EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 396-6

April 1998

Source: TETRA

Reference: DE/RES-06007-6

ICS: 33.020

Key words: Direct Mode, security, TETRA

Terrestrial 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
Internet: secretariat@etsi.fr - http://www.etsi.fr - http://www.etsi.org

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

Contents

Blank page

Foreword

This European Telecommunication Standard (ETS) has been produced by the Terrestrial Trunked Radio (TETRA) Project of the European Telecommunications Standards Institute (ETSI).

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

Part 1: "General network design".

Part 2: "Direct MS-MS Air Interface- Radio Aspects".

Part 3: "Direct MS-MS Air Interface- Protocol".

Part 4: "Repeater Mode Air Interface".

Part 5: "Gateway Mode Air Interface".

Part 6: "Security".

Transposition dates	
Date of adoption of this ETS:	3 April 1998
Date of latest announcement of this ETS (doa):	31 July 1998
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 January 1999
Date of withdrawal of any conflicting National Standard (dow):	31 January 1999

Blank page

1 Scope

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

This part describes the security mechanisms in TETRA Direct Mode. It provides mechanisms for confidentiality of control signalling and user speech and data at the AI.

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

- Clause 5 describes authentication mechanisms for direct mode. 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 AI, for circuit mode speech, circuit mode data, packet (short) data and control information. This clause then details the protocol concerning control of encryption at the AI.

- Clause 7 describes the key management mechanism, and includes a description of the 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 stream cipher units for U-plane traffic by means of a frame stealing device for synchronization of the units.

- Annex A defines the mapping of protocols in TETRA V+D Security to those of DMO Security for each of OTAR and Enable/Disable.

The use of AI encryption gives confidentiality protection against eavesdropping only. The addition of a synchronized time variant initialization 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 300 392-2: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

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

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

[4] ETS 300 396-2: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Direct Mode; Part 2: Direct MS-MS Air Interface - Radio Aspects".

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

[6] ETS 300 396-3: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Direct Mode; Part 3: Direct MS-MS Air Interface - Protocol".

[7] ETS 300 396-5: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Speech codec for full-rate traffic channel Part 1: General description of speech functions".

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

[9] ETS 300 395-1: "Terrestrial Trunked Radio (TETRA); Speech CODEC for full-rate traffic channel; Part 1: General description of speech functions".

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 [2]).

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

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

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 KSG in the receiving terminal synchronized with the Key Stream Generator (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 unencrypted 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 AI.

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 cipher key that is independent of any other key.

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 a cryptographic process used for either of the security processes authentication or encryption.

time stamp: Is 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
C-PLANE	Control-PLANE
CT	Cipher Text
DLL	Data Link Layer
DM	Direct Mode
DMCC	Direct Mode Call Control
DMO	Direct Mode Operation
EKSG	End-to-end Key Stream Generator
EKSS	End-to-end Key Stream Segment
F	Function
FN	Frame Number
HSC	Half-Slot Condition
HSI	Half-Slot Importance
HSN	Half-Slot Number
HSS	Half-Slot Stolen
HSSE	Half-Slot Stolen by Encryption unit
ITSI	Individual TETRA Subscriber Identity
IV	Initialization Value
K	authentication Key
KH	Key Holder
KS	Session Key
KSG	Key Stream Generator
KSL	Key SeaLer
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
OTAR	Over The Air Rekeying
PDU	Protocol Data Unit

PT	Plain Text
RAND	RANDom challenge
RES	RESponse
RS	Random Seed
RSO	Random Seed for OTARSession Key OTAR
SAP	Service Access Point
SCH	Signalling CHannel
SCH/F	Full SCH
SCH/H	Half SCH
SCH/S	Synchronization SCH
SCK	Static Cipher Key
SCK-VN	SCK Version Number
SCKN	Static Cipher Key Number
SDS	Short Data Service
SDU	Service Data Unit
SHSI	Stolen Half-Slot Identifier
SS	Synchronization Status
SSCK	Sealed Static Cipher Key
STCH	STolen CHannel
SV	Synchronization Value
SwMI	Switching and Management Infrastructure
TA	TETRA Algorithm
TCH	Traffic CHannel
TDMA	Time Division Media Access
TEI	TETRA Equipment Identity
TN	Timeslot Number
TSI	TETRA Subscriber Identity
TVP	Time Variant Parameter
Tx	Transmit
U-PLANE	User-PLANE
V+D	Voice + Data
XRES	eXpected RESponse

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 changeovers that are bounded by initial call setup and final call cleardown. Call pre-emption when successful may mark the start of a new call.

NOTE: A DMO 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 direct mode call slot 1 of the TDMA structure shall be used by the transmitter for transmission, and slot 3 of the TDMA structure shall be used by the transmitter to send or receive control messages. In frequency efficient operation the other 2 slots of the TDMA structure shall be used in like manner.

4.1 Single-Hop Calls

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

- 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 SCK;
- Source and Destination MS have common KSG.

Call setup in DMO is a single pass operation with an allowed exception for individual calls to allow a presence check acknowledgement (2 pass call setup). 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 [6], subclause 9.1.1).

4.2 Multi-Hop Calls

DMO 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 Key Stream Generator (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 shall not be 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 DMO call initiator shall be synchronized to the gateway.

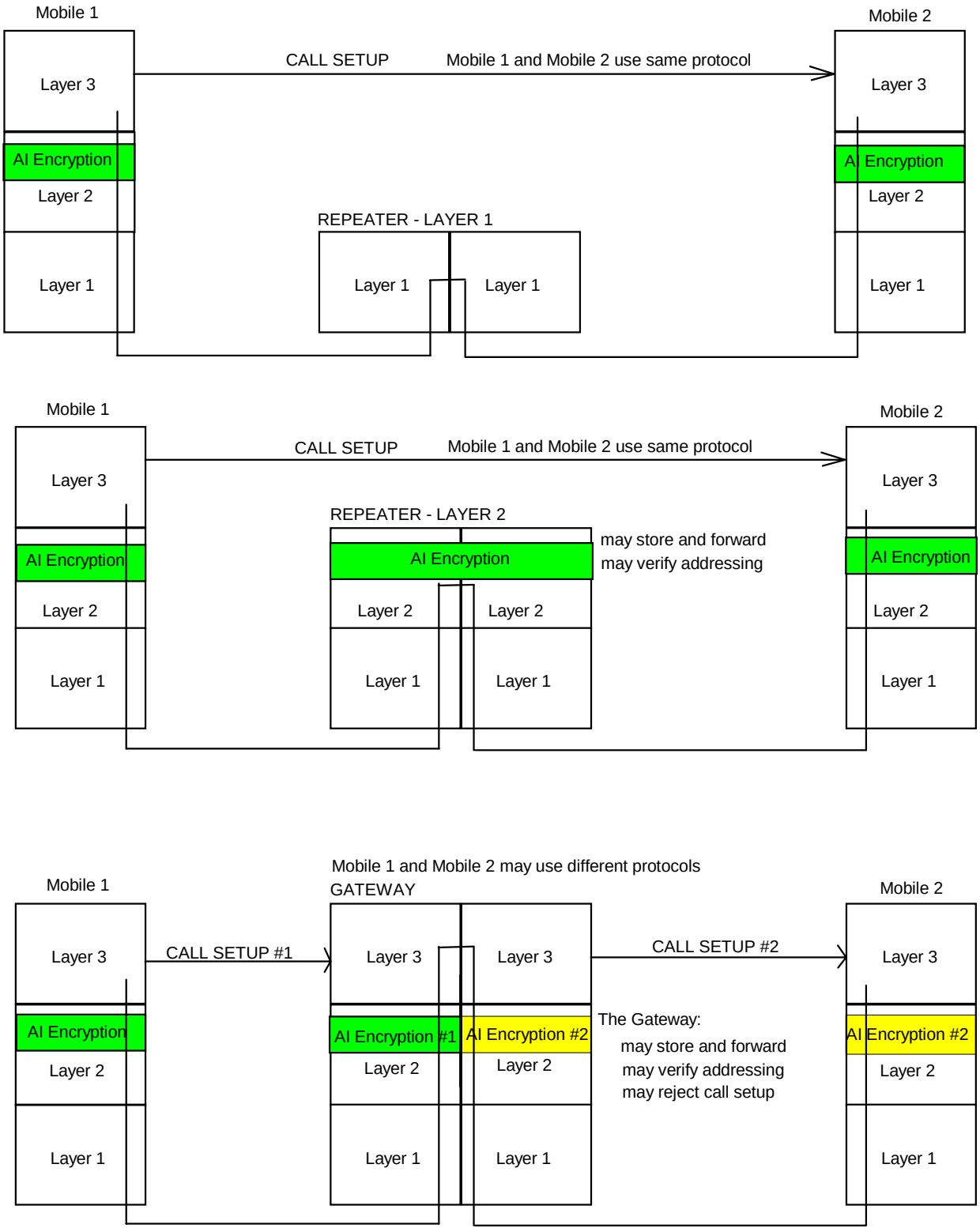


Figure 1: Protocol stacks for multi-hop calls

4.3 Call Synchronization

In DMO there is no centralized synchronization master. Each call transaction 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.

In DMO the encryption synchronization shall apply only to the current call transaction. All slaves shall set the values of Frame Number (FN), Timeslot Number (TN) and TVP from the first synchronization burst and increment each value as appropriate for the duration of the call transaction. (See ETS 300 396-2 [4], subclauses 9.3.2 and 9.3.3 for full definitions of FN and TN, and ETS 300 396-2 [4], subclause 7.3.2 for definitions of the incrementing of these counters.)

NOTE 1: Call setup refers to the establishment of a single call transaction.

The encryption state for all call transactions in the call shall be set by the first call master. The initial value of TVP shall be chosen by the first call master. This initial TVP may be chosen randomly or may contain a time of day element to prevent replay. Each new transmitting party shall establish a new TVP, however the TVP sequence may be continuous over a set of call transactions.

TVP shall be incremented on every timeslot with a cycle of 2^{29} timeslots, except during call setup where the following exception shall apply:

During call setup 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 timeslot of the first frame following the synchronization burst as shown in figure 2.

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

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

NOTE 2: Normal traffic transmission slots are shown shaded.

Figure 2: Incrementing of TVP after call setup synchronization bursts for DM-SETUP

For call setup with presence checking (DM-SETUP PRES) the above process shall be followed, where TVP is incremented on the first traffic slot after completion of transmission of the DM-SETUP PRES messages.

NOTE 2: The foregoing scheme is common to all initial synchronization bursts of a call transaction.

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.

4.3.1 Synchronization of calls through a repeater

Calls through a repeater may modify the normal synchronization burst pattern and repeat a received synchronization burst (one timeslot) over a frame. Traffic shall follow in the first timeslot of the first frame following the synchronization frame. In the synchronization frame where the timeslot is replicated TVP shall not be incremented.

	FN18				FN1				FN2				FN3			
…	TN1	TN2	TN3	TN4	TN1	TN2	TN3	TN4	TN1	TN2	TN3	TN4	TN1	TN2	TN3	TN4
…	Synchronization												Traffic			
…	TVP_S	TVP_S	TVP_S										TVP_S +1	TVP_S +2	TVP_S +3	TVP_S +4

Master to repeater

Repeater to Slave

	FN18				FN1				FN2				FN3			
	TN1	TN2	TN3	TN4	TN1	TN2	TN3	TN4	TN1	TN2	TN3	TN4	TN1	TN2	TN3	TN4
	Synchronization				Synchronization								Traffic			
	TVP_S	TVP_S	TVP_S	TVP_S	TVP_S	TVP_S	TVP_S	TVP_S					TVP_S +1	TVP_S +2	TVP_S +3	TVP_S +4

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

NOTE 2: The first traffic slot from the master is in the first slot of the first frame after the repeater has finished repeating the synchronization data (TN1 of FN3 in above example).

NOTE 3: Normal traffic transmission slots are shown shaded.

Figure 3: Incrementing of TVP across a repeater

Further synchronization examples for calls through a repeater demonstrate the same principle. In call set up with a presence check traffic from the master to the repeater follows in the first slot of the first frame following receipt of the presence check and not as above in the first slot of the first frame after receiving the repeated synchronization bursts.

In the case where a PDU is fragmented the first part of the PDU is sent repeatedly in the synchronization frames as above and the following MAC-FRAG and MAC-END PDUs are sent as per normal traffic.

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

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

In multi-slot interleaved calls the original traffic burst is expanded to cover 4 or 8 bursts (TCH/2.4, TCH/4.8). The interleaving follows encryption at the transmitter, and decryption follows de-interleaving at the receiver.

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

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

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

NOTE 2: Actual TVP value is to be used for decryption of non-traffic bursts.

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

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

Transmission across frame 18 shall be treated as shown in figure 5:

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

NOTE: TVP_{Start} is the value of TVP used in the first traffic frame in this example.

Figure 5: Treatment of TVP for TCH/4.8 or TCH/2.4 with interleaving depth of 4 at frame 18

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

4.3.2.1 Recovery of stolen frames from interleaved data

If the stolen frame has been stolen from the C-plane it shall not be treated as if it were interleaved and shall therefore be decrypted with the "actual" value of TVP for immediate delivery to the C-plane.

If the stolen frame has been stolen from circuit mode data in the U-plane it shall be treated as interleaved and shall follow the same rules as for data traffic.

NOTE: Speech and full rate data transmissions are not subject to multi-slot interleaving (see ETS 300 396-3 [6]).

5 Authentication Mechanisms

5.1 Mobile to mobile 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 mobile stations as belonging to the same DMO net when successful communication takes place.

5.2 Dual Watch Operation

In dual-watch mode a DM-MS shall be a valid member of the TETRA V+D network and may authenticate to that network using the procedures defined in ETS 300 392-7 [5], 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 setup 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 [5], clause 4.

The gateway shall be considered as having two synchronized protocol stacks with the V+D network acting as the synchronization master for the call (see figure 6).

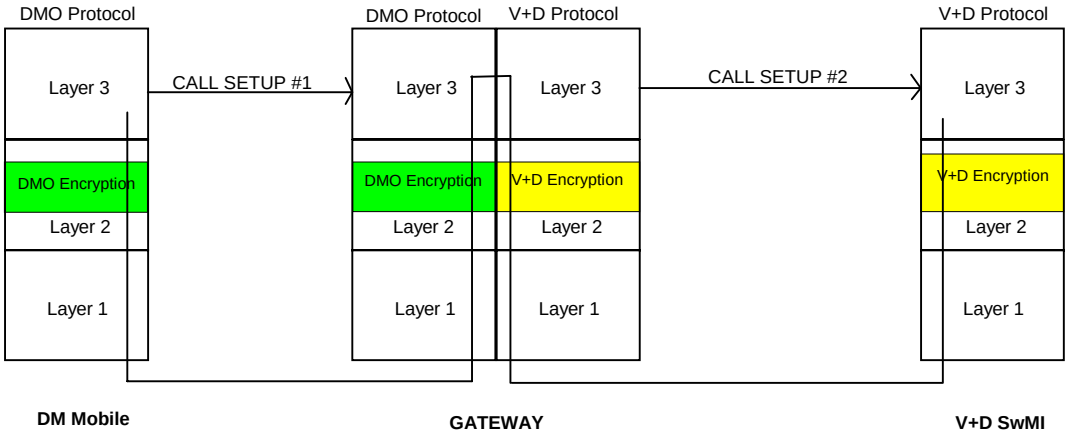


Figure 6: TETRA DMO to TETRA V+D Gateway

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 AI encryption as defined in ETS 300 392-7 [5], clause 6. On initial call setup the keys in use are as shown in figure 7.

