FINAL DRAFT

EUROPEAN
TELECOMMUNICATION
STANDARD

pr ETS 300 392-7

September 1996

Source: ETSI TC-RES

Reference: DE/RES-06001-7

ICS: 33.060, 33.060.50

Key words: TETRA, V+D, security

Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

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

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

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

Contents

Foreword

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

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

Part 1:	"General network design".
Part 2:	"Air Interface (AI)".
Part 3:	"Inter-working - Basic Operation", (DE/RES-06001-3).
Part 4:	"Gateways for Basic Services", (DE/RES-06001-4).
Part 5:	"Terminal equipment interface", (DE/RES-06001-5).
Part 6:	"Line connected stations", (DE/RES-06001-6).
Part 7:	**"Security".**
Part 8:	"Management services", (DE/RES-06001-8).
Part 9:	"Performance objectives", (DE/RES-06001-9).
Part 10:	"Supplementary Services (SS) Stage 1".
Part 11:	"Supplementary Services (SS) Stage 2".
Part 12:	"Supplementary Services (SS) Stage 3".
Part 13:	"SDL Model of the Air Interface".
Part 14:	"PICS Proforma" (DE/RES-06001-14).
Part 15:	"Inter-working - Extended Operations", (DE/RES-06001-15).

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

Blank page

1 Scope

This European Telecommunication Standard (ETS) defines the Trans-European Trunked Radio system (TETRA) supporting Voice plus Data (V+D). It specifies the air interface, the inter-working between TETRA systems and to other systems via gateways, the terminal equipment interface on the mobile station, the connection of line stations to the infrastructure, the security aspects in TETRA networks, the management services offered to the operator, the performance objectives, and the supplementary services that come in addition to the basic and teleservices.

This part describes the security mechanisms in TETRA V+D. It provides mechanisms for confidentiality of control signalling and user speech and data at the air interface, authentication and key management mechanisms for the air interface, and end-to-end confidentiality mechanisms between users.

Clause 4 describes the authentication and key management mechanisms for the TETRA air interface. The following two authentication services have been specified for the air-interface in ETR 086-3 [3], based on a threat analysis:

- authentication of a user by the TETRA infrastructure;

- authentication of the TETRA infrastructure by a user.

Clause 5 describes the mechanisms and protocol for a secure enable and disable of both the mobile station equipment and the mobile station user’s subscription.

Air interface encryption may be provided as an option in TETRA. Where employed, clause 6 describes the confidentiality mechanisms using encryption on the air interface, for circuit mode speech, circuit mode data, packet data and control information. Clause 6 describes both encryption mechanisms and mobility procedures. It also details the protocol concerning control of encryption at the air interface.

Clause 7 describes the end-to-end confidentiality for V+D. End-to-end confidentiality can be established between two users or a group of users. In clause 7 the logical part of the interface to the encryption mechanism is described. Electrical and physical aspects of this interface are not described, nor are the encryption algorithms for end-to-end confidentiality described.

This part of the ETS does not address the detail handling of protocol errors or any protocol mechanisms when TETRA is operating in a degraded mode. These issues are implementation specific and therefore fall outside the scope of the TETRA standardization effort.

The detail description of the Authentication Centre is outside the scope of this part of the ETS.

2 Normative references

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

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

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

[3] ETR 086-3: "Radio Equipment and Systems (RES); Trans European Trunked Radio (TETRA) systems; Technical requirements specification; Part 3: Security aspects".

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

[5] prETS 300 395-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Speech codec for full-rate traffic channel; Part 1: General description of speech functions".

[6] prETS 300 395-3: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Speech codec for full-rate traffic channel; Part 3: Specific operating features".

3 Definitions and abbreviations

3.1 Definitions

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

Authentication Code (AC): A (short) sequence to be entered by the user into the MS.

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

CCK Identity (CCK-Id): Distributed with the CCK. It serves the identification of the active key and the protection against replay of old keys.

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 (see ISO 7498-2 [4]).

Common Cipher Key (CCK): A cipher key that is generated by the infrastructure to protect group addressed signalling and traffic. There is one CCK for each location area.

decipherment: The reversal of a corresponding reversible encipherment (see ISO 7498-2 [4]).

Derived Cipher Key (DCK): DCK is generated during authentication for use in protection of individually addressed signalling and traffic.

derived key: A sequence of symbols that controls the KSG inside the end-to-end encryption unit and that is derived from the cipher key.

encipherment: The cryptographic transformation of data to produce cipher text (see ISO 7498-2 [4]).

encryption mode: The choice between static (SCK) and dynamic (DCK/CCK) encipherment.

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 KSG in the transmitting terminal in case synchronization data is not received correctly.

Group Cipher Key (GCK): A long lifetime cipher key generated by the infrastructure to protect group addressed signalling and traffic. Not used directly at the air interface but modified by CCK to give a Modified Group Cipher Key (MGCK). There is one GCK for each GTSI.

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 CCK has been incorrectly recovered.

Personal Identification Number (PIN): Entered by the user into the MS and used to generate the authentication Key (K) together with the User Authentication Key (UAK).

