EUROPEAN
TELECOMMUNICATION
STANDARD

DRAFT
pr ETS 300 396-6
December 1996

Source: ETSI TC-RES

Reference: DE/RES-06007-6

ICS: 33.020

Key words: TETRA, DMO, security

Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

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

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Blank page

Foreword

This draft European Telecommunication Standard (ETS) has been produced by the Radio Equipment and Systems (RES) Technical Committee of the European Telecommunications Standards Institute (ETSI), and is now to be submitted fore the Public Enquiry phase of the ETSI standards approval procedure.

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

Part 1: "General network design";

Part 2: "Radio Aspects";

Part 3: "Mobile Station to Mobile Station (MS-MS) Air Interface (AI) protocol";

Part 4: "Repeater type 1";

Part 5: "Gateways", (DE/RES-06007-5);

Part 6: "Security";

Part 7: "Repeater type 2";

Part 8: "Protocol Implementation Conformance Statement (PICS) proforma";

Part 9: "SDL model".

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

Blank page

1 Scope

This European Telecommunication Standard (ETS) defines the Trans-European Trunked Radio (TETRA) Direct Mode Operation (DMO). It specifies the basic air interface, the inter-working between Direct Mode (DM) groups via Repeaters, and inter-working with the TETRA trunked system via Gateways. It also specifies the security aspects in TETRA DMO, and the intrinsic services that are supported in addition to the basic bearer and teleservices.

This part of this ETS describes the security mechanisms in TETRA DMO. It provides mechanisms for confidentiality of control signalling and user speech and data at the air interface.

- Clause 4 describes the general condition for which security of calls at the air interface can be met. This clause introduces conditions that all other clauses must follow.

- Clause 5 describes authentication mechanisms for DM. The differences between peer-to-peer authentication mechanisms and client-server authentication mechanisms are covered by this clause as are the principles of operation in gateway mode.

- Clause 6 describes the confidentiality mechanisms using encryption on the air interface, for circuit mode speech, circuit mode data, packet data and control information. This clause then details the protocol concerning control of encryption at the air interface.

- Clause 7 describes the key management mechanism, and includes a description of the Over The Air Re-keying (OTAR) mechanism and protocol.

- Clause 8 describes the enable/disable mechanism and includes a description of the protocol.

- Clause 9 describes the mechanism to be used to support end-to-end encryption using synchronous cipher units for U-plane traffic by means of a frame stealing device for synchronisation of the units.

The use of air interface encryption gives confidentiality protection against eavesdropping only. The addition of a synchronised time variant initialisation value for the encryption algorithm gives a restrictive degree of replay protection.

2 Normative references

This ETS incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETS 300 392-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

[2] ETS 300 392-2: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

[3] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic reference model - Part 2: Security Architecture".

[4] ETS 300 396-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 1: General network design".

[5] ETS 300 396-2: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 2: Radio aspects".

[6] ETS 300 392-7: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[7] ETS 300 396-3: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 3: Mobile Station to Mobile Station (MS-MS) Air Interface (AI) protocol".

3 Definitions and abbreviations

3.1 Definitions

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

Authentication Key (K): The primary secret, the knowledge of which has to be demonstrated for authentication.

cipher key: A value that is used to determine the transformation of plain text to cipher text in a cryptographic algorithm.

cipher text: The data produced through the use of encipherment. The semantic content of the resulting data is not available (ISO 7498-2) [3].

decipherment: The reversal of a corresponding reversible encipherment (ISO 7498-2) [3].

encipherment: The cryptographic transformation of data to produce cipher text (ISO 7498-2) [3].

encryption state: Encryption on or off.

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

flywheel: A mechanism to keep the Key Stream Generator (KSG) in the receiving terminal synchronized with the KSG in the transmitting terminal in case synchronization data is not received correctly.

Initialization Value (IV): A sequence of symbols that initializes the KSG inside the encryption unit.

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

Key Stream Generator (KSG): A cryptographic algorithm which produces a stream of binary digits which can be used for encipherment and decipherment. The initial state of the KSG is determined by the initialization value.

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

Manipulation Flag (MF): Used to indicate that the Static Cipher Key (SCK) has been incorrectly recovered in an OTAR exchange.

plain text: The un-encrypted source data. The semantic content is available.

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

SCK-set: The collective term for the group of 32 SCK associated with each Individual TETRA Subscriber Identity (ITSI).

Sealed Static Cipher Key (SSCK): A static cipher key cryptographically sealed with a particular user's secret key. In this form the keys are distributed over the air interface.

spoofer: An entity attempting to obtain service from or interfere with the operation of the system by impersonation of an authorized system user or system component.

Static Cipher Key (SCK): A predetermined cipher key that may be used if no (successful) authentication has taken place.

synchronization value: A 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: An encryption method in which a cipher text symbol completely represents the corresponding plain text symbol. 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: The mathematical description of the cryptographic process used for either of the security processes authentication or encryption.

time stamp: A sequence of symbols that represents the time of day.

3.2 Abbreviations

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

AC	Authentication Centre
AI	Air Interface
AESI	Alias Encrypted Short Identity
ASSI	Alias Short Subscriber Identity
C-PLANE	Control-PLANE
CT	Cipher Text
DM	Direct Mode
DMO	Direct Mode Operation
EKSG	End-to-end Key Stream Generator
EKSS	End-to-end Key Stream Segment
ESI	Encrypted Short Identity
F	Function
FEC	Forward Error Correction
GESI	Group Encrypted Short Identity
GSSI	Group Short Subscriber Identity
GTSI	Group TETRA Subscriber Identity
HSC	Half-Slot Condition
HSI	Half-Slot Importance
HSN	Half-Slot Number
HSS	Half-Slot Stolen
HSSE	Half-Slot Stolen by Encryption unit
IESI	Individual Encrypted Short Identity
ISSI	Individual Short Subscriber Identity
ITSI	Individual TETRA Subscriber Identity
IV	initialization Value
K	authentication Key
KG	Key Generator
KH	Key Holder
KSG	Key Stream Generator
KSO	Session Key OTAR
KSS	Key Stream Segment
KU	Key User
LLC	Logical Link Control
MAC	Medium Access Control
MF	Manipulation Flag
MNI	Mobile Network Identity
MS	Mobile Station
MSC	Message Sequence Chart
PDU	Protocol Data Unit
PT	Plain Text
RSO	Random Seed for OTAR
SAP	Service Access Point
SCK	Static Cipher Key
SCK-VN	SCK Version Number
SCKN	Static Cipher Key Number
SDU	Service Data Unit

SHSI	Stolen Half-Slot Identifier
SS	Synchronization Status
SSCK	Sealed Static Cipher Key
SSI	Short Subscriber Identity
SwMI	Switching and Management Infrastructure
SV	Synchronization Value
TA	TETRA Algorithm
TCH	Traffic Channel type
TSI	TETRA Subscriber Identity
U-PLANE	User-PLANE
V+D	Voice plus Data

4 Operational security

This clause describes the operational use of security features in TETRA Direct Mode Operation (DMO).

For this clause a call is defined as the group of transmissions and handovers that are bounded by initial call set-up and final call cleardown. Call pre-emption when successful shall mark the start of a new call.

NOTE: A DM call may be considered as a series of unidirectional call transactions with each new call transaction having a new call master (the current transmitter).

A new call master (i.e. call master for the current call transaction) should not be able to change the encryption parameters set at the start of the call. A call shall remain in the same encryption state in all call transactions.

In a standard DM call, slot 1 of the Time Division Multiple Access (TDMA) structure shall be used by the transmitter for transmission, and slot 3 of the TDMA structure shall be used by the transmitter to receive control messages. In frequency efficient operation, slots 2 and 4 of the TDMA structure shall be used in a like manner.

4.1 Single-hop calls

A DM call is considered a single-hop call in the following cases:

- Mobile Station (MS) to individual MS;
- MS to group of MSs.

A single hop call can only be made secure (encrypted) if the following conditions apply:

- source and destination MS share Static Cipher Key (SCK);
- source and destination MS have common Key Stream Generator (KSG).

Call set-up in DMO is a single pass operation with an allowed exception for individual calls to allow a presence check acknowledgement (2 pass call set-up). All call parameters are contained in the synchronization bursts which contain two data blocks of 60 bits and 124 bits respectively. The first data block (logical channel SCH/S) shall contain the parameters for encryption. The second data block (logical channel SCH/H) shall contain the addressing data for the call (see ETS 300 396-3 [7], subclause 9.1.1).

4.2 Multi-hop calls

DM calls that pass through a repeater or gateway shall be considered multi-hop calls.

A multi-hop call can only be made secure (encrypted) if one of the following apply (in addition to the conditions for single hop calls):

- the Time Variant Parameter (TVP) used to synchronize the KSG is unaltered by the transmission;
- intermediate terminations decrypt and re-encrypt the call on each side of the hop.

Calls made through a layer-1 repeater are not considered by this ETS. The term "repeater" when used in later clauses of this ETS shall refer to a layer-2 repeater.

In the case of a call through a gateway to TETRA V+D the DM call initiator shall be synchronized to the gateway.

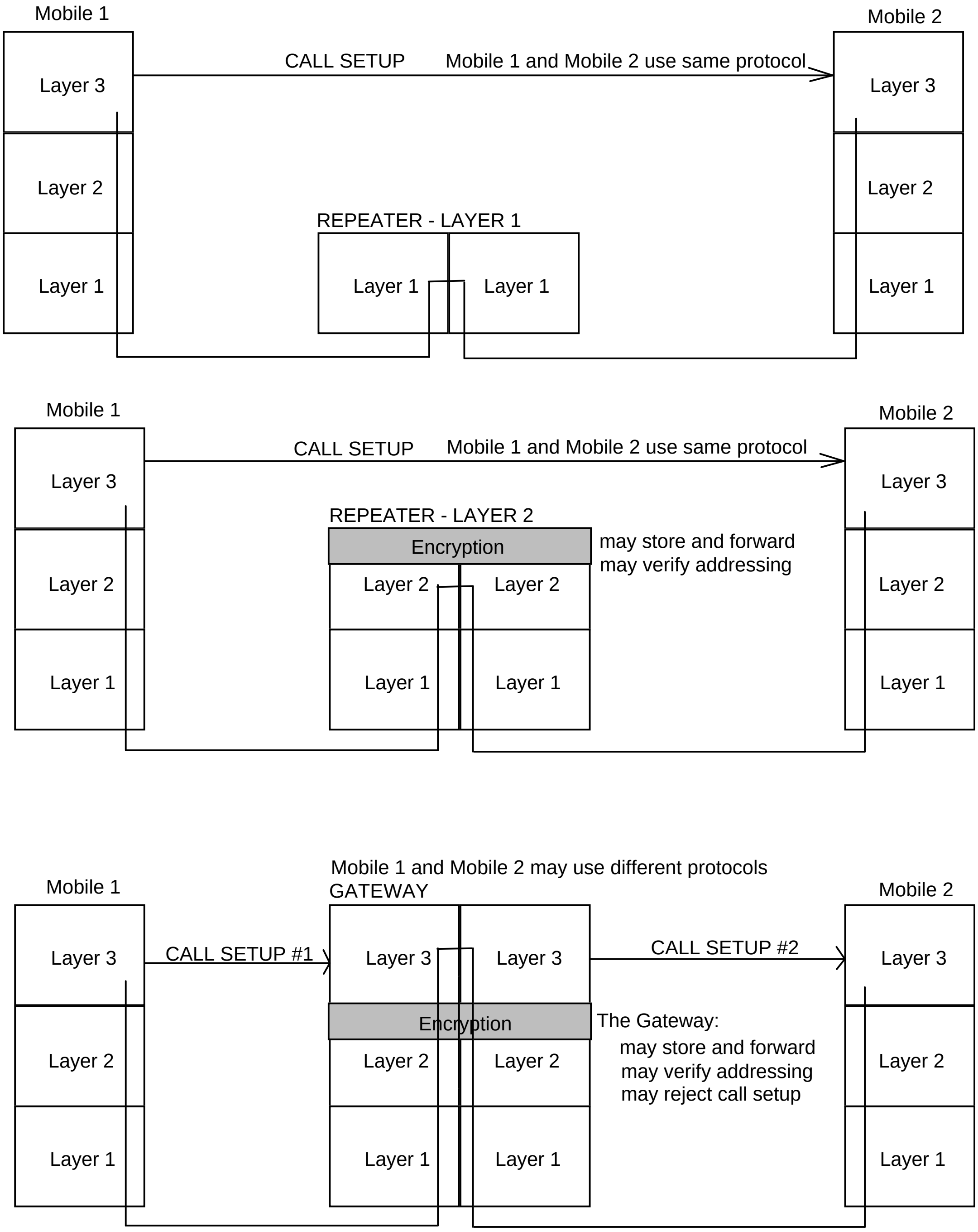


Figure 1: Protocol stacks for multi-hop calls

4.3 Call synchronization

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

The first call master should establish the synchronization for the entire call. 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. (See ETS 300 396-2 [5], subclauses 9.3.2 and 9.3.3 for full definitions of FN and TN, and ETS 300 396-2 [5], subclause 7.3.2 for definitions of the incrementing of these counters).

In DMO the encryption synchronization shall apply only to the current call. The initial value of TVP should be randomly chosen by the call master. TVP on messages from master to slave shall be independent of TVP on messages from slave to master.

TVP shall be incremented on every frame with a cycle of 2^{29} frames.

During call set-up TVP shall not be incremented during the synchronization bursts but shall be repeated across each slot of the synchronization frames. TVP shall be first incremented on the first frame following the synchronization burst as shown in figure 2.

FN17	FN18	FN1	FN2	FN3	FN4
Sync	Synch				
TVP_S	TVP_S	TVP_S+1	TVP_S+2	TVP_S+3	...

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

Figure 2: Incrementing of TVP after call set-up synchronization bursts

TVP may contain a time of day element to prevent replay. This suggests that each mobile should maintain a real time clock reference. The specification of such a reference is not covered by this ETS.

5 Authentication mechanisms

5.1 MS to MS operation

An explicit authentication protocol between mobile terminals in DMO shall not be provided. The fact that static cipher keys are used (which are generated, controlled and distributed through the DMO system security management) provides an implicit authentication between MSs as belonging to the same DMO net when successful communication takes place.

5.2 Dual Watch (DW) operation

In DW mode a DM-MS shall be a valid member of the TETRA V+D network and should authenticate to that network using the procedures defined in ETS 300 392-7 [6], clause 4.

5.3 Gateway mode operation.

Calls established through a gateway shall be considered as multi-hop calls and as such shall use a multi-pass call set-up protocol.

For secure calls the gateway shall authenticate itself to the TETRA V+D network. Details of authentication procedures are contained in ETS 300 392-7 [6], clause 4.

There shall be two modes of operation when using a gateway from DMO to TETRA V+D:

- DM-MS may act as a full member of the TETRA V+D network (i.e. DMO Individual TETRA Subscriber Identity (ITSI) is registered or known by Switching and Management Infrastructure (SwMI);

- DM-MS may use a gateway as an agent to access the TETRA V+D network (i.e. DMO ITSI is not registered or not known by SwMI other than by pre-configuring of the gateway).

5.3.1 DM-MS as a member of TETRA V+D network

In this mode the DM-MS shall be a dual mode terminal switched to use the V+D protocol. In this mode the gateway shall act as a TETRA V+D base-station repeater. This ETS does not consider this mode of operation.

5.3.2 Gateway as agent of TETRA V+D network

The gateway shall be considered as having two synchronized protocol stacks with the V+D network acting as the synchronisation master for the call (see figure 3).

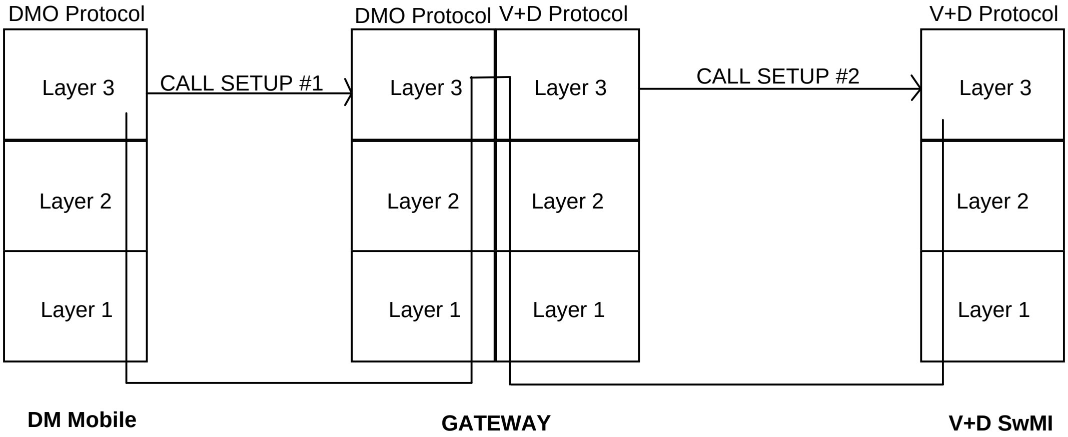


Figure 3: TETRA DMO to TETRA V+D gateway

The gateway shall be registered and authenticated to the SwMI. Therefore the SwMI shall recognize the gateway as a valid addressee (the gateway shall have an ITSI). After successful registration the gateway shall be able to communicate with the TETRA SwMI using air interface encryption as defined in ETS 300 392-7 [6], clause 6. On initial call set-up the keys in use are as shown in figure 4.

