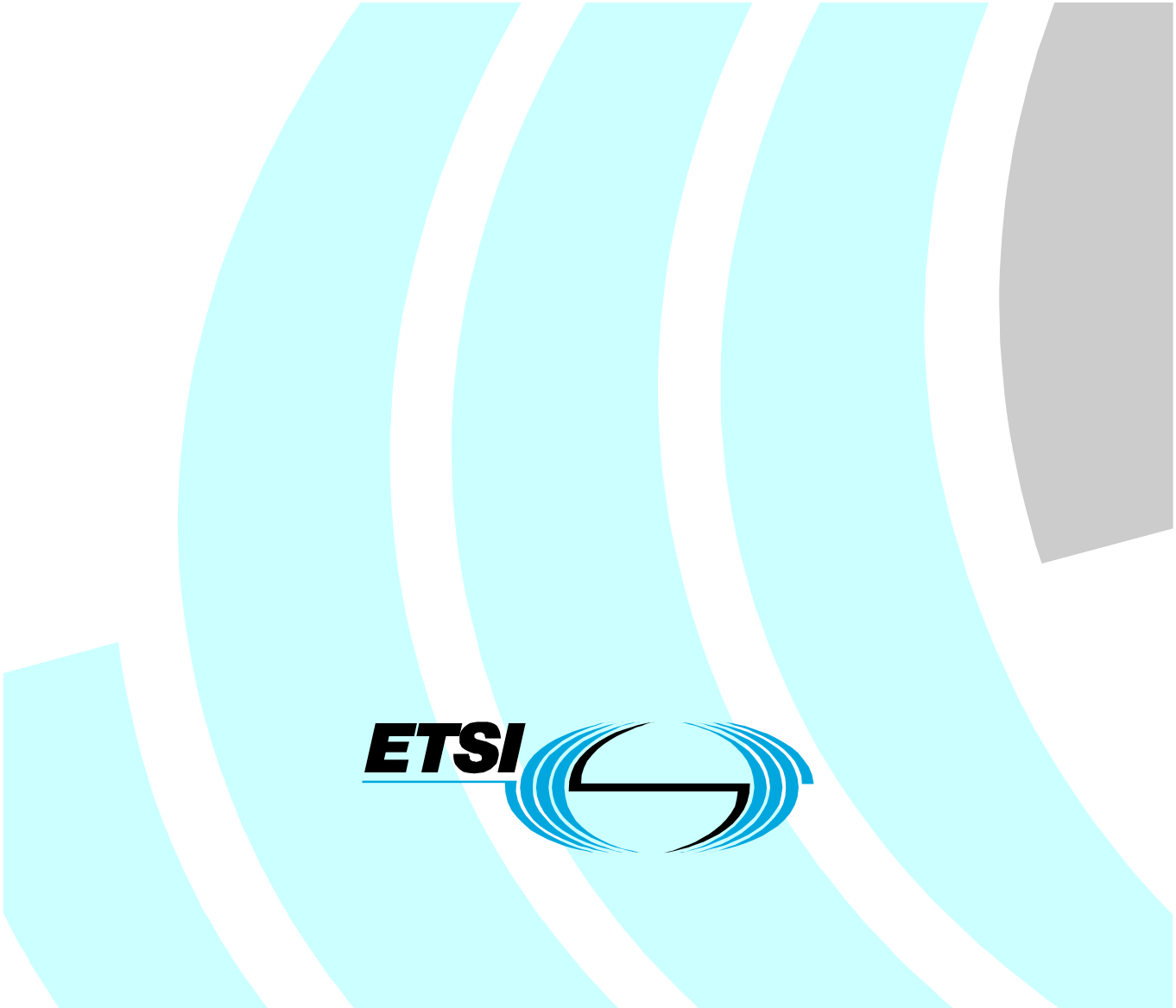
ETSI EN 302 109 V1.1.1 (2003-10)

European Standard (Telecommunications series)

Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption



Reference
DEN/TETRA-06117

Keywords
air interface, data, DMO, security, speech,
TETRA

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

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

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Project Terrestrial Trunked Radio (TETRA).