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

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

RANDdom challenge (RAND1, RAND2): A random value generated by the infrastructure to authenticate a user or in an MS to authenticate the infrastructure, respectively.

Random Seed (RS): A random value used to derive a session authentication key from the authentication key.

RESponse (RES1, RES2): A value calculated in the MS from RAND1 and the KS to prove the authenticity of a user to the infrastructure or by the infrastructure from RAND2 and the KS' to prove its authenticity to a user, respectively.

SCK-set: The collective term for the group of 32 SCK associated with each ITSI.

Sealed Common Cipher Key (SCCK): A common cipher key cryptographically sealed with a particular user's derived cipher key. In this form the keys are distributed over the air interface.

Sealed Group Cipher Key (SGCK): A group cipher key cryptographically sealed with a particular user's derived cipher key. In this form the keys are distributed over the air interface.

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

Session Authentication Key (KS, KS'): Generated from the authentication key and a random seed for authentication. It has a more limited lifetime than the authentication key and can be stored in less secure places and forwarded to visited networks.

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

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

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

synchronous stream cipher: An encryption method in which a cipher text symbol completely represents the corresponding plain text symbol. The encryption is based on a key stream that is independent of the cipher text. In order to synchronize the KSGs in the transmitting and the receiving terminal synchronization data is transmitted separately.

TETRA algorithm: The mathematical description of 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.

User Authentication Key (UAK): Stored in a (possibly detachable) module within the MS and used to derive the authentication key (with or without a PIN as an additional parameter).

3.2 Abbreviations

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

AC	Authentication Code
AI	Air Interface
AS	Alias Stream
AESI	Alias Encrypted Short Identity
ASSI	Alias Short Subscriber Identity
BS	Base Station
CCK	Common Cipher Key
CCK-id	CCK identifier
C-PLANE	Control-PLANE
CT	Cipher Text
DCK	Derived Cipher Key
DCK1	Part 1 of the DCK
DCK2	Part 2 of the DCK
DK	Derived Key
EKSG	End-to-end Key Stream Generator
EKSS	End-to-end Key Stream Segment
ESI	Encrypted Short Identity
F	Function
FEC	Forward Error Correction
GCK	Group Cipher Key
GCK-VN	GCK-Version Number
GESI	Group Encrypted Short Identity
GSSI	Group Short Subscriber Identity
GTSI	Group TETRA Subscriber Identity
HSC	Half-Slot Condition
HSI	Half-Slot Importance
HSN	Half-Slot Number
HSS	Half-Slot Stolen
HSSE	Half-Slot Stolen by Encryption unit
IESI	Individual Encrypted Short Identity
ISSI	Individual Short Subscriber Identity
ITSI	Individual TETRA Subscriber Identity
IV	Initialization Value
K	authentication Key
KS, KS’	Session authentication Key
KSG	Key Stream Generator
KSO	Session Key OTAR
KSS	Key Stream Segment
LA	Location Area
LLC	Logical Link Control
MAC	Medium Access Control
MF	Manipulation Flag
MGCK	Modified Group Cipher Key
MLE	Mobile Link Entity
MM	Mobility Management
MNI	Mobile Network Identity
MS	Mobile Station
MSC	Message Sequence Chart
PDU	Protocol Data Unit
PIN	Personal Identification Number
PT	Plain Text
RAND1	RANDom challenge 1
RAND2	RANDom challenge 2
RES1	RESponse 1
RES2	RESponse 2
RS	Random Seed

RSO	Random Seed for OTAR
SAP	Service Access Point
SCCK	Sealed Common Cipher Key
SCK	Static Cipher Key
SCK-VN	SCK Identifier
SCKN	Static Cipher Key Number
SDU	Service Data Unit
SGCK	Sealed GCK
SHSI	Stolen Half-Slot Identifier
SS	Synchronization Status
SSCK	Sealed SCK
SSI	Short Subscriber Identity
SV	Synchronization Value
SwMI	Switching and Management Infrastructure
TA	TETRA Algorithm
TCH	Traffic Channel type
TEI	TETRA Equipment Identity
TSI	TETRA Subscriber Identity
UAK	User Authentication Key
U-PLANE	User-PLANE
XRES1	eXpected RESponse 1
XRES2	eXpected RESponse 2

4 Air Interface authentication and key management mechanisms

4.1 Air interface authentication mechanisms

4.1.1 Overview

Authentication is optional, however if it is used it shall be as described in this clause.

The authentication method described is a symmetric secret key type. In this method one secret, the authentication key, shall be shared by each of the authenticating parties, and there should be strictly two parties with knowledge of the secret. Authentication shall be achieved by the parties proving to each other knowledge of the shared secret.

The authenticating parties shall be the authentication centre of the Switching and Management Infrastructure (SwMI) and the Mobile Station (MS). The MS is considered, for the purposes of authentication, to represent the user as defined by the Individual TETRA Subscriber Identity (ITSI). At the air interface the Base Station (BS) is assumed to be trusted by the SwMI and the authentication exchange proves knowledge given to the BS by the authentication centre. This knowledge shall be the session authentication key.