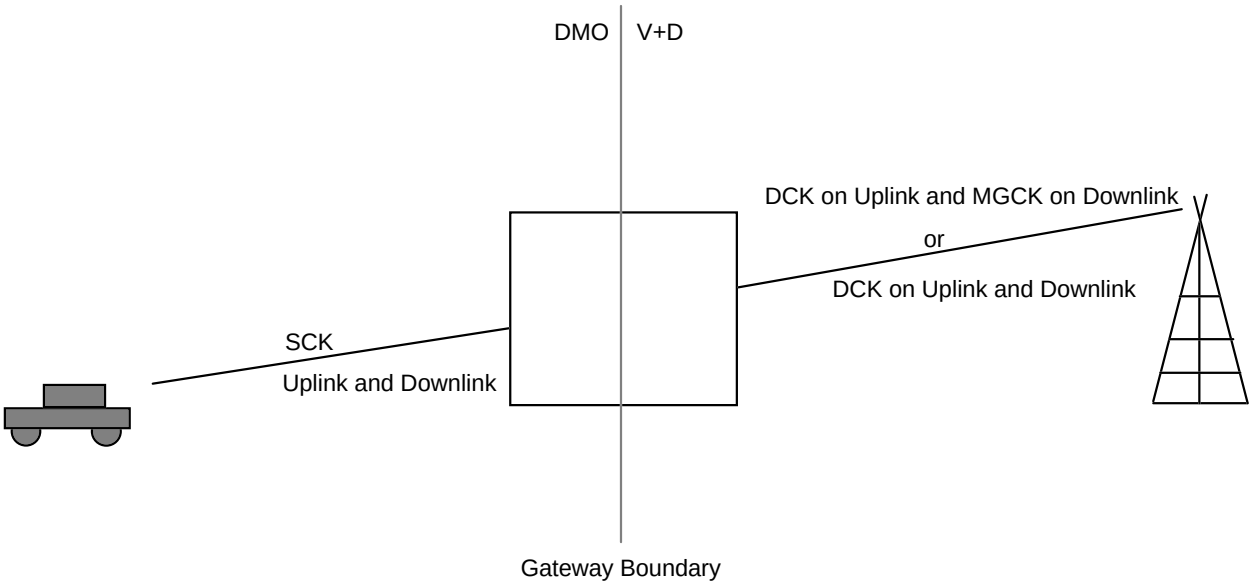


Figure 7: Gateway Initial Key allocations

Throughout an encrypted call (which may include the call setup phase) each layer 2 (i.e. the DMO-protocol layer 2 and the 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 part of the ETS shall not describe methods for correcting this delay.

If the DM-MS is a party to a group call with some members of the group being on the TETRA V+D mode network there may be a delay for any call transaction through the gateway. This part of the ETS shall not describe methods for correcting this delay.

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 encryption operates by combining the output of a Key Stream Generator (KSG) with the contents of messages to be transmitted across the AI. 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 that is to be encrypted is replaced by a bit of cipher text to avoid error propagation.

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 [3], subclause 7.2, these shall be independent of AI encryption; thus a service invoked without end-to-end encryption may still be encrypted over the AI.

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. (See ETS 300 392-7 [5], subclause 6.1.1).

The KSG shall have two inputs, a Time Variant Parameter (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. AI 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	0000_2	TEA1
		0001_2	TEA2
		0010_2 to 0111_2	Other TETRA standard algorithms
		$1xxx_2$	Proprietary TETRA algorithms

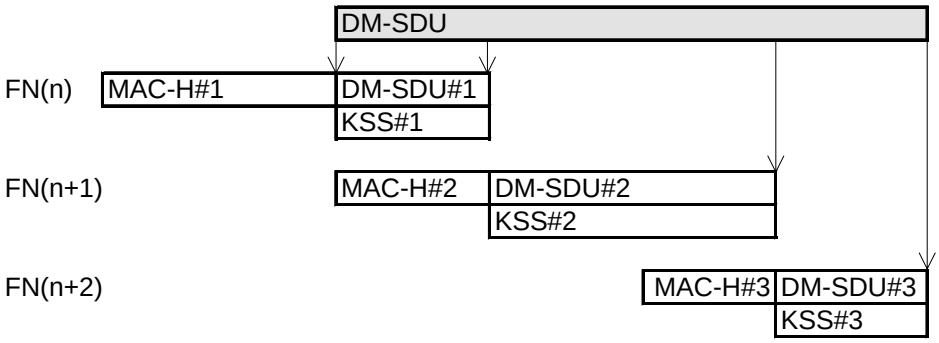
The TETRA standard algorithms shall only be available on a restricted basis from ETSI.

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.

In DMO the use of the TDMA framing structure is strictly enforced (see ETS 300 396-3 [6] subclause 4.3.1). There is no support for multi-slot communication and where a PDU is fragmented over many slots the KSS is restarted on each slot as shown in figure 8.



NOTE 1: The example DM-SDU is fragmented over 3 slots by breaking it into DM-SDU#1, DM-SDU#2 and DM-SDU#3

NOTE 2: KSS#1 is used to encrypt DM-SDU#1, KSS#2 for DM-SDU#2, and KSS#3 for DM-SDU#3

NOTE 3: Length of DM-SDU#1 = L#1. KSS#1(0,..,L#1-1) is used to encrypt DM-SDU#1. The remainder of KSS#1 is discarded (KSS#!(L#1, ..., 431)). Similarly for fragments 2 and 3.

Figure 8: Allocation of KSS to encrypt an example fragmented PDU

The physical nature of the TETRA AI is that each TDMA slot is broken into 2 half-slots. In all cases the KSS is split between those slots as follows:

KSS(0, …, 215) shall be used to encrypt the first half slot;

KSS(216, …, 431) shall be used to encrypt the second half slot.

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 timeslot. The TVP shall be a value 29 bits long represented as TVP(0)….TVP(28), where TVP(0) shall be the least significant bit and TVP(28) the most significant bit of TVP.

The initial value of TVP is a transmitted parameter that shall be sent in the synchronization bursts by the current call master. The TVP shall be maintained as described in subclause 4.3.

After the synchronization frames TVP shall be incremented by 1 on each timeslot transition (see also subclause 4.3).

NOTE: TVP is independent of FN and TN.

6.3.1.2 Cipher Key

The ciphering process shall be as shown in figure 9. 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.

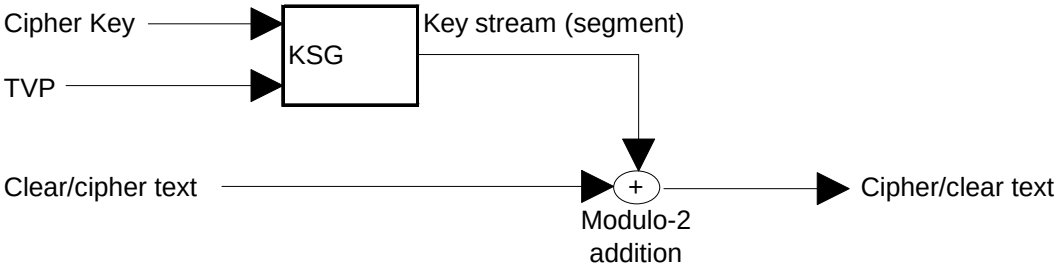


Figure 9: Speech and control information encryption

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

- the Static Cipher Key (SCK).

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

For use in Direct Mode SCKs exist in groups of 32. The convention SCKN, $1 \leq N \leq 32$, shall be used to refer to specific members of this set.

Once an SCK has been established for a call transaction no changes to the ciphering parameters shall be allowed within that call transaction.

If the parties to a call load different keys from each other, the receiving party will decode messages incorrectly. This shall 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 [6], 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.

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 [6], subclause 9.1.1) and the DMAC-DATA PDU (see ETS 300 396-3 [6], subclause 9.2.1) contain an AI Encryption State element (see ETS 300 396-3 [6], subclause 9.3.2) 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 copied here (see table 2).

The AI Encryption State element indicates whether the current PDU has been encrypted and if so at what point in the PDU the encryption is applied.

Table 2: AI Encryption state element contents

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 and onwards, and any related traffic is AI encrypted
		10_2	The DM-SDU and any related traffic is AI encrypted
		11_2	The destination address (SSI), DM-SDU and any related traffic are AI encrypted

NOTE 1: The above table modifies that found in ETS 300 396-3 [6], subclause 9.3.1

For calls through a repeater which has no encrypt/decrypt capability calls with AI Encryption State element equal to 01_2 shall not apply.

In figures 10 through 13 the way in which the MAC-PDU is constructed is shown. In these diagrams the MAC-H is not the same as that referred to in ETS 300 396-3 in order to allow clarification of the encryption process.

NOTE 2: E-MAC-H is equivalent to the MAC Header defined in ETS 300 396-6.

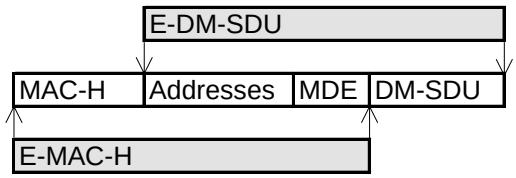
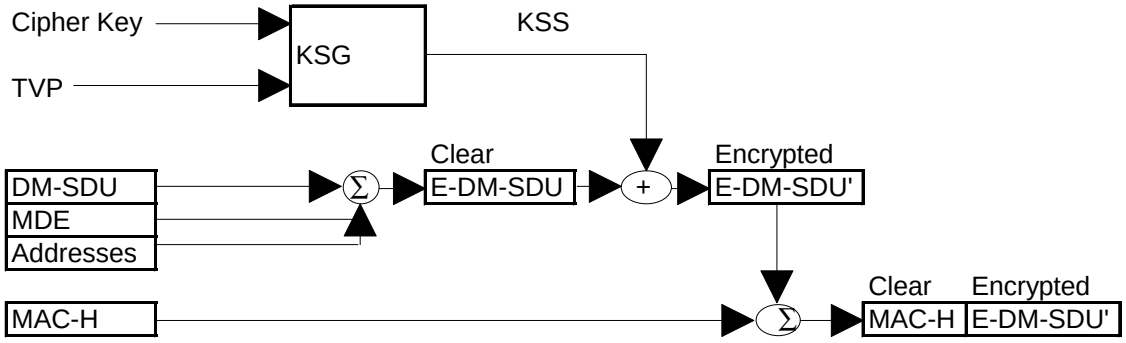


Figure 10: Concatenated structure of TETRA DMO elements



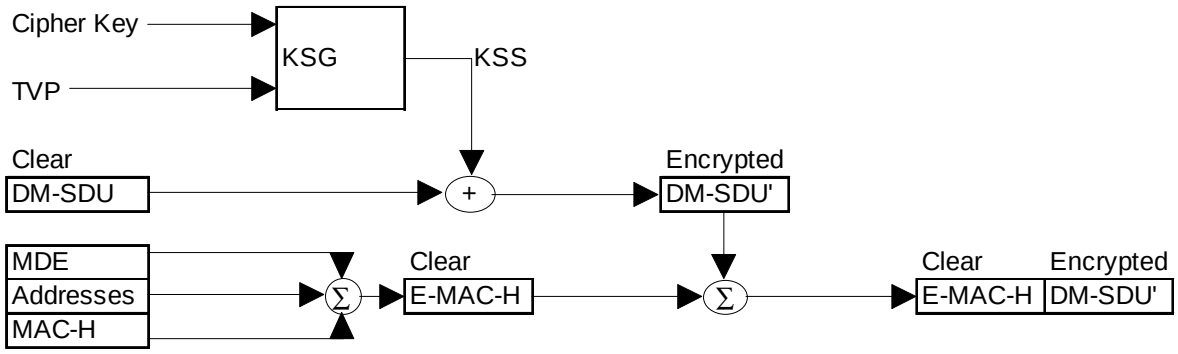
NOTES: E-DM-SDU = Extended DM-SDU

MDE = Message Dependent Elements

∑ = Concatenation of incoming elements

+ = Modulo-2 addition of incoming elements

Figure 11: Encryption process as it occurs in TETRA DMO mode 01_2

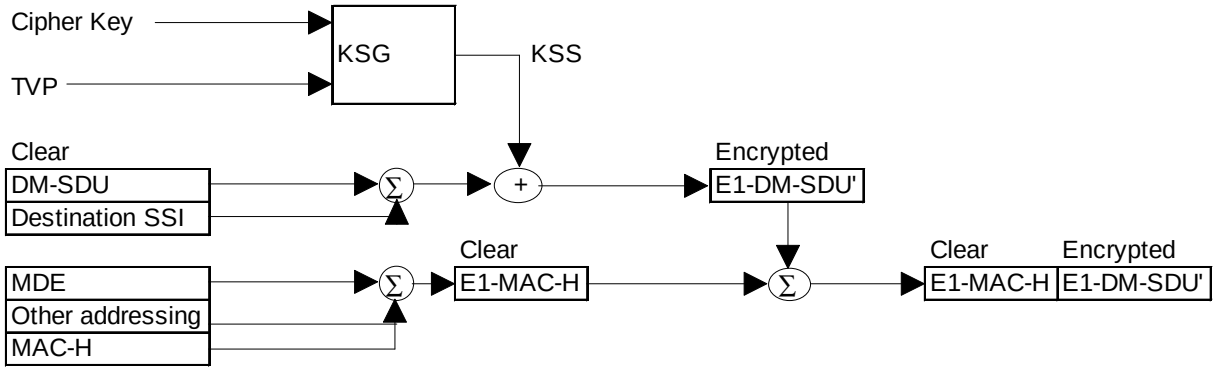


NOTES: MDE = Message Dependent Elements

E-MAC-H = Extended MAC Header

Σ = Concatenation of incoming elements

Figure 12: Encryption process as it occurs in TETRA DMO mode 10_2



NOTES: MDE = Message Dependent Elements

E1-DM-SDU = DM-SDU combined with destination address

E1-MAC-H = MAC-H combined with MDE and other addressing

Σ = Concatenation of incoming elements

Figure 13: Encryption process as it occurs in TETRA DMO mode 11_2

The difference between modes 01_2 and 10_2 for DMO encryption is that in the latter case the MAC-H is extended by including the message dependent elements and the address fields to give an Extended MAC Header (E-MAC-H), whilst in the former case the DM-SDU is extended by including the message dependent elements and the address fields to give an Extended DM-SDU (E-DM-SDU).

When encryption is applied $\text{MAC-H}_{(01)}$/$\text{E-MAC-H}_{(10)}$ is sent in clear, and the $\text{E-DM-SDU}_{(01)}$/$\text{DM-SDU}_{(10)}$ is sent encrypted.

6.3.2.1.1 DMAC-SYNC PDU encryption

See ETS 300 396-3 [6], subclause 9.1.1 for a full description of this PDU.

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

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

- encryption state 00_2 shall always be in clear;

- in encryption state 01_2 if the fragmentation flag (bit 12) is set then bits 1 to 18 shall be in clear, all other bits shall be encrypted, else if the fragmentation flag (bit 12) is not set then bits 1 to 12 shall be in clear and all other bits shall be encrypted;

- in encryption state 10_2 the bit at which encryption is started is dependent on the DM-SDU contained in the final field of the PDU where the message dependent elements shall be clear in order to facilitate repeater operation (where the repeater has no encrypt/decrypt facility) and where the presence of addressing fields is conditional on call type;

- in encryption state 11_2 the KSS shall be applied in the following manner:

    - KSS(0,…, 23) shall be used to encrypt the destination address;
      KSS(24,…, 24+n) shall be discarded (where n is the number of bits between the end of the destination address field and the start of the DM-SDU field);
      KSS(24+n+1, …, 24+n+1+m) shall be used to encrypt the DM-SDU (where m is the length of the DM-SDU carried in the DMAC-SYNC PDU).

6.3.2.1.2 DMAC-DATA PDU encryption

See ETS 300 396-3 [6], subclause 9.2.1 for a full description of this PDU.

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

- encryption state 00_2 shall always be in clear;

- in encryption state 01_2 bits 1 to 10 shall be in clear, all other bits shall be encrypted;

- in encryption state 10_2 the bit at which encryption is started is dependent on the DM-SDU contained in the final field of the PDU where the message dependent elements shall be clear in order to facilitate repeater operation (where the repeater has no encrypt/decrypt facility) and where the presence of addressing fields is conditional on call type;

- in encryption state 11_2 the KSS shall be applied in the following manner:

    - KSS(0,…, 23) shall be used to encrypt the destination address;
      KSS(24,…, 24+n) shall be discarded (where n is the number of bits between the end of the destination address field and the start of the DM-SDU field);
      KSS(24+n+1, …, 24+n+1+m) shall be used to encrypt the DM-SDU (where m is the length of the DM-SDU carried in the DMAC-DATA PDU).

6.3.2.2 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.

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

6.4 AI encryption protocol

6.4.1 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.

6.4.1.1 Positioning of encryption process

The encryption process shall be located in the upper part of the MAC layer.

