3 [5], clause 9.2.3 for a full description of this PDU.

The DMAC-END PDU shall be encrypted as follows (see figure 8.3):

- the DMAC-END header, bits 1 to 4, shall be in clear, all other bits shall be encrypted (i.e. DMAC-END[0] ... DMAC-END[3] shall be in clear);
- the first bit of the SDU fragment shall be encrypted with KSS(0).

EXCEPTION: The first bit of the SDU fragment shall be encrypted with KSS(216) if the PDU is sent on the STCH in the second half slot.



NOTE 1: The example DM-SDU is fragmented over 3 slots by breaking it into DM-SDU#1, DM-SDU#2 and DM-SDU#3.
NOTE 2: KSS#1 is used to encrypt DM-SDU#1, KSS#2 for DM-SDU#2, and KSS#3 for DM-SDU#3.
NOTE 3: Length of DM-SDU#1 = L#1. KSS#1(0,..,L # 1-1) is used to encrypt DM-SDU#1. The remainder of KSS#1 is discarded (KSS#1(L#1, ..., 431)). Similarly for fragments 2 and 3.

Figure 8.3: Allocation of KSS to encrypt an example fragmented PDU in security class DM-2-A

8.3.2.5 DMAC-U-SIGNAL PDU encryption

The SSI input to TB6 shall be the SSI used in the DMAC-SYNC PDU as described in clause A.3.1.1.

See EN 300 396-3 [5], clause 9.2.4 for a full description of this PDU.

The DMAC-U-SIGNAL PDU shall be encrypted as follows:

- bits 1 to 3 shall be in clear, all other bits shall be encrypted (i.e. DMAC-U-SIGNAL[0] ... DMAC-U-SIGNAL[2] shall be in clear);
- the first bit of the U-PLANE SDU shall be encrypted with KSS(0).

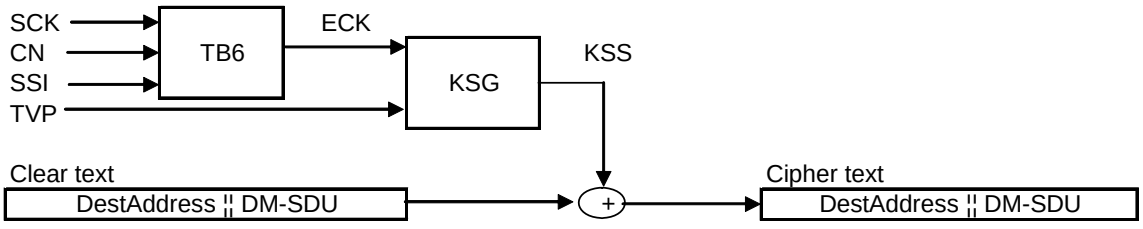
EXCEPTION: The first bit of the U-PLANE SDU shall be encrypted with KSS(216) if the PDU is sent on the STCH in the second half slot.

8.3.2.6 Traffic channel encryption

Traffic channels may be transporting speech or data. The information shall be encrypted prior to channel encoding and KSS shall be allocated as defined in table 8.1.

8.3.3 Class DM-2B

In class DM-2B the destination address (SSI), DM-SDU and any related traffic are AI encrypted (see figure 8.4).



NOTE: For decryption the input is cipher text and output is clear text.

Figure 8.4: Encryption process as it occurs in TETRA DMO Class DM-2-B

8.3.3.1 DMAC-SYNC PDU encryption

See EN 300 396-3 [5], clause 9.1.1 for a full description of this PDU.

The DMAC-SYNC PDU contained in logical channel SCH/S shall always be in clear.

The DMAC-SYNC PDU contained in logical channel SCH/H shall be encrypted as follows:

- KSS(0, …, 23) shall be used to encrypt the destination address;
- KSS(24, …, 24 +m-1) shall be used to encrypt the DM-SDU (where m is the length of the DM-SDU carried in the DMAC-SYNC PDU).

NOTE: If the destination address is not present KSS(0, ... , m-1) is to be used to encrypt the DM-SDU (where m is the length of the DM-SDU carried in the DMAC-SYNC PDU).

8.3.3.2 DMAC-DATA PDU encryption

The SSI input to TB6 shall be the SSI used in the DMAC-SYNC PDU as described in clause A.3.1.1.

See EN 300 396-3 [5], clause 9.2.1 for a full description of this PDU.

The DMAC-DATA PDU, sent in either a full signal slot (logical channel SCH/F) or using a stolen channel (STCH), shall be encrypted as follows:

- KSS(0,…, 23) shall be used to encrypt the destination address;
- KSS(24, …, 24 +m-1) shall be used to encrypt the DM-SDU (where m is the length of the DM-SDU carried in the DMAC-DATA PDU).

NOTE 1: If the destination address is not present KSS(0, ..., m-1) is to be used to encrypt the DM-SDU (where m is the length of the DM-SDU carried in the DMAC-DATA PDU).

NOTE 2: If the PDU is sent on the STCH in the second half slot and includes a destination address:

- KSS(216, …, 239) shall be used to encrypt the destination address;
- KSS(240, …, 240+m-1) shall be used to encrypt the DM-SDU (where m is the length of the DM-SDU carried in the DMAC-DATA PDU).

NOTE 3: If the PDU is sent on the STCH in the second half slot and has no destination address:

- KSS(216, …, 216+m-1) shall be used to encrypt the DM-SDU (where m is the length of the DM-SDU carried in the DMAC-DATA PDU).

8.3.3.3 DMAC-FRAG PDU encryption

The SSI input to TB6 shall be the SSI used in the DMAC-SYNC PDU as described in clause A.3.1.1.

See EN 300 396-3 [5], clause 9.2.2 for a full description of this PDU.

The DMAC-FRAG PDU shall be encrypted as follows:

- bits 1 to 4 shall be in clear, all other bits shall be encrypted (i.e. DMAC-FRAG[0] ... DMAC-FRAG[3] shall be in clear); and
- the first bit of the SDU fragment shall be encrypted with KSS(0).

8.3.3.4 DMAC-END PDU encryption

The SSI input to TB6 shall be the SSI used in the DMAC-SYNC PDU as described in clause A.3.1.1.

See EN 300 396-3 [5], clause 9.2.3 for a full description of this PDU.

The DMAC-END PDU shall be encrypted as follows:

- bits 1 to 4 shall be in clear, all other bits shall be encrypted (i.e. DMAC-END[0] ... DMAC-END[3] shall be in clear);
- the first bit of the SDU fragment shall be encrypted with KSS(0).

EXCEPTION: The first bit of the SDU fragment shall be encrypted with KSS(216) if the PDU is sent on the STCH in the second half slot.