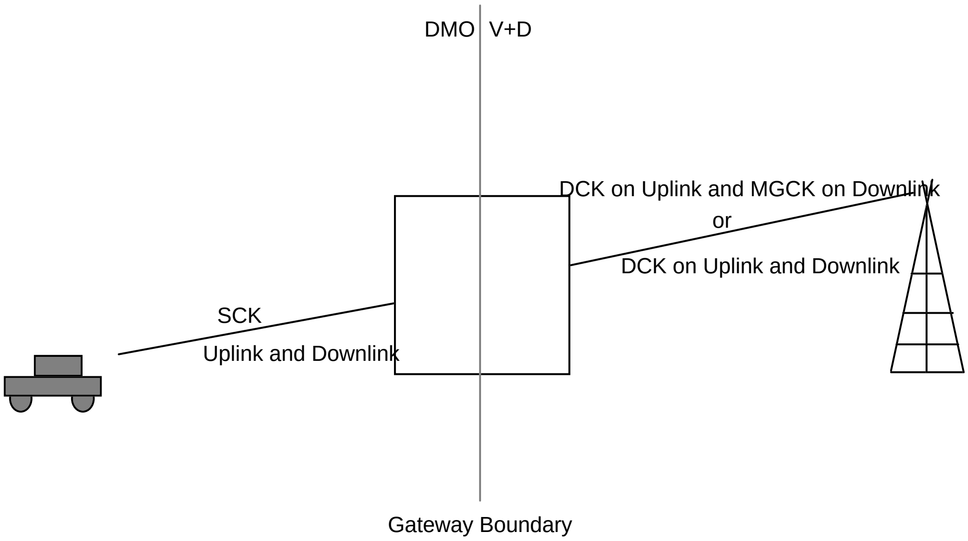

DMO
V+D
DCK on Uplink and MGCK on Downlink
or
DCK on Uplink and Downlink
SCK
Uplink and Downlink
Gateway Boundary

Figure 4: Gateway initial key allocations

Throughout an encrypted call (which may include the call set-up phase) each layer 2 (i.e. the DMO-protocol layer 2 and the V+D-protocol layer 2) shall decrypt incoming messages and encrypt outgoing messages. This may impose some delay on the end-to-end link. This ETS does 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 V+D mode network there may be a delay for any call transaction through the gateway. This ETS does not describe methods for correcting this delay.

Call set-up from DM-MS to gateway shall be with a presence check.

NOTE: On group calls the presence check is to the gateway only. On individual calls there may be two presence check acknowledgements, the first from the gateway (mandatory) and the second from the addressee (optional).

6 Air Interface (AI) encryption

6.1 General principles

AI encryption shall provide confidentiality on the radio link between a DM-MS and either a single DM-MS or a group of DM-MSs.

AI operates by combining the output of a KSG with the contents of messages to be transmitted across the air interface. 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.

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

An encryption mechanism for TETRA addresses is provided which enables addresses contained in MAC headers, and hence the identities of the MS's involved in communication, to be concealed from eavesdropping.

AI encryption shall be a separate function to the end-to-end encryption service described in clause 9. Information that has already been encrypted by the end-to-end service may be encrypted again by the AI encryption function. Where TETRA provides for clear or encrypted circuit mode services in ETS 300 396-1 [4], subclause 7.2, these shall be independent of air interface encryption; thus a service invoked without end-to-end encryption may still be encrypted over the air interface.

6.2 Key Stream Generator (KSG)

Encryption shall be realized using an encryption algorithm implemented in a KSG. The KSG shall form an integral part of a DM-MS.

NOTE: The KSG to be used in TETRA DMO can be the same as that used in TETRA V+D.

The KSG shall have two inputs, a TVP and a cipher key. These parameters shall be as specified in subclause 6.3.1. The KSG shall produce one output as a sequence of key stream bits referred to as a Key Stream Segment (KSS).

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, which enables encryption of an unprotected data channel TCH/7,2.

6.2.1 KSG numbering and selection

There shall be at least one TETRA standard algorithm. Air interface signalling shall identify which algorithm is in use (see table 1).

The values 0000_2 to 0111_2 of KSG-id used in signalling shall be reserved for the TETRA standard algorithms.

Table 1: KSG Number element contents

Information Element	Length	Value	Remark
KSG Number	4	$0xxx_2$	TETRA Standard Algorithms
		$1xxx_2$	Proprietary TETRA Algorithms

The TETRA standard algorithm shall only be available on a restricted basis from ETSI.

6.3 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. KSS(0) shall be XORed with the first transmitted bit of the first DM-SDU, and so on.

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, KSS(0) to KSS(M-1) shall be utilized, KSS(M) to KSS(n-1) shall be discarded.

Figure 5 illustrates the process where each PDU occupies one complete timeslot.

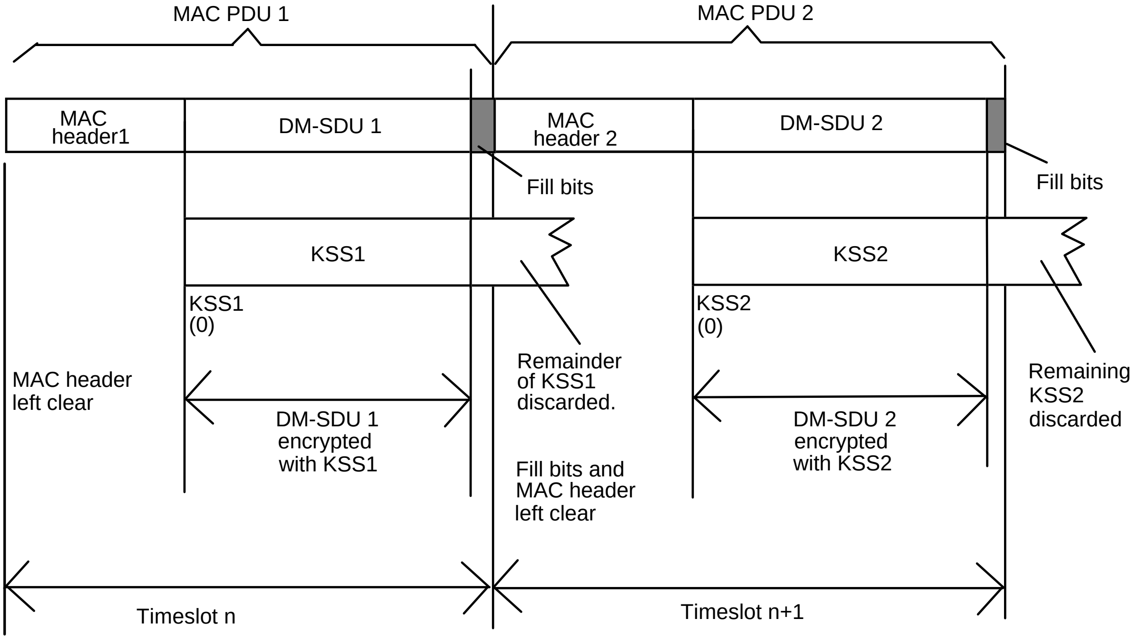


Figure 5: Allocation of KSS to encrypt MAC PDUs

6.3.1 Interface parameters

6.3.1.1 Time Variant Parameter (TVP)

The TVP shall be used to initialize the KSG at the start of every slot. 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 TVP is a transmitted parameter that shall be sent in the synchronization bursts by the current call master.

The initial value of TVP shall be randomly chosen by the first call master in the first call transaction. Succeeding call transactions should continue the TVP sequence. TVP should be reinitialised for each call.

TVP shall be incremented on each frame transition.

NOTE: TVP is independent of FN and TN.

6.3.1.2 Cipher key

The ciphering process shall be as shown in figure 6. A cipher key shall be used in conjunction with a KSG and a TVP to generate a key stream for encryption and decryption of information at the MAC layer.

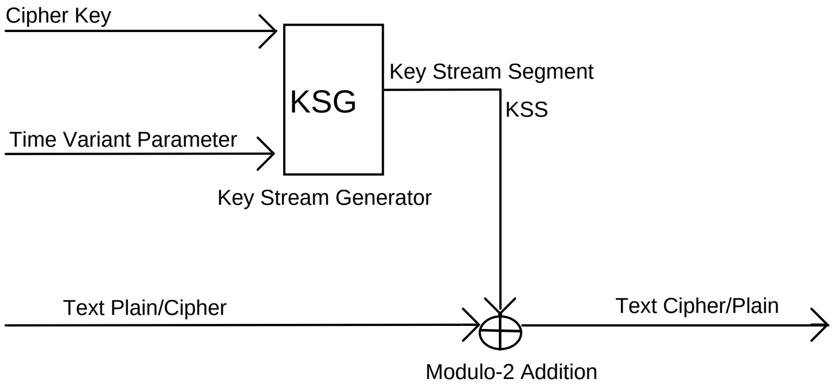


Figure 6: Speech and control information encryption

In DMO only one type of cipher key is defined i.e. SCK.

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

For use in DMO SCKs exist in groups of 32. The convention SCKN, 0≤N≤31, shall be used to refer to specific members of this set.

Once an SCK has been established no changes to the ciphering parameters shall be allowed.

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

NOTE: The content of each SCK-set and the initial distribution of this set is not covered by this ETS.

6.3.1.3 Identification of cipher keys

The encryption parameters are identified in DMAC-SYNC PDU (ETS 300 396-3 [7], subclause 9.1.1).

The AI Encryption State element shall also indicate the state of the MAC header encryption mechanism as described in subclause 6.3.2.1, and the encrypted short identity mechanism described in subclause 6.3.2.2.

6.3.2 Data to be encrypted

6.3.2.1 Encryption of MAC header elements

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

The DMAC-SYNC PDU (see ETS 300 396-3 [7], subclause 9.1.1) and the DMAC-DATA PDU (see ETS 300 396-3 [7], subclause 9.2.1) contain an AI Encryption State element (see ETS 300 396-3 [7], subclause 9.3.1) that indicates how encryption is to be applied to the PDU and to the succeeding call.

For ease of reading of this part of the ETS the table showing the coding for AI Encryption State element is reproduced in this subclause.

The Air Interface Encryption State element indicates whether the current PDU includes encryption and if so at what point in the PDU the encryption is applied.

Information element	Length	Value	Remark
Air Interface Encryption State	2	00_2	PDU not encrypted, and traffic not encrypted
		01_2	PDU Encrypted from destination address type element onwards and related traffic is AI encrypted
		10_2	The DM-SDU and any related traffic is AI encrypted
		11_2	Reserved

NOTE: The reference for the contents of this table is ETS 300 396-3 [7], subclause 9.3.1

For calls through a repeater only cases where the Air Interface Encryption State element is equal to 00_2 and 10_2 shall apply.

6.3.2.2 Encrypted Short Identity mechanism

The Encrypted Short Identity (ESI) mechanism shall provide a means of protection of identities transmitted over the air interface. ESI shall be enabled whenever the AI Encryption State element $\neq 00_2$.

This subclause describes a mechanism that allows an MS to encrypt addresses. The mechanism is valid only for networks with AI encryption applied. The mechanism shall be integrated with the use of SCK. ESI shall be sent instead of the true identity whenever the AI Encryption State element (in DMAC-SYNC PDU) $\neq 00_2$. The mechanism shall use algorithm TA61 as shown in figure 7.

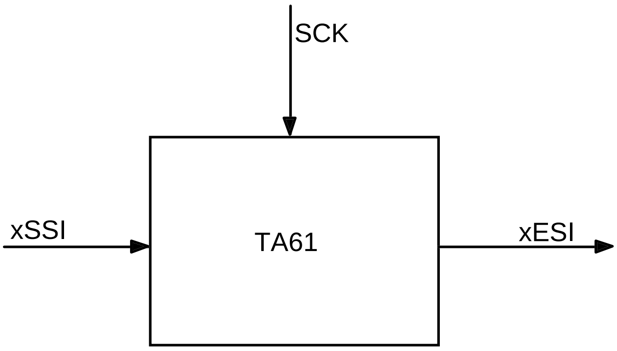


Figure 7: Generation of ESI from SSI and a cipher key

xSSI are all short addresses valid for the user (ISSI, GSSI, ASSI). The output xESI (IESI, GESI, AESI) shall be a cryptographically modified address. Only users with the correct value of SCK shall be able to identify messages addressed for their attention.

6.3.2.3 Traffic channel encryption control

Traffic channels may be transporting speech or data. The information shall be encrypted prior to channel encoding.

The state of encryption on the U-plane shall follow the state of encryption of the C-plane signalling message which causes the switch to the U-plane.

NOTE: Encryption state is either on or off.

A MS may indicate its current encryption state to its user.

6.4 Mobility procedures

In DMO there is no implicit concept of mobility. However when a DM-MS is acting as a gateway the rules for mobility defined in ETS 300 392-2 [2] shall apply.

6.5 AI encryption protocol

6.5.1 General

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

The AI encryption protocol shall be 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 protocol shall involve layer 3 (DMCC), and layer 2 (MAC) of the TETRA protocol stack.

6.5.1.1 Positioning of encryption process

The encryption process shall be located in the upper part of the MAC layer, which is the lower part of layer 2. Situating the encryption process at this point, prior to channel coding at the transmitting end and after channel decoding at the receiving end, enables the MAC headers to be left unencrypted. This allows the appropriate channel coding to be used, and enables receiving parties to determine the applicability of a message received over air for them, and so enables them to apply the correct key for the decryption process. Figure 8 illustrates this interconnection:

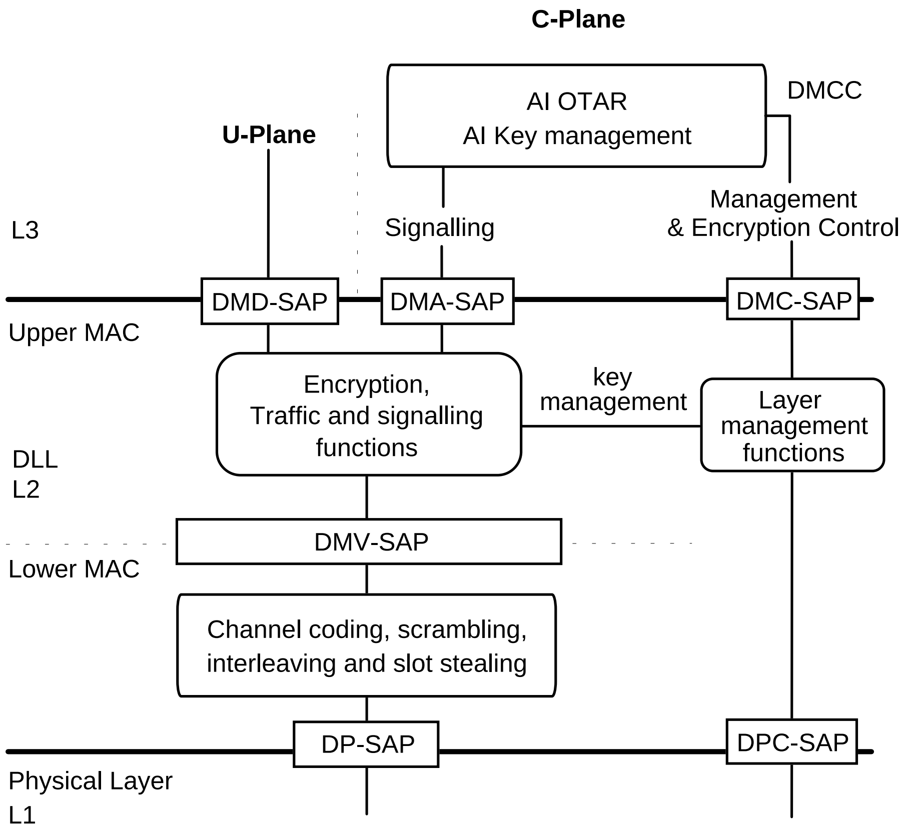


Figure 8: Relationship of security functions to layer functions

6.5.2 Service description and primitives

Each layer in the protocol stack provides a set of services to the layer above. This subclause describes the services that are added to those provided by each layer due to the incorporation of encryption, in addition to those specified in ETS 300 396-3 [7]. The primitives that are passed between the layers are also described.

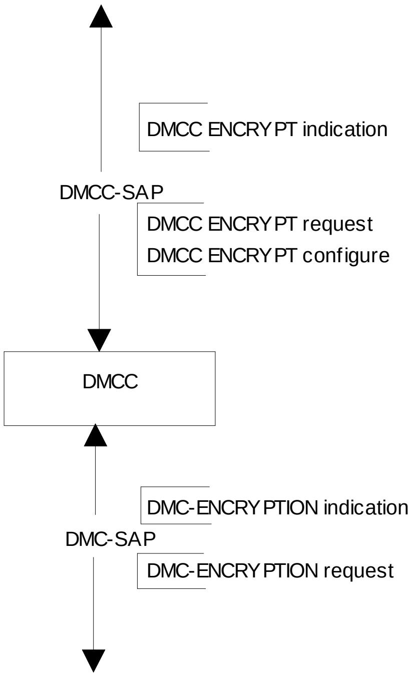


Figure 9: Encryption related services in DMO

The following services shall be provided at the DMCC-SAP:

- DMCC-ENCRYPT indication shall be used by DMCC to indicate to the application the encryption state and key data for the current call.