National transposition dates	
Date of adoption of this EN:	3 October 2003
Date of latest announcement of this EN (doa):	31 January 2004
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 July 2004
Date of withdrawal of any conflicting National Standard (dow):	31 July 2004

Introduction

The present document replaces the end-to-end encryption clause in each of EN 300 392-7 and ETS 300 396-6.

1 Scope

The present document defines the Terrestrial Trunked Radio system (TETRA) synchronization operation for end-to-end encryption algorithms that employ streaming ciphers for voice. The method defined applies equally to Direct Mode Operation (as defined in EN 300 396 (see bibliography)) and to Trunked Mode Operation (as defined in EN 300 392 (see bibliography)).

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

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

[1] ETSI EN 300 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

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

[3] ETSI 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 the present document, the following terms and definitions apply:

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

cipher text: data produced through the use of encipherment

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

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

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

encryption state: encryption on or off

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

flywheel: 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): sequence of symbols that initializes the KSG inside the encryption unit

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

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

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

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

plain text: unencrypted source data

NOTE: The semantic content is available.

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

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

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

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

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

3.2 Abbreviations

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

AI	Air Interface
CK	Cipher Key
C-plane	Control-plane
CT	Cipher Text
DMD-SAP	Direct Mode D Service Access Point
DMO	Direct Mode Operation
EKSG	End-to-end Key Stream Generator
EKSS	End-to-end Key Stream Segment
F	Function
HSC	Half-Slot Condition
HSI	Half-Slot Importance
HSN	Half-Slot Number
HSS	Half-Slot Stolen
HSSE	Half-Slot Stolen by Encryption unit
IV	Initialization Value
KSG	Key Stream Generator
KSS	Key Stream Segment
L1	Layer 1
L2	Layer 2
L3	Layer 3
MAC	Medium Access Control
MS	Mobile Station
PT	Plain Text
SAP	Service Access Point
SHSI	Stolen Half-Slot Identifier
STCH	Stolen Channel
SV	Synchronization Value
T/DMA-SAP	Trunked or Direct Mode A Service Access Point
T/DMC-SAP	Trunked or Direct Mode C Service Access Point
T/DMD-SAP	Trunked or Direct Mode D Service Access Point
TMD-SAP	Trunked Mode D Service Access Point
Tx	Transmit
U-plane	User-plane
V+D	Voice + Data

4 End-to-end encryption

4.1 Introduction

End-to-end encryption algorithms and key management are outside the scope of the present document. 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 uses the Stealing Channel, STCH, for synchronization during transmission (see EN 300 392-2 [1], clause 23.8.4).

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.

4.2 Voice encryption and decryption mechanism

Figure 1 shows a functional diagram of the voice encryption and decryption mechanism based on the synchronous stream cipher principle. 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.