8.3.3.5 DMAC-U-SIGNAL PDU encryption

The SSI input to TB6 shall be the SSI used in the DMAC-SYNC PDU as described in clause A.3.1.1.

See EN 300 396-3 [5], clause 9.2.4 for a full description of this PDU.

The DMAC-U-SIGNAL PDU shall be encrypted as follows:

- bits 1 to 3 shall be in clear, all other bits shall be encrypted (i.e. DMAC-U-SIGNAL[0] ... DMAC-U-SIGNAL[2] shall be in clear); and
- the first bit of the U-PLANE SDU shall be encrypted with KSS(0).

EXCEPTION: The first bit of the U-PLANE SDU shall be encrypted with KSS(216) if the PDU is sent on the STCH in the second half slot.

8.3.3.6 Traffic channel encryption

Traffic channels may be transporting speech or data. The information shall be encrypted prior to channel encoding and KSS shall be allocated as defined in table 8.5.

8.3.4 Class DM-2C

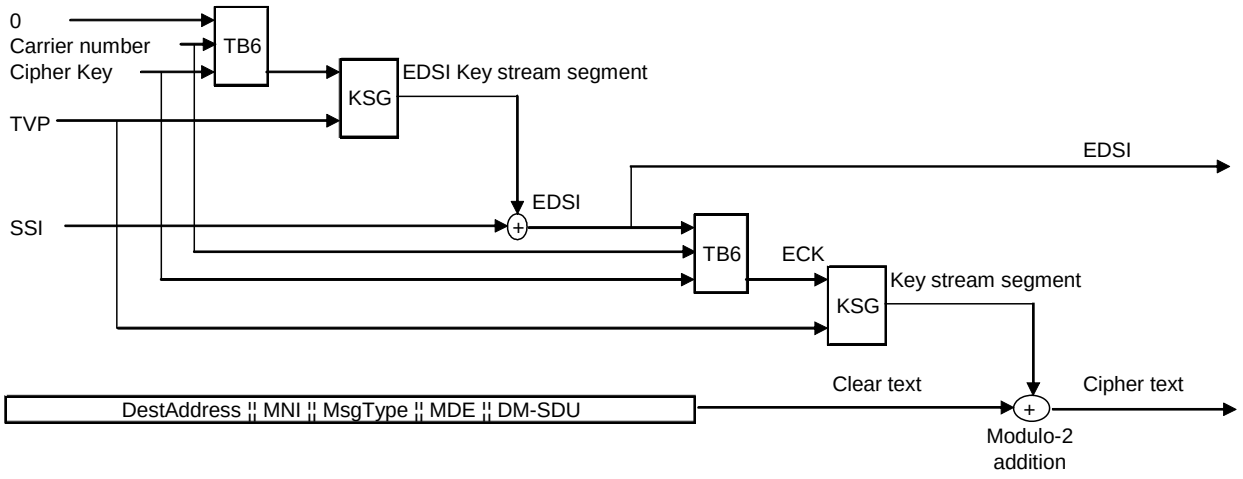
In class DM-2C the KSG and TB6 are run twice for each timeslot. The first pass generates KSS for the purpose of generating the Encrypted DMO Short Identity (EDSI). The second pass uses EDSI as an input to generate KSS for encrypting the payload.

To produce EDSI the inputs to the KSG are TVP and the output of TB6 with the address element set to zero (see figure 8.5). EDSI is dynamic and changes every timeslot.

EDSI shall be used as an input to the second pass of TB6 to produce the keystream used to encrypt the rest of the SDU and traffic. The SDU is then encrypted from the destination address element and onwards using the KSS and excluding the source address type element which is left clear and the source address which has already been encrypted as EDSI, and any related traffic is AI encrypted.

NOTE 1: For operating conditions of the KSG refer to annex A.

NOTE 2: EDSI is used as input to the scrambling code which therefore also changes every timeslot (see EN 300 396-3 [5], clause 8.2.4).



NOTE 1: MDE = Message Dependent Elements.
NOTE 2: ¦¦ = Concatenation of incoming elements.
NOTE 3: ⊕ = Modulo-2 addition of incoming elements.
NOTE 4: For decryption the input is cipher text and output is clear text.

Figure 8.5: Encryption process as it occurs in TETRA DMO Class DM-2-C

8.3.4.1 DMAC-SYNC PDU encryption

See EN 300 396-3 [5], clause 9.1.1 for a full description of this PDU.

The DMAC-SYNC PDU contained in logical channel SCH/S shall always be in clear.

The DMAC-SYNC PDU contained in logical channel SCH/H shall be encrypted as follows:

- if the fragmentation flag (bit 12) is set then bits 1 to 18 shall be in clear, all other bits shall be encrypted following the rules for address encryption; else
- if the fragmentation flag (bit 12) is not set then bits 1 to 14 shall be in clear and all other bits shall be encrypted following the rules for address encryption.

The encryption process shall operate as follows:

- the source address, if present, shall be replaced by EDSI generated as described above;
- the EDSI is used as an input to TB6, to produce a second KSS that is used to encrypt the remainder of the PDU as described in the following bullets:
  - if a destination address is present KSS(0) shall be applied to the first bit of the destination address element, and KSS(24) shall be applied to the first bit of the Mobile Network Identity element, if present, or the first bit of the Message Type element if no MNI is present;
  - if a destination address is not present, KSS(0) shall be applied to the first bit of the MNI element, if present, or the first bit of the Message Type element if no MNI is present;
  - the source address type element shall not be encrypted;
  - the destination address type element shall not be encrypted;
  - if the source address is not present an EDSI shall be generated using a source address set to "0". This EDSI shall be used as input to TB6 to generate the second KSS.

8.3.4.2 DMAC-DATA PDU encryption

See EN 300 396-3 [5], clause 9.2.1 for a full description of this PDU.

The DMAC-DATA PDU, sent in either a full signal slot (logical channel SCH/F) or using a stolen channel (STCH), shall be encrypted as follows:

- bits 1 to 10 shall be in clear, all other bits shall be encrypted (i.e. DMAC-DATA[0] ... DMAC-DATA[9] shall be in clear);
- the EDSI that is used as an input to TB6 is generated using TVP from the current timeslot and the SSI from the DMAC-SYNC PDU which carried the DM-SETUP or DM-CONNECT ACK or DM-OCCUPIED message that initiated the current traffic transmission. This SSI may be different from the source address in the DMAC-DATA PDU. The second KSS produced using EDSI is used to encrypt the remainder of the PDU as described in the following bullets:
  - KSS(0) shall be applied to the first bit of the destination address type element, and all successive bits of the PDU (including the source address type, and the source address if present) shall be encrypted using successive bits of KSS.

NOTE: If the PDU is sent on the STCH in the second half slot KSS(216) is used in placed of KSS(0).