- DMCC-ENCRYPT request should be used in conjunction with DMCC SETUP (see ETS 300 396-3 [7], subclause 5.3.6) to set the encryption parameters for the current call and may supersede for the current call only the parameters established by DMCC-ENCRYPT configure.

- DMCC-ENCRYPT configure shall be used to pre-configure the preferred encryption parameters for all calls initiated by DMCC.

  NOTE: This primitive may be considered a special case of DMCC-ENCRYPT request.

The following services shall be provided at the DMC-SAP:

- DMC-ENCRYPTION request shall be used to instruct the MAC to load the identified encryption parameters to the encryption unit.

- DMC-ENCRYPTION indication shall be used to inform DMCC of the encryption state and key parameters for the current call (or call request).

6.5.2.1 DMCC-ENCRYPT primitive

Table 2: DMCC-ENCRYPT parameters

Parameter	Request	Configure	Indication
Key download type	M	M	-
KSG Number (note 1)	O	M	-
SCK (note 2)	C	M	-
SCKN	-	M	M
Cipher usage (note 1)	O	M	-
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.

6.5.2.2 DMC-ENCRYPTION primitive

At the DMC SAP the following services shall be provided to DMCC:

- loading of keys;
- start and stop ciphering.

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

Table 3: DMC-ENCRYPTION parameters

Parameter	Request	Indication
Key download type	M	-
KSG Number (note 1)	O	-
SCK (note 2)	C	-
SCKN	-	M
Cipher usage (note 1)	O	-
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.

Key download type parameter indicates which encryption keys, if any, are downloaded to the MAC in this request.

Key download type =

no keys downloaded;
SCK.

KSG Number parameter indicates the KSG (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;
Transmitter (TX), traffic encrypted and PDU encrypted from destination address;
TX, DM-SDU encrypted and traffic encrypted;
Receiver (RX).

6.5.3 Protocol functions

Each functional entity in the protocol stack shall communicate with its peer entity using a defined protocol, e.g. the DMCC entity in the originating DM-MS communicates with its peer DMCC entity in the receiving DM-MS.

On receiving DMCC-ENCRYPT (request/configure) from the DMCC-SAP, DMCC shall, with DMCC-SETUP request, be incorporated into the DMC-ENCRYPTION request primitive and sent by the DMC-SAP.

In the MAC on receiving DMC-ENCRYPTION request from the DMC-SAP, the MAC shall determine 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 shall send DMCC-ENCRYPT indication to the DMCC-SAP.

7 AI key management mechanisms

DMO shall only use SCK. The set of SCK shall be fixed and should be known to every terminal in the DMO net. It shall be distributed in a secure manner to every terminal. The mechanism for selection and transmission of SCK is outside the scope of this ETS.

The SCK can be chosen by the system manager and manually entered in MS. It may have an indefinite lifetime. The allocation of an SCK shall be carried out in the home network of the MS.

NOTE 1: The choice and distribution of the SCK is outside the scope of this ETS.

NOTE 2: The home network is defined as that network that is assigned a Mobile Network Identity (MNI) by the appropriate body.

NOTE 3: For encrypted communication between parties with different MNI, the SCK used by the parties should be common even though they may belong to different SCK-sets (e.g. SCK3 of set 1 = SCK3 of set 2).

7.1 Key numbering and storage

Separate SCK sets may be stored within each MS. 32 keys may be stored for each SCK set.

7.2 Over The Air Re-keying (OTAR)

Keys for the air interface encryption unit (i.e. KSG) may be transmitted over the air interface in a secure manner. This shall require the establishment of a peer-to-peer messaging service between the layer 3 entities responsible for key management. To provide an explicit authentication service between the key generator and the key receiving terminal, the key to be transmitted shall be sealed using a mechanism that includes the ITSI related secret key K.

NOTE: OTAR as defined for DMO can only operate if each DM-MS holds an authentication key, K, known to the authentication centre.

For OTAR, SCKs may be generated in and distributed from any network entity.

Two typical cases may be the following:

- SCKs shall be generated in the same entity that stores the users' authentication keys, i.e. an authentication centre. This case is shown in figure 10.
- SCKs shall be generated and distributed in a key generator mobile. In this case, as shown in figure 11, the KSO shall be forwarded from the authentication centre to the key generator in a secure way.

It shall be possible for any mobile to store and forward SSCKs in direct mode, i.e. to act as a key holder, to allow the distribution of SCKs to a mobile that is outside the coverage of the key generator.

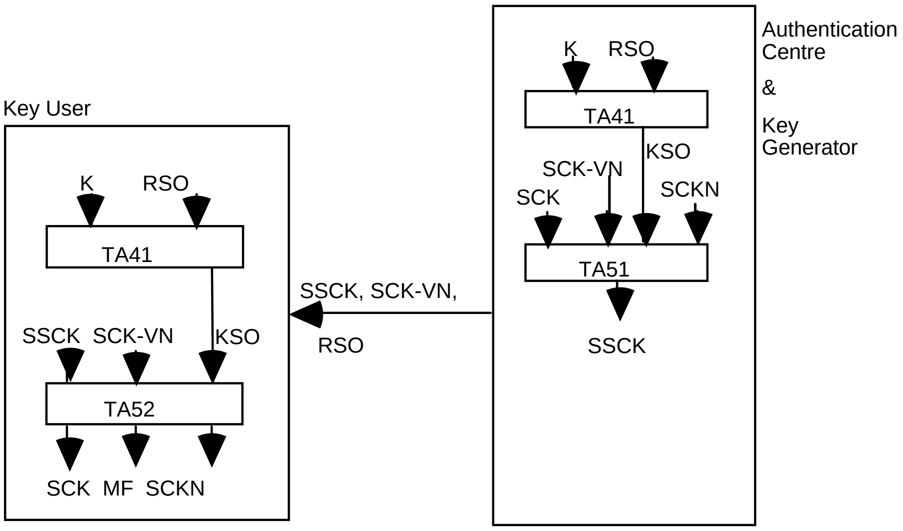


Figure 10: Distribution of SCK by an authentication centre

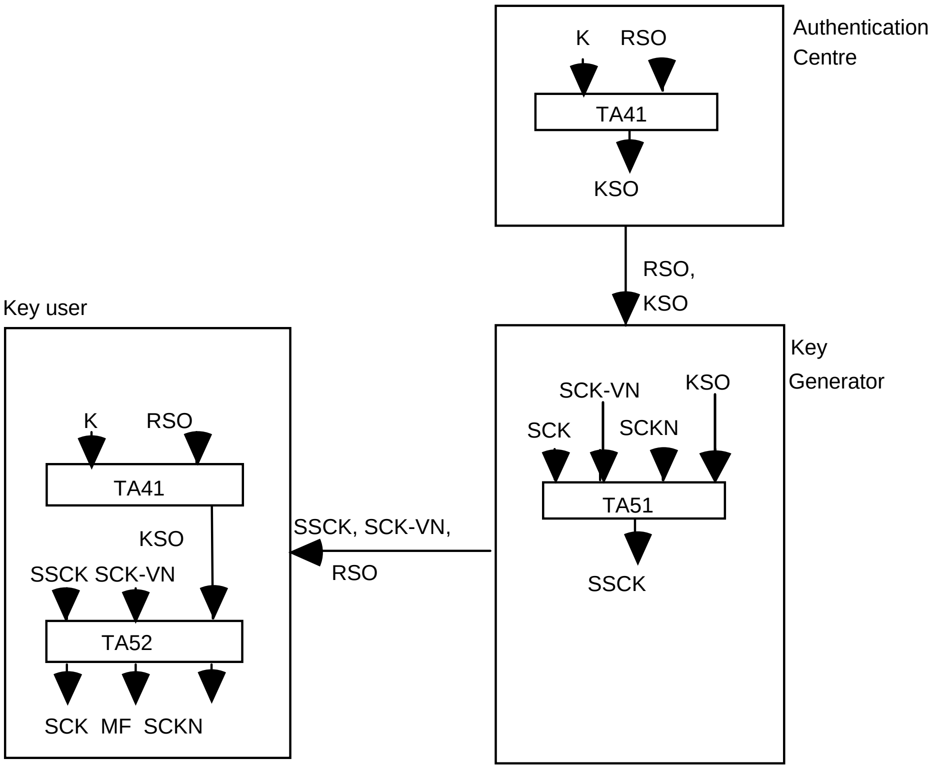


Figure 11: Distribution of SCK by a key generator

7.3 OTAR service description and primitives

7.3.1 SCK transfer primitives

A service shall be provided to allow an application to receive new SCKs either on demand or initiated by the Key Generator (KG). The primitives required shall be as follow:

- DM-OTAR-SCK indication shall be used to provide the MS application with the SCKN and version number of each key received.

- DM-OTAR-SCK confirm shall be used by the MS application to confirm that the key information received is acceptable, or provide the reject reasons if not.

- DM-OTAR-SCK request shall be used to request the distribution of a new static cipher key. It shall contain the number (of 32 possible values) of each SCK requested. More than one SCK may be requested in one transaction.

Table 4: DM OTAR SCK service primitives

GENERIC NAME	Specific name	PARAMETERS
DM-OTAR-SCK	indication	SCKN, SCK-VN
DM-OTAR-SCK	confirm	Result
DM-OTAR-SCK	request	SCKN

The parameters used in the above primitives should be coded as follows:

result =

SCK received successfully;
SCK failed to decrypt;

SCKN =

1;
2;
3;
…
32.

Version number =

0;
…
2^{16}-1.

7.4 OTAR SCK protocol functions

There shall be three functional entities in the SCK OTAR chain, distinguished by the algorithms each holds:

Authentication Centre	Shall contain TA41
Key Generator	Shall contain TA51
Key User	Shall contain TA41+TA52

The Authentication Centre (AC) and Key Generator (KG) may be combined in one unit (this is the case in TETRA V+D). The Key User (KU) shall be a DM-MS.

NOTE: It is assumed in DMO that AC and KG are physically separated and that they communicate over an air Interface. It is also assumed that a KG acts as a key server for a predetermined user group (collection of ITSIs).

In addition there shall be a functional entity able to hold sealed keys but with no ability to manipulate them algorithmically. This shall be a Key Holder (KH).

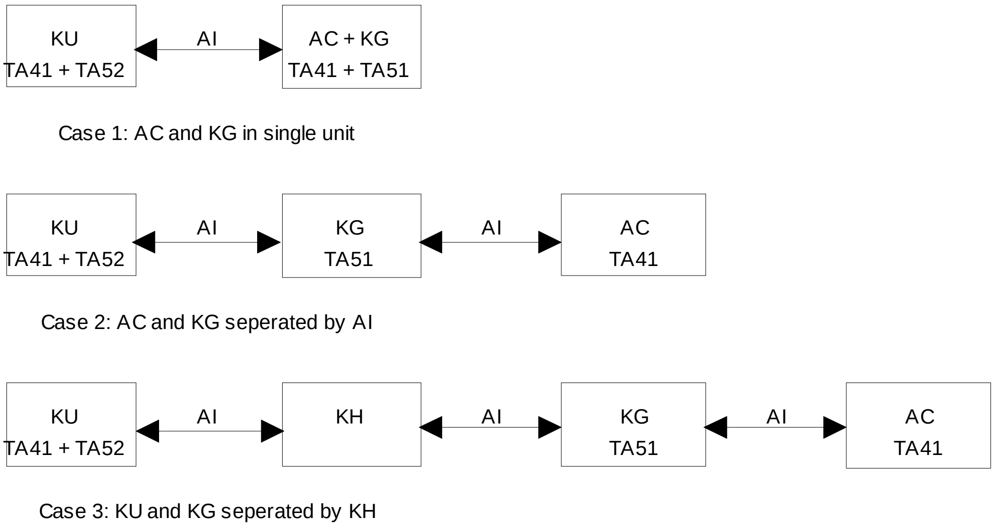

KU
TA41 + TA52
AI
AC + KG
TA41 + TA51
Case 1: AC and KG in single unit
KU
TA41 + TA52
AI
KG
TA51
AI
AC
TA41
Case 2: AC and KG seperated by AI
KU
TA41 + TA52
AI
KH
AI
KG
TA51
AI
AC
TA41
Case 3: KU and KG seperated by KH

Figure 12: OTAR transmission chains

Figure 12 shows the possible OTAR cases that shall be addressed by the protocol.

A DM-MS may request one or several SCKs to be distributed from KG using the "OTAR SCK Provide" PDU. In order to respond to any demand KG can be pre-configured with the SCKs for its client group by using the "OTAR SCK Configure" PDU directed to AC. AC may provide key data to KG either on demand (i.e. in response to an OTAR SCK Configure PDU) or automatically by using the "OTAR SCK Prepare" PDU.

The normal SCK provision cases are described by the Message Sequence Charts (MSCs) and protocol description in the following subclauses. The MSCs and protocol models consider only cases where AC, KG and KU are in the DMO domain.

7.4.1 OTAR protocol models

The transport mechanism for OTAR shall be Short Data Service (SDS) with type 101_2. A logical switch or router at the SDS entity shall direct messages as shown in figure 13:

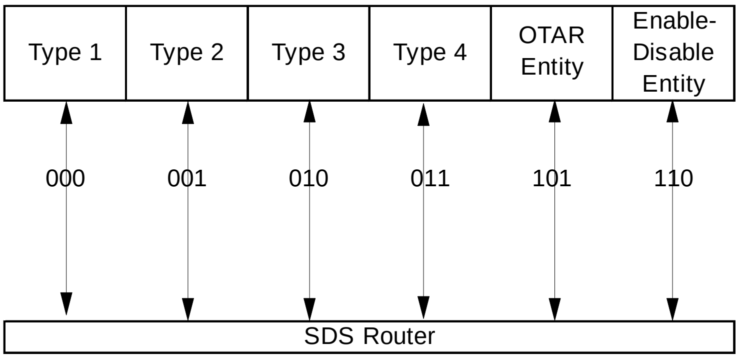


Figure 13: Routing of SDS messages to terminating entities

In all OTAR instances the SDS transport shall be encrypted (as described in clause 6).