For AI encryption mode 10_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. Using the same position for the AI encryption process in AI encryption mode 01_2 (i.e. prior to channel encoding) the MAC header of DMAC-SYNC PDU in SCH/H can be partially encrypted. 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 14 illustrates this interconnection:

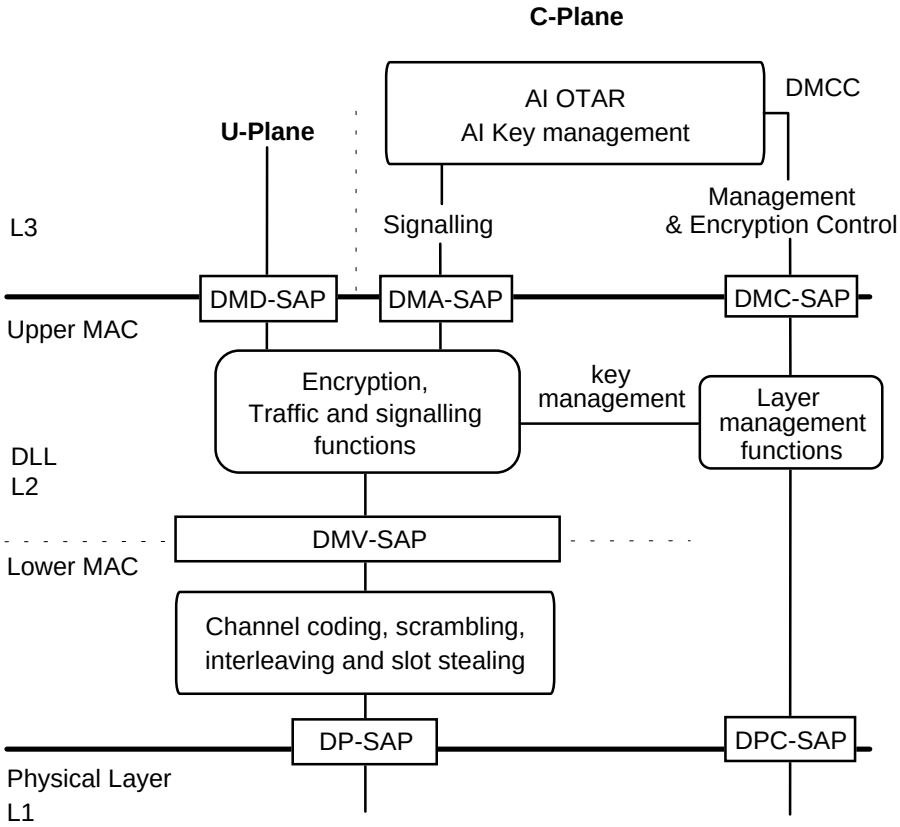


Figure 14: Relationship of security functions to layer functions

6.4.2 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 [6]. The primitives that are passed between the layers are also described.

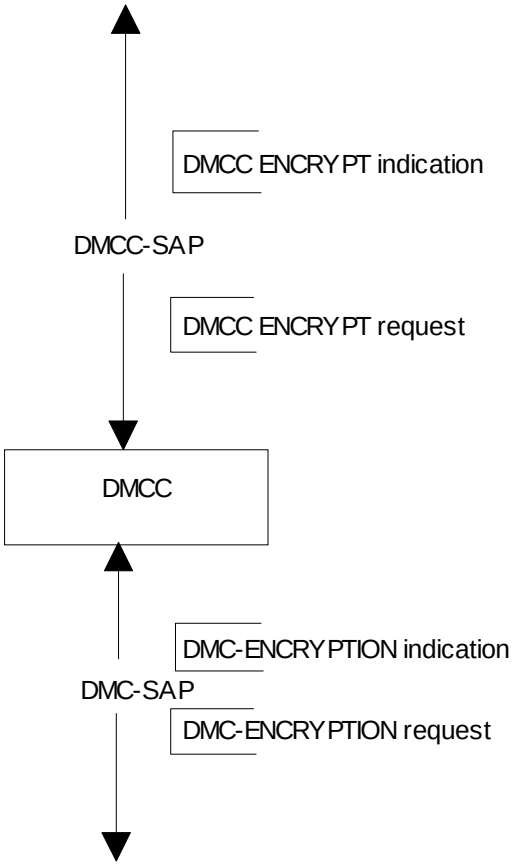


Figure 15: Encryption related services in DMO

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 [6], subclause 5.3.6) to set the encryption parameters for the current call. This primitive may also be used to preconfigure the preferred encryption parameters for all calls initiated by DMCC.

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).

6.4.2.1 DMCC-ENCRYPT primitive

Table 3: DMCC-ENCRYPT parameters

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

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

The parameters shall be encoded as follows:

Key download type =
- no keys downloaded
- SCK

KSG Number =
- KSG 1
- KSG 2
- KSG 3
- . . .
- KSG 16

Cipher usage =
- encryption off
- TX, traffic encrypted and PDU encrypted from destination address
- TX, DM-SDU encrypted and traffic encrypted
- RX

SCKN =
- 1
- 2
- 3
- …
- 32

SCK =
- 0
- …
- 2^{80}-1

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

Configuration data =
- Configuration
- Current call

6.4.2.2 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 4: DMC-ENCRYPTION parameters

Parameter	Request	Indication
KSG Number	M	-
SCK	C	-
SCKN	-	M
Cipher usage	M	M

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

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

KSG Number =
KSG 1
KSG 2
KSG 3
. . .
KSG 16

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

Cipher usage =
encryption off
TX, traffic encrypted and PDU encrypted from destination address
TX, DM-SDU encrypted and traffic encrypted
RX

SCKN =
1
2
3
…
32

SCK =
0
…
2^{80}-1

6.4.3 Protocol Functions

Each functional entity in the protocol stack shall communicate with its peer entity using a defined protocol; for example the DMCC entity in the originating DM-MS communicates with its peer DMCC entity in the receiving DM-MS.

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

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 Air Interface (AI) key management mechanisms

DMO shall only use SCK for AI encryption. Each MS may be provided with up to 32 SCKs in an SCK set. Where a group of MSs wish to communicate with each other, they shall have at least one common SCK in their respective SCK sets.

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

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

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

NOTE 2: The home network is defined as that network which has common MNI with the MS.

Over The Air Rekeying (OTAR) is an optional service, but if implemented shall be done so as described in this clause.

7.1 Key numbering and storage

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

7.2 Over The Air Rekeying

Keys for the AI encryption unit (KSG) may be transmitted over the AI 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 sealer 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 in this ETS for DMO can only operate if each DM-MS holds an authentication key, K, known to the authentication centre.

SCKs shall be generated and made known to a key sealing mobile and distributed from there as shown in figure 13. The SCK and the ITSI parameters, Session Key OTAR (KSO) and Random Seed for OTAR (RSO), should be forwarded from the authentication centre to the key generator in a secure way.

A mobile with OTAR capability may be able 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 sealer (as shown in figure 16 by the transparent Key Holder box).

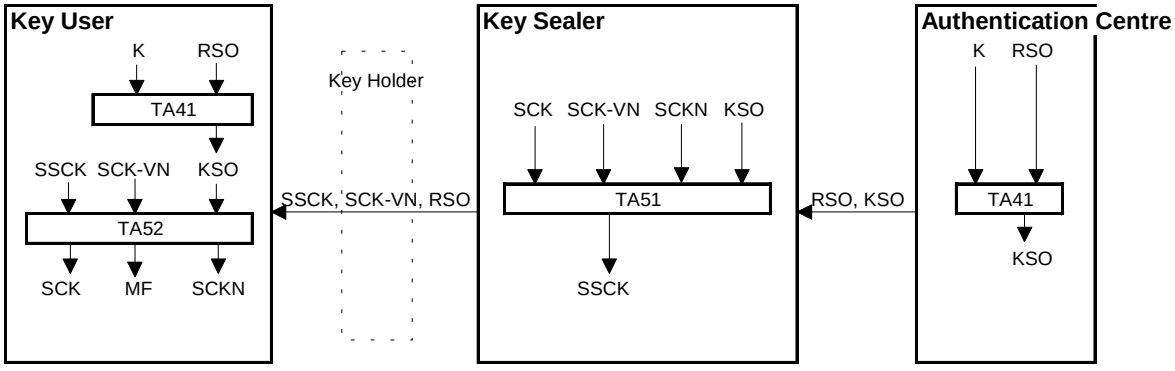


Figure 16: Distribution of SCK by a key sealer

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 Holder (KH). The primitives required shall be as follow:

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

- DM-OTAR-SCK confirm shall be used to provide the MS application with confirmation that the key information received is acceptable, or provide the reject reasons if not. It shall also give the SCKN of each key received.

- DM-OTAR-SCK request shall be used by the MS application to request the distribution of a new static cipher key. It shall contain the number (of 32 possible values) of each SCK requested and the identity of the KH that holds it. More than one SCK may be requested in one transaction.

Table 5: DM OTAR SCK service primitives

Parameter	Request	Indication	Confirm
SCKN	M	M	M
SCK-VN	-	M	-
KH-id	M	-	-
Result	-	-	M

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

result =
SCK received successfully
SCK failed to decrypt
KH or KSL unavailable

SCKN =
1
2
3
…
32

KH-id =
ITSI of KH for current SCKN

SCK-VN =
0
…
2^{16}-1

7.4 OTAR SCK protocol functions

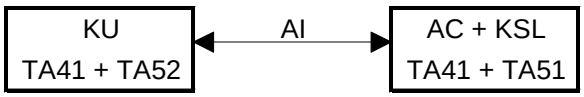
There shall be three functional entities in the SCK OTAR chain, distinguished by the algorithms each holds:

Table 6: Role identification by algorithm for OTAR

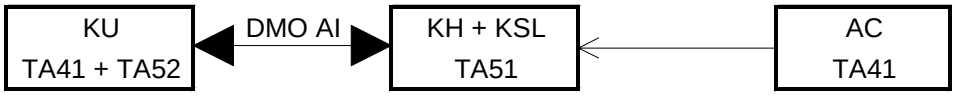
Authentication Centre	Shall contain TA41
Key Sealer	Shall contain TA51
Key User	Shall contain TA41+TA52

The Authentication Centre (AC) and Key Sealer (KSL) may be combined in one unit (this is the case in TETRA V+D). The Key User (KU) shall be a DM-MS. The actions of the AC and any interface between AC and KSL is outside the scope of this ETS.

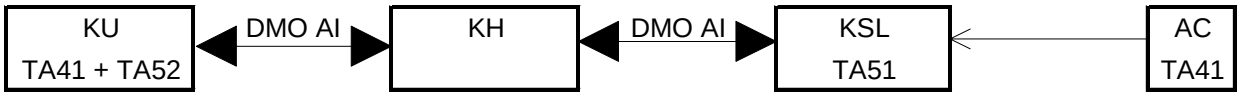
In addition there shall be a functional entity able to hold sealed keys but with no ability to manipulate them algorithmically. This shall be a Key Holder (KH).



Case 1: AC and KSL in single unit (V+D Case, NOT DEFINED IN THIS ETS)



Case 2: KH and KSL in a single unit separated from AC



Case 3: KU and KSL separated by KH

Figure 17: OTAR transmission chains

Figure 17 shows the possible OTAR cases that shall be addressed by the protocol.

A DM-MS (KU) may request one or several SCKs to be distributed from KH using the "OTAR SCK Provide" PDU.

The data held by the KU shall indicate, for each SCKN, the KH to whom KU will communicate in order to update the relevant SCK.

Table 7: Data storage requirements for each OTAR entity

KU data	SCKN
	SCK-VN
	SCK
	KH-id (ITSI)
KH data	KU-id (ITSI)
	KSL-id (ITSI)
KSL data	KU-id (ITSI)
	KH-id (ITSI)
	SCKN
	SCK-VN
	SCK
	KSO
	RSO

The KSL shall know by pre-arrangement the KSO and RSO of each ITSI it supports. It shall also know which SCKN it is allowed to update for each ITSI it supports.

The normal SCK provision cases are described by the Message Sequence Charts (MSCs) and protocol description in the following subclauses.

7.4.1 OTAR protocol models

The transport mechanism for OTAR shall be Short Data Service (SDS) with type 0101_2. A logical switch or router at the SDS entity shall direct messages as shown in figure 18:

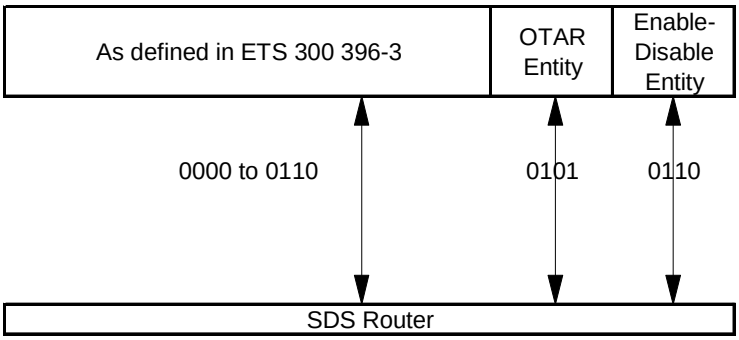


Figure 18: Routing of SDS messages to terminating entities

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

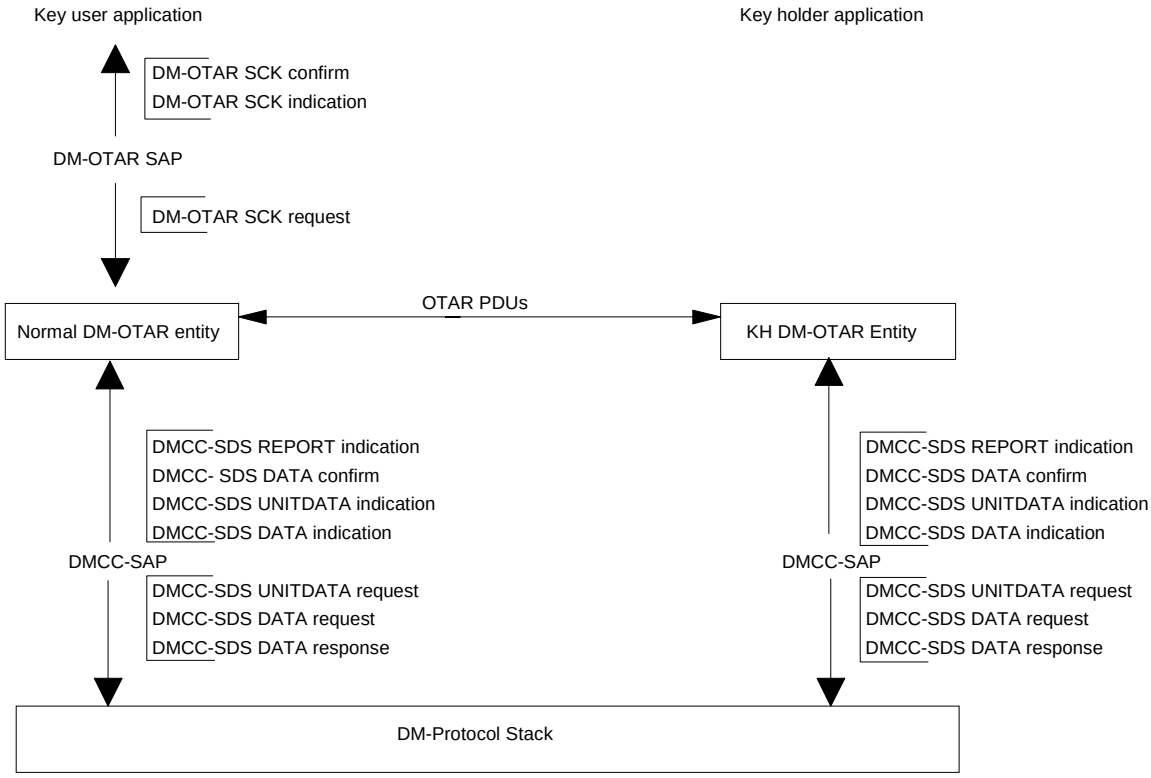


Figure 19: Model for MS to KH protocol

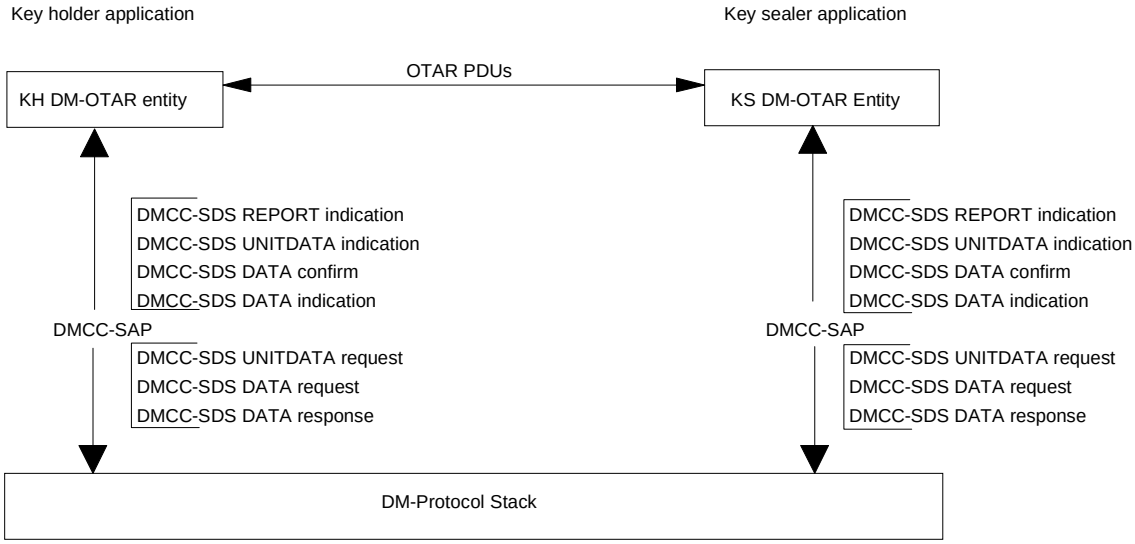


Figure 20: Model for KH to KSL protocol

7.5 OTAR Protocol MSCs

The MSCs that follow reflect the cases shown in figure 17.