8.3.4.3 DMAC-FRAG PDU encryption

See EN 300 396-3 [5], clause 9.2.2 for a full description of this PDU.

The DMAC-FRAG PDU shall be encrypted as follows:

- bits 1 to 4 shall be in clear, all other bits shall be encrypted (i.e. DMAC-FRAG[0] ... DMAC-FRAG[3] shall be in clear);
- the first bit of the SDU fragment shall be encrypted with KSS(0).

8.3.4.4 DMAC-END PDU encryption

See EN 300 396-3 [5], clause 9.2.3 for a full description of this PDU.

The DMAC-END PDU shall be encrypted as follows:

- bits 1 to 4 shall be in clear, all other bits shall be encrypted (i.e. DMAC-END[0] ... DMAC-END[3] shall be in clear);
- the first bit of the SDU fragment shall be encrypted with KSS(0).

NOTE: The first bit of the SDU fragment is to be encrypted with KSS(216) if the PDU is sent on the STCH in the second half slot.

8.3.4.5 DMAC-U-SIGNAL PDU encryption

See EN 300 396-3 [5], clause 9.2.4 for a full description of this PDU.

The DMAC-U-SIGNAL PDU shall be encrypted as follows:

- bits 1 to 3 shall be in clear, all other bits shall be encrypted (i.e. DMAC-U-SIGNAL[0] ... DMAC-U-SIGNAL[2] shall be in clear);
- the first bit of the U-PLANE SDU shall be encrypted with KSS(0).

NOTE: The first bit of the U-PLANE SDU is to be encrypted with KSS(216) if the PDU is sent on the STCH in the second half slot.

8.3.4.6 Traffic channel encryption

Traffic channels may be transporting speech or data. The information shall be encrypted prior to channel encoding and KSS shall be allocated as defined in table 8.1.

8.4 Encryption of identities in repeater and gateway presence signal

The EDSI mechanism for protection of addresses should be applied in class DM-2-B and DM-2-C repeaters, gateways and combined repeater-gateways and be referred to as EDSI-URTC. The indication of where EDSI-URTC applies is given by the URT field as shown in table 8.3, and the encryption mechanism is shown in figure 8.6.

Table 8.3: URT encoding

Value	Remark	URT Confidentiality
0000_2 to 0111_2	Refer to EN 300 396-5 [8] and to EN 300 396-4 [9]	Does not apply
1000_2	URTC Restricted to single MNI	Applies
1001_2	URTC Restricted to single address (TSI)	Applies
1010_2	URTC Restricted to 1 address (SSI)	Applies
1011_2	URTC Restricted to 2 addresses (SSI+SSI)	Applies
1100_2 to 1111_2	Refer to EN 300 396-5 [8] and to EN 300 396-4 [9]	Does not apply

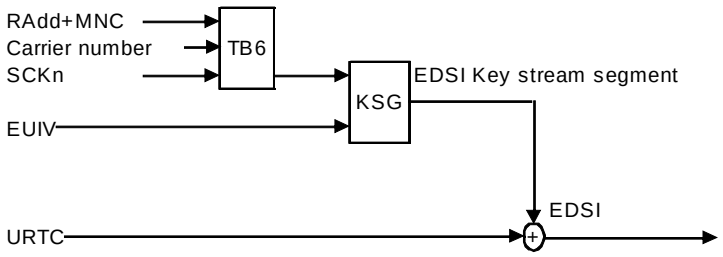


Figure 8.6: EDSI-URTC KSS generation mechanism

The following inputs to TB6 shall be made for EDSI-URTC:

- Input 1(Cipher Key): SCKn (EDSI-URTC key indicated in presence signal).
- Input 2 (Carrier Number): CN of Repeater/Gateway/Rep-gate (i.e. that which the repeater/gateway/rep-gate operates on).
- Input 3 (SSI): Repeater address (10 bits) concatenated with the MNC of the Repeater, or Gateway or Rep-Gate (14 bits).

The resultant output will be a modified CK for use with KSG to generate a KSS for encryption of the address field in presence messages where the EDSI-URTC Initialisation Vector (EUIV) input to the KSG shall be as defined below.

48 bits of KSS shall be generated. The KSS shall be utilised as follows:

- URT $1000_2$and 1010_2: The first generated 24 bits of KSS shall be XORed with the single 24 bit address (MNI or SSI) which follows the EUIV. The remaining KSS shall be discarded, and the following 24 reserved bits shall not be encrypted.
- URT $1001_2$and 1011_2: The 48 bits of KSS shall be XORed with the 48 bits of addressing (single TSI or two SSIs) that follow the EUIV.

The EUIV in this instance shall be considered as a 29 bit vector [$EUIV_0$, $EUIV_1$, …, $EUIV_{28}$] where bits 0 to 9 shall be populated with the repeater, rep-gate or gateway address, and bits 10 to 28 shall be populated with the content of the "address encryption time variant parameter" element. The bits shall be ordered such that the least significant bit of the repeater, gateway or rep-gate address is mapped to $EUIV_0$ and the least significant bit of the "address encryption time variant parameter" shall be mapped to $EUIV_{10}$. The frequency of update of EUIV is not defined but it should be updated in practice at least on change of the DM-PRES-SYNC PDU address field contents but may be fixed for cyclic transmissions of address field contents (e.g. EUIV#1 for address field content #1, EUIV#2 for address field content #2, and on retransmission of address field content #1 revert to EUIV#1).

The EUIV should be changed sufficiently frequently such that a change of URT is not obvious to an eavesdropper and not so frequently that EUIV is reused within the lifetime of the present SCK.

The allocation of addresses when URTC is deployed is also shown in figure 8.7.