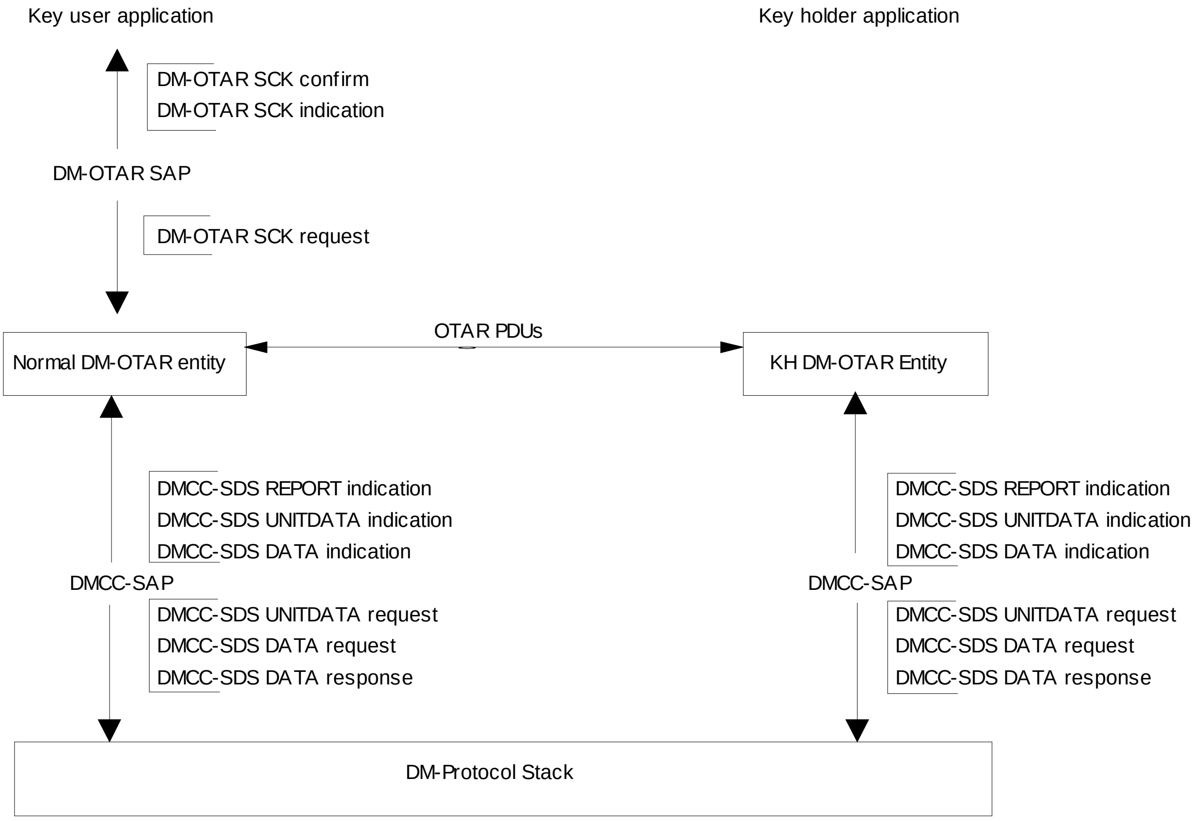


Figure 14: Model for MS to KH protocol

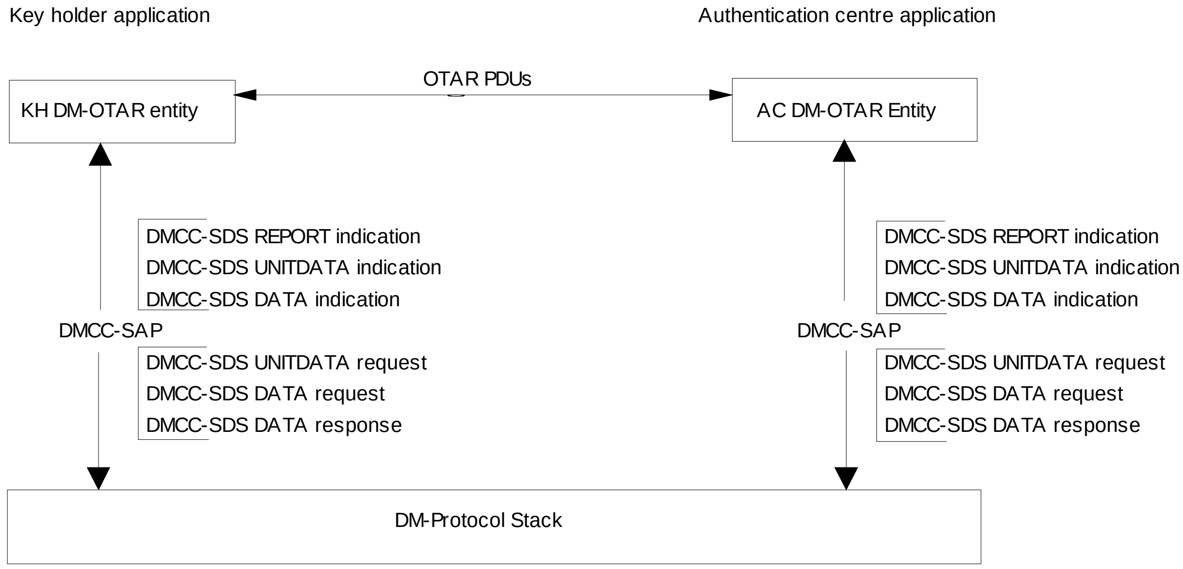


Figure 15: Model for KH to AC protocol

7.5 OTAR Protocol MSCs

The MSCs that follow reflect the cases shown in figure 12.

7.5.1 Case 1: KU requests key from combined AC and KG

The normal message sequence in this case shall be according to figure 17. The indication of which SDS message contains the PDU is given for information only.

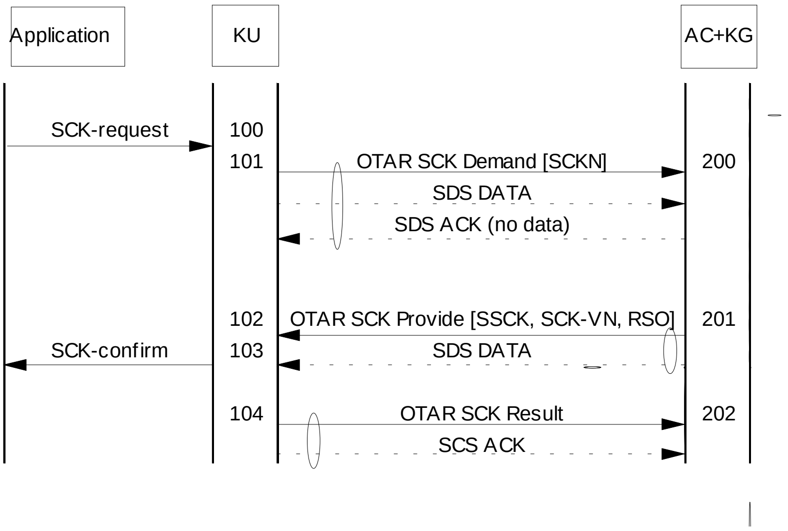


Figure 16: SCK change initiated by KU where KH has key data

100 The user application requests one or more SCKs by SCKN.

101 KU shall request one or more SCKs by SCKN from the known KH (in this case a combined AC and KG) in the OTAR SCK Demand PDU.

200 The combined entity AC+KG shall generate the Random Seed for OTAR (RSO) and run algorithm TA41 with the secret key K of KU and RSO to generate the Session Key for OTAR (KSO). It shall then run algorithm TA51 with the following inputs for each key requested: SCK, SCK-VN, SCKN and KSO to give SSCK.

201 The combined entity AC+KG shall send RSO and, for each key requested, the pair (SSCK, SCK-VN) to KU in the OTAR SCK Provide PDU.

102 KU shall retrieve RSO and with K shall generate KSO using algorithm TA41. For each key provided it shall then run algorithm TA52 to recover the pair SCK, SCKN. In each case KU shall examine the Manipulation Flag (MF) to check if the key has been decoded properly.

103 KU shall inform the user application of the result of the SCK request using the SCK-confirm primitive.

104 KU shall acknowledge receipt of the provided keys by sending the OTAR SCK Result PDU to the known KH (in this case a combined AC and KG).

202 The KH (in this case a combined AC and KG) may delete those SSCK that have been successfully delivered.

7.5.2 Case 2: KU requests key from KG which is separated by an air interface from AC

The normal message sequence in this case shall be according to figure 17. The indication of which SDS message contains the PDU is given for information only.

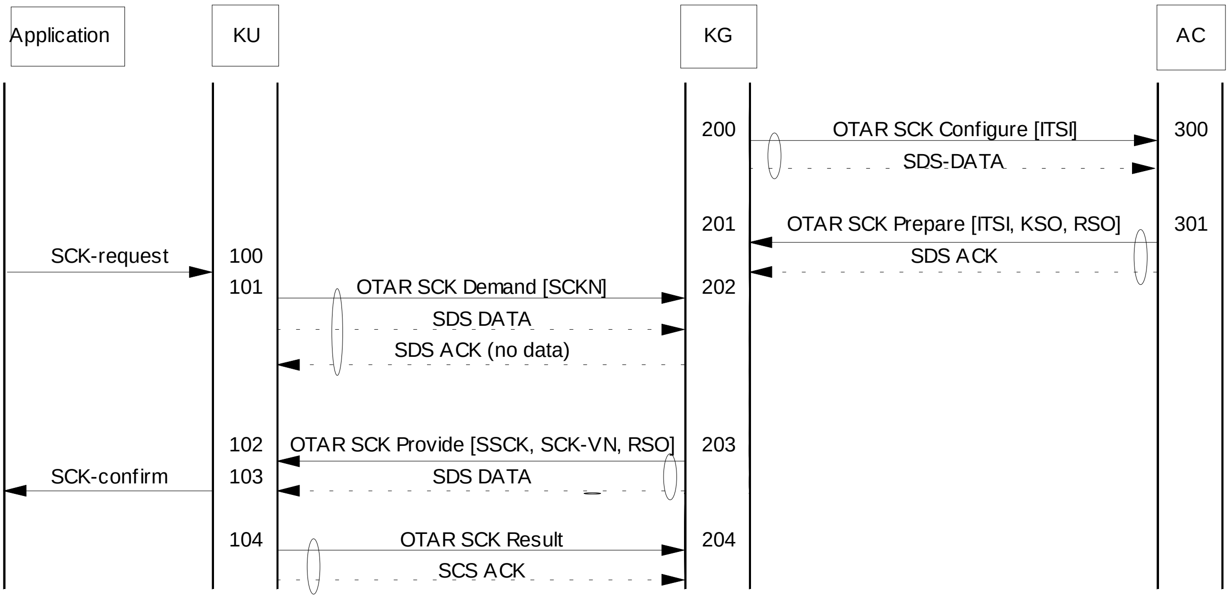


Figure 17: SCK change initiated by KU where KH has key data

200 KG shall request the SCK session key (KSO) and random seed (RSO) for one or more ITSIs from the authentication centre using the OTAR SCK Configure PDU.

300 AC shall identify K for the ITSIs given by KG and shall generate RSO. RSO and K shall be used as inputs to TA41 to generate KSO.

301 AC shall send the triple, (KSO, RSO, ITSI), to KG for each ITSI in the OTAR SCK Prepare PDU.

201 KG shall retrieve RSO and KSO for each ITSI. KG shall generate (or retrieve) the (SCK, SCK-VN, SCKN) triple and input it with KSO to algorithm TA51 to give SSCK.

100 The application may request one or more SCK by SCKN.

101 KU shall request one or more SCK (identified by SCKN) from KH in the OTAR SCK Demand PDU.

202 KH, in this instance KG, shall identify the ITSI and the requested SCK from the received OTAR SCK Demand PDU.

NOTE: If KG does not have the key generation parameters for the received ITSI it can at this stage implement steps 200 to 201 as above.

203 KH shall deliver the sealed SCK (SSCK) with SCK-VN and RSO to KU in the OTAR SCK Provide PDU.

102 KU shall retrieve RSO, SCK-VN and SSCK from the OTAR SCK Provide PDU. KU shall load RSO and K to TA41 to generate KSO, and input KSO, SSCK, SCK-VN to algorithm TA52 to give SCK, SCKN and MF.

103 If MF is TRUE KU shall notify the application that a failure of SCK provision was detected. If MF is FALSE KU may notify the application that SCK was successfully provided.

104 KU shall notify KH the result for each SCK provided using the OTAR SCK Result PDU.

204 KH may delete those SSCK/ITSI combinations that have been successfully provided.

7.5.3 Case 3: KU requests key from KH acting as a relay for KG

The normal message sequence in this case shall be according to figure 17. The indication of which SDS message contains the PDU is given for information only.

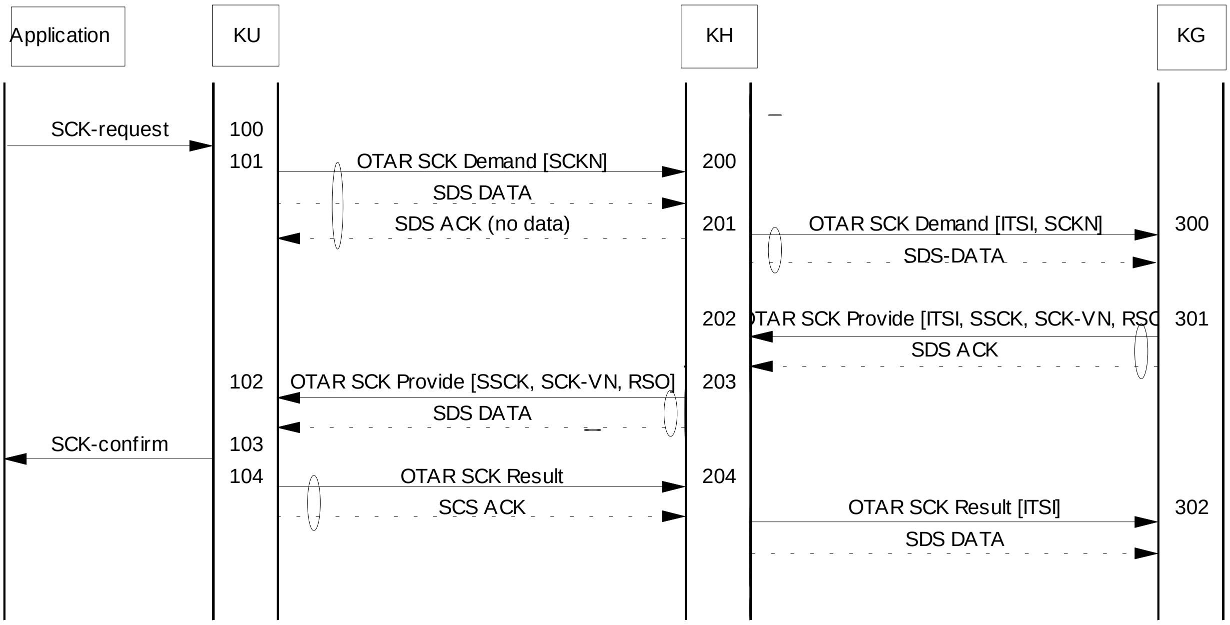


Figure 18: SCK change initiated by KU where KH has key data

100 The user application shall request one or more SCK by SCKN.

101 KU shall request one or more SCK by SCKN from KH using the OTAR SCK Demand PDU.

200 KH shall receive the demand from KU and check if the keys are already available. If the keys are available it shall move to step 203, else it shall move to step 201.

201 KH shall request one or more SCK from KG by SCKN and ITSI

300 KG shall check if KSO and RSO are available for the supplied ITSI. If the generating parameters are available KG shall generate new keys in algorithm TA51. If the generating parameters are not available KG shall request them from AC as shown in 741.

301 KS shall send RSO and ITSI, and for each key requested SSCK and SCK-VN to KH in the OTAR SCK Provide PDU.

202 KH shall retrieve RSO and ITSI and, for each key requested, SSCK and SCK-VN from the OTAR SCK Provide PDU.

203 KH shall deliver the sealed SCK (SSCK) with SCK-VN and RSO to KU in the OTAR SCK Provide PDU.

102 KU shall retrieve RSO, SCK-VN and SSCK from the OTAR SCK Provide PDU. KU shall load RSO and K to TA41 to generate KSO, and input KSO, SSCK, SCK-VN to algorithm TA52 to give SCK, SCKN and MF.

103 If MF is TRUE KU shall notify the application that a failure of SCK provision was detected. If MF is FALSE KU may notify the application that SCK was successfully provided.

104 KU shall notify KH the result for each SCK provided using the OTAR SCK Result PDU.

204 KH may delete those SSCK/ITSI combinations that have been successfully provided.

302 KG may delete those SSCK/ITSI combinations that have been successfully provided.

7.6 PDU descriptions

The PDUs detailed within this subclause shall be visible at the Ud reference point (see ETS 300 396-1 [4], subclause 4.1). The PDUs shall be transported in a SDS-5 message block. The use of SDS as a transport service shall only be used in the acknowledged service type.

In the tables that follow the contents of each PDU are presented in the order of transmission. Where elements can be repeated the order of these elements shall be maintained.

7.6.1 OTAR SCK Provide

Shall be used by KH to provide SCK to KU.

Direction:	KH to KU;
Service used:	SDS;
Response to:	OTAR SCK Demand or none;
Response expected:	OTAR SCK Result.

Table 5: OTAR SCK Provide PDU contents

Information Element	Length	Type	C/O/M	Remark
OTAR SCK sub-type	3	1	M	Provide
Random seed	80	1	M	
Number of SCKs provided	3	1	M	
ITSI	48	1	C	note 1
SCK key and identifier	141	1	C	note 2
Proprietary element		3	O	

NOTE 1: If the PDU is sent from KG to KH on behalf of KU the ITSI of KU shall be included

NOTE 2: The SCK and identifier element is conditional on the Number of SCKs element. There shall be as many SCK and identifier elements in the PDU as indicated by the Number of SCKs element. If "Number of SCKs" = 0, there shall be no "SCK key and identifier" elements in the PDU.

7.6.2 OTAR SCK Configure

Shall be used by KH to request key data from AC.

Direction:	KH to AC;
Service used:	SDS;
Response to:	none;
Response expected:	OTAR SCK Prepare.

Table 6: OTAR SCK Configure PDU contents

Information Element	Length	Type	C/O/M	Remark
OTAR SCK sub-type	3	1	M	Configure
Number of ITSIs requested	2	1	M	
ITSI	48	1	C	note 1
Proprietary element		3	O	

NOTE 1: The ITSI element is conditional on the Number of ITSIs element. There shall be as many ITSI elements in the PDU as indicated by the Number of ITSIs element.

7.6.3 OTAR SCK Prepare

Shall be used by the AC to deliver key data to KH.

Direction:	AC to KH;
Service used:	SDS;
Response to:	OTAR SCK Configure or none;
Response expected:	none.

Table 7: OTAR SCK Prepare PDU contents

Information Element	Length	Type	C/O/M	Remark
OTAR SCK sub-type	3	1	M	Prepare
ITSI	48	1	M	
RSO	80	1	M	
KSO	128	1	M	
Proprietary element		3	O	

7.6.4 OTAR SCK Demand

Shall be used by KU to request SCK from KH.

Direction:	KU to KH, KH to KG;
Service used:	SDS;
Response to:	none;
Response expected:	OTAR SCK Provide.

Table 8: OTAR SCK Demand PDU contents

Information Element	Length	Type	C/O/M	Remark
OTAR SCK sub-type	3	1	M	Demand
ITSI	48	1	C	note 1
Number of SCKs requested	2	1	M	
SCK number (SCKN)	5	1	C	note 2
Proprietary element		3	O	
NOTE 1: If the PDU is sent from KH to KG on behalf of KU the ITSI of KU shall be included. NOTE 2: The SCK number element is conditional on the Number of SCKs element. There shall be as many SCK number elements in the PDU as indicated by the Number of SCKs element.				