- KU requests key from KH;
- KU receives unsolicited key distribution from KH;
- KU requests key from KH where KH has to go to KSL for data.

In addition the following error cases are shown:

- KU or KH experiencing SDS acknowledgement timeout;
- KSL or KH reporting SCKs are unavailable.

7.5.1 Case 1: KU requests key from KH

The normal message sequence in this case shall be according to figure 21. The indication of which SDS message contains the PDU is given for information only.

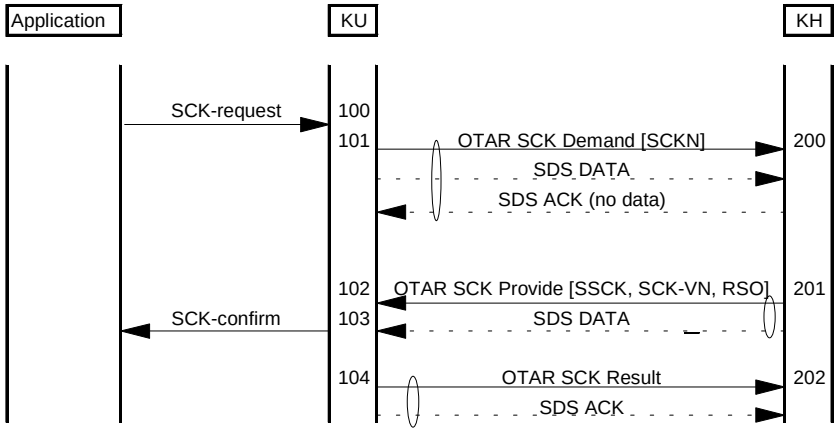


Figure 21: SCK change initiated by KU where KH has key data

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 using the OTAR SCK Demand PDU.

200 The KH shall verify that it is the correct KH for the combination of KN and SCKN.

201 The KH 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.

202 The KH may delete those SSCK that have been successfully delivered.

7.5.2 Case 2: KU requests key from KH acting as a relay for KSL

The normal message sequence in this case shall be according to figure 22. The indication of which SDS message contains the PDU is given for information only.

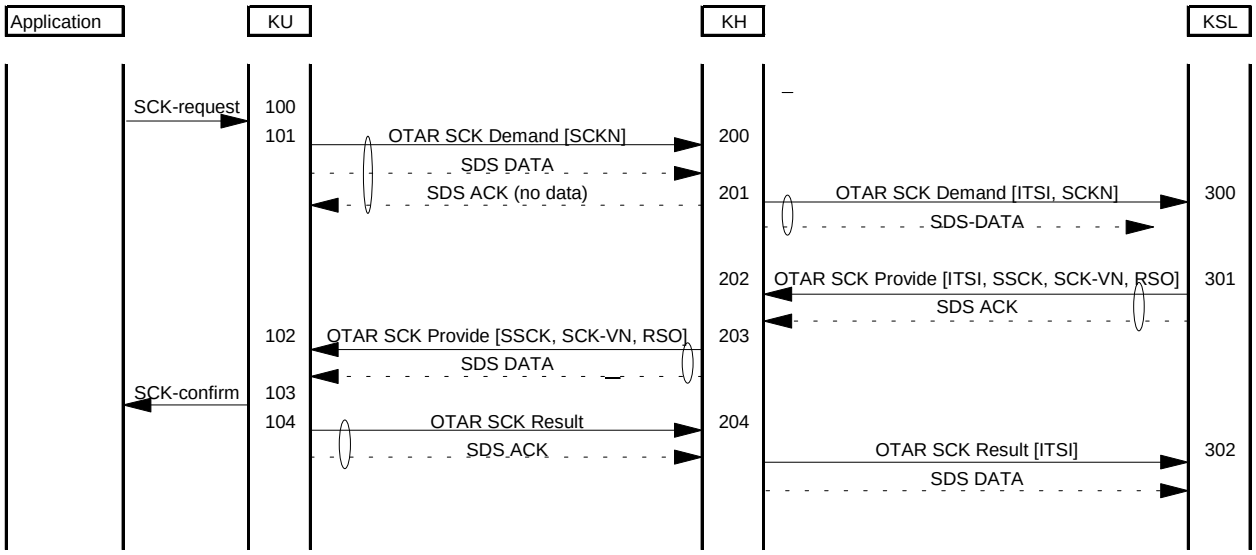


Figure 22: SCK change initiated by KU where KSL has key data

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 KSL by SCKN and ITSI

300 KSL shall check if KSO and RSO are available for the supplied ITSI, and if a new SCK is available for the indicated SCKN. If the sealing parameters are available KSL shall seal the keys using algorithm TA51.

301 KSL 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 shall 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 KSL may delete those SSCK/ITSI combinations that have been successfully provided.

7.5.3 Case 3: KH distributing SCK unsolicited

The normal message sequence in this case shall be according to figure 23. The indication of which SDS message contains the PDU is given for information only.

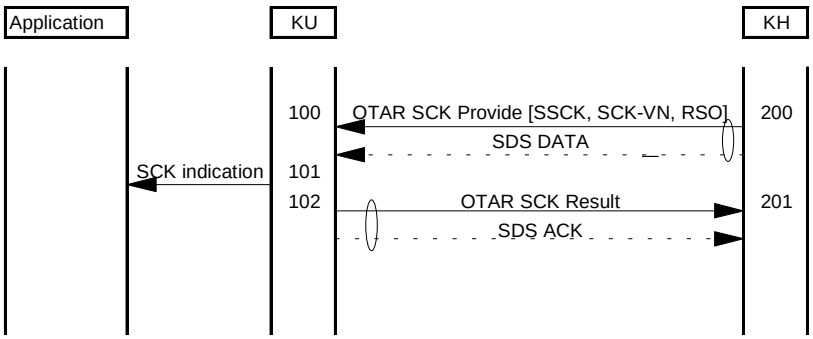


Figure 23: KH distributing SCK unsolicited

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

100 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.

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

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

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

7.5.4 Case 4: Error scenarios with SDS timeout from KU or KH

The normal message sequence in this case shall be according to figure 24. The indication of which SDS message contains the PDU is given for information only.

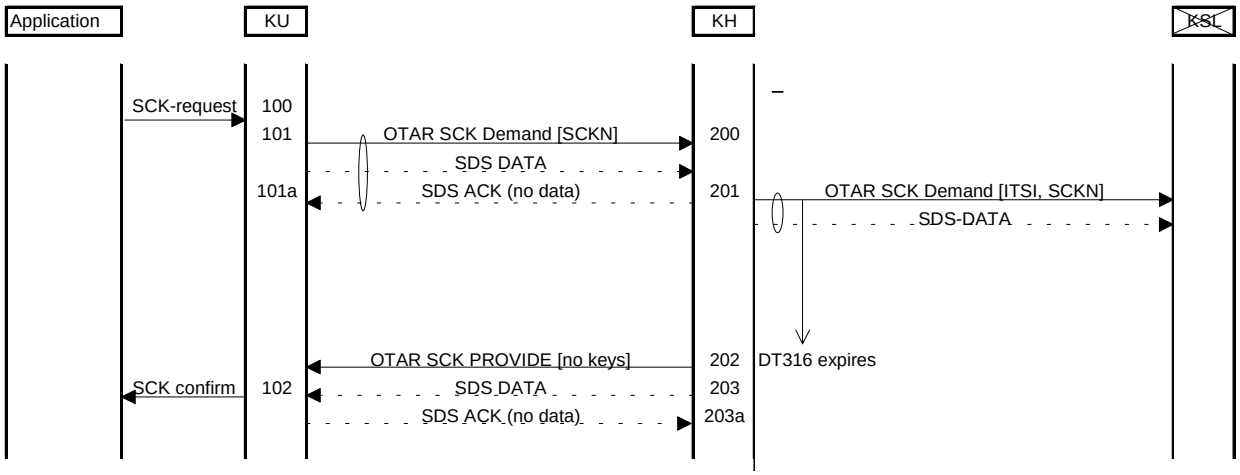


Figure 24: Error scenarios in SCK transfer

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.
101a If SDS ACK is received goto 200, else goto 102.

200 KH shall receive the demand from KU and check if the keys are already available. In this instance the keys are unavailable.

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

202 SDS-ACK not received in time DT 316. KH shall assume that KSL is unavailable.

203 The KH shall send OTAR SCK PROVIDE to KU with number of SCKs provided set to zero and result reason set as "Key sealer unavailable".

102 KU shall notify the application of the result in the DMCC-OTAR SCK Confirm primitive with result set to "KH or KSL unavailable".

7.5.5 Case 5: Error scenarios where KH provides no keys in response to demand

The normal message sequence in this case shall be according to figure 25. The indication of which SDS message contains the PDU is given for information only.

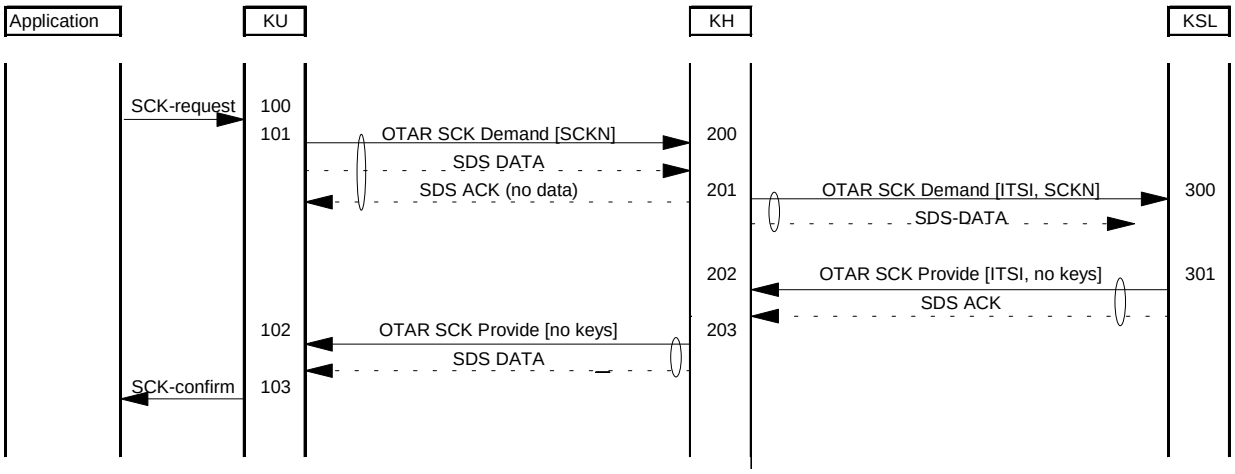


Figure 25: Error scenarios in SCK transfer

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. In this scenario the keys are not available.

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

300 KSL shall check if KSO and RSO are available for the supplied ITSI, and if a new SCK is available for the indicated SCKN. In this scenario the keys or one or more of the sealing parameters is unavailable (may have expired).

301 KSL shall send notice to KH that no keys are provided for the ITSI in the OTAR SCK Provide PDU. KSL shall not expect an OTAR SCK Result PDU from KH.

202 KH shall decode the received OTAR SCK Provide PDU and recognize that no keys are provided.

203 KH shall send notice to KU that no keys are provided in the OTAR SCK Provide PDU. KH shall not expect an OTAR SCK Result PDU from KU.

102 KU shall decode the received OTAR SCK Provide PDU and recognize that no keys are provided.

103 KU shall notify the application that not keys were received.

7.6 PDU descriptions

The PDUs detailed within this subclause shall be visible at the Ud reference point (see ETS 300 396-1 [3], 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, KSL to KH
Service used: SDS
Response to: OTAR SCK Demand or none
Response expected: OTAR SCK Result

Table 8: 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	
SCK key and identifier	141	1	C	note 2
Provision result	3	1	C	If number of SCKs provided = 000_2
ITSI flag	1	1	M	note 1
ITSI	48	1	C	note 1
Proprietary element		3	O	

NOTE 1: If the PDU is sent from KSL to KH on behalf of KU the ITSI of KU shall be included (ITSI flag shall be true, else ITSI flag shall be false).

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 Demand

Shall be used by KU to request SCK from KH.

Direction: KU to KH, KH to KSL
Service used: SDS
Response to: none
Response expected: OTAR SCK Provide

Table 9: OTAR SCK Demand PDU contents

Information Element	Length	Type	C/O/M	Remark
OTAR SCK sub-type	3	1	M	Demand
ITSI flag	1	1	M	note 1
ITSI	48	1	C	note 1
Number of SCKs requested	3	1	M	
SCK number (SCKN)	5	1	C	note 2
Proprietary element		3	O	

NOTE 1: If the PDU is sent from KH to KSL on behalf of KU the ITSI of KU shall be included (ITSI flag shall be true, else ITSI flag shall be false).

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.

7.6.3 OTAR SCK Result

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

Direction: KU to KH, KH to KSL
Service used: SDS
Response to: OTAR SCK Provide
Response expected: none

Table 10: OTAR SCK Result PDU contents

Information Element	Length	Type	C/O/M	Remark
OTAR SCK sub-type	3	1	M	Result
ITSI flag	1	1	M	note 1
ITSI	48	1	C	note 1
Number of SCKs requested	3	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 KSL on behalf of KU the ITSI of KU shall be included (ITSI flag shall be true, else ITSI flag shall be false).

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 7.6 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 as defined in table 11:

Table 11: 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 ITSI

The subscriber identity.

Table 12: ITSI element contents

Information Element	Length	Type	C/O/M	Remark
Short Subscriber Identity	24	1	M	
Address extension	24	1	M	

7.7.3 ITSI flag

This element is used top indicate the presence in the PDU of the conditional element ITSI.

Table 13: ITSI flag element contents

Information Element	Length	Value	Remark
ITSI flag	1	0	ITSI not provided
		1	ITSI provided

7.7.4 Mobile country code

The mobile country code of a TETRA network. For a full definition see ETS 300 396-1 [3], clause 6.

Table 14: Mobile country code element contents

Information element	Length	Value	Remark
Mobile country code	10	any	

7.7.5 Mobile network code

The mobile network code of a TETRA network. For a full definition see ETS 300 396-1 [3], clause 6.

Table 15: Mobile network code element contents

Information element	Length	Value	Remark
Mobile network code	14	any	

7.7.6 Number of SCKs provided

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

Table 16: 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

7.7.7 Number of SCKs requested

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

Table 17: Number of SCKs requested element contents

Information element	Length	Value	Remark
Number of SCKs requested	3	000_2	Reserved
		001_2	1 SCK requested
		010_2	2 SCKs requested
		011_2	3 SCKs requested
		100_2	4 SCKs requested
		others	Reserved

7.7.8 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 18: 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

7.7.9 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 ETS.

7.7.10 Provision result

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

Table 19: 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	KH or KSL unavailable
		101_2 to 111_2	Reserved

7.7.11 Random seed (OTAR)

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 KSL to KH, and from KH to MS.

Table 20: Random seed element contents

Information element	Length	Value	Remark
Random seed (OTAR) [RSO]	80	Any	

7.7.12 SCK key and identifier

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

Table 21: 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	

7.7.13 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 22: 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

7.7.14 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 23: 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	

7.7.15 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 24: SCK version number element contents

Information element	Length	Value	Remark
SCK version number	16	Any	

7.7.16 Sealed Key

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

Table 25: Sealed Key element contents

Information element	Length	Value	Remark
Sealed Key	120	Any	

7.7.17 Session key (OTAR)

The session key is derived from the secret "K".