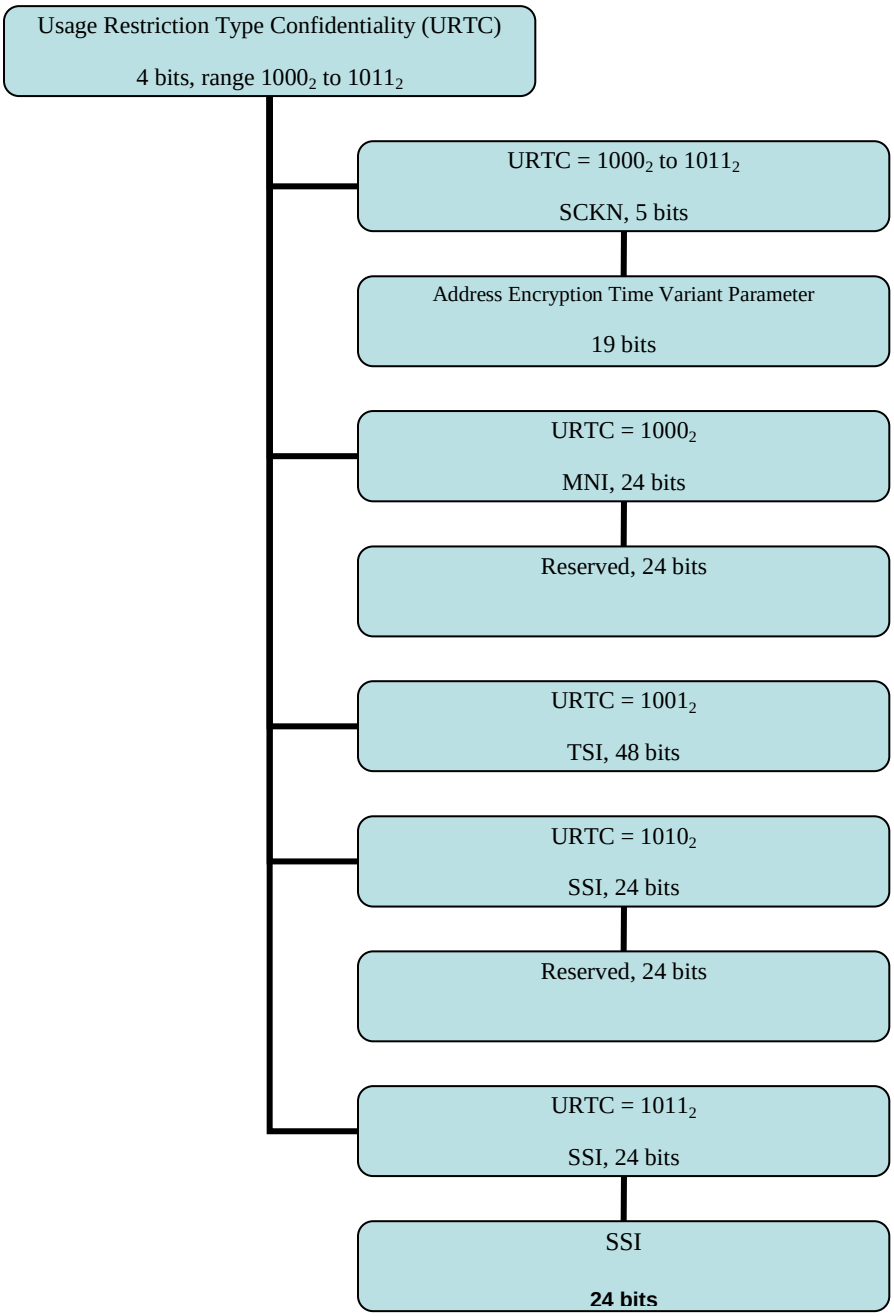


Figure 8.7: Allocation of addresses for URTC range of URT

9 Encryption synchronization

9.1 General

In DMO there is no centralized synchronization master. Each call transaction has a rotating master-slave relationship, with the master-role being that of the current transmitter, and the slave-role being that of the current receivers.

In DMO the encryption synchronization shall apply only to the current call transaction. All slaves shall set the values of Frame Number (FN), Timeslot Number (TN) and TVP from the first synchronization burst and increment each value as appropriate for the duration of the call transaction. (See EN 300 396-2 [3], clauses 9.3.2 and 9.3.3 for full definitions of FN and TN, and EN 300 396-2 [3], clause 7.3.2 for definitions of the incrementing of these counters.)

NOTE 1: In cases where a Direct Mode Synchronisation Burst (DSB) (see EN 300 396-3 [5] for the full definition) is transmitted the receiving MSs are able to find the value of TVP from the DSB transmission in order to be able to decrypt the content.

The initial value of TVP shall be chosen by each call transaction master. Each initial TVP shall be chosen randomly to prevent replay.

Each transmitting party shall establish a new TVP for new call transactions, for slave response messages (e.g. DM-CONNECT, DM-DISCONNECT and DM-SDS ACK (possibly fragmented)), and for random access messages (e.g. pre-emption or changeover or timing change requests).

NOTE 2: This includes retries of random access messages.

TVP shall be incremented on every timeslot with a cycle of 2^{29} timeslots other for those PDUs shown in table 9.1.

Table 9.1: Exceptions to normal TVP increment

Message type
DM-SETUP
DM-SETUP PRES
DM-CONNECT
DM-DISCONNECT
DM-SDS UDATA
DM-SDS DATA
DM-SDS ACK
DM-GSETUP
DM-GTX REQUEST (MS has pre-empted another MS)
DM-GREGISTER REQUEST (free)
DM-GREGISTER CANCEL
DM-GCANCEL ACK

EXAMPLE: For call setup without presence checking (DM-SETUP), TVP = TVP_S + 1 on the first slot of the first frame after completion of transmission of the DM-SETUP messages, where TVP_S is the value of TVP used in the call setup synchronization bursts. This is shown in figure 9.1. In the example shown in figure 9.1, the first slot of the first frame after completion of transmission of the DM-SETUP messages is also the first traffic slot.

NOTE 3: Call setup refers to the establishment of a single call transaction.

FN17				FN18				FN1				FN2			
TN1	TN2	TN3	TN4	TN1	TN2	TN3	TN4	TN1	TN2	TN3	TN4	TN1	TN2	TN3	TN4
Synchronization				Synchronization				Traffic							
TVP_S	TVP_S	TVP_S	TVP_S	TVP_S	TVP_S	TVP_S	TVP_S	TVP_S +1	TVP_S +2	TVP_S +3	TVP_S +4	TVP_S +5	TVP_S +6	TVP_S +7	TVP_S +8

NOTE 1: TVP_S is the value of TVP used in the call setup synchronization bursts.

NOTE 2: Normal traffic transmission slots are shown shaded.

Figure 9.1: Incrementing of TVP after call setup synchronization bursts for DM-SETUP

For call setup with presence checking (DM-SETUP PRES) the above process shall be followed, where TVP for the master to slave direction is incremented on the first slot of the first frame after completion of transmission of the DM-SETUP PRES messages. On receipt of DM-CONNECT in the presence check acknowledgement slot the TVP established by the acknowledging slave shall be used by the master to decrypt the DM-CONNECT message.

In the case where a DM-SDS DATA or DM-SDS UDATA message is fragmented, the first part of the short data message is sent repeatedly in the short data setup synchronization bursts as above and the following DMAC-FRAG and DMAC-END PDUs are sent as per normal traffic (i.e. as in figure 9.1).

In frequency efficient mode TVP is independent for each call and is incremented on every timeslot, even though each call does not use all timeslots.