7.6.5 OTAR SCK Result

Shall be used by KU to explicitly accept or reject the SCKs provided by KH.

Direction:	KU to KH;
Service used:	SDS;
Response to:	OTAR SCK Provide;
Response expected:	none.

Table 9: OTAR SCK Result PDU contents

Information Element	Length	Type	C/O/M	Remark
OTAR SCK sub-type	3	1	M	Result
ITSI	48	1	C	note 1
Number of SCKs requested	2	1	M	
SCK number and result	8	1	C	note 2
Proprietary element		3	O	
NOTE 1: If the PDU is sent from KH to KG on behalf of KU the ITSI of KU shall be included. NOTE 2: The SCK number and result element is conditional on the Number of SCKs requested element. There shall be as many SCK number and result elements in the PDU as indicated by the Number of SCKs requested element. Note that this PDU reports the result of a number of SCKs which were provided which may not be the same as the number of SCKs actually requested in the first place.				

7.7 PDU Information elements coding

The encoding of the elements for the PDUs described in subclause 75 is given in the following subclauses. The most significant bit of the values shown in the tables is transmitted first.

7.7.1 Address extension

The address extension element is used to indicate the full TSI address given in table 10.

Table 10: Address extension element contents

Information Element	Length	Type	C/O/M	Remark
Mobile country code	10	1	M	
Mobile network code	14	1	M	

7.7.2 Mobile Country Code (MCC)

The mobile country code of a TETRA network. For a full definition see ETS 300 396-1 [4], clause 6.

Table 11: MCC element contents

Information element	Length	Value	Remark
Mobile country code	10	any	

7.7.3 Mobile Network Code (MNC)

The mobile network code of a TETRA network. For a full definition see ETS 300 396-1 [4], clause 6.

Table 12: MNC element contents

Information element	Length	Value	Remark
Mobile network code	14	any	

7.7.4 Number of SCKs provided

The Number of SCKs element indicates how many static cipher keys there are to follow in the PDU.

Table 13: Number of SCKs provided element contents

Information element	Length	Value	Remark
Number of SCKs provided	3	000_2	No SCKs provided
		001_2	1 SCK provided
		010_2	2 SCKs provided
		011_2	3 SCKs provided
		100_2	4 SCKs provided
		101_2 to 111_2	Reserved

7.7.5 Number of SCKs requested

The Number of SCKs element indicates how many static cipher keys are requested by the MS.

Table 14: Number of SCKs requested element contents

Information element	Length	Value	Remark
Number of SCKs requested	2	00_2	1 SCK requested
		01_2	2 SCKs requested
		10_2	3 SCKs requested
		11_2	4 SCKs requested

7.7.6 OTAR SCK sub-type

The OTAR sub-type indicates whether the PDU is a demand for SCK, or the result of a key transfer.

Table 15: OTAR sub-type element contents

Information element	Length	Value	Remark
OTAR SCK sub-type	3	000_2	Demand
		001_2	Provide
		010_2	Result
		011_2	Configure
		100_2	Prepare
		101_2	Reserved
		110_2	Reserved
		111_2	Reserved

7.7.7 Proprietary

Proprietary is an optional, variable length element and shall be used to send and receive proprietary defined information appended to the PDUs.

The use, size and structure of the Proprietary element is outside the scope of this standard.

7.7.8 Provision result

The provision result is sent by the MS to the SwMI to indicate whether or not the MS was able to decrypt the sealed key (SCK).

Table 16: Provision result element contents

Information element	Length	Value	Remark
Provision result	3	000_2	Sealed key accepted
		001_2	Sealed key failed to decrypt
		010_2	Incorrect SCK-VN
		011_2	Incorrect SCKN
		100_2 to 111_2	Reserved

7.7.9 Random Seed (RS)

The random seed is an 80 bit number used as the input to the session key generation algorithm, which is used in the authentication and OTAR processes. Only one random seed is used per OTAR PDU, irrespective of the number of keys contained in the PDU. It is provided from AC to KH, and from KH to MS.

Table 17: RS element contents

Information element	Length	Value	Remark
Random seed (RS)	80	Any	

7.7.10 SCK version number

The SCK version number (SCK-VN) is the numerical value associated with a version number of a key being transferred in an OTAR SCK transaction. Multiple SCK-VNs shall be sent where multiple keys are transferred, one SCK-VN per key.

Table 18: SCK version number element contents

Information element	Length	Value	Remark
SCK version number	16	Any	

7.7.11 SCK key and identifier

The SCK key and identifier contains the sealed SCK which is identified by the SCK number.

Table 19: SCK key and number element contents

Information Element	Length	Type	C/O/M	Remark
SCK number (SCKN)	5	1	M	
SCK version number (SCK-VN)	16	1	M	
Sealed key (SSCK)	120	1	M	

7.7.12 SCK number

The SCK number is a five bit value associated with an SCK. Where multiple SCKs are transferred, this element is repeated with each SCK number related to the SCKs being transferred.

Table 20: SCK number element contents

Information element	Length	Value	Remark
SCK number	5	00000_2	SCK number 1
		00001_2	SCK number 2
		…..	
		etc.	SCK numbers in turn
		…..	
		11111_2	SCK number 32

7.7.13 SCK number and result

The SCK number and result contains the result of the SCK key transfer for the key identified by the SCK number.

Table 21: SCK number and result element contents

Information Element	Length	Type	C/O/M	Remark
SCK number (SCKN)	5	1	M	
Provision result (SCK)	3	1	M	

7.7.14 Sealed Key (SK)

The Sealed Key is the key transferred by an OTAR transaction, in a protected (encrypted) manner.

Table 22: SK element contents

Information element	Length	Value	Remark
Sealed Key	120	Any	

8 Secure enable and disable mechanism

8.1 Overview

The mechanisms described in this clause are optional, but if implemented shall be implemented as described in this clause. The mechanisms allow an authorized DM-MS to disable or enable another DM-MS over the air interface. The disablement may be of two classes, i.e. permanent; and temporary.

There may a number of reasons for wishing to enable a DM-MS, e.g. faulty equipment operation; illegal or damaging use of radio resource by user; etc. The mechanisms described in this clause are not an alternative to subscriber and terminal management but are one way (there may be others) of enabling it.

In the case of a temporary disablement the disabled DM-MS may be enabled over the air interface by an authorized DM-MS. A permanent disablement shall only be reversible at an authorized service centre.

The term enable/disable target user (hereinafter referred to as target-user) shall refer to the ITSI of the DM-MS that is to be enabled or disabled.

The term enable/disable target equipment (hereinafter referred to as target-equipment) shall refer to the TEI of the DM-MS that is to be enabled or disabled.

Where enable/disable can apply to either target-user or target-equipment the generic term target shall be used.

The term enable/disable manager (hereinafter referred to as manager) shall refer to the DM-MS that is requesting the target to be enabled or disabled.

The following security management constraints are imposed:

- the target shall authenticate the manager prior to accepting, and acting upon, any enable-disable request. The authentication shall be based upon a secret key known by pre-arrangement to the manager and target;

- the authentication mechanism shall provide some protection against replay by use of a time variant parameter (time-stamp or counter);

- the peer-to-peer communication shall make use of the acknowledged SDS service for transport;

- the secret key used for authentication may be one of the SCK-set.

8.2 General relationships

The relationship of user subscription, and the identifying identity, ITSI, and the hardware of the MS, identified by TEI, is shown in figure 19. The TEI is fixed and associated with the hardware of the MS. The user subscription, identified by ITSI, may be contained in a separable module. If ITSI is not contained in a separable module, it may still be changed by field programming equipment.

ITSI and TEI are described in ETS 300 396-1 [4], clause 6.

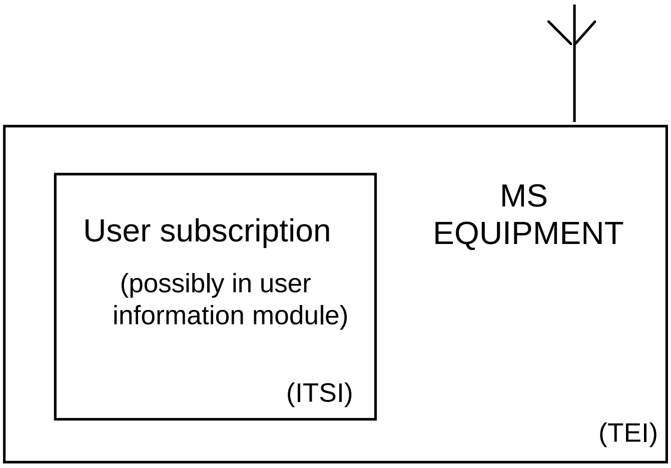
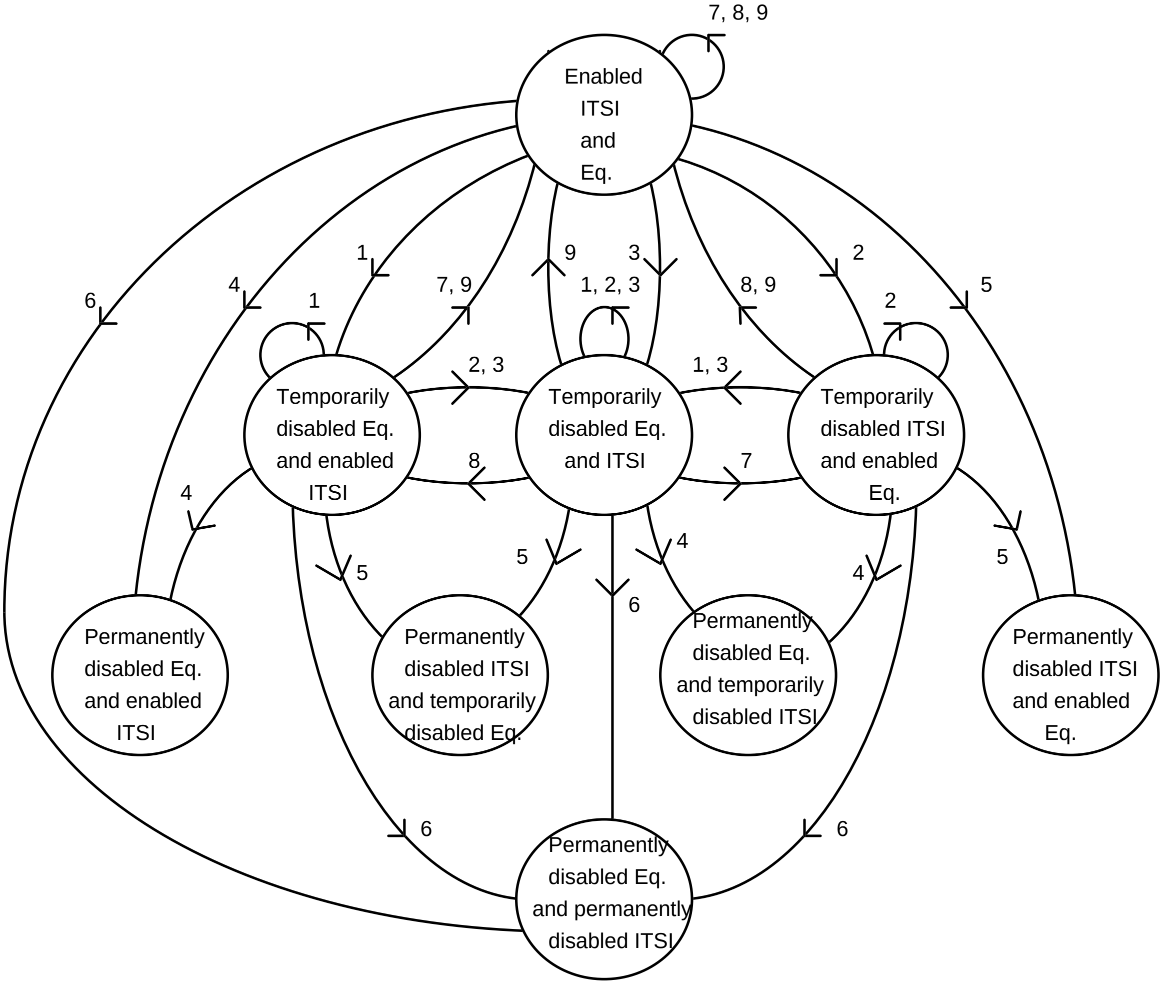


Figure 19: Relationship of TEI and ITSI in DM-MS

8.3 Enable/Disable state transitions

The state diagram in figure 20 shows all possible enabled and disabled states of a target. This diagram does not show state transitions due to separation of ITSI from, or fitting of ITSI into, a DM-MS equipment.


7, 8, 9
Enabled ITSI and Eq.
6
4
1
1
7, 9
9
3
1, 2, 3
8, 9
2
2
5
2, 3
1, 3
Temporarily disabled Eq. and enabled ITSI
Temporarily disabled Eq. and ITSI
Temporarily disabled ITSI and enabled Eq.
8
7
4
5
5
4
6
4
5
Permanently disabled Eq. and enabled ITSI
Permanently disabled ITSI and temporarily disabled Eq.
Permanently disabled Eq. and temporarily disabled ITSI
Permanently disabled ITSI and enabled Eq.
6
6
Permanently disabled Eq. and permanently disabled ITSI

1) temporary disabling of equipment;

2) temporary disabling of ITSI;

3) temporary disabling of equipment and ITSI;

4) permanent disabling of equipment;

5) permanent disabling of ITSI;

6) permanent disabling of equipment and ITSI;

7) enabling of equipment;

8) enabling of ITSI;

9) enabling of equipment and ITSI.

Figure 20: State transitions of Enable/Disable mechanism

8.4 Mechanisms

There shall be six transactions of the enable/disable procedure to allow disable and enable of the target-user, target-equipment, or both. These are detailed in subclauses 8.4.1 to 8.4.6 All transactions should be carried out with air interface encryption applied to avoid visibility of the TEI at the air interface.

There may be other mechanisms that withdraw service or disable the equipment that are outside the scope of this part of the ETS.

Equipment or subscriptions that have been temporarily disabled may be enabled by the enable mechanisms described in subclauses 8.4.4 to 8.4.6. Equipment or subscriptions that have been permanently disabled shall not be enabled by these mechanisms.

8.4.1 Disable of MS equipment

The target equipment shall be disabled by the manager either temporarily or permanently in such a manner that it shall enter the disabled state, and remain disabled even if a separable module is used to contain the ITSI, and that module is changed. If the ITSI is contained in a separable module, it may be detached and connected to a different MS equipment; and may then operate providing that the new MS equipment has not also been disabled.

8.4.2 Disable of MS subscription

The target user’s subscription shall be disabled by the SwMI either temporarily or permanently. If the ITSI is contained in a separable module, and this module is then connected to a different MS equipment, the composite MS shall remain disabled. The MS equipment shall operate if a different module containing a subscription containing ITSI that has itself not been disabled is connected.

8.4.3 Disable an MS subscription and equipment

The MS equipment and its user’s subscription shall be disabled by the SwMI either temporarily or permanently in such a manner that neither the separable module nor the MS equipment shall individually function even if the module is connected to a different MS equipment, or the MS equipment is connected to a different module.

8.4.4 Enable an MS equipment

The MS equipment shall be enabled if addressed to ITSI and referenced to TEI. Only MS equipment that has been temporarily disabled may be enabled by this method: if the MS subscription has also been disabled, whether the ITSI is contained in a separable module or not, it shall not be enabled by this mechanism.

8.4.5 Enable an MS subscription

The MS subscription shall be enabled if addressed by ITSI. If the MS equipment has also been disabled, whether the ITSI is contained in a separable module or not, the composite MS shall not be enabled solely by this mechanism. Only a subscription that has been temporarily disabled may be enabled by this mechanism.

8.4.6 Enable an MS equipment and subscription

The MS equipment and subscription shall be enabled by signalling addressed to both ITSI and TEI; and shall be enabled whether the subscription or equipment has previously been disabled, or both. Equipment, subscriptions, or both, that have been temporarily disabled may be enabled by this mechanism.

Where the ITSI is not separable, an MS may be disabled by utilizing any of the mechanisms described in subclauses 8.4.1, 8.4.2, and 8.4.3. However, to re-enable an MS the SwMI shall use the corresponding mechanism or a mechanism including it. Therefore, an MS temporarily disabled using the mechanism described in subclause 8.4.1 shall only be enabled using the mechanisms described in subclauses 8.4.4 or 8.4.6; an MS disabled by the mechanism described in subclause 8.4.2 shall only be enabled by the mechanisms described in subclauses 8.4.5 or 8.4.6; and an MS disabled by the mechanism described in subclause 8.4.3 shall only be enabled by the mechanism described in subclause 8.4.6.