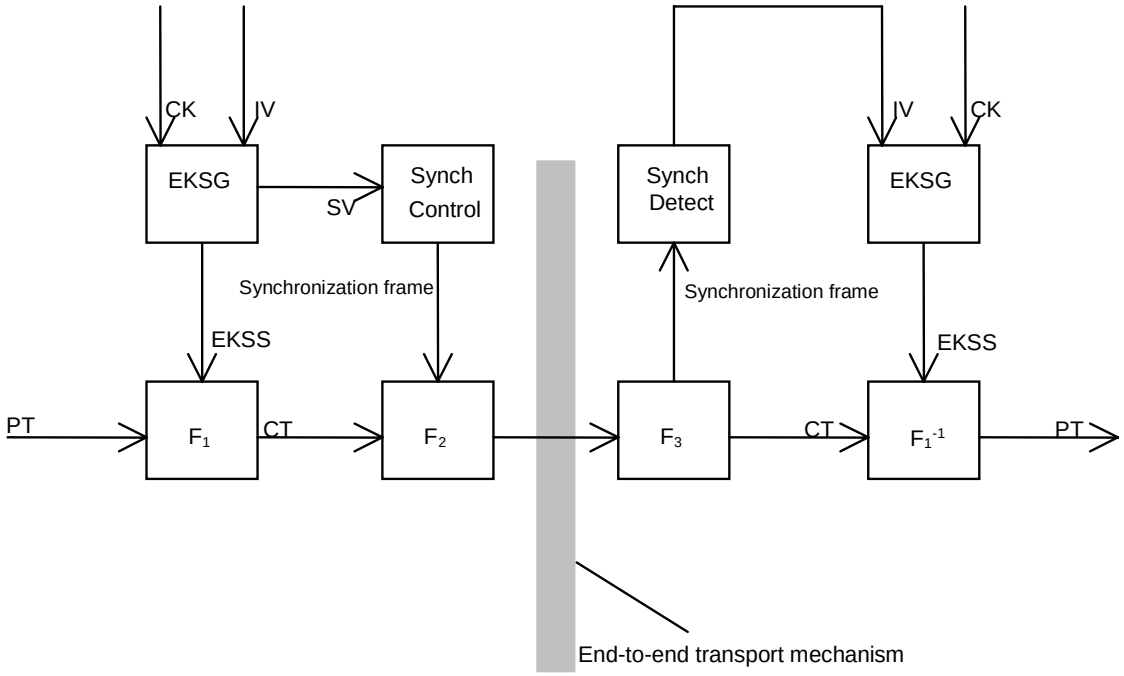


Figure 1: Functional diagram of voice encryption and decryption mechanisms

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).

4.2.1 Protection against replay

Protection against replay should be obtained by use of a time variant initialization value or 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 the present document.

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 the present document.

4.3 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.

4.4 Exchange of information between encryption units

Two different cases shall be identified by an appropriate MAC header (see clause 4.4.2):

- synchronization information in clear; or
- encrypted information.

The use of exchanged encrypted information between encryption units is out of the scope of the present document.

4.4.1 Synchronization of encryption units

Figure 1 shows the processing blocks "synchronization control" and "synchronization detect" and their associated functions F_2 and F_3 that 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.

Occurrence of stealing in the receiver shall be locally reported to the U-plane application at the TMD-SAP in TETRA V+D and at the DMD-SAP in TETRA DMO. In each case the primitive shall be of type UNITDATA. Table 1 shows the DMD-UNITDATA primitive (for DMO) that shall be used by the frame stealing mechanism to address the MAC (request) and to inform the U-plane (indication). The parameters in the TMD-UNITDATA primitive in TETRA V+D are identical and are not repeated here.

Table 1: 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	-	May be defined as: 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

Table 2 shows the parameters of the DMD-REPORT primitive that shall be used for any further communication from MAC to the U-plane. The parameters in the TMD-REPORT primitive in TETRA V+D are identical and are not repeated here.

Table 2: Parameters used in the DMD-REPORT primitive

Parameter	Indication	Remark
Half slot synchronization	O	
Circuit Mode information	O	
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.

4.4.2 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 T/DMD-SAP.

NOTE: The nomenclature T/DMD-SAP is used as shorthand for TMD-SAP (in V+D applications) or DMD-SAP (in DMO applications). Similar shorthand is used in reference to primitives.

Table 1 shows the T/DMD-UNITDATA primitive that shall be used by the frame stealing mechanism to address the MAC (request) and to inform the U-plane (indication).

Table 2 shows the parameters of the T/DMD-REPORT primitive that shall be used for any further communication from MAC to the U-plane.

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.

4.4.3 Transmission

The encryption control unit shall intercept T/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 T/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 no more than four half-slots should be stolen per second.