9.1.1 Algorithm to establish frame number to increment TVP

9.1.1.1 Master DM-MS operation

For the transmitting master DM-MS, where:

W: The frame number of the frame containing the master DM-MS's final transmission of any PDU where TVP is not incremented during repetition (see table 9.1);

Y: The frame number of the frame in which the master DM-MS shall first increment TVP on slot 1.

Then:

$Y = W \bmod 18 + 1$.

9.1.1.2 Slave DM-MS operation

For the receiving slave DM-MS, where:

X: The frame number of the frame containing a PDU where TVP is not incremented during repetition (see table 9.1);

Y: The frame number of the frame in which the slave DM-MS shall first increment TVP on slot 1;

F: "frame countdown" counter observed in the received setup synchronization burst.

Then:

$Y = (X + F) \bmod 18 + 1$.

These rules shall apply even if Y = 18.

NOTE: $18 \bmod 18 = 0$.

9.2 TVP used for reception of normal bursts

For call setup with presence check, the slave DM-MS deduces the TVP for the traffic from the TVP in the DM-CONNECT ACK message (where the TVP is incremented on every timeslot following the reception of the DM-CONNECT ACK).

For late entry, the slave DM-MS deduces the TVP for the traffic from the TVP in the DM-OCCUPIED message (where the TVP is incremented on every timeslot following the reception of the DM-OCCUPIED message).

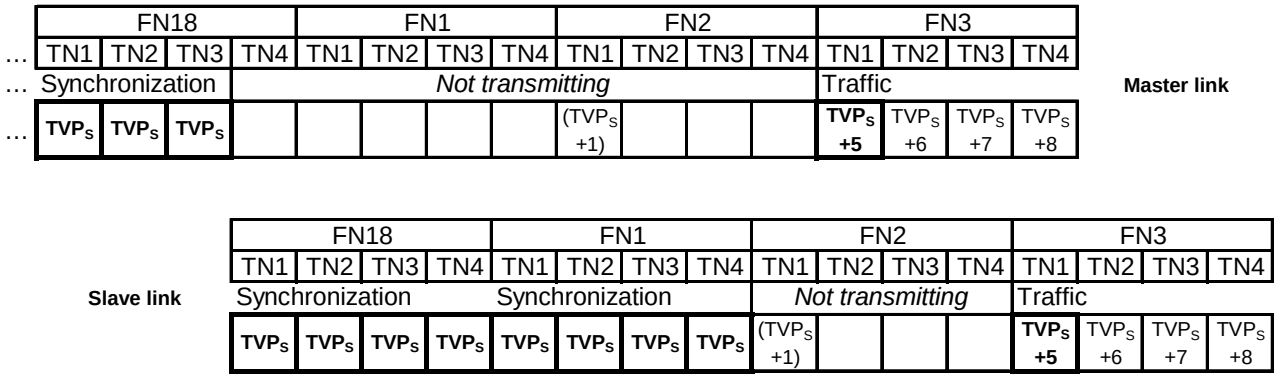
When receiving a fragmented DM-SDS ACK message, the slave DM-MS deduces the TVP for the continuation fragment from the TVP in the DM-SDS ACK synchronization burst (where the TVP is incremented on every timeslot following the reception of the last slot of the last repetition of DM-SDS ACK synchronization burst (see table 9.1)).

9.3 Synchronization of calls through a repeater

A repeater modifies the normal call setup synchronization burst pattern and repeats a received set-up synchronization burst over a number of frames.

During call set-up, TVP shall not be incremented during call setup synchronization bursts but shall be repeated across each slot of the frames containing the DM-SETUP or DM-SETUP PRES messages or short data setup synchronization bursts on both the link from the master to the repeater and the link from the repeater to the slaves. In the slave, TVP shall first be incremented on the first timeslot of the first slave link frame after the repeater has finished repeating the DM-SETUP or DM-SETUP PRES messages or short data setup synchronization bursts on the slave link.

This is shown for a call setup without presence checking in figure 9.2. The TVP is first incremented on the first slot of the first slave link frame after the repeater has finished repeating the DM-SETUP messages on the slave link. In the example shown in figure 9.2, the first traffic slot from the master is in the first slot of the first master link frame after the repeater has finished repeating the DM-SETUP messages on the slave link.



NOTE 1: TVP_S is the value of TVP used in the synchronization bursts.
NOTE 2: The first traffic slot from the master is in the first slot of the first frame after the repeater has finished repeating the synchronization data (TN1 of FN3 in above example).
NOTE 3: Transmission slots are shown in bold and with enhanced borders.

Figure 9.2: Incrementing of TVP of DM-SETUP across a type-1 repeater

For call setup with presence checking the above process shall be followed, so TVP for the master to slave direction is incremented on the first slot of the first slave link frame after the repeater has finished repeating the DM-SETUP PRES messages on the slave link. On receipt of DM-CONNECT in the presence check acknowledgement slot the TVP established by the acknowledging slave shall be used by the master to decrypt the DM-CONNECT message.

In the case where a DM-SDS DATA or DM-SDS UDATA message is fragmented, the first part of the short data message is sent repeatedly in the short data setup synchronization bursts as above and the following DMAC-FRAG and DMAC-END PDUs are sent as per normal traffic (i.e. as in figure 9.2).

9.3.1 Algorithm to establish frame number to increment TVP

9.3.1.1 Master DM-MS operation

For the transmitting master DM-MS, where:

W: The frame number of the master link frame containing the master DM-MS's final transmission of a DM-SETUP or DM-SETUP PRES message or short data setup synchronization burst (i.e. a synchronization burst for a DM-SDS DATA or DM-SDS UDATA message).

Y: The frame number of the master link frame in which the master DM-MS shall first increment TVP on slot 1.

DN232: The number of frames in which the repeater transmits the DM-SETUP or DM-SETUP PRES message on the slave link (see clause 10.3.18 of EN 300 396-4 [9]).

DN233: The number of frames in which the repeater transmits the short data setup synchronization burst on the slave link (see clause 10.3.18 of EN 300 396-4 [9]).

NOTE: The DM-MS knows the values of DN232 and DN233 only if it has received a presence signal from the device repeater. Where covert devices are in use (no presence signal transmitted) these values should be pre-configured at the DM-MS. In the latter case it should be better to use the frame countdown value get from the set-up PDU (belonging to echo) in order to calculate the frame number where to increment TVP.

Then, either, following a DM-SETUP or DM-SETUP PRES message:

$Y = (W + DN232 - 1) \bmod 18 + 1$.

Or, following a short data setup synchronization burst:

$Y = (W + DN233 - 1) \bmod 18 + 1$.

This rule shall apply for all values of Y.

9.3.1.2 Slave DM-MS operation

For the receiving slave DM-MS, where:

X: The frame number of the slave link frame containing a received DM-SETUP or DM-SETUP PRES message or short data setup synchronization burst (i.e. a synchronization burst for a DM-SDS DATA or DM-SDS UDATA message).