8.5 Enable/disable authentication mechanism

The enable/disable mechanism shall always include an authentication exchange based upon a shared secret key (KED). The mechanism shall have 4 air interface passes of the form: command request; authenticate challenge; authenticate response and command confirm; command accept/reject and authentication accept/reject. In all cases the process shall be initiated by the manager and the authentication initiated by the target. The mechanism is described below:

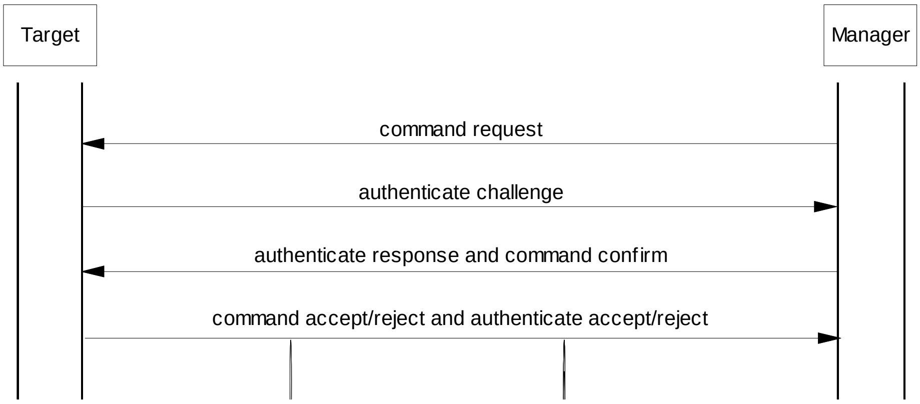

Target
Manager
command request
authenticate challenge
authenticate response and command confirm
command accept/reject and authenticate accept/reject

Figure 21: AI passes for enable/disable mechanism

8.5.1 Authentication of the manager by the target

Authentication of the manager by the target shall be carried out in similar fashion to the authentication mechanisms described in ETS 300 392-7 [6], subclause 4.1.3.

The authentication mechanism shall prove to the target the identity of the manager and that the manager has knowledge of the authentication key, KED (which may be one of the 32 SCKs).

The target shall generate a challenge, RAND, and send it to the manager. On receipt of the challenge the manager shall generate a random seed RS and use this together with the identities of the target and the manager (ITSI-T and ITSI-M) and the key KED to generate a session key for enable/disable (KSED) using algorithm TA91. KEDS and the challenge RAND are input to algorithm TA92 to give response RES at the manager, and XRES at the target. The target shall compare RES and XRES and set the result, R, to TRUE if they are equal and set R to FALSE if they are not equal. The process is summarized in figure 22. When R is TRUE the manager is deemed authenticated to the target.

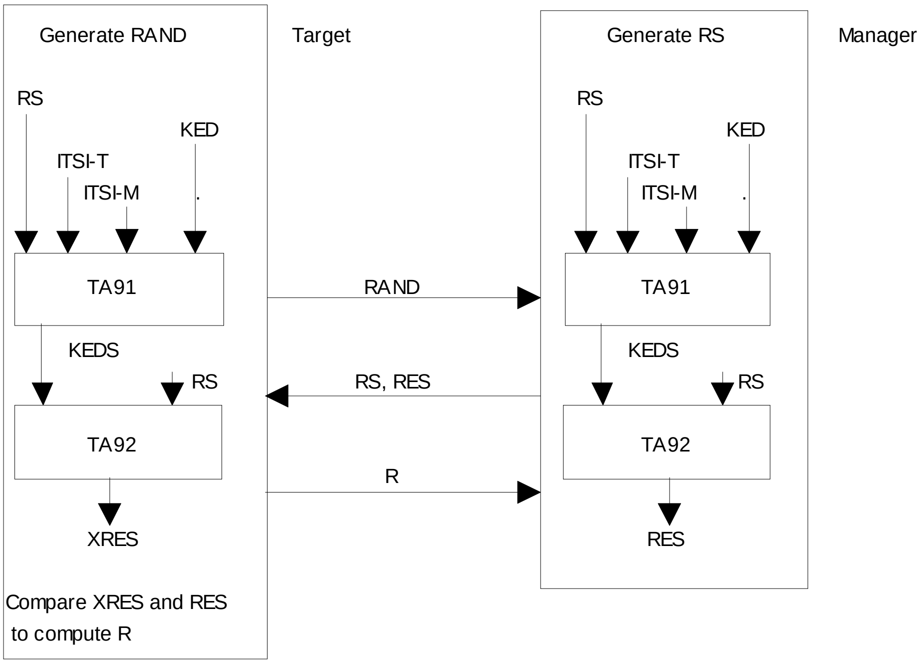


Figure 22: Authentication of the manager by the target

8.5.2 Enable/Disable authentication algorithm specifications

TA91: shall be used to compute KEDS from KED, ITSI-M, ITSI-T and RS.

Input 1: Bit string of length |KED|;
Input 2: Bit string of length |ITSI-M|;
Input 3: Bit string of length |ITSI-T|;
Input 4: Bit string of length |RS|;

Output 1: Bit string of length |KEDS|.

The algorithm should be designed such that is difficult to infer any information about input 1 from knowledge of the other inputs and the output (even if the details of the algorithm are known).

TA92: shall be used to compute (X)RES from KEDS and RS.

Input 1: Bit string of length |KEDS|;
Input 2: Bit string of length |RS|;

Output: BOOLEAN.

The algorithm should be designed such that is difficult to find for a fixed input 1 a value for input 2 that results in the output assuming the value TRUE, provided that input 1 is unknown.

8.6 Enable/disable service description and primitives

8.6.1 Enable/disable primitives

A service shall be provided to allow a manager application to initiate and report on the progress of an enable/disable exchange. A similar service shall exist at the target to indicate the progress of an enable/disable exchange. The primitives required shall be as follows:

- DM-ENDIS-M indication shall be used to provide the manager application with result of an enable/disable exchange.

- DM-ENDIS-M request shall be used by the manager application to initiate an enable or disable exchange with a target.

- DM-ENDIS-T indication shall be used to provide the target application with the result of an incoming enable/disable exchange.

Table 23: DM ENDIS service primitives

GENERIC NAME	Specific name	PARAMETERS
DM-ENDIS-M	request	ITSI, Enable/Disable, Class
DM-ENDIS-M	indication	Result
DM-ENDIS-T	indication	Result

The parameters used in the above primitives should be coded as follows:

result =

TEI enabled;
TEI temporarily disabled;
TEI permanently disabled;
ITSI enabled;
ITSI temporarily disabled;
ITSI permanently disabled.

ITSI =

0;
1;
2;
…
2^{48}-1.

Enable/disable =

Enable;
Disable.

Class =

Permanent TEI;
Temporary TEI;
Permanent ITSI;
Temporary ITSI.

The elements are presented in table 24.

Table 24: DM-ENDIS-M parameters

Parameter	Request	Indication
ITSI	M	-
Enable/disable	M	-
Class (note)	C	-
Result	-	M
NOTE: Only present if enable/disable = disable		

Key: M = Mandatory; C = Conditional; O = Optional.

Table 25: DM-ENDIS-T parameters

Parameter	Indication
Result	M

Key: M = Mandatory; C = Conditional; O = Optional.

A service shall be provided to DMCC to inhibit and enable the communication protocol layers.

On receipt of a validated disable request the target shall inhibit the lower layers of the TETRA DMO protocol stack using the following primitives:

- DMC-CLOSE shall reversibly close operation of the MAC layer for any validated disable request (if the disable is of a subscription then all details relating to that subscription shall be marked as invalid even if that data is held on a removable module).

- DMC-DEACTIVATE shall irreversibly close the MAC layer for a validated permanent disable request (if the disable is of a subscription then all details relating to that subscription (ITSI, K, SCK, etc.) shall be deleted (or in some equivalent manner destroyed) even if the data is held on a removable module).

- DMC-OPEN shall open the MAC layer to normal operation on receipt of a validated enable request when the MAC had been previously closed by a validated temporary disable request (if the enable is of a subscription then all details relating to that subscription previously marked as invalid shall be marked as valid).

No parameters are associated with these primitives.

8.7 Enable/disable protocol

8.7.1 General case

All signalling should be directed to a target by ITSI: this implies that the manager should already know the ITSI/TEI binding where necessary. The target should authenticate the manager by ensuring that the ITSI of the manager matches that assigned by pre-arrangement.

8.7.2 Enable/disable protocol models

The transport mechanism for enable/disable shall be SDS with type 6 (110_2). A logical switch or router at the SDS entity shall direct messages as shown in figure 23 below:

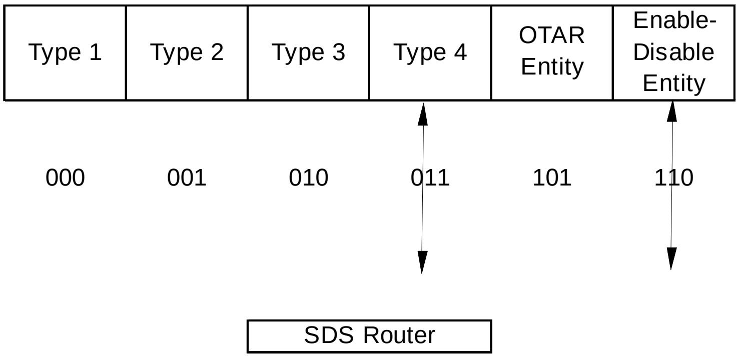


Figure 23: Relationship of security functions to layer functions

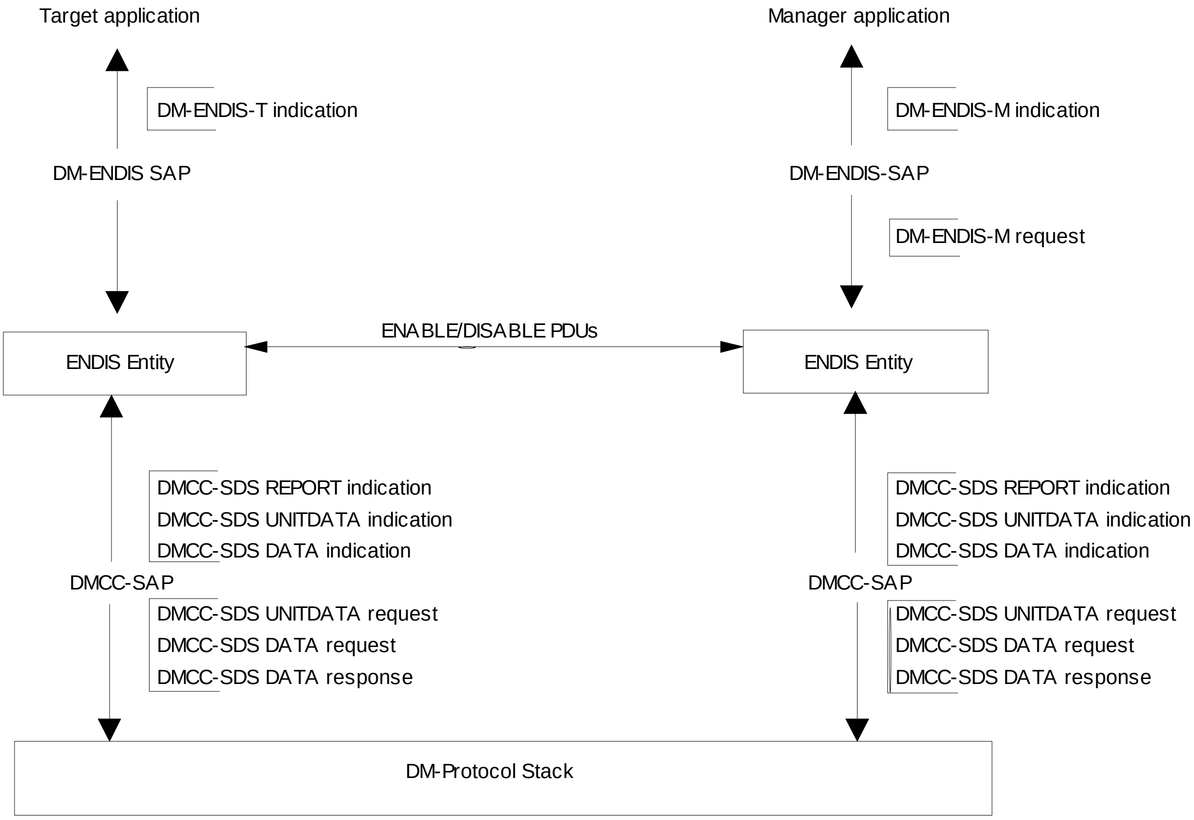


Figure 24: Model for manager to target protocol

The transport mechanism for ENABLE/DISABLE PDUs in DMO shall be acknowledged SDS with SDS message type 6 (110_2) as shown in figure 24.

8.7.3 Specific protocol exchanges

The normal message exchanges for the disable and enable cases shall be according to subclauses 8.7.3.1and 8.7.3.2 respectively.

8.7.3.1 Disable a target

The protocol is shown in figure 25 and described below.

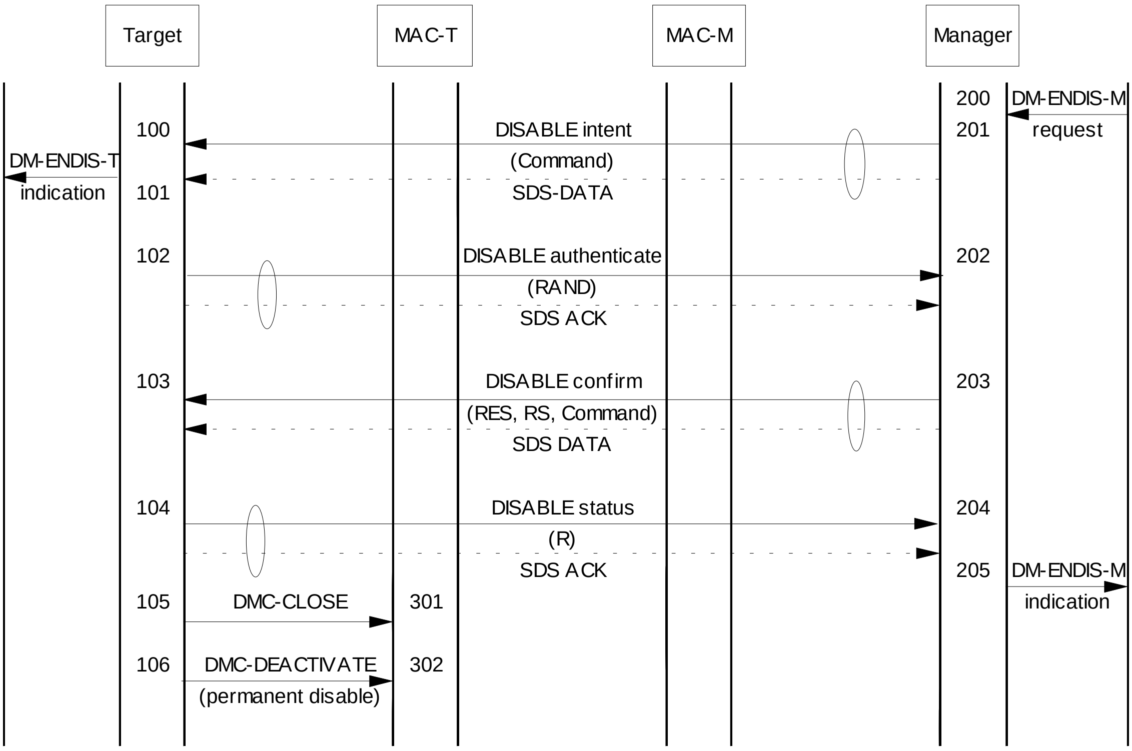


Figure 25: Disabling a target

200 The user application shall request the manager application to disable a target by ITSI, TEI, or both, either temporarily or permanently.

201 The manager application shall send the command to the target using the DISABLE intent PDU.

100 The target application shall decode the command received from the manager and prepare the authentication process by generating the challenge RAND.

101 The target application shall inform the user application of the intent of the received enable/disable message.

102 The target application shall challenge the manager to authenticate itself using the DISABLE authenticate PDU.

202 The manager application shall respond to the authenticate challenge by generating RS and running algorithm TA91 with KED, RS, ITSI-M and ITSI-T to give KEDS. The incoming challenge RAND shall be input to algorithm TA92 with KEDS to give RES.

203 The manager application shall respond to the authentication challenge and confirm the enable/disable command by sending RS, RES and command in the DISABLE confirm PDU to the target.

103 The target shall retrieve RES and RS from the DISABLE confirm PDU. The target shall run algorithm TA91 with inputs ITSI-T, ITSI-M, KED and RS to generate KEDS which it shall input to algorithm TA92 with RAND to give XRES. The target shall compare RES and XRES. If they are equal and the confirmed command is the same as the original command received the target shall implement the command, else it shall ignore the command.

104 The target shall inform the manger application of the result of the authentication process and the action taken in response to the command by using the DISABLE status PDU.

204 The manger application shall decode the DISABLE status of the target and may update its local database.

205 The manager application shall inform the user application of the result of the DISABLE command.

105 The target shall close the lower layers of the protocol stack using the DMC-CLOSE primitive for a valid disable request.

301 The DMAC shall inhibit communication to the upper layers of the protocol stack.

106 If the valid disable request was for permanent disable the target shall deactivate the equipment using the DMC-DEACTIVATE primitive.