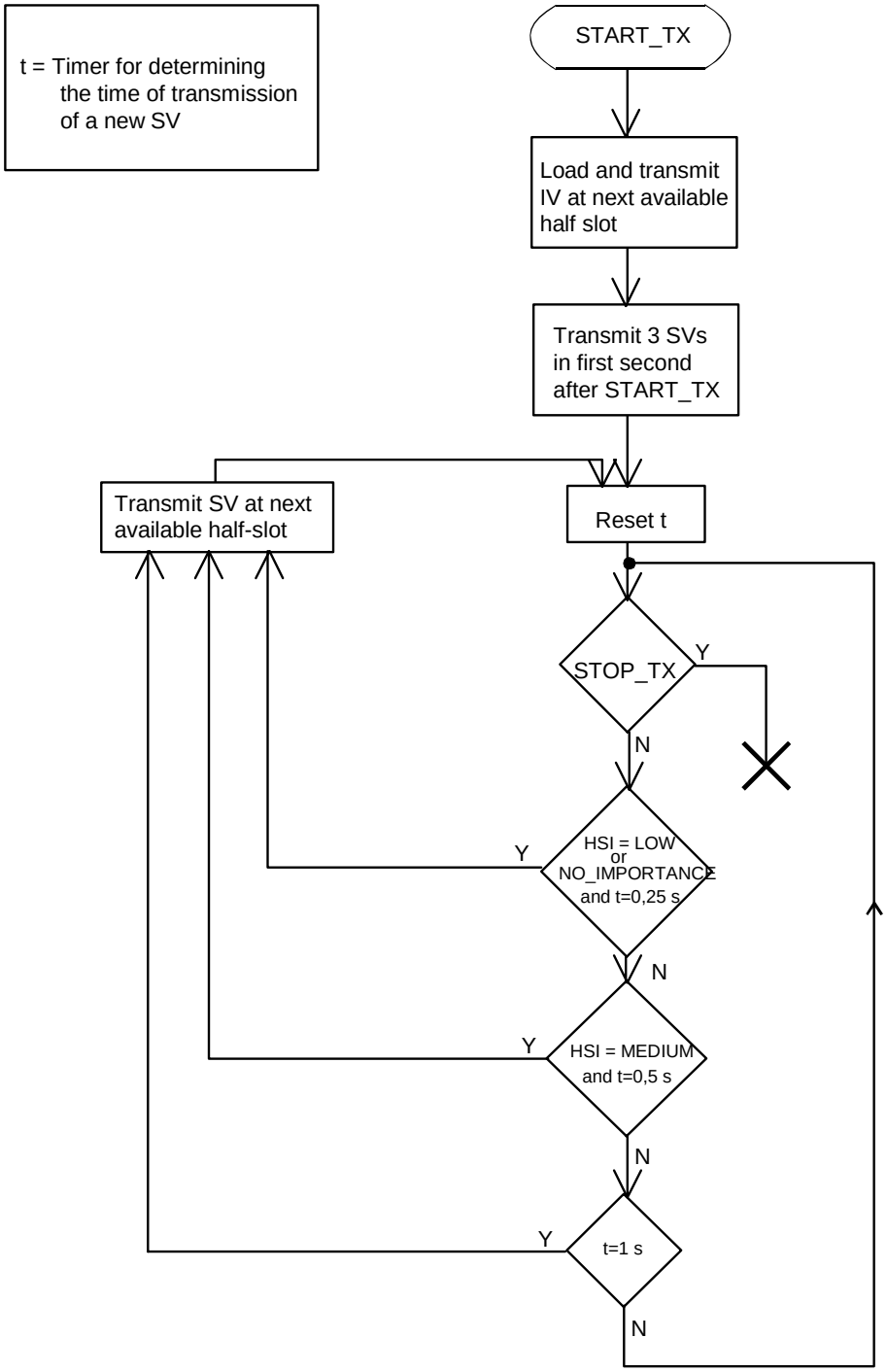
The distribution of the stolen slots for initial synchronization is not defined; they may be placed consecutively at the start of the transmission, before any speech is transmitted, or may be well spaced, with only a single Half-Slot Stolen before speech transmission commences. The first SV transmitted 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 the present document. 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. On receipt of a T/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 2 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 SVs may be transmitted to improve reliability of synchronization and to allow for late entry.



NOTE: Less frequent transmission of the SV may be appropriate in the case of circuit mode data transmission.