Y: The frame number of the slave link frame in which the slave DM-MS shall first increment TVP on slot 1.

F: The "frame countdown" counter observed in received setup synchronization burst.

Then:

$Y = (X + F) \bmod 18 + 1$.

This rule shall apply for all values of Y.

NOTE: $18 \bmod 18 = 0$.

9.4 Synchronization of calls through a gateway

In circuit mode calls established through a gateway the DM-MS uses two synchronization phases:

- DM-GSETUP to call the gateway; then
- DM-SETUP normal call setup.

In both cases the gateway acts as timing master for the call.

The calls on each side of the gateway are considered independent in terms of encryption synchronization and the synchronization behaviour described in clause 9.1 shall apply for a DM-MS operating with a DM-GATE. The synchronization behaviour described in clause 9.3 shall apply for a DM-MS operating with a DM-REP/GATE.

9.5 Synchronization of data calls where data is multi-slot interleaved

NOTE: The examples below assume that the data call is a single slot call transmitted on timeslot 1 of each frame.

In multi-slot interleaved calls the original traffic burst is expanded to cover 4 or 8 bursts (TCH/2,4, TCH/4,8). The interleaving follows encryption at the transmitter, and decryption follows de-interleaving at the receiver (see figure 9.3).

Transmitted Traffic	T1	T2	T3	T4	T5	T6	T7	T8
Transmitted Frame	FN1	FN2	FN3	FN4	FN5	FN6	FN7	FN8
Encryption TVP value	TVP_S+1	TVP_S+5	TVP_S+9	TVP_S+13	TVP_S+17	TVP_S+21	TVP_S+25	TVP_S+29
	T1 (1 of 4)	T1(2 of 4)	T1 (3 of 4)	T1 (4 of 4)	T5 (1 of 4)	T5 (2 of 4)	T5 (3 of 4)	T5 (4 of 4)
Interleaving	null	T2 (1 of 4)	T2 (2 of 4)	T2 (3 of 4)	T2 (4 of 4)	T6 (1 of 4)	T6 (2 of 4)	T6 (3 of 4)
over 4 frames	null	null	T3 (1 of 4)	T3 (2 of 4)	T3 (3 of 4)	T3 (4 of 4)	T7 (1 of 4)	T7 (2 of 4)
	null	null	null	T4 (1 of 4)	T4 (2 of 4)	T4 (3 of 4)	T4 (4 of 4)	T8 (1 of 4)

Recovered traffic frame	T1	T2	T3	T4	T5
Decryption TVP value	TVP_S+1	TVP_S+5	TVP_S+9	TVP_S+13	TVP_S+17
Actual TVP value	TVP_S+13	TVP_S+17	TVP_S+21	TVP_S+25	TVP_S+29

NOTE 1: TVPS is the value of TVP used in the synchronization bursts.
NOTE 2: Actual TVP value is to be used for decryption of non-traffic bursts.

Figure 9.3: Value of TVP to be used for TCH/4.8 or TCH/2.4 with interleaving depth of 4

The actual TVP value is to be used by the receiver for the synchronization bursts and any bursts that are not (interleaved) traffic. The value of TVP to be used in the receiver shall be "TVP_A - 4 × (interleaving depth - 1)", where TVP_A is the actual value of TVP.

Transmission across frame 18 shall be treated as shown in figure 9.4.

Transmitted Traffic	T15	T16	T17	Synch.	T18	T19	T20	T21
Transmitted Frame	FN15	FN16	FN17	FN18	FN1	FN2	FN3	FN4
Encryption TVP value	TVP_{Start}	TVP_{Start}+4	TVP_{Start}+8	TVP_{Start}+12	TVP_{Start}+16	TVP_{Start}+20	TVP_{Start}+24	TVP_{Start}+28
	T15 (1 of 4)	T15 (2 of 4)	T15 (3 of 4)		T15 (4 of 4)	T19 (1 of 4)	T19 (2 of 4)	T19 (3 of 4)
Interleaving	T12 (4 of 4)	T16 (1 of 4)	T16 (2 of 4)		T16 (3 of 4)	T16 (4 of 4)	T20 (1 of 4)	T20 (2 of 4)
over 4 frames	T13 (3 of 4)	T13 (4 of 4)	T17 (1 of 4)		T17 (2 of 4)	T17 (3 of 4)	T17 (4 of 4)	T21 (1 of 4)
	T14 (2 of 4)	T14 (3 of 4)	T14 (4 of 4)		T18 (1 of 4)	T18 (2 of 4)	T18 (3 of 4)	T18 (4 of 4)
Recovered traffic frame	T12	T13	T14	Synch.	T15	T16	T17	T18
Decryption TVP value				TVP_{Start}+12	TVP_{Start}	TVP_{Start}+4	TVP_{Start}+8	TVP_{Start}+16
Actual TVP value	TVP_{Start}	TVP_{Start}+4	TVP_{Start}+8	TVP_{Start}+12	TVP_{Start}+16	TVP_{Start}+20	TVP_{Start}+24	TVP_{Start}+28

NOTE: TVPStart is the value of TVP used in the first traffic frame in this example.

Figure 9.4: Treatment of TVP for TCH/4,8 or TCH/2,4 with interleaving depth of 4 at frame 18

For traffic frames starting, but not fully received, before frame 18, the value of TVP to be used for decryption shall be "TVP_A - 4 × (interleaving depth - 1) - 4", where TVP_A is the actual value of TVP.

9.5.1 Recovery of stolen frames from interleaved data

If a frame has been stolen it shall not be treated as if it were interleaved and shall therefore be decrypted with the "actual" value of TVP.

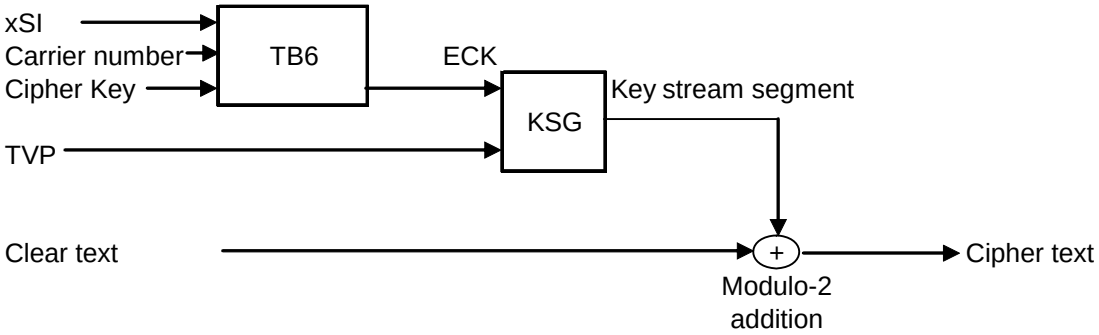
NOTE: Speech and full rate data transmissions are not subject to multi-slot interleaving (see EN 300 396-3 [5]).