302 The DMAC shall permanently deactivate the DM-MS mobile.

8.7.3.2 Enable a target

The protocol is shown in figure 26 and described below:

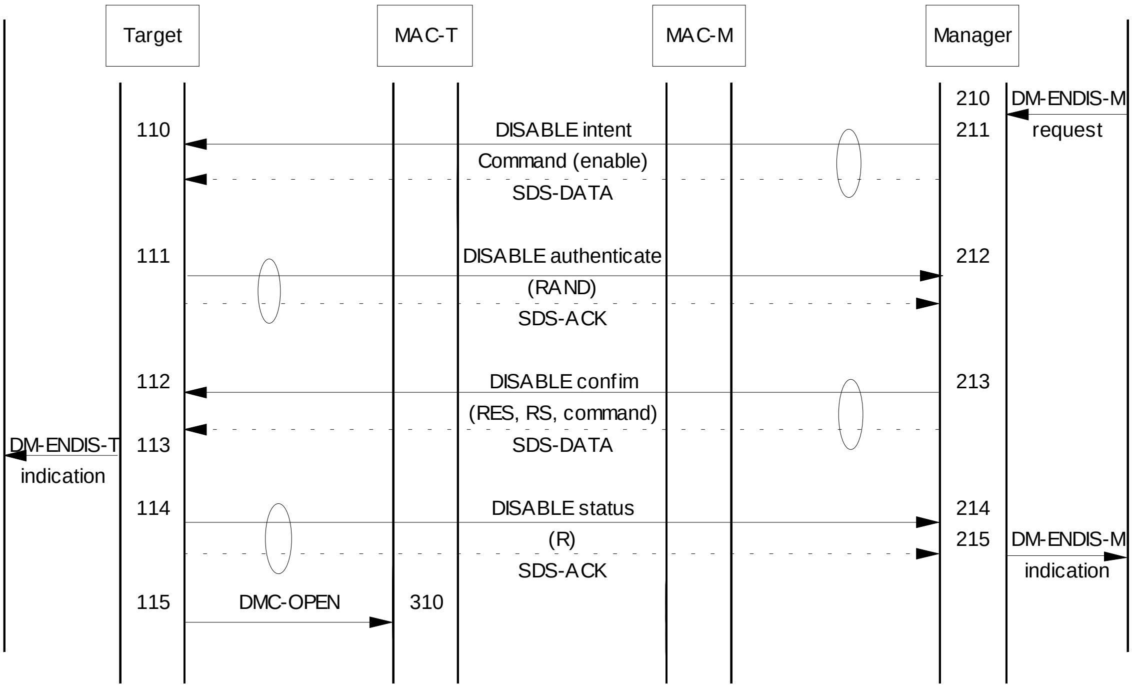


Figure 26: Enabling a target

210 The user application shall request the manager application to enable a target by ITSI, TEI, or both, either temporarily or permanently.

211 The manager application shall send a DISABLE intent PDU to the target with the command set to enable following the request from the user application.

110 The target application shall decode the command and prepare to authenticate the manager by generating the challenge RAND.

111 The target application shall challenge the manager to authenticate itself by sending RAND in the DISABLE authenticate PDU.

212 The manager application shall respond to the authenticate challenge by generating RS and running algorithm TA91 with KED, RS, ITSI-M and ITSI-T to give KEDS. The incoming challenge RAND shall be input to algorithm TA92 with KEDS to give RES.

213 The manager application shall respond to the authentication challenge and confirm the enable/disable command by sending RS, RES and command in the DISABLE confirm PDU to the target.

112 The target shall retrieve RES and RS from the DISABLE confirm PDU. The target shall run algorithm TA91 with inputs ITSI-T, ITSI-M, KED and RS to generate KEDS which it shall input to algorithm TA92 with RAND to give XRES. The target shall compare RES and XRES. If they are equal and the confirmed command is the same as the original command received the target shall implement the command, else it shall ignore the command.

113 The target application shall inform the user application of the result of the received enable/disable message.

114 The target shall inform the manger application of the result of the authentication process and the action taken in response to the command by using the DISABLE status PDU.

214 The manager application shall decode the DISABLE status of the target and may update its local database.

215 The manager application shall inform the user application of the result of the ENABLE command.

115 The target shall open the lower layers of the protocol stack using the DMC-OPEN primitive for a valid enable request.

310 The DMAC shall allow communication to the upper layers of the protocol stack.

8.7.4 Protocol messages

The PDUs described in this subclause shall be carried by SDS type 6 messages on a point-to-point basis. In each case the return message may be contained in the SDS-ACK message to an incoming SDS-DATA message.

8.7.4.1 DISABLE intent

Message: DISABLE intent
Response to: -
Response expected: DISABLE authenticate
Short description: The message is sent by the manager to indicate that the target shall be disabled (permanently or temporarily)

Table 26: DISABLE intent contents

Information element	Length	Type	C/O/M	Remark
DISABLE PDU type	2	1	M	00_2 Intent
Command	6	1	M	
Proprietary		3	O	

8.7.4.2 DISABLE authenticate

Message:	DISABLE authenticate
Response to:	DISABLE intent
Response expected:	DISABLE confirm
Short description:	The message is sent by the target to authenticate the manager before accepting and acting upon a command

Table 27: DISABLE authenticate contents

Information element	Length	Type	C/O/M	Remark
DISABLE PDU type	2	1	M	01_2 Authenticate
Authentication challenge (RAND)	80	1	M	
Proprietary		3	O	

8.7.4.3 DISABLE confirm

Message:	DISABLE confirm
Response to:	DISABLE authenticate
Response expected:	DISABLE status
Short description:	The message is sent by the manager to the target in response to the authentication challenge and to confirm the command send in the initial DISABLE intent

Table 28: DISABLE confirm contents

Information element	Length	Type	C/O/M	Remark
DISABLE PDU type	2	1	M	10_2 Confirm
Command	6	1	M	
Authentication response (RES)	32	1	M	
Random Seed (RS)	80	1	M	
Proprietary		3	O	

8.7.4.4 DISABLE status

Message:	DISABLE status
Response to:	DISABLE confirm
Response expected:	None
Short description:	The message is sent by the target to inform the manager of its response to an enable or disable request and its resulting status.

Table 29: DISABLE status contents

Information element	Length	Type	C/O/M	Remark
DISABLE PDU type	2	1	M	11_2
Authentication result (R)	1	1	M	
Equipment status	2	1	M	Indicates disabled state of equipment
Subscription status	2	1	M	Indicates disabled state of subscription
Enable/Disable result	2	1	M	
Address Extension	24	1	C	Present only if enable/disable result = 000_2
TETRA Equipment Identity	60	1	C	Present only if enable/disable result = 000_2
Proprietary		3	O	

8.7.5 MM Information elements coding

8.7.5.1 Address extension

The Address Extension Element shall be used to indicate the extended part of TSI address.

Table 30: Address Extension element contents

Information sub element	Length	Type	Remark
Mobile Country Code (MCC)	10	1	
Mobile Network Code (MNC)	14	1	

8.7.5.2 Authentication challenge

The Authentication challenge element shall contain the random challenge (RAND) from the target to manager.

Table 31: Authentication challenge element contents

Information sub element	Length	Type	Remark
Random challenge RAND	80	1	

8.7.5.3 Authentication response

The Authentication response element shall contain the output of algorithm TA92 (RES) from the manager to the target.

Table 32: Authentication challenge element contents

Information sub element	Length	Type	Remark
Authentication response (RES)	32	1	

8.7.5.4 Authentication result

The Authentication result element shall contain the result of the comparison by the target of RES and XRES.

Table 33: Authentication challenge element contents

Information sub element	Length	Type	Remark
Authentication result (R)	1	1	

8.7.5.5 Command

The command shall be used by the manager to instruct the target which action is required.

Table 34: Command element contents

Information element	Length	Value	Remark
Command sub-type	2	00_2	Enable
		01_2	Disable
		10_2	Provide TEI
		11_2	Reserved
Subscription	1	0	Command does not apply to subscription
		1	Command applies to subscription
Equipment	1	0	Command does not apply to equipment
		1	Command applies to equipment
Temporary/Permanent Disable	1	0	Temporary disable (default)
		1	Permanent Disable
Reserved for expansion	1		Value of 0 by default

NOTE: The temporary enable/disable bit has no meaning for command sub-types 00_2 and 10_2.

8.7.5.6 Enable/disable result

The purpose of the enable/disable result element shall be to indicate whether or not enabling or disabling was successful.

Table 35: Enable/disable result element contents

Information element	Length	Value	Remark
Enable/Disable result	2	00_2	enable/disable successful
		01_2	enable/disable failure, address extension mismatch
		10_2	enable/disable failure, TEI mismatch
		11_2	enable/disable failure, TEI and address extension mismatch

8.7.5.7 Equipment status

The purpose of the Equipment status element shall be to indicate the enabled or disabled state of the equipment.

Table 36: Equipment status element contents

Information element	Length	Value	Remark
Equipment status	2	00_2	Equipment enabled
		01_2	Equipment temporarily disabled
		10_2	Equipment permanently disabled
		11_2	Reserved

8.7.5.8 Proprietary

Proprietary is an optional, variable length element and shall be used to send and receive proprietary defined information appended to the PDUs.

The use, the size and the structure of the Proprietary element is outside the scope of this ETS.

8.7.5.9 Random seed

The random seed element shall contain the random seed generated by the manager as input to TA91.

Table 37: Authentication challenge element contents

Information sub element	Length	Type	Remark
Random seed RS	80	1	

8.7.5.10 Subscription status

The purpose of the Subscription status element shall be to indicate the enabled or disabled state of the subscription.

Table 38: Subscription status element contents

Information element	Length	Value	Remark
Subscription status	2	00_2	Subscription enabled
		01_2	Subscription temporarily disabled
		10_2	Subscription permanently disabled
		11_2	Reserved

8.7.5.11 TETRA Equipment Identity (TEI)

The TETRA Equipment Identity element shall be used to indicate the TETRA Equipment Identity (TEI).

Table 39: TETRA Equipment Identity element contents

Information element	Length	Value	Remark
TETRA Equipment Identity	60		See ETS 300 392-1 [1] clause 7

9 End-to-end encryption

9.1 Introduction

End-to-end encryption algorithms and key management are outside the scope of this ETS. This clause describes a standard mechanism for synchronization of the encryption system that shall be employed when using a synchronous stream cipher. The mechanism also permits transmission of encryption related and other signalling information. The mechanism shall apply only to U-plane traffic. The method described shall use the Stealing Channel, STCH, for synchronization during transmission (see ETS 300 396-3 [7], subclause 8.6.5).

NOTE: This mechanism does not apply for self-synchronizing ciphers, or for block ciphers.

The following are requirements on the end-to-end encryption mechanism:

- the same mechanisms shall apply in both directions;
- the synchronization processes shall be independent in each direction;
- end-to-end encryption shall be located in the U-plane (above the MAC resident air-interface encryption);
- transport of plain text and cipher text within the SwMI shall maintain the timing and ordering of half-slot pairing (half slots shall be restored in the same order and with the same boundary conditions at each end of the link);
- the encryption mechanisms described in this clause are valid for one call instance.

9.2 Voice encryption and decryption mechanism

A functional diagram of the voice encryption and decryption mechanism based on the synchronous stream cipher principle is given in figure 27. This demonstrates the symmetry of transmitter and receiver with each side having common encryption units.

It is assumed that the encryption unit shall generate a key stream in a similar way to the air interface encryption unit. The encryption unit is then termed the End-to-end Key Stream Generator (EKSG). EKSG shall have two inputs, a cipher key and an initialization value. The initialization value should be a time variant parameter (e.g. a sequence number or a timestamp) that is used to initialize synchronization of the encryption units. The output of EKSG shall be a key stream segment termed EKSS.

Function F_1 shall combine the Plain Text (PT) bit stream and EKSS resulting in an encrypted Cipher Text (CT) bit stream. Function F_1^{-1} shall be the inverse of F_1 and shall combine the bit streams CT and EKSS resulting in the decrypted bit stream PT.

Function F_2 shall replace a half slot of CT with a synchronization frame provided by the "sync control" functional unit.

Function F_3 shall recognize a synchronization frame in the received CT, and shall supply them to "sync detect" functional unit.

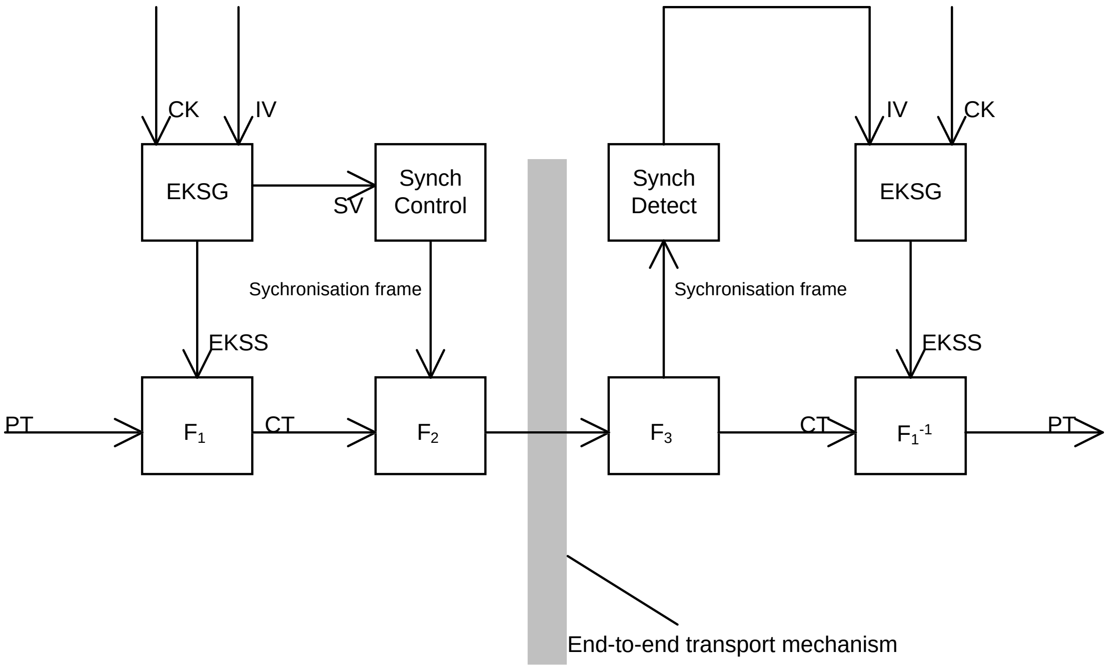


Figure 27: Functional diagram of voice encryption and decryption mechanisms.

Associated with the functional mechanism shall be a crypto-control interface that shall allow the following:

- selection of CK by use of a key selection value;
- selection of algorithm by use of an algorithm number;
- selection of encryption state (on/off).

9.2.1 Protection against replay

Protection against replay should be obtained by use of a time variant initialization value and a similarly time variant cipher key.

Possible examples for a time variant initialization value are a timestamp or sequence number. Time variance of the cipher key may be achieved by deriving a key for each encrypted call. The manner in which time variance is achieved is not addressed by this ETS.

Recording and replaying of an entire call can be prevented by use of additional data. For example a shared call-id range, or a shared real time clock, that validates messages may be used. Means of protecting against call replay are outside the scope of this ETS.

9.3 Data encryption mechanism

Encryption of circuit mode data preferably should be implemented in the application requiring transport of data. However encryption of circuit mode data may also be achieved by using the voice encryption mechanism.

Using the voice encryption mechanism can only gain confidentiality. In order to achieve data integrity other precautions should be taken.

NOTE: Any frame stealing will result in loss of some user application data and alternative mechanisms for recovery of the data should be taken.

9.4 Exchange of information between encryption units

Two different cases shall be identified by an appropriate MAC header (see subclause 9.4.5):

- synchronization information in clear; or
- encrypted information.

The use of exchanged encrypted information between encryption units is out of the scope of this ETS.

9.4.1 Synchronization of encryption units

In figure 27, the processing blocks "synchronization control" and "synchronization detect" and their associated functions F_2 and F_3 shall provide the means of synchronizing the EKSG.

There shall be two synchronization cases to consider:

- initial synchronization; and
- re-synchronization.

NOTE: Late entry may be considered a special case of re-synchronization.

Both cases shall use frame stealing as a means of inserting synchronization data in the traffic path (see ETS 300 396-3 [7], subclause 8.6.5).

Occurrence of stealing in the receiver shall be locally reported to the U-plane application at the DMD-SAP.

The frame stealing shall make use of the DMD-UNITDATA primitive to address the MAC (request) and to inform the U-plane (indication) as shown in table 40.

Table 40: Parameters used in the DMD-UNITDATA primitive

Parameter	Request	Indication	Remark
Half slot content	M	M	
Half slot position (HSN)	C	C	1st half slot or 2nd half slot
Half slot importance (HSI)	M	-	No importance, Low, Medium or High
Stolen indication (HSS)	M	M	Not Stolen, Stolen by C-plane, or Stolen by U-plane
Half slot condition (HSC)	-	M	GOOD, BAD, NULL

Further communication from MAC to the U-plane shall use the DMD-REPORT primitive shown in table 41.

Table 41: Parameters used in the DMD-REPORT primitive

Parameter	Indication	Remark
Half slot synchronization	C	
Circuit Mode information	C	
Report	M	

The transfer of synchronization data shall be achieved by stealing speech frames (half-slots) from the U-plane traffic. SF shall be transmitted as individual half-slots via STCH for initial as well as for re-synchronization.