Table 26: Session key element contents

Information element	Length	Value	Remark
Session key (OTAR) [KSO]	128	Any	

7.7.18 Short subscriber identity

The short form of the subscriber's identity. For a full definition see ETS 300 396-1 [3], clause 6.

Table 27: Short subscriber identity element contents

Information element	Length	Value	Remark
Short subscriber identity	24	any	

8 Secure Enable and Disable mechanism

NOTE: An enable or disable applied to a subscription or an equipment in DMO will also apply in V+D and vice-versa.

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 AI. The disablement may be of two classes: permanent; and temporary.

There may a number of reasons for wishing to disable a DM-MS: 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 they are one way (there may be others) of performing it.

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

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

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 manager shall initiate an authentication exchange on making any enable-disable request. The target shall make the authentication mutual. The authentication shall be based upon a secret key known by pre-arrangement to the manager and target;

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

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 26. 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 [3], clause 6.

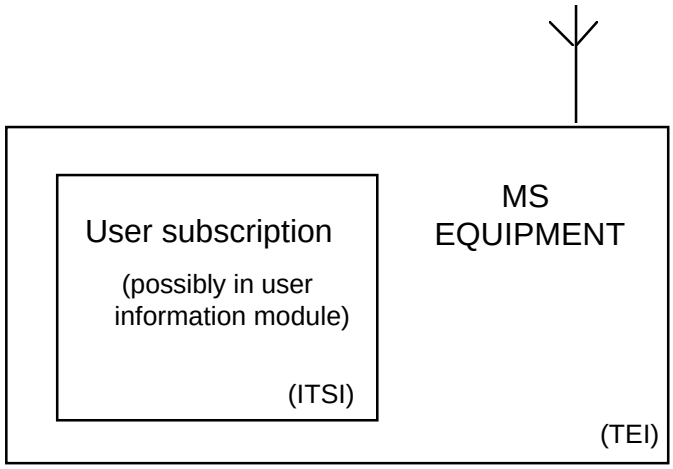
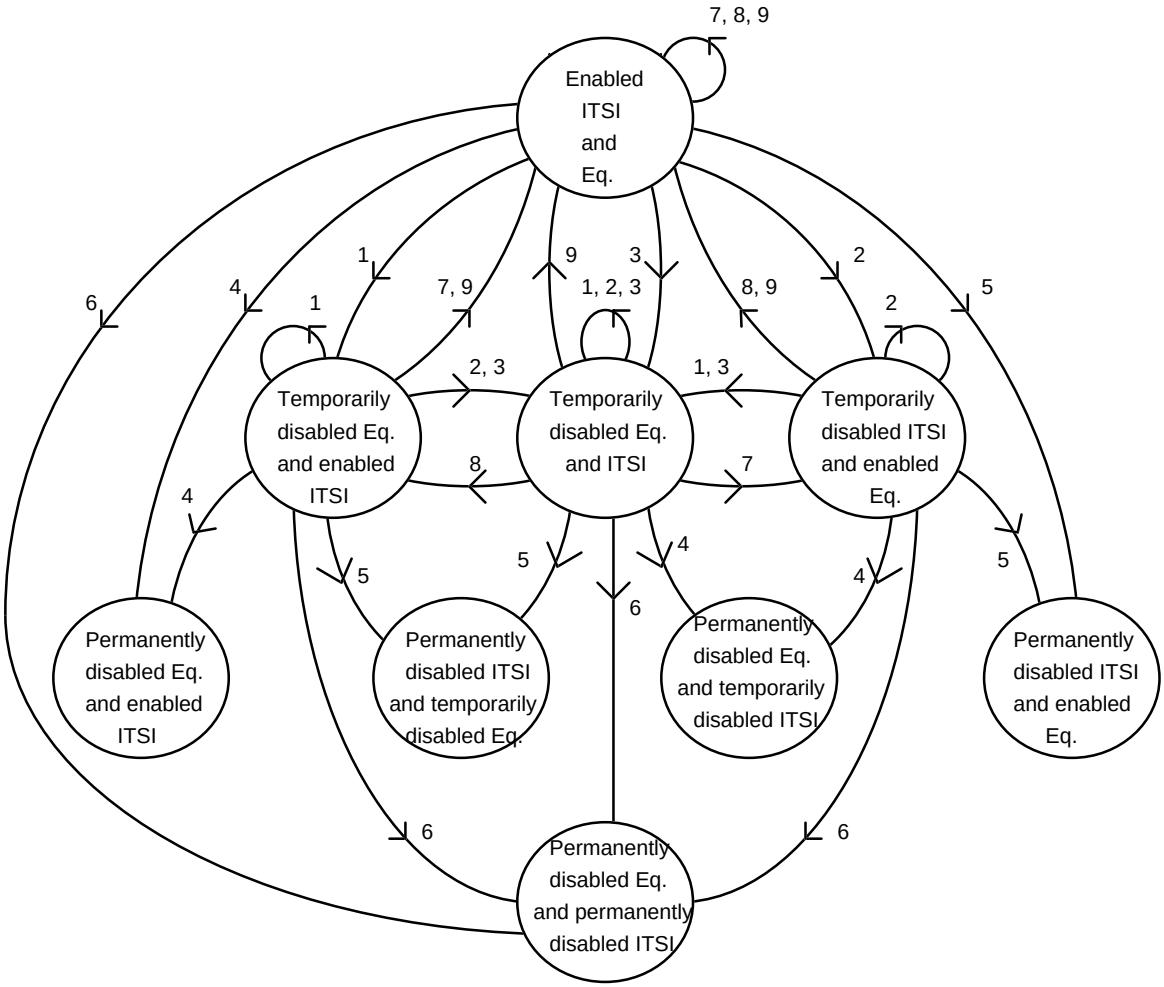


Figure 26: Relationship of TEI and ITSI in DM-MS

8.3 Enable/Disable state transitions

The state diagram in figure 27 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.



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 27: 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 AI encryption applied to avoid visibility of the TEI at the AI.

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 manager 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 manager 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. Equipments, 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 manager 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 subclause 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 subclause 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.

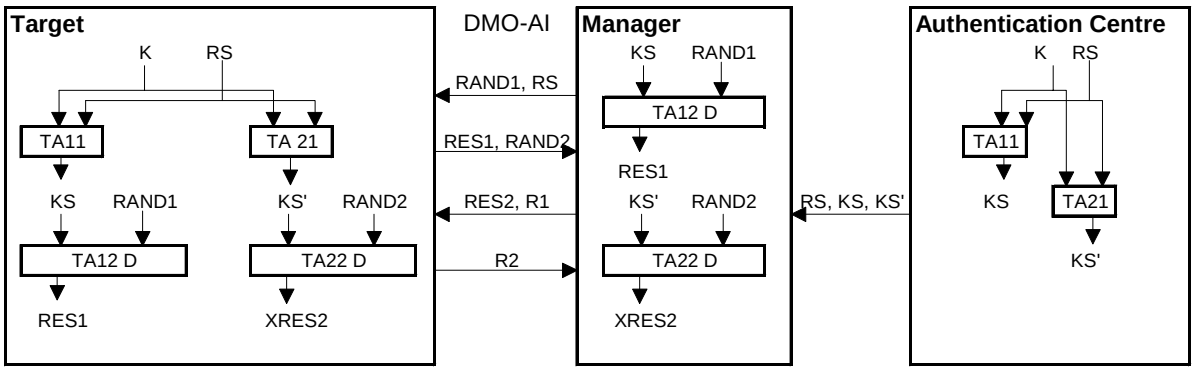
8.5 Enable/disable authentication mechanism

The authentication mechanism shall follow that defined in ETS 300 392-7 [5], subclause 4.1.4. There shall be three roles defined: Authentication centre; Manager; Target. Each role shall be identified by the algorithms the holding entity has:

Table 28: Role identification by algorithm for enable-disable

Authentication centre	Shall contain TA11 and TA21.
Manager	Shall contain TA12-D and TA22-D
Target	Shall contain TA11, TA12-D, TA21 and TA22-D

Authentication shall always be mutual and shall be initiated by the manager.



NOTE 1: The algorithms TA11, TA12-D, TA21 and TA22-D can be the same as those defined in ETS 300 392-7 with some outputs ignored.

NOTE 2: The authentication centre can be the same entity as that defined for OTAR in subclause 7.4.

NOTE 3: The actions of the AC, and the interface between the AC and the manager are outside the scope of this ETS.

Figure 28: Mutual authentication initiated by the manager

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.

The elements are present as follows:

Table 29: 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 30: DM-ENDIS-T parameters

Parameter	Indication
Result	M

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

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
- Enable rejected, invalid TEI
- Enable rejected, invalid ITSI
- Disable rejected, invalid TEI
- Disable rejected, invalid ITSI

ITSI =
- 0
- 1
- 2
- …
- $2^{48}-1$

Enable/Disable =
- Enable
- Disable

Class =
- Permanent TEI
- Temporary TEI
- Permanent ITSI
- Temporary ITSI

A service shall be provided to DMCC to inhibit and enable the communication protocol layers as follows:

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.

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 29.

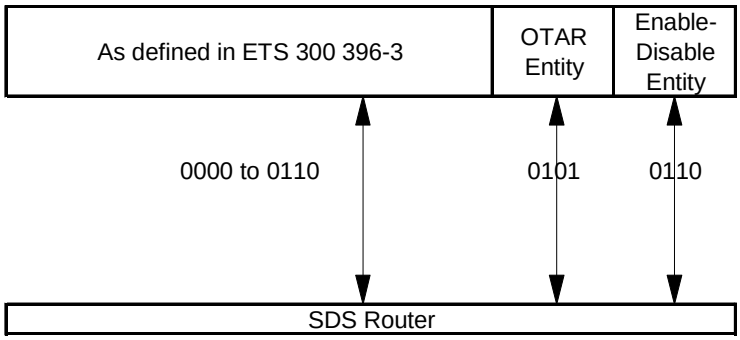


Figure 29: Routing of SDS messages to terminating entities

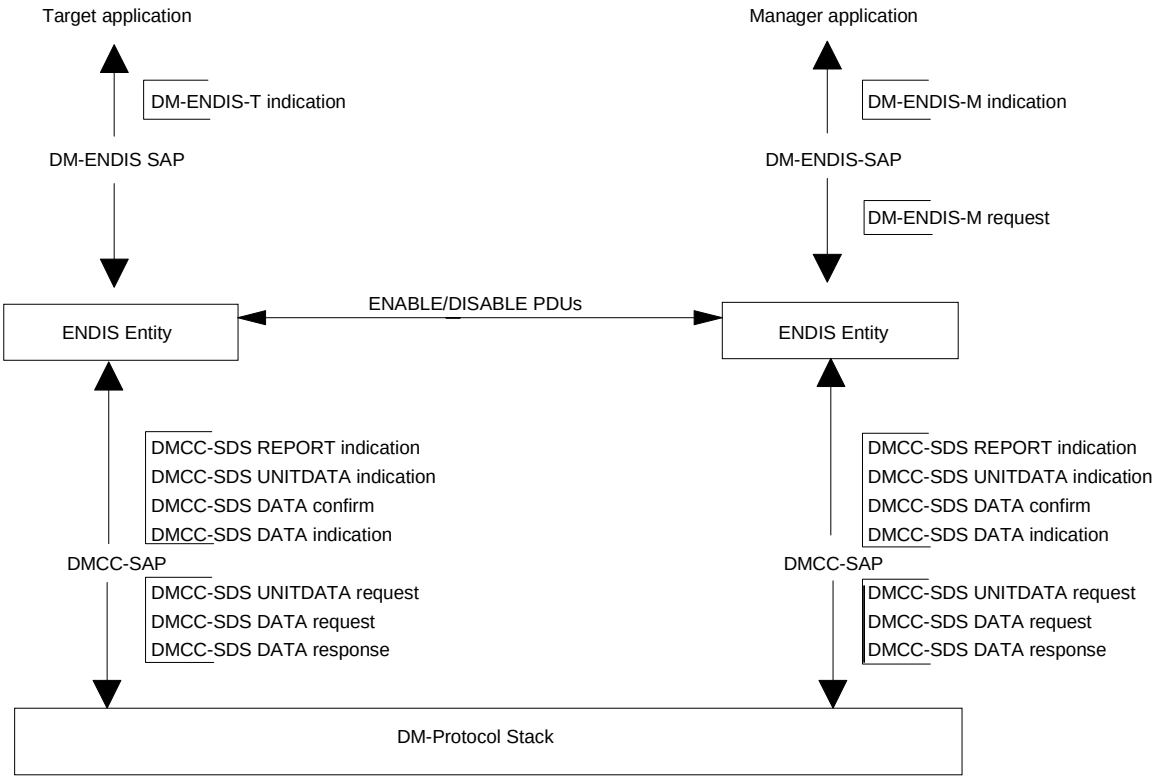


Figure 30: Model for manger to target protocol

The transport mechanism for ENABLE/DISABLE PDUs in DMO shall be acknowledged SDS with SDS message type 6 (0110_2) as shown in figure 29.

8.7.3 Specific Protocol Exchanges

The following exchanges are described for enable and disable:

1) Disable equipment temporarily with mutual authentication

2) Disable equipment permanently with mutual authentication

3) Disable subscriber temporarily with mutual authentication

4) Disable subscriber permanently with mutual authentication

5) Disable equipment and subscriber temporarily with mutual authentication

6) Disable equipment and subscriber permanently with mutual authentication

7) Enable equipment with mutual authentication

8) Enable subscriber with mutual authentication

9) Enable equipment and subscriber with mutual authentication

10) Provide TEI with mutual authentication

11) Failure with TEI mismatch

12) Failure with ITSI mismatch

Prior to performing an enable or disable of TEI the manager should ensure that the TEI-ITSI pairing is known and confirmed. Whilst this relationship may have been given by pre-arrangement there is no guarantee that an ITSI (held on a removable device) has not been inserted in a new equipment. Therefore before enabling or disabling an equipment the manager should first request TEI from the prospective target.

8.7.3.1 Successful disabling of a target with mutual authentication

NOTE 1: The target in this case can be ITSI, TEI or ITSI and TEI.

NOTE 2: The disabling can be permanent or temporary.

The protocol is shown in figure 31 and described below.

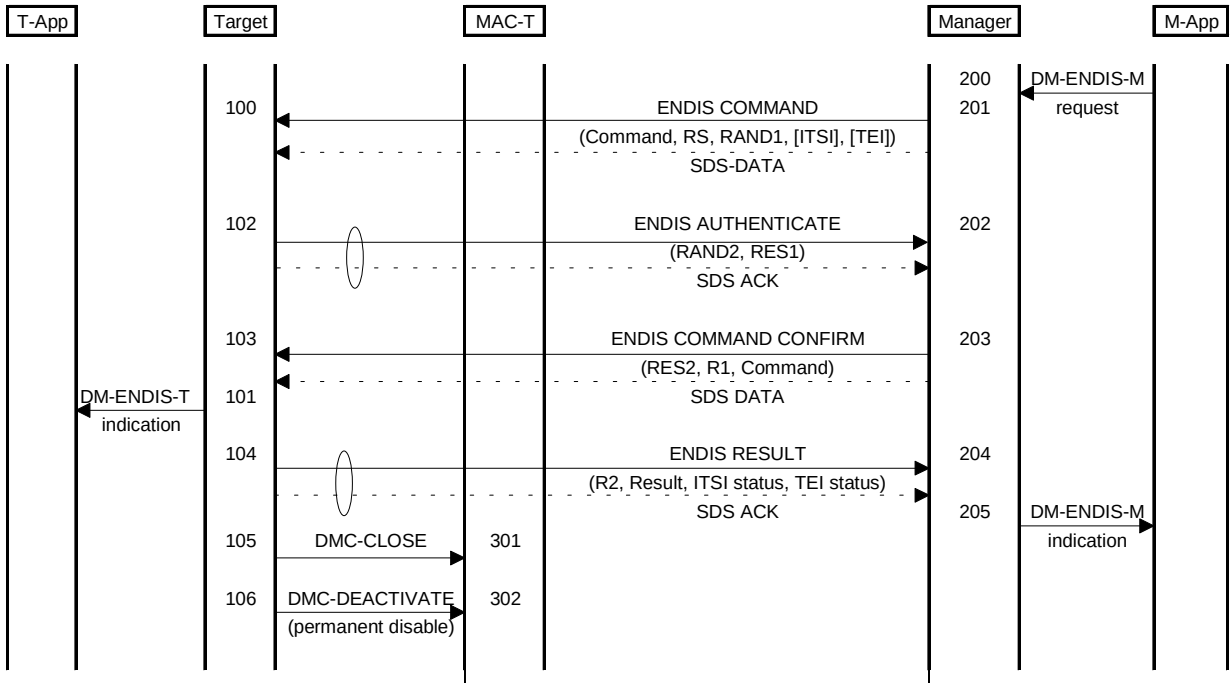


Figure 31: Disabling a target

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, the authentication seed RS and the authentication challenge RAND1 to the target using the ENDIS COMMAND PDU. The manager shall run algorithm TA12 to determine XRES1.