Figure 2: Flow chart of an example transmitter "sync-control" process

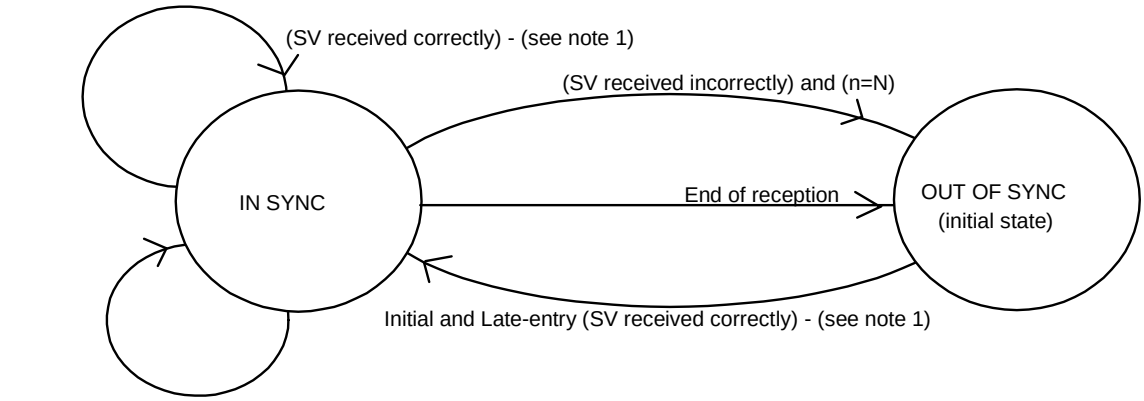
4.4.4 Reception

The encryption control unit shall intercept T/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.

Figure 3 shows a state diagram of an example sync detect process.



n = number of successive wrongly received SVs.
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 3: 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.

4.4.5 Stolen frame format

Table 3 defines the format of a stolen frame (half-slot).

Table 3: Stolen frame format (half-slot)

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

HSSE and SHSI shall not be encrypted, whether the remaining contents of the stolen frame are encrypted or not.

If the stolen half slot contains U-plane data not originated by the end-to-end encryption unit, identified by HSSE=0, the frame shall be encrypted.

If the stolen half slot contains end-to-end encryption synchronization information, identified by HSSE=1 and SHSI=0, no end-to-end encryption shall be applied.

If the stolen half slot contains other signalling data used by the encryption unit, identified by HSSE=1 and SHSI=1, the use of encryption for this half slot shall be system specific and defined by the encryption application.

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 4) indicates the terminating devices for stolen frames based upon the values of HSSE and SHSI where a codec is present:

Table 4: 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; and, signalling path. It is understood that the encryption unit is self contained and both synchronization and signalling originate and terminate within the unit.

4.5 Location of security components in the functional architecture

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

Figure 4 shows that 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 [3]), or any circuit mode data unit.