A half-slot stolen (HSS) indication shall be associated with each speech frame of a pair making up a transmission slot. The valid combinations shall be:

- neither half-slot stolen;
- first half-slot stolen;
- both half-slots stolen;
- second half-slot stolen, only if this is the first half-slot available to the U-plane at the start of transmission.

9.4.2 Encrypted information between encryption units

Frame stealing shall be used as a means of inserting any encryption related data in the traffic path in a manner similar to that used to exchange synchronization information.

Occurrence of stealing in the receiver shall be locally reported to the U-plane application at the DMD-SAP.

The frame stealing shall make use of the DMD-UNITDATA primitive to address the MAC (request) and to inform the U-plane (indication) as shown in table 40.

Further communication from MAC to the U-plane shall use the DMD-REPORT primitive as shown in table 41.

The transfer of encryption related data shall be achieved by stealing speech or data frames (half-slots) from the U-plane traffic. This information shall be transmitted as individual half-slots via STCH.

A half-slot stolen (HSS) indication shall be associated with each speech or data frame of a pair making up a transmission slot. The valid combinations shall be:

- neither half-slot stolen;
- first half-slot stolen;
- both half-slots stolen;
- second half-slot stolen, only if this is the first half-slot available to the U-plane at the start of transmission.

9.4.3 Transmission

The encryption control unit shall intercept DMD-UNITDATA request from the Codec (or traffic generator in the case of circuit mode data calls). If the half-slot has already been stolen the encryption unit shall forward DMD-UNITDATA request to the MAC with no changes. If the half-slot has not been stolen and the encryption unit wishes to insert a synchronization frame the rules for frequency of stealing of half-slots as defined in table 42 should be followed, however no more than four half-slots should be stolen per second:

Table 42: Maximum average frequency of stealing

HSI	Maximum average frequency of stealing	
	Initial synchronization	**Re-synchronization**
High	4/second	1/second
Medium	4/second	2/second
Low	4/second	4/second
No importance	4/second	4/second

The distribution of the stolen slots for initial synchronization is not defined; they may be placed consecutively at the start of the transmission, before any speech is transmitted, or may be well spaced, with only a single half-slot stolen before speech transmission commences. The first SV transmitted at the start of each transmission shall be termed IV. Insertion of synchronization frames should not be regular, for example to make jamming more difficult.

The distribution of encryption related information is not defined in this ETS. However the same recommendations as defined for encryption synchronization may be followed.

If the encryption unit steals a frame it shall update the header of the stolen frame and set HSI to HIGH in DMD-UNITDATA request. On receipt of a DMD-UNITDATA request that indicates a stolen frame the MAC shall generate the appropriate training sequence for the air interface to allow the receiving MS to recognize a stolen frame.

If both half slots are stolen the same procedure shall be followed.

Figure 28 gives an example for determining the points of time of transmitting a new SV by the "sync-control" process. Transmission of a new SV may be forced after a period of 1 second after the last transmission of an SV. More SV's may be transmitted to improve reliability of synchronization and to allow for late entry.

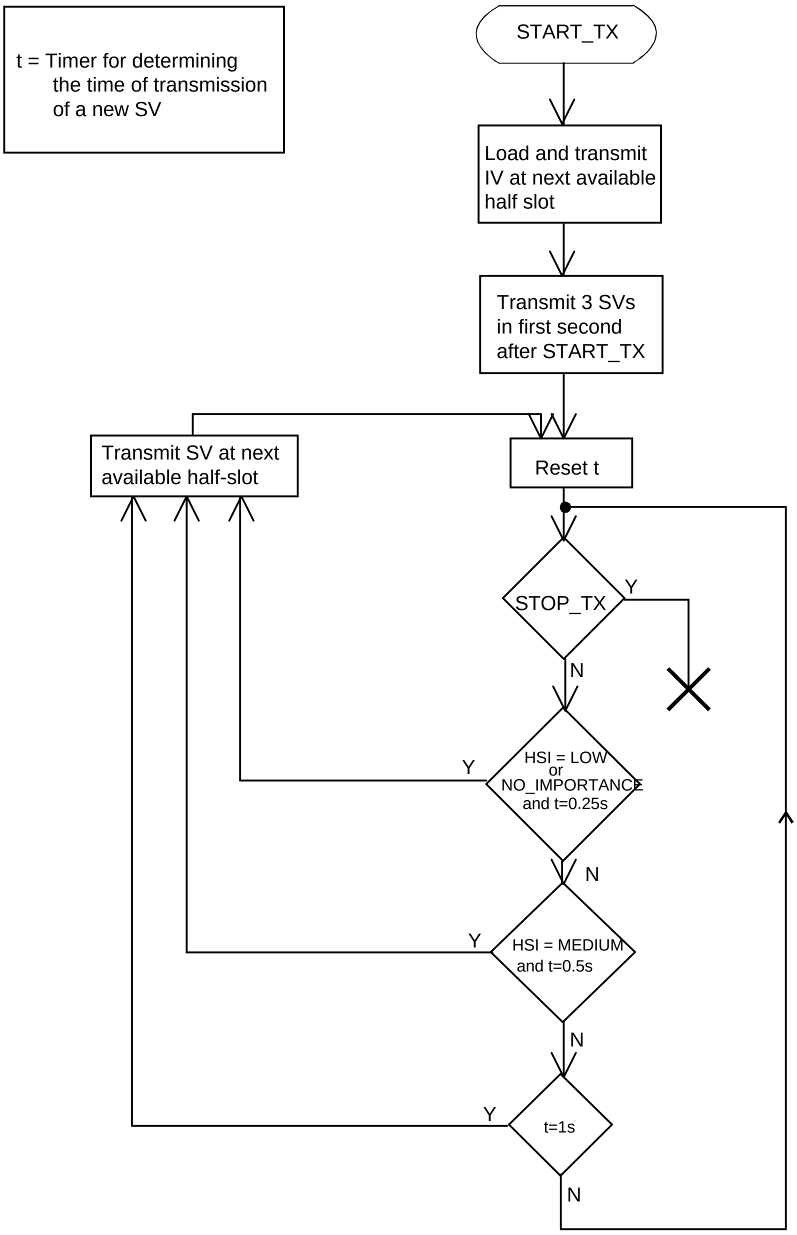

t = Timer for determining the time of transmission of a new SV
START_TX
Load and transmit IV at next available half slot
Transmit 3 SVs in first second after START_TX
Transmit SV at next available half-slot
Reset t
STOP_TX
Y
N
HSI = LOW or NO_IMPORTANCE and t=0.25s
Y
N
HSI = MEDIUM and t=0.5s
Y
N
t=1s
Y
N

Figure 28: Flow chart of the transmitter "sync-control" process.

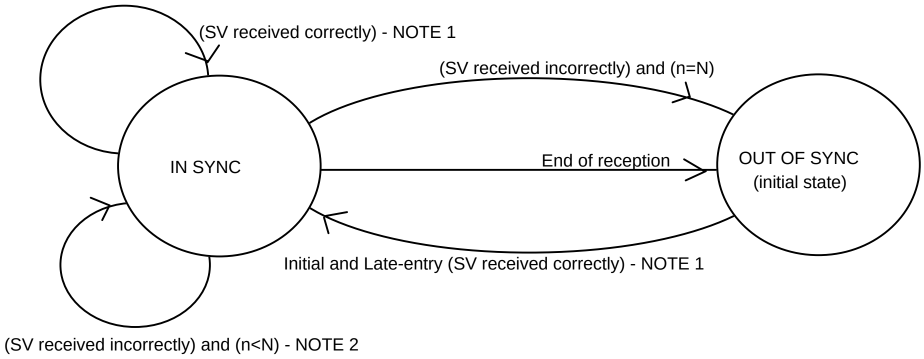
9.4.4 Reception

The encryption control unit shall intercept DMD-UNITDATA indication from the MAC. The frame shall also be forwarded to the Codec or traffic sink irrespective of its content.

If a stolen is recognized by the MAC as having been stolen by the U-plane (indicated by HSS) the encryption control unit shall interrogate the header of the stolen frame. If HSSE=1 and SHSI=0, and if HSC=GOOD, the half slot content shall be treated as SF and passed to the Synchronization Detect Unit.

If HSSE=1 and SHSI=0, but HSC≠GOOD, the half slot content should be discarded and a flywheel mechanism in the synchronization detect unit should be used to maintain synchronization until a valid SF is received.

A state diagram of an example sync detect process is given in figure 29.


(SV received correctly) - NOTE 1
(SV received incorrectly) and (n=N)
IN SYNC
End of reception
OUT OF SYNC
(initial state)
Initial and Late-entry (SV received correctly) - NOTE 1
(SV received incorrectly) and (n<N) - NOTE 2

n = number of successive wrongly received SV's
NOTE 1: IV:=(received SV) and load IV into EKSG and n:=0
NOTE 2: Do not load IV into EKSG and n:=n+1 (flywheel)

Figure 29: State diagram of the "sync-detect" process in the receiver.

In the flywheel mechanism the receiver should use locally generated SV’s if an SV is not received correctly. After a fixed number (N) of successive SV’s are missed the receiver should be considered out of sync. Incrementing, or generation of, SV should be pre-determined by the encryption units.

9.4.5 Stolen frame format

The format of a stolen frame (half-slot) shall be as defined in table 43.

Table 43: Stolen frame format (half-slot)

Information element	Length	Type	Value	Remark
Half-slot stolen by encryption unit	1	1	0	Not stolen by encryption unit
(HSSE)			1	Stolen by encryption unit
Stolen half-slot identifier (SHSI)	1	1	0	Synchronization frame
			1	Other signalling data
Signalling data block	119	1		

HSSE and SHSI shall not be encrypted, whether the remaining contents of SF are encrypted or not. The remainder of SF shall be encrypted unless the half slot contains synchronization information.

In case of an SF the signalling data block should contain some or all of the following parameters:

- algorithm number;
- key number;
- synchronization value (SV).

Where a codec is the U-plane traffic source/sink it should not make any interpretation of data in a stolen frame if that data has been stolen by the encryption unit. The matrix below indicates the terminating devices for stolen frames based upon the values of HSSE and SHSI where a codec is present:

Table 44: U-plane terminating devices for stolen frames

HSSE	SHSI	Terminating Device
0	0	Codec
0	1	U-plane (undefined)
1	0	Encryption Synchronization
1	1	Encryption control

The end-to-end encryption unit therefore should have two addressable control paths, i.e. synchronization path and signalling path. It is understood that the encryption unit is self contained and both synchronization and signalling originate and terminate within the unit.

9.5 Location of security components in the functional architecture

This subclause describes the location of the encryption unit in the U-plane.

In figure 30 the end-to-end encryption unit shall lie between the Traffic Source/Sink and DMD-SAP. The traffic source/sink may be a speech codec (see ETS 300 395-1 [9]), or any circuit mode data unit.

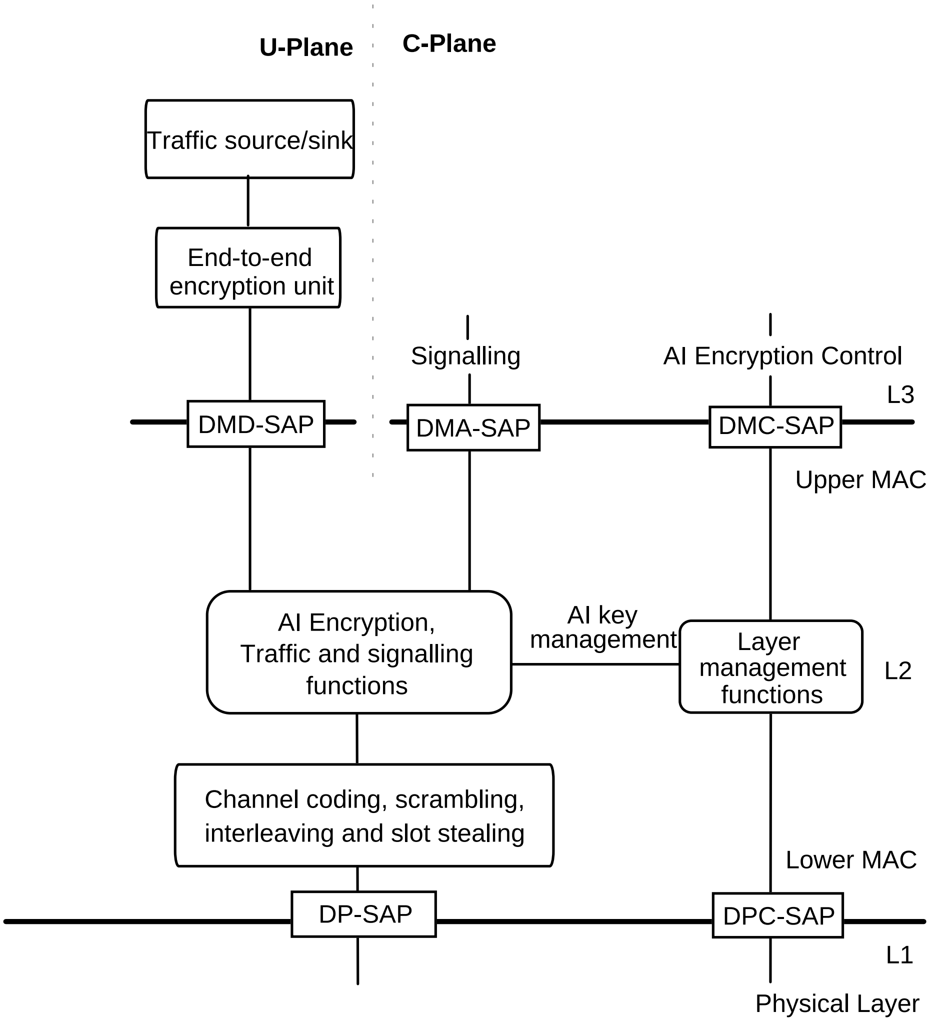

U-Plane
C-Plane
Traffic source/sink
End-to-end encryption unit
Signalling
AI Encryption Control
L3
DMD-SAP
DMA-SAP
DMC-SAP
Upper MAC
AI Encryption, Traffic and signalling functions
AI key management
Layer management functions
L2
Channel coding, scrambling, interleaving and slot stealing
Lower MAC
DP-SAP
DPC-SAP
L1
Physical Layer

Figure 30: Position of end-to-end encryption unit in MS

The services offered on the U-Plane side, as shown in figure 30, is further expanded in figure 31.

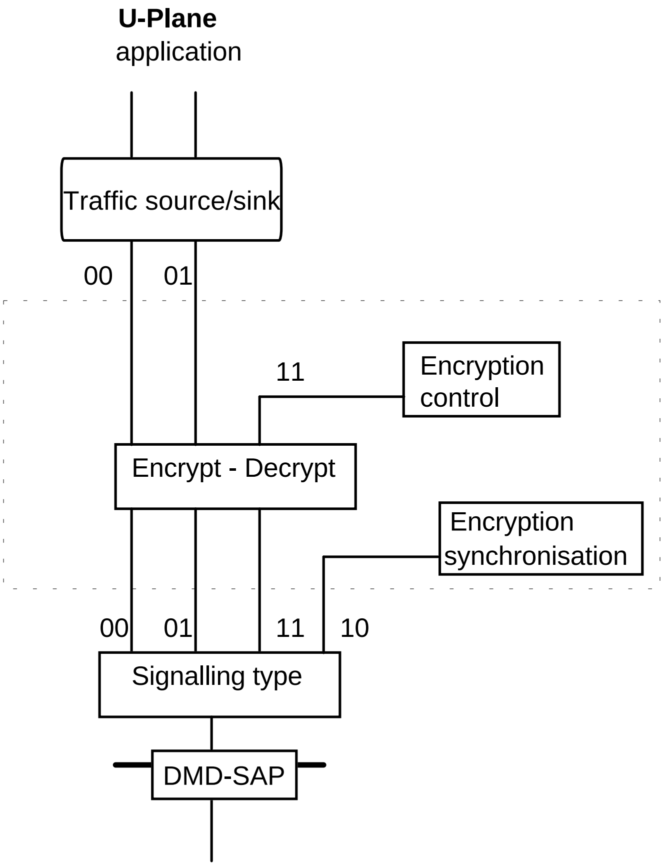


Figure 31: Functional model of the encryption unit

9.6 End-to-end key management

The key used by the end-to-end encryption unit is managed outside the context of TETRA. However as for end-to-end encryption TETRA shall provide a standard mechanism for transfer of keys.

The end-to-end key management facility shall utilize the standard TETRA SDS with user defined data content. The key management message should include the following parameters:

- Encryption key number;
- Encryption unit identity;
- Sealed encryption key.

The SDS type 4 shall incorporate a header in the first byte of the user defined content.

The definition of user defined data type 4, given in ETS 300 392-2 [2], subclause 14.8.52 shall be replaced by the definition given in table 45.

Table 45: User defined data-4 element contents

Information element	Length	Value	Remark
SDS type 4 header	8	00000000_2	Reserved for future expansion
		00000001_2	End to end encryption key management
		others	Reserved
User-defined Data-4	varies	varies	All values available for the user application (see note).
NOTE: The length of the data element is as defined in ETS 300 392-2 [2] subclause 14.8.52 with the first byte reserved as a header.			

History

Document history	
December 1996	Public Enquiry PE 121: 1996-12-30 to 1997-04-25