100 The target application shall decode the command received from the manager. It shall use inputs RS and RAND1 in algorithms TA11 and TA12 (with the stored secret key, K) to generate RES1. It shall also generate the mutual authentication challenge RAND2, and using this generate XRES2.

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

102 The target application shall challenge (RAND2) the manager to authenticate itself using the ENDIS AUTHENTICATE PDU, and also return the authentication response RES1.

202 The manager shall compare the received XRES1 and RES1 to give R1. The manager shall use KS' RS and RAND2 to generate RES2 using algorithm TA22.

203 The manager shall confirm the enable/disable command by sending R1, RES2 and command in the ENDIS CONFIRM PDU.

103 The target shall compare XRES2 and RES2 to give R2. If R2=R1=TRUE and the received confirmed command is equal to the original received command then the target shall act on the command.

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

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 ENDIS RESULT PDU.

204 The manger application shall decode the ENDIS RESULT PDU from 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 Successful enabling of a target with mutual authentication

NOTE: The target in this case can be ITSI, TEI or ITSI and TEI.

The protocol is shown in figure 32 and described below.

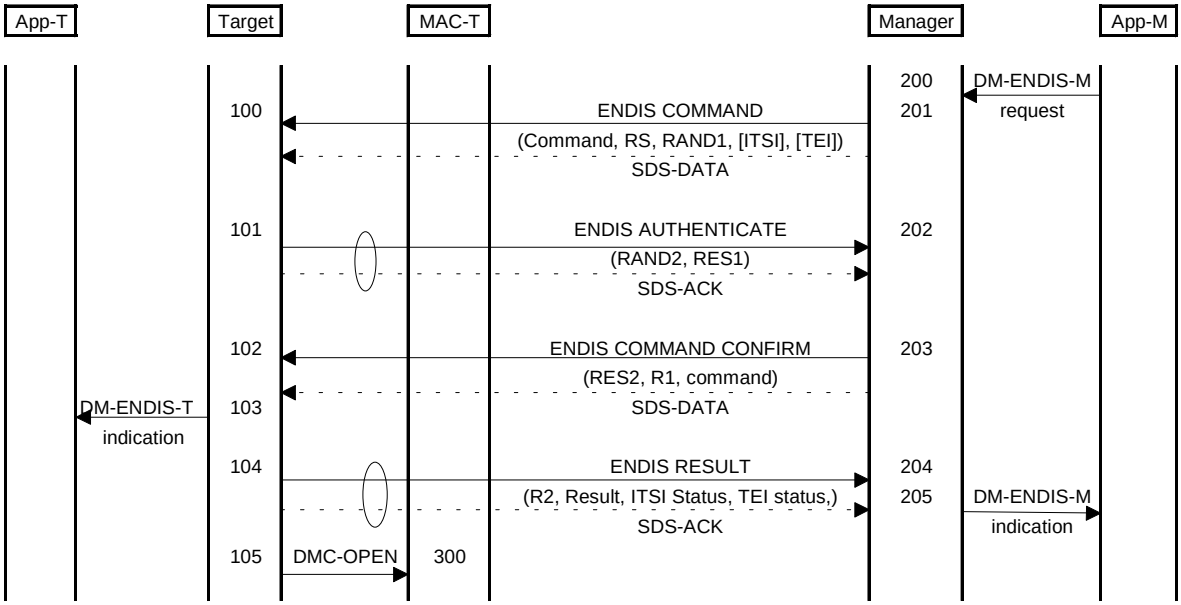


Figure 32: Enabling a target

200 The user application shall request the manager application to enable a previously temporarily disabled target by ITSI, TEI, or both.

201 The manager application shall send the command, the authentication seed RS and the authentication challenge RAND1 to the target using the ENDIS COMMAND PDU. The manager shall run algorithm TA12 to determine XRES1.

100 The target application shall decode the command received from the manager. It shall use inputs RS and RAND1 in algorithms TA11 and TA12 (with the stored secret key, K) to generate RES1. It shall also generate the mutual authentication challenge RAND2, and using this generate XRES2.

101 The target application shall challenge (RAND2) the manager to authenticate itself using the ENDIS AUTHENTICATE PDU, and also return the authentication response RES1.

202 The manager shall compare the received XRES1 and RES1 to give R1. The manager shall use KS' RS and RAND2 to generate RES2 using algorithm TA22.

203 The manager shall confirm the enable/disable command by sending R1, RES2 and command in the ENDIS CONFIRM PDU.

102 The target shall compare XRES2 and RES2 to give R2. If R2=R1=TRUE and the received confirmed command is equal to the original received command then the target shall act on the command.

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

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 ENDIS RESULT PDU.

204 The manger application shall decode the ENDIS RESULT PDU from the target and may update its local database.

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

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

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

8.7.3.3 Successful delivery of TEI with mutual authentication

The protocol is shown in figure 33 and described below.

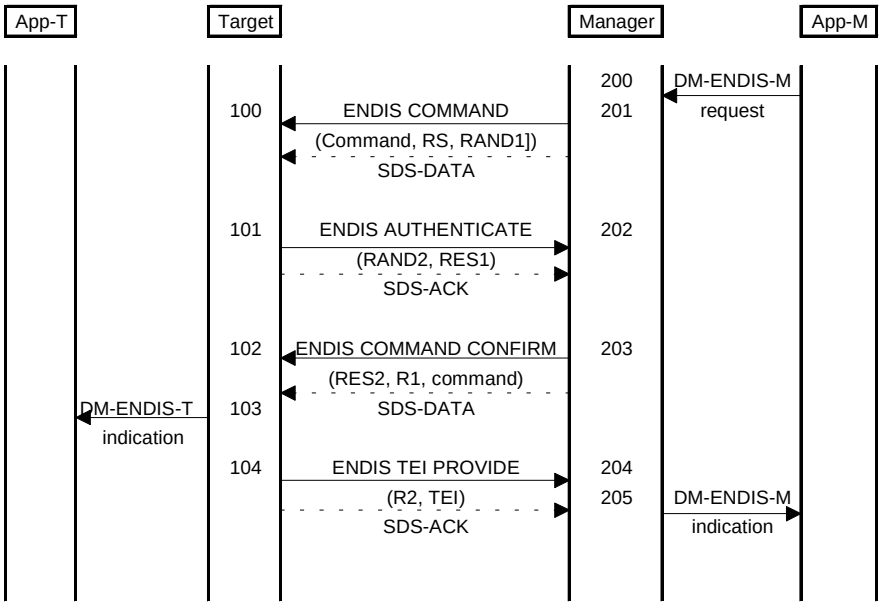


Figure 33: Delivery of TEI

200 The user application shall request the manager application to recover the TEI of a subscriber.

201 The manager application shall send the command, the authentication seed RS and the authentication challenge RAND1 to the target using the ENDIS COMMAND PDU. The manager shall run algorithm TA12 to determine XRES1.

100 The target application shall decode the command received from the manager. It shall use inputs RS and RAND1 in algorithms TA11 and TA12 (with the stored secret key, K) to generate RES1. It shall also generate the mutual authentication challenge RAND2, and using this generate XRES2.

101 The target application shall challenge (RAND2) the manager to authenticate itself using the ENDIS AUTHENTICATE PDU, and also return the authentication response RES1.

202 The manager shall compare the received XRES1 and RES1 to give R1. The manager shall use KS' RS and RAND2 to generate RES2 using algorithm TA22.

203 The manager shall confirm the enable/disable command by sending R1, RES2 and command in the ENDIS CONFIRM PDU.

102 The target shall compare XRES2 and RES2 to give R2. If R2=R1=TRUE and the received confirmed command is equal to the original received command then the target shall act on the command.

103 The target application shall inform the user application of the intent of the received command.

104 The target shall inform the manger application of the result of the authentication process and shall send the result (R2) and TEI in the ENDIS TEI PROVIDE PDU.

204 The manger application shall decode the ENDIS TEI PROVIDE PDU from the target and may update its local database.

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

8.7.3.4 Rejection of ENDIS command

The protocol is shown in figure 34 and described below.

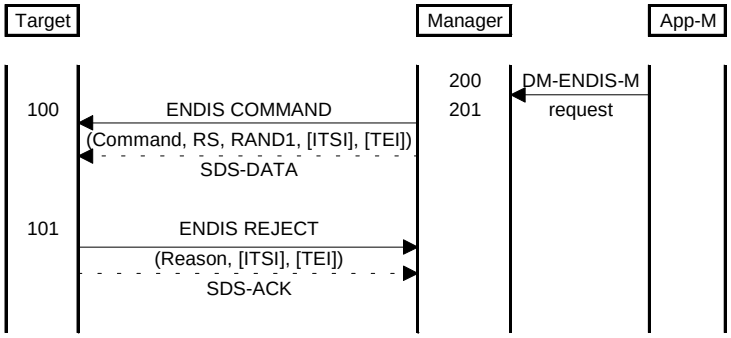


Figure 34: Rejecting a command

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, the authentication seed RS and the authentication challenge RAND1 to the target using the ENDIS COMMAND PDU. The manager shall run algorithm TA12 to determine XRES1.

100 The target application shall decode the command received from the manager. If the ITSI, TEI or command is invalid then the command shall be rejected.

101 The target application shall send the ENDIS REJECT PDU to the manager with the reason why the command is rejected.

8.7.3.5 Authentication failure during ENDIS exchange

If any authentication exchange fails the sequence shall be as described in figure 35.

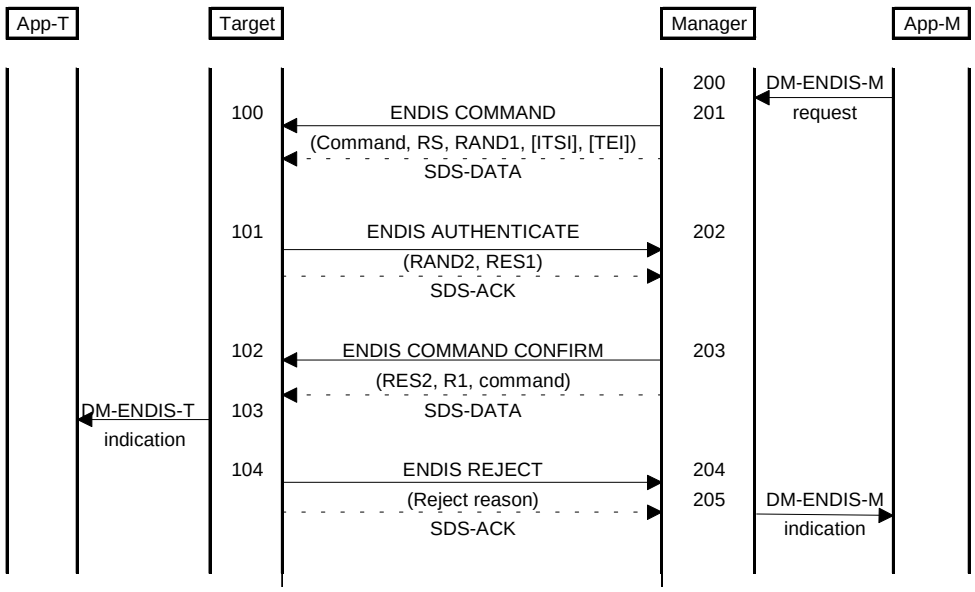


Figure 35: Treating authentication failure during ENDIS exchange

200 The user application shall request the manager application to make any ENDIS command.

201 The manager application shall send the command, the authentication seed RS and the authentication challenge RAND1 to the target using the ENDIS COMMAND PDU. The manager shall run algorithm TA12 to determine XRES1.

100 The target application shall decode the command received from the manager. It shall use inputs RS and RAND1 in algorithms TA11 and TA12 (with the stored secret key, K) to generate RES1. It shall also generate the mutual authentication challenge RAND2, and using this generate XRES2.

101 The target application shall challenge (RAND2) the manager to authenticate itself using the ENDIS AUTHENTICATE PDU, and also return the authentication response RES1.

202 The manager shall compare the received XRES1 and RES1 to give R1. The manager shall use KS' RS and RAND2 to generate RES2 using algorithm TA22.

203 The manager shall confirm the enable/disable command by sending R1, RES2 and command in the ENDIS CONFIRM PDU.

102 The target shall compare XRES2 and RES2 to give R2. If R2 OR R1 is FALSE, or if the received confirmed command is not equal to the original received command then the target shall indicate failure of the exchange.

103 The target application shall inform the user application of the intent of the received command.

104 The target shall inform the manger application of the result of the authentication process and reject the command using the ENDIS REJECT PDU with reject reason set accordingly.

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 ENDIS COMMAND

Message: ENDIS COMMAND
Response to: -
Response expected: ENDIS AUTHENTICATE or ENDIS REJECT
Message path: From manager to target
Short description: The message is sent by the manager to indicate that the target shall be disabled (permanently or temporarily) or enabled, or to request a TEI.

Table 31: ENDIS COMMAND contents

Information element	Length	Type	C/O/M	Remark
ENDIS PDU type	3	1	M	000_2
Command	6	1	M	Multi field element
Random seed (RS)	80	1	M	
Authentication challenge (RAND1)	80	1	M	
ITSI	48	1	C	If command application = 01_2 or 11_2
TEI	60	1	C	If command application = 10_2 or 11_2
Proprietary		3	O	

8.7.4.2 ENDIS AUTHENTICATE

Message: ENDIS AUTHENTICATE
Response to: ENDIS COMMAND
Response expected: ENDIS COMMAND CONFIRM
Message path: From target to manager
Short description: The message is sent by the target to authenticate the manager before accepting and acting upon a command

Table 32: ENDIS AUTHENTICATE contents

Information element	Length	Type	C/O/M	Remark
ENDIS PDU type	3	1	M	001_2
Authentication challenge (RAND2)	80	1	M	
Authentication response RES1		1	M	
Proprietary		3	O	

8.7.4.3 ENDIS COMMAND CONFIRM

Message: ENDIS COMMAND CONFIRM
Response to: ENDIS AUTHENTICATE
Response expected: ENDIS STATUS or ENDIS TEI PROVIDE
Message path: From manager to target
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 33: ENDIS COMMAND CONFIRM contents

Information element	Length	Type	C/O/M	Remark
ENDIS PDU type	3	1	M	010_2
Command	6	1	M	
Authentication response (RES2)	32	1	M	
Authentication result (R1)	1	1	M	
Proprietary		3	O	

8.7.4.4 ENDIS RESULT

Message: ENDIS RESULT
Response to: ENDIS COMMAND CONFIRM
Response expected: None
Message path: From target to manager
Short description: The message is sent by the target to inform the manager of the result of an enable or disable command, and the status of the target as a result of that command.

Table 34: ENDIS RESULT contents

Information element	Length	Type	C/O/M	Remark
ENDIS PDU type	3	1	M	011_2
Authentication result (R2)	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	1	1	M	
Reject reason	3	1	C	Present if Enable/disable result = failure
Proprietary		3	O	

8.7.4.5 ENDIS TEI PROVIDE

Message: ENDIS TEI PROVIDE
Response to: ENDIS COMMAND CONFIRM
Response expected: None
Message path: From target to manager
Short description: The message is sent by the target to give the manager its TEI.

Table 35: ENDIS TEI PROVIDE contents

Information element	Length	Type	C/O/M	Remark
ENDIS PDU type	3	1	M	101_2
Authentication result (R2)	1	1	M	
TETRA Equipment Identity	60	1	M	
Proprietary		3	O	

8.7.4.6 ENDIS REJECT

Message: ENDIS REJECT
Response to: ENDIS COMMAND
Response expected: None
Message path: From target to manager
Short description: The message is sent by the target to inform the manager of its response to an enable or disable request.