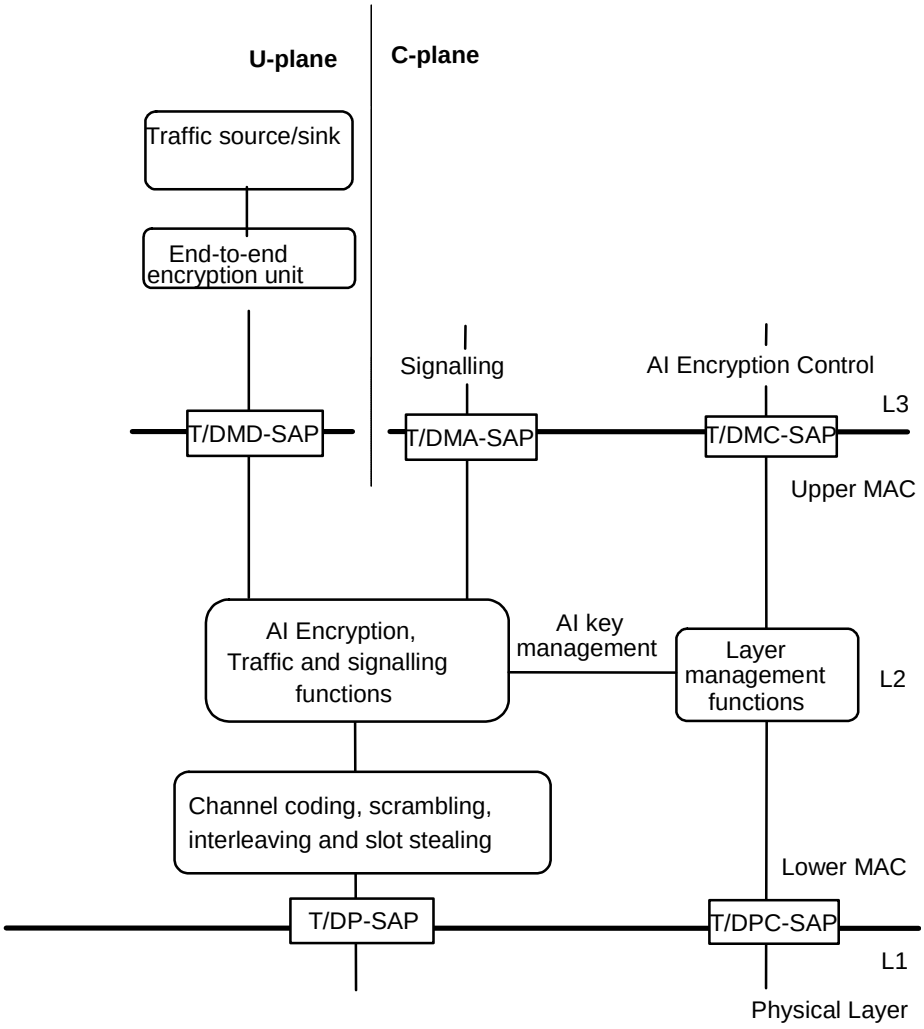


Figure 4: Position of end-to-end encryption unit in MS

The services offered on the U-plane side, as shown in figure 4, may be further expanded as shown in figure 5.

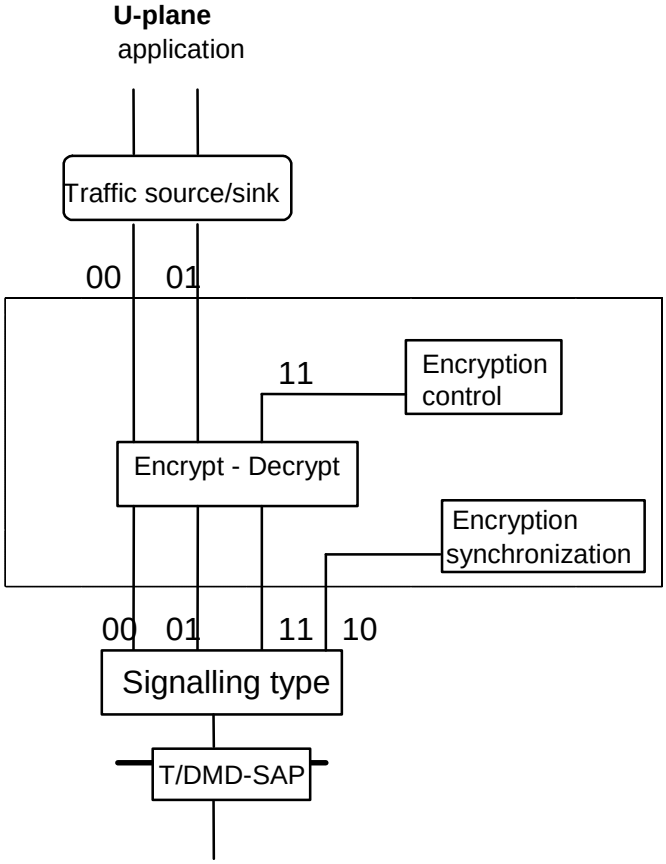


Figure 5: Functional model of the encryption unit

4.6 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 as given by EN 300 392-2 [1], clause 29.3.5.8.

Annex A (informative): Bibliography

ETSI EN 300 396 (all parts): "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO)".

ETSI EN 300 392 (all parts): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D)".

ETSI ETS 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

ETSI TS 100 392-15: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 15: TETRA frequency bands, duplex spacings and channel numbering".

History

Document history		
V1.1.1	January 2003	Publication as ES 202 109
V1.1.1	June 2003	One-step Approval Procedure OAP 20031003: 2003-06-04 to 2003-10-03
V1.1.1	October 2003	Publication