Annex A (normative): Key Stream Generator (KSG) boundary conditions

NOTE: The KSG defined for TETRA DMO is the same as that defined for TETRA TMO with modification only of the derivation of the Encryption Cipher Key (ECK).

A.1 Overview

The ciphering process shall be as shown in figure A.1. A cipher key shall be used in conjunction with a KSG to generate a key stream for encryption and decryption of information at the MAC layer.



NOTE 1: In class 2A and class 2B xSI = SSI.
NOTE 2: In class 2C xSI = EDSI.

Figure A.1: Speech and control information encryption

TETRA supports both standard and proprietary algorithms. Synchronization signalling shall identify which algorithm is in use.

An MS may have more than one algorithm but shall use the algorithm indicated in the synchronization signalling.

Table A.1 shows that the values 0000_2 to 0111_2 of KSG number used in signalling shall be reserved for the TETRA standard algorithms (see also EN 300 396-3 [5], clause 9.3.14).

Table A.1: KSG number element contents

Information element	Length	Value	Remark
KSG Number	4	0000_2	TETRA Standard Algorithm, TEA1
		0001_2	TETRA Standard Algorithm, TEA2
		0010_2	TETRA Standard Algorithm, TEA3
		0011_2	TETRA Standard Algorithm, TEA4
		0100_2 to 0111_2	Reserved for future expansion
		$1xxx_2$	Proprietary TETRA Algorithms

The TETRA standard algorithms are only available on a restricted basis. The management rules for these algorithms can be found via the ETSI Web Portal (http://www.etsi.org/WebSite/OurServices/Algorithms/algorithms.aspx) and on request to the custodian of the required algorithm.

A.2 Use

The KSG shall only be used to protect the confidentiality of traffic, signalling and identities on the air interface link between a DM-MS and one or more of the following:

- a DM-MS;
- a group of DM-MSs;
- a DM-REP; or
- a DM-GATE or DM-REP/GATE.

The KSG shall form an integral part of a DM-MS, a DM-REP or a DM-GATE or a DM-REP/GATE.

A.3 Interfaces to the algorithm

The KSG shall have two inputs, a Time Variant Parameter (TVP) and an Encryption Cipher Key (ECK). The KSG shall produce one output as a sequence of key stream bits referred to as a Key Stream Segment (KSS).

A.3.1 ECK

ECK shall be formed using algorithm TB6 from the following input parameters:

- Static Cipher Key (SCK).
- Carrier Number (CN) (modulo 4000). Where a repeater is in use the value of CN shall be equal to the value on the downlink.

NOTE 1: CN is defined in EN 300 392-2 [1], clause 16.10.8A and in TS 100 392-15 [6], and input to TB6 as Cnmod4000.

- Short Subscriber Identity (SSI) or Encrypted DMO Short Identity (EDSI).

NOTE 2: In security class DM-2-A and DM-2-B the SSI that is the source address is to be used as input to TB6.

NOTE 3: In security class DM-2-C the EDSI is to be used as input to TB6 instead of SSI.

NOTE 4: In security class DM-2-A and DM-2-B if no source SSI input is available the SSI input to TB6 is to be set to all "0".

NOTE 5: In security class DM-2-C, if no source SSI input is available, the EDSI input to TB6 is to be created using an SSI input which is set to all "0".

A.3.1.1 Use of ECK in class DM-2-A and DM-2-B

For encryption and decryption of traffic and PDUs sent on STCH, the key stream generator shall use the ECK derived using the SSI from the DMAC-SYNC PDU which carried the DM-SETUP or DM-CONNECT ACK message that initiated the current traffic transmission.

For decryption by a late entrant of traffic and PDUs sent on STCH, the key stream generator shall use the ECK derived using the SSI from the DMAC-SYNC PDU which carried the DM-OCCUPIED message.

For encryption and decryption of PDUs sent on SCH/F, the key stream generator shall use the ECK derived using the SSI from the DMAC-SYNC PDU that initiated the fragmentation.

A.3.1.2 Use of ECK in class DM-2-C

For encryption and decryption of traffic and PDUs sent on STCH, the key stream generator shall use the ECK derived using the EDSI which is itself generated from the SSI sent in the appropriate DMAC-SYNC PDU (see clause A.3.1.1) and the TVP for the current timeslot.

A.3.2 Keystream

A KSS of length n shall be produced to encrypt every timeslot. The bits of KSS are labelled KSS(0), … KSS(n-1), where KSS(0) is the first bit output from the generator. The bits in the KSS shall be used to encrypt or decrypt the data of the control or traffic field. The maximum value of n shall be 432 (MAXLENGTH = 432), which enables encryption of a TCH/7.2 unprotected traffic channel.

KSS: the output keystream segment.

KSS [0], KSS [1], …, KSS [MAXLENGTH-1].

A.3.3 Time Variant Parameter (TVP)

The TVP shall be used to initialize the KSG at the start of every timeslot. The TVP shall be a value 29 bits long represented as TVP(0) …. TVP(28), where TVP(0) shall be the least significant bit and TVP(28) the most significant bit of TVP.

The initial value of TVP is a transmitted parameter that shall be sent in the call setup synchronization bursts by the current call master. The TVP shall be maintained as described in clause 9.

After the synchronization frames TVP shall be incremented by 1 on each timeslot transition (see also clause 9).

NOTE: TVP is independent of FN and TN.

Annex B (normative): Boundary conditions for cryptographic algorithm TB6

TB6: Shall be used to compute Encryption Cipher Key (ECK) from selected Cipher Key (CK), SSI and carrier number CN. The algorithm shall have the following properties:

Input 1: Bit string of length ¦CK¦;

Input 2: Bit string of length ¦CN¦;

Input 3: Bit string of length ¦SSI¦;

Output: Bit string of length ¦ECK¦.

The algorithm should be designed such that the output is dependent upon every bit of all inputs where the lengths of each input are given in table B.1.

Table B.1: Dimensioning of cryptographic parameters

Abbreviation	No. of bits
CK	80
CN	12
ECK	80
SSI	24

NOTE: EDSI may be used instead of SSI as input to TB6. EDSI is also 24 bits in length.

Annex C (informative): Encryption control in DM-MS

NOTE: There is no testable behaviour within an MS other than by examination of the protocol at the air interface. In light of this the material given in this clause is illustrative of the protocol development process but does not impose a requirement on the design of terminals.

C.1 General

Call security in the MS is be controlled by DMCC, which may indicate its security state to the MS application through the DMCC SAP.