Table 36: ENDIS REJECT contents

Information element	Length	Type	C/O/M	Remark
ENDIS PDU type	3	1	M	100_2
Reject reason	3	1	M	
ITSI	48	1	C	
TETRA Equipment Identity	60	1	C	
Proprietary		3	O	

8.7.5 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 37: Address Extension element contents

Information sub element	Length	Value	Remark
Mobile Country Code (MCC)	10	any	
Mobile Network Code (MNC)	14	any	

8.7.5.2 Authentication challenge

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

Table 38: Authentication challenge element contents

Information sub element	Length	Value	Remark
Random challenge RAND	80	any	

8.7.5.3 Authentication response

The Authentication response element shall contain the output of algorithms TA11 and TA12 (RES).

Table 39: Authentication challenge element contents

Information sub element	Length	Value	Remark
Authentication response (RES)	32	any	

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 40: Authentication challenge element contents

Information sub element	Length	Value	Remark
Authentication result (R)	1	0	Fail
		1	Success

8.7.5.5 Command

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

Table 41: Command element contents

Information element	Length	Value	Remark
Command sub-type	2	00_2	Enable
		01_2	Disable
		10_2	Provide TEI (note 2)
		11_2	Reserved
Command application	2	00	Reserved (also by default)
		01	Command applies to subscription
		10	Command applies to equipment
		11	Command applies to equipment and
Temporary/Permanent Disable	1	0	Temporary disable (default) (note 1)
		1	Permanent Disable
Reserved for expansion	1		Value of 0 by default
NOTE 1: The temporary enable/disable bit has no meaning for command sub-types 00_2 and 10_2.			
NOTE 2: If command sub-type is Provide TEI then all remaining fields shall be set to 0.			

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 42: Enable/Disable result element contents

Information element	Length	Value	Remark
Enable/Disable result	1	0	Successful
		1	Fail

8.7.5.7 ENDIS PDU type

This element indicates the specific ENDIS class PDU.

Table 43: ENDIS PDU type element contents

Information element	Length	Value	Remark
ENDIS PDU type	3	000_2	ENDIS COMMAND
		001_2	ENDIS AUTHENTICATE
		010_2	ENDIS COMMAND CONFIRM
		011_2	ENDIS RESULT
		100_2	ENDIS REJECT
		101_2	ENDIS TEI PROVIDE
		110_2	Reserved
		111_2	Reserved

8.7.5.8 Equipment status

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

Table 44: 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

8.7.5.9 ITSI

The subscriber identity.

Table 45: ITSI element contents

Information Element	Length	Type	C/O/M	Remark
Short Subscriber Identity	24	1	M	
Address extension	24	1	M	

8.7.5.10 Mobile country code

The mobile country code of a TETRA network. For a full definition see ETS 300 396-1 [3], clause 6.

Table 46: Mobile country code element contents

Information element	Length	Value	Remark
Mobile country code	10	any	

8.7.5.11 Mobile network code

The mobile network code of a TETRA network. For a full definition see ETS 300 396-1 [3], clause 6.

Table 47: Mobile network code element contents

Information element	Length	Value	Remark
Mobile network code	14	any	

8.7.5.12 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.

8.7.5.13 Random seed

The random seed is an 80 bit number used as the input to the session key generation algorithm, which is used in the authentication process.

Table 48: Random seed element contents

Information element	Length	Value	Remark
Random seed [RS]	80	Any	

8.7.5.14 Reject reason

This is used to inform the manager of a major error in the ENDIS process.

Table 49: Reject reason element contents

Information element	Length	Value	Remark
Reject reason	3	000_2	Reserved
		001_2	Invalid TEI
		010_2	Authentication error (R1=FALSE)
		011_2	Authentication error (R2=FALSE)
		100_2	Invalid command
		101_2 to 111_2	Reserved

8.7.5.15 Session key

The session key is derived from the secret "K".

Table 50: Session key element contents

Information element	Length	Value	Remark
Session key [KS or KS']	128	Any	

8.7.5.16 Short subscriber identity

The short form of the subscriber's identity. For a full definition see ETS 300 396-1 [3], clause 6.

Table 51: Short subscriber identity element contents

Information element	Length	Value	Remark
Short subscriber identity	24	any	

8.7.5.17 Subscription status

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

Table 52: 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

8.7.5.18 TETRA equipment identity

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

Table 53: TETRA Equipment Identity element contents

Information element	Length	Value	Remark
TETRA Equipment Identity	60		See ETS 300 392-1 [8] 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 may 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 and U-plane signalling. The method described shall use the Stealing Channel, STCH, for synchronization during transmission (see ETS 300 396-3 [6], 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 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 36. 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 AI 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.

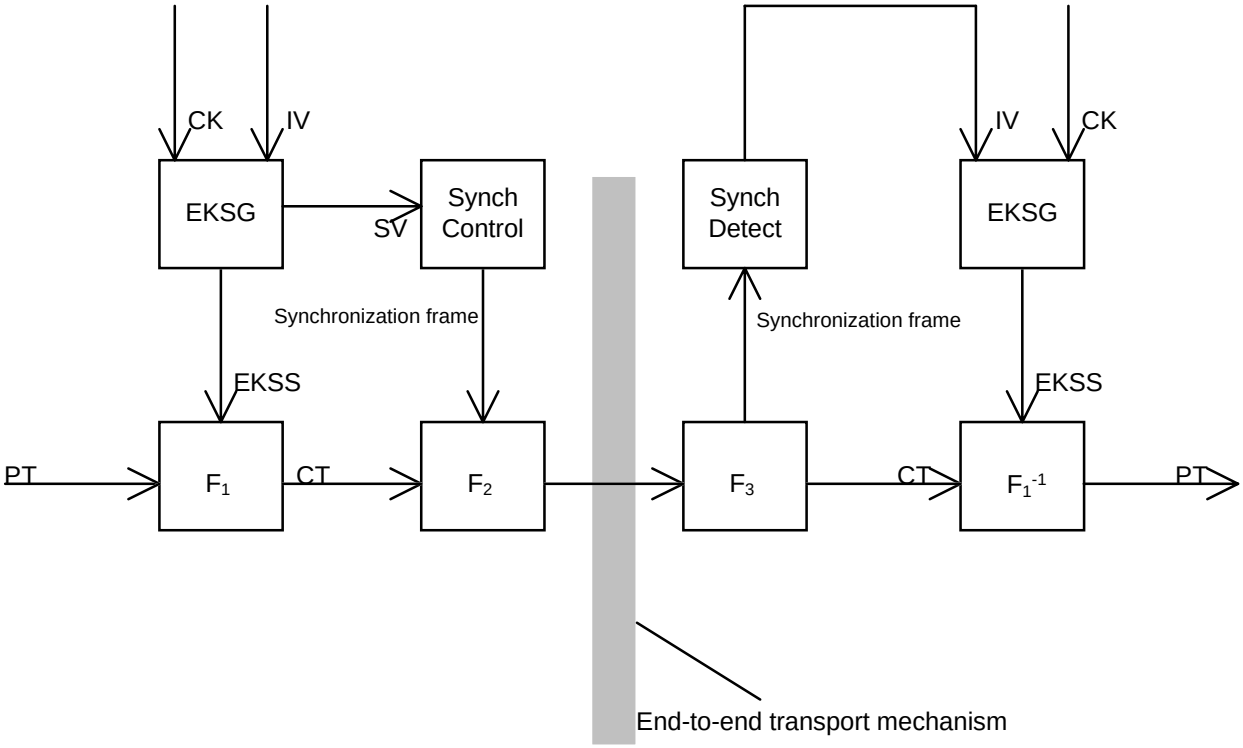


Figure 36: Functional diagram of voice encryption and decryption mechanisms

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 36 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 [6], 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 54.

Table 54: 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 55.

Table 55: 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. Synchronization frames 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 54.

Further communication from MAC to the U-plane shall use the DMD-REPORT primitive as shown in table 55.

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 56 should be followed, however no more than four half-slots should be stolen per second:

Table 56: 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 AI to allow the receiving MS to recognize a stolen frame.

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

Figure 37 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 s after the last transmission of an SV. More SV's may be transmitted to improve reliability of synchronization and to allow for late entry.

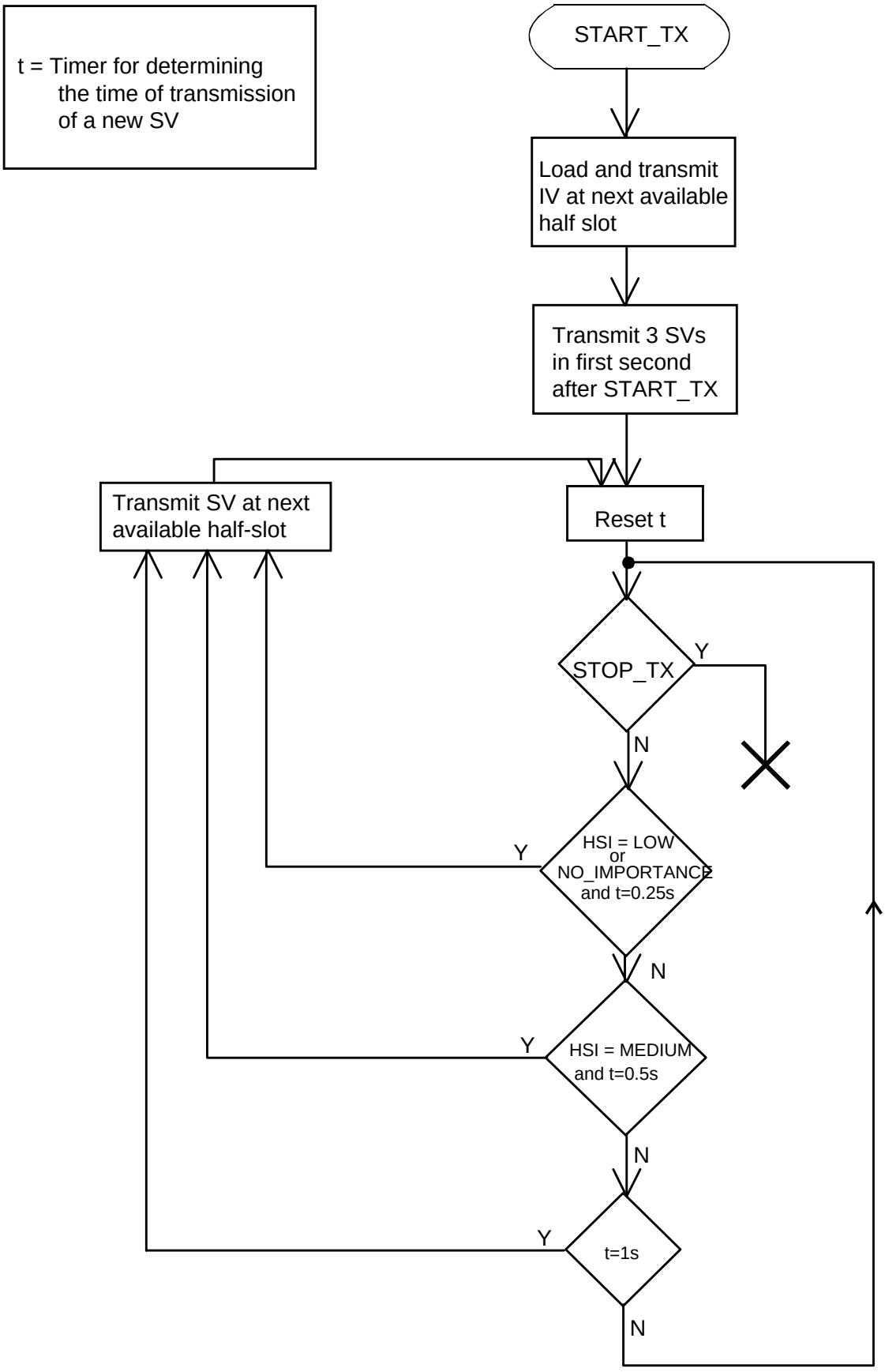


Figure 37: Flow chart of an example transmitter "sync-control" process

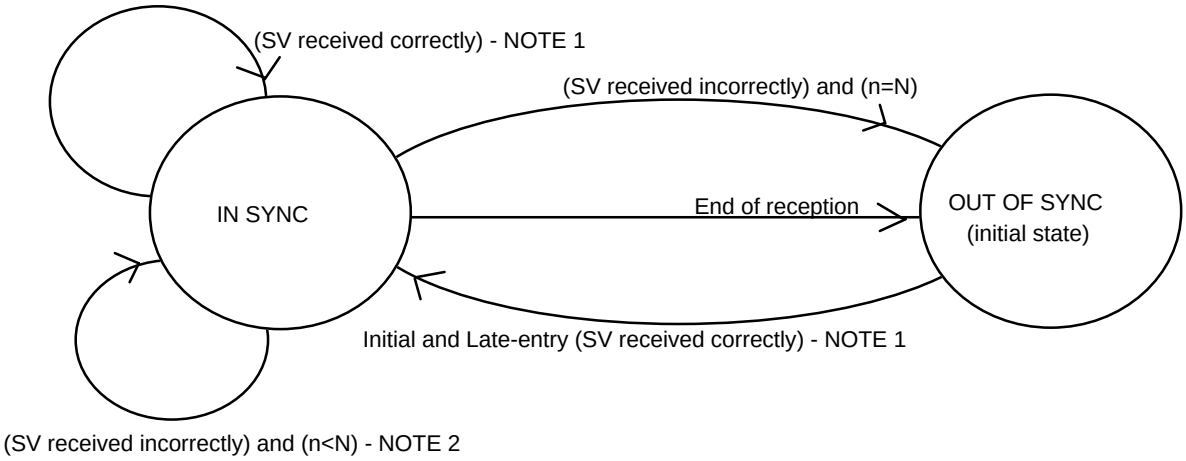
9.4.4 Reception

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 half-slot 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 a synchronization frame and passed to the Synchronization Detect Unit.

If 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 synchronization frame is received.

A state diagram of an example sync detect process is given in figure 38.



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 38: State diagram of an example "sync-detect" process in the receiver

In the flywheel mechanism the receiver should use locally generated Synchronization Values (SVs) if an SV is not received correctly. 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 57:

Table 57: Stolen frame format (half-slot)

Information element	Length	Type	Value	Remark
Half-slot stolen by encryption unit (HSSE)	1	1	0	Not stolen by encryption unit
			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 the synchronization frame are encrypted or not. The remainder of the synchronization frame shall be encrypted unless the half slot contains synchronization information.

In case of a synchronization frame the signalling data block should contain some or all of the following parameters:

- algorithm number;
- key number;
- 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 (see table 58) indicates the terminating devices for stolen frames based upon the values of HSSE and SHSI where a codec is present:

Table 58: 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: synchronization path; 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 39 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.

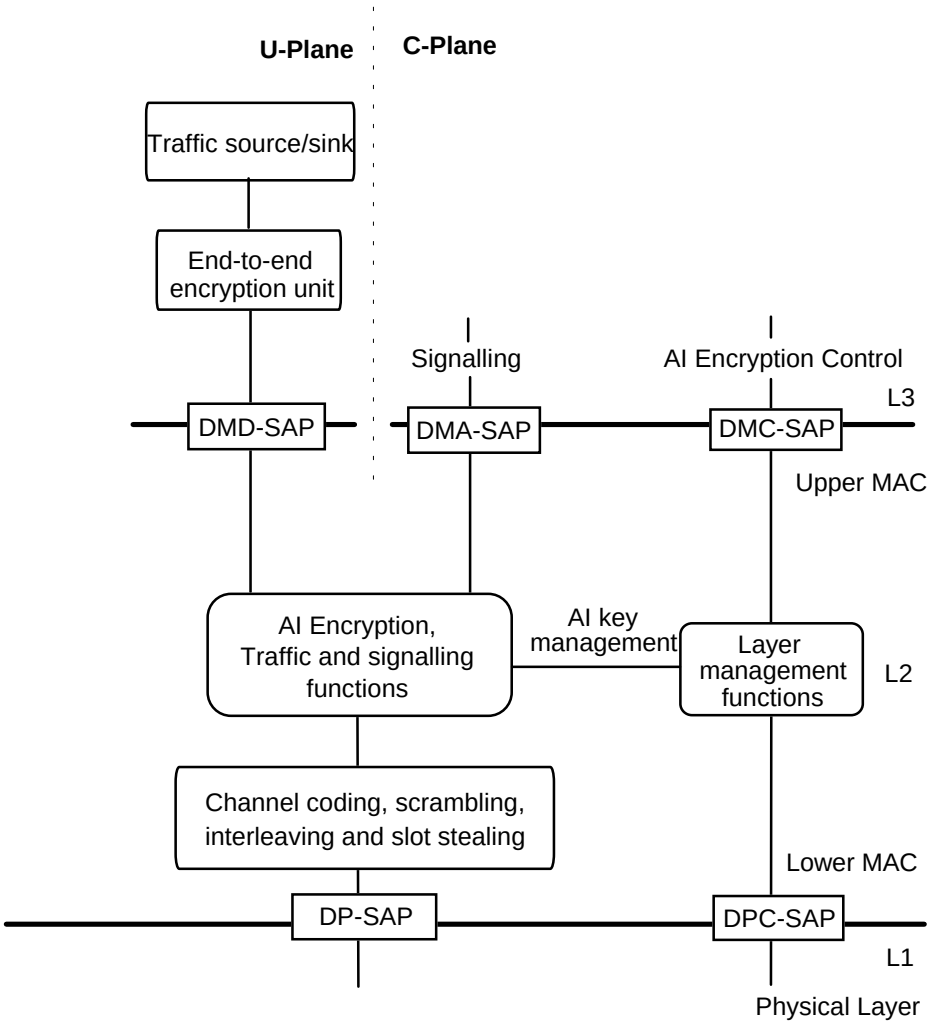


Figure 39: Position of end-to-end encryption unit in MS

The services offered on the U-Plane side, as shown in figure 37, may be further expanded as shown in figure 40.

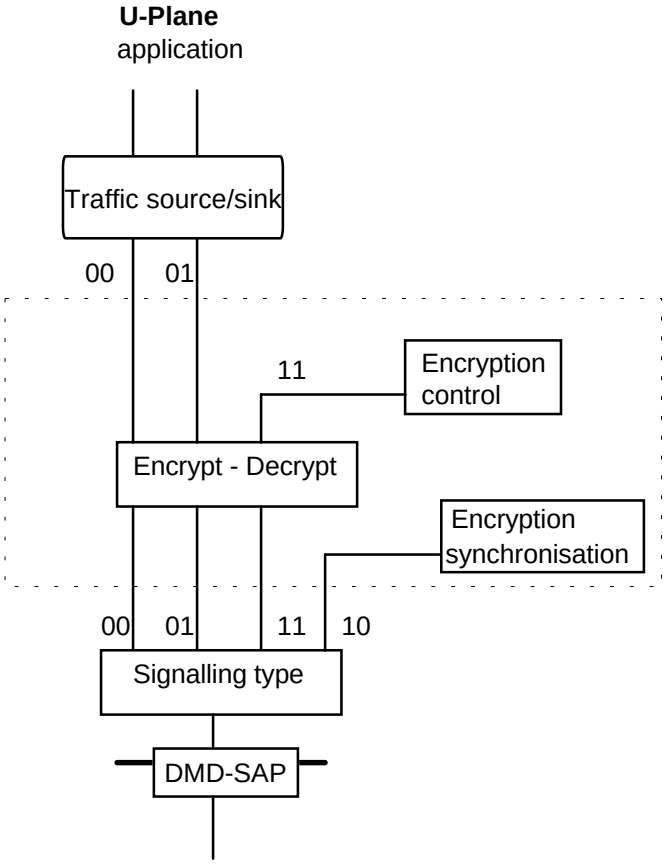


Figure 40: Functional model of the encryption unit

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 Short Data Service with user defined data content. The key management message should include the following parameters:

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

The short data service 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 [1], subclause 14.8.52 shall be replaced by the definition given in table 59:

Table 59: 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	Available for other applications
Data	0-2039	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 [1], subclause 14.8.52, with the first byte reserved as a header.			

Annex A (normative): Protocol mapping between V+D and DMO for gateway operations

A.1 OTAR mapping

Assumption 1: The gateway is acting as a V+D terminal to the V+D SwMI and as a key holder to the DMO-net.

Assumption 2: ETS 300 396-5 [7] (Gateway in DMO) defines the type 3 element "DM-MS address" which can be added to any V+D PDU.

Assumption 3: The SwMI is the master for any OTAR transaction (i.e. contains AC and KSL).

The basic scenarios are as from ETS 300 392-7 [5] for OTAR SCK and from clause 7 of this ETS.

The mapping shall be performed at the PDU level with inputs and outputs from the OTAR SCK PDUs of DMO and the U-/D-OTAR SCK PDUs of V+D.

Table A.1: Mapping of Key User and Key Holder PDUs to equivalent PDUs in V+D

DMO OTAR PDU		V+D OTAR PDU	
Name	**Elements**	**Mapped name**	**Mapped elements**
OTAR SCK Demand	-	U-OTAR SCK Demand	PDU type
	OTAR SCK sub-type		OTAR sub-type
	ITSI		-
	Number of SCKs requested		Number of SCKs requested
	SCK number (SCKN)		SCK number
	Proprietary element		Proprietary element
OTAR SCK Provide	-	D-OTAR SCK Provide	PDU type
	OTAR SCK sub-type		OTAR sub-type
	Random seed		Random seed
	Number of SCKs provided		Number of SCKs provided
	ITSI		-
	SCK, key and identifier		SCK, key and identifier
	Proprietary element		Proprietary element
OTAR SCK Result		U-OTAR SCK Result	PDU-type
	OTAR SCK sub-type		OTAR sub-type
	ITSI		-
	Number of SCKs requested		Number of SCKs requested
	SCK number and result		SCK number and result
	Proprietary element		Proprietary element

A.1.1 DM-GWAY requests provision of SCK(s) from SwMI on behalf of a DM-MS

This scenario shows the case where the MS requests provision of one or more SCKs in use on a system. The MS may initiate this procedure at any time.

This case is an extension of that given in subclause 7.5.2 where the gateway is acting as KH. The V+D SwMI shall act as KSL.

The normal message sequence in this case shall be according to figure A.1.

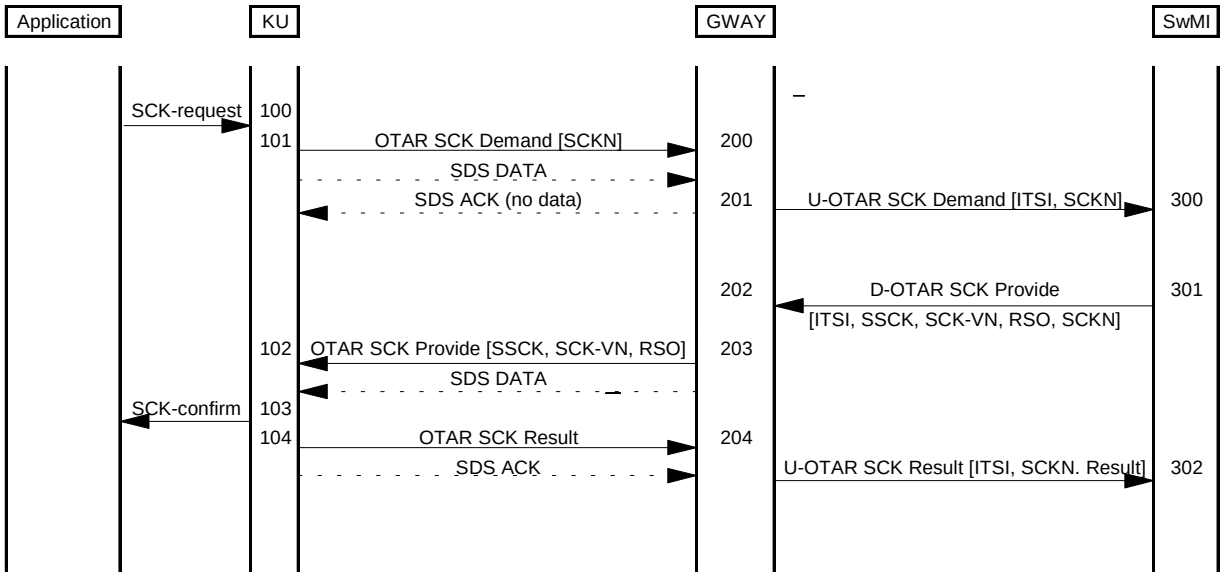


Figure A.1: SCK delivery initiated by MS

The gateway shall map the elements of the PDUs as shown in table A.1. In addition the ITSI element present in the PDUs on the DMO side shall be mapped to the type-3 element "DM-MS address" on the V+D side.

A.2 Enable-Disable mapping

The gateway shall act as manager to the enable/disable exchange on the DMO side. The V+D SwMI shall invoke the manager process by adding the target ITSI to the type 3 element "DM-MS address" which is added to the V+D secure enable/disable PDUs as defined in ETS 300 392-7 [5], clause 5.

A.2.1 DM-GWAY acting as intermediary in Secure enable/disable procedure

A.2.1.1 Disable

NOTE: The actions of the target MAC, and the location of ENDIS primitives are not shown on the following MSC.

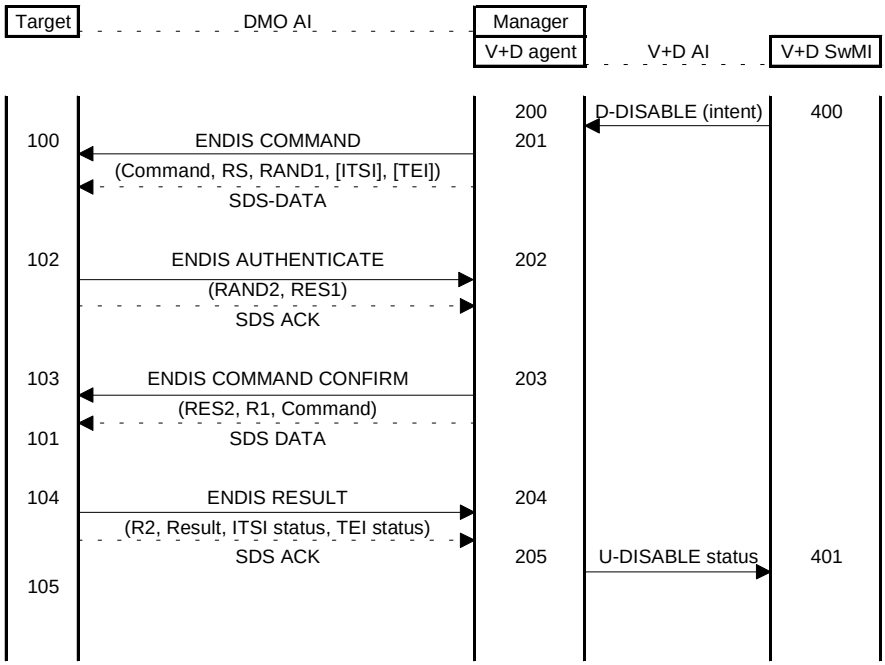


Figure A.2: DM-GWAY acting as V+D agent in secure enable/disable exchange

The AI actions of the manager and target are the same as those described in subclause 8.7. In the V+D side of the exchange the D-DISABLE intent and U-DISABLE status PDUs shall be as described in ETS 300 392-7 [5], subclause 5.4.2.2 with the addition of the type 3 element "DM-MS address" to the PDUs.

The V+D agent actions shall be as follows:

200 On receipt of a D-DISABLE intent message with destination ITSI set to a valid target identity the V+D agent shall act with the manager application to map the D-DISABLE elements to ENDIS COMMAND elements as in table A.2:

Table A.2: Mapping of V+D and DMO PDU elements (D-DISABLE intent)

D-DISABLE element	ENDIS RESULT element
PDU type	Command.(Command sub-type)
Intent/confirm	-
Disabling type	Command.(Temporary/permanent disable)
Equipment disable	Command.(Command application)
TEI	TEI
Subscription disable	Command.(Command application)
Address extension	ITSI.(Address extension)
Authentication challenge	RAND1 (note 2)
NOTE 1: The convention element.(sub element) is used to refer to sub-elements in the command and ITSI elements of the ENDIS COMMAND PDU.	
NOTE 2: The manager shall know by pre-arrangement the authentication session keys (KS and KS') and the random seed used in their generation. It shall therefore discard the RS given in the D-DISABLE intent PDU (or the element may be given a null value by the SwMI).	

205 On receipt of ENDIS RESULT from the target the manager application shall act with the V+D agent to map the contents of the ENDIS RESULT PDU to the U-DISABLE status PDU, as shown in table A.3 below:

Table A.3: Mapping of V+D and DMO PDU elements (U-DISABLE status)

ENDIS RESULT element	U-DISABLE STATUS element
ENDIS PDU type	PDU type
Authentication result R2	
Equipment status	Equipment status
Subscription status	Subscription status
Enable/Disable result	Enable/disable result
Reject Reason	

A.2.1.2 Enable

NOTE: The actions of the target MAC, and the location of ENDIS primitives are not shown on the following MSC.

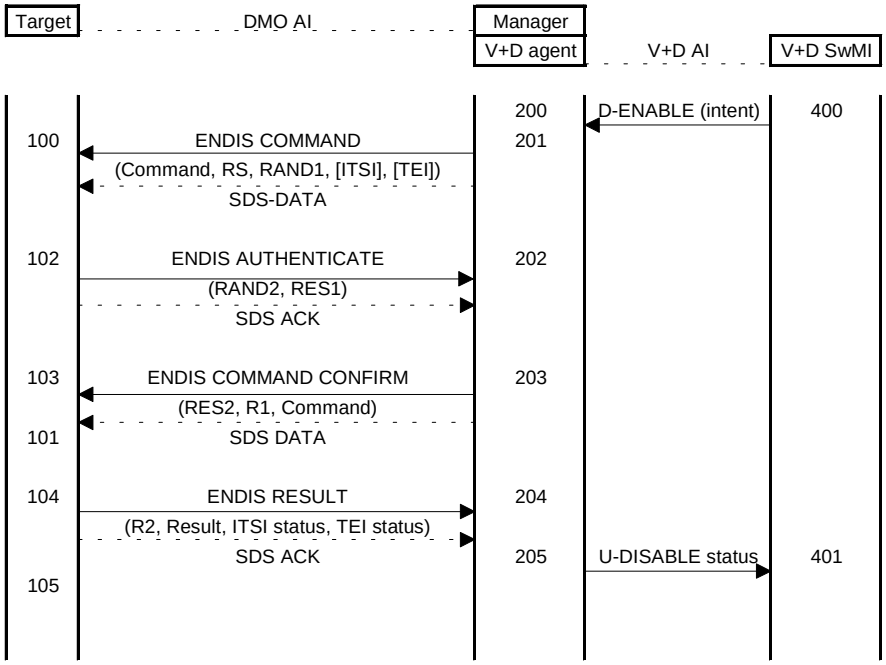


Figure A.3: DM-GWAY acting as V+D agent in secure enable/disable exchange

The AI actions of the manager and target are the same as those described in subclause 8.7. In the V+D side of the exchange the D-DISABLE intent and U-DISABLE status PDUs shall be as described in ETS 300 392-7 [5], subclause 5.4.2.4 with the addition of the type 3 element "DM-MS address" to the PDUs.

The V+D agent actions shall be as follows:

200 On receipt of a D-ENABLE intent message with destination ITSI set to a valid target identity the V+D agent shall act with the manager application to map the D-ENABLE elements to ENDIS COMMAND elements as in table A.4:

Table A.4: Mapping of V+D and DMO PDU elements (D-DISABLE intent)

D-DISABLE element	ENDIS RESULT element
PDU type	Command.(Command sub-type)
Intent/confirm	-
Equipment enable	Command.(Command application)
TEI	TEI
Subscription enable	Command.(Command application)
Address extension	ITSI.(Address extension)
Authentication challenge	RAND1 (note 2)
NOTE 1: The convention element.(sub element) is used to refer to sub-elements in the command and ITSI elements of the ENDIS COMMAND PDU.	
NOTE 2: The manager shall know by pre-arrangement the authentication session keys (KS and KS') and the random seed used in their generation. It shall therefore discard the RS given in the D-ENABLE intent PDU (or the element may be given a null value by the SwMI).	

205 On receipt of ENDIS RESULT from the target the manager application shall act with the V+D agent to map the contents of the ENDIS RESULT PDU to the U-DISABLE status PDU, as shown in table A.5 below:

Table A.5: Mapping of V+D and DMO PDU elements (U-DISABLE status)

ENDIS RESULT element	U-DISABLE STATUS element
ENDIS PDU type	PDU type
Authentication result R2	
Equipment status	Equipment status
Subscription status	Subscription status
Enable/Disable result	Enable/disable result
Reject Reason	

History

Document history			
December 1996	Public Enquiry	PE 121:	1996-12-30 to 1997-04-25
January 1998	Vote	V 9813:	1998-01-27 to 1998-03-27
April 1998	First Edition		

ISBN 2-7437-2137-5
Dépôt légal : Avril 1998