The AI encryption control service is used to:

- start or stop the encryption service;
- identify the KSG;
- identify the cipher key used;
- initiate the loading of the cipher key to the KSG.

The control service involves layer 3 (DMCC), and layer 2 (MAC) of the TETRA protocol stack.

C.2 Service description and primitives

Each layer in the protocol stack provides a set of services to the layer above. This clause describes the services that are added to those provided by each layer due to the incorporation of encryption, in addition to those specified in EN 300 396-3 [5]. The primitives that are passed between the layers are also described.

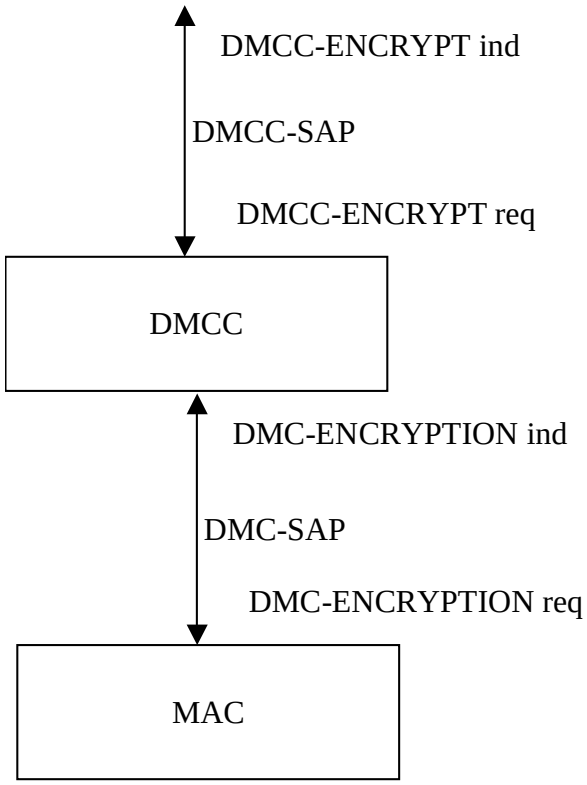


Figure C.1: Encryption related services in DMO

The following services are provided at the DMCC-SAP:

- DMCC-ENCRYPT indication is used by DMCC to indicate to the application the encryption state and key data for the current call.
- DMCC-ENCRYPT request is used in conjunction with DMCC SETUP (see EN 300 396-3 [5], clause 5.3.7) to set the encryption parameters for the current call. This primitive may also be used to pre-configure the preferred encryption parameters for all calls initiated by DMCC.

The following services are provided at the DMC-SAP:

- DMC-ENCRYPTION request is used to instruct the MAC to load the identified encryption parameters to the encryption unit.
- DMC-ENCRYPTION indication is used to inform DMCC of the encryption state and key parameters for the current call (or call request).

C.2.1 DMCC-ENCRYPT primitive

Table C.1: DMCC-ENCRYPT parameters

Parameter	Request	Indication
Key download type	M	-
Configuration data	M	
KSG Number (note 1)	C	-
SCK (note 2)	C	-
SCKN	C	M
Cipher usage (note 1)	C	-
NOTE 1: May be omitted if the state of the parameter has not changed from the previous request. NOTE 2: Key download type indicates which fields are present.		
Key: M = Mandatory; C = Conditional; O = Optional		

The parameters are encoded as follows:

Key download type =

no keys downloaded

SCK

KSG Number =

KSG 1

KSG 2

KSG 3

…

KSG 16

Cipher usage =

encryption off (Class 1)

TX, Class 2-A

TX, Class 2-B

TX, Class 2-C

RX

SCKN =

1

2

3

…

32

SCK =

0

…

2^{80}-1

The configuration data parameter indicates if the data in the Request applies only to the current call or is configuration data for all calls.

Configuration data =

Configuration

Current call

C.2.2 DMC-ENCRYPTION primitive

At the DMC SAP the following services are provided to DMCC:

- loading of keys;
- start and stop ciphering.

These services are achieved by passing information to the MAC layer using the DMC-ENCRYPTION request primitive. The MAC indicates to DMCC the current SCKN that is received in the DMAC-SYNC PDU.

Table C.2: DMC-ENCRYPTION parameters

Parameter	Request	Indication
KSG Number	M	-
SCK	C	-
SCKN	-	M
Cipher usage	M	M
Key: M = Mandatory; C = Conditional; O = Optional		

KSG Number parameter indicates the Key Stream Generator (one of 16 possible) in use.

KSG Number =

KSG 1

KSG 2

KSG 3

…

KSG 16

Cipher usage parameter indicates to the MAC whether the transmitted messages should be encrypted and whether the MAC should try to decrypt received encrypted messages.

Cipher usage =

encryption off (Class 1)

TX, Class 2-A

TX, Class 2-B

TX, Class 2-C

RX

SCKN =

1

2

3

…

32

SCK =

0

…

2^{80}-1

C.3 Protocol functions

Each functional entity in the protocol stack communicates with its peer entity using a defined protocol.

EXAMPLE: The DMCC entity in the originating DM-MS communicates with its peer DMCC entity in the receiving DM-MS.

On receiving DMCC-ENCRYPT request from the DMCC-SAP the DMCC process maps the parameters into the DMC-ENCRYPTION request primitive and sends it via the DMC-SAP to the MAC.

In the MAC on receiving DMC-ENCRYPTION request from the DMC-SAP, the MAC determines the value of the AI Encryption State element and the content of the associated 39 conditional bits of DMAC-SYNC PDU.

On receiving DMC-ENCRYPTION indication from the DMC-SAP DMCC sends DMCC-ENCRYPT indication to the DMCC-SAP.

Annex D (informative): Bibliography

- ETSI EN 300 396-1: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 1: General network design".
- ETSI EN 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

Annex E (informative): Change request history

The following CRs have been incorporated in the present document.

CR	Date	Version	Short description	Status
001	13-10-05	V1.2.1	Clarification of key selection for master and slave during pre-emption and follow on	WG6 Approved
101	14-07-08	V1.3.1	Addition of EDSI-URTC mechanism	WG6 Approved
201	01-11-10	V1.4.1	Choice of pre-emption key	WG6 Approved
202	14-09-11	V1.4.2	Implementation of multiple SCK sets	WG6 Approved
203	30-01-12	V1.4.3	Use of KSS with EDSI-URTC	WG6 Approved

History

Document history		
Edition 1	May 1998	Publication as ETS 300 396-6
V1.2.1	May 2004	Publication
V1.3.1	June 2006	Publication
V1.4.1	July 2010	Publication
V1.5.0	May 2012	One-step Approval Procedure OAP 20120914: 2012-05-17 to 2012-09-14
V1.5.1	September 2012	Publication