Authentication and provision of keys for use at the air interface shall be linked by the use of a common algorithm set. This algorithm set shall include a means of providing keys for use in group calls. The controlling party in all authentication exchanges shall be the SwMI.

The authentication process describes a 3-pass challenge-response-result protocol.

It is assumed that the intra-system interface linking the BS to the authentication centre is adequately secure.

4.1.2 Authentication of a user

In this subclause, a mechanism is described that shall be used to achieve the authentication of a user of an MS by the SwMI. This shall be done using a challenge response protocol, with a session authentication key derived from an authentication key that shall be shared by the user and the infrastructure. The session authentication key shall be provided by an authentication centre of the home system.

The computation of the session authentication key shall be carried out by an algorithm, TA11. The computation of the response shall be done by another algorithm, TA12, which at the same time shall produce a derived cipher key.

The BS shall generate a random number as a challenge RAND1. The MS shall compute a response, RES1, and the BS shall compute an expected response, XRES1. A derived cipher key shall be generated by this process, labelled DCK1. The BS on receipt of RES1 from the MS shall compare it with XRES1. If the values are equal the result R1 shall be set to TRUE, else the result R1 shall be set to FALSE.

The process is summarized in figure 1.

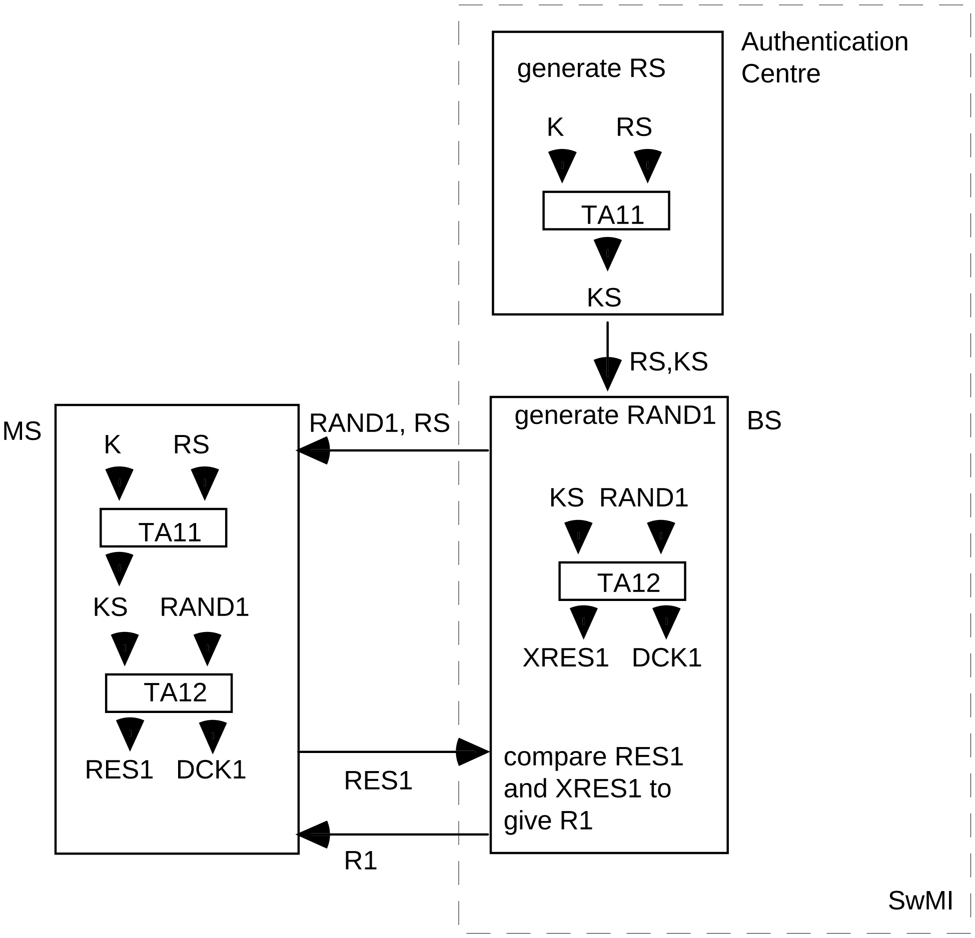


Figure 1: Authentication of a user by the infrastructure

4.1.3 Authentication of the infrastructure

Authentication of the infrastructure by a user shall be carried out in the same way as described in subclause 4.1.2 with the roles of the claimant and verifier reversed. The MS shall generate a challenge, RAND2, the BS shall generate an actual response, RES2, and the MS shall generate an expected response, XRES2. A derived cipher key shall be generated by this process, labelled DCK2. The MS on receipt of RES2 from the BS shall compare it with XRES2. If the values are equal the result R2 shall be set to TRUE, else the result R2 shall be set to FALSE.

The same authentication key K shall be used as in the case of authentication of the user by the infrastructure together with a random seed RS. However, the algorithms shall be different: TA11 shall be replaced by TA21 and TA12 by TA22. Hence, there should also be a different value for the session authentication key, KS'. The process is summarized in figure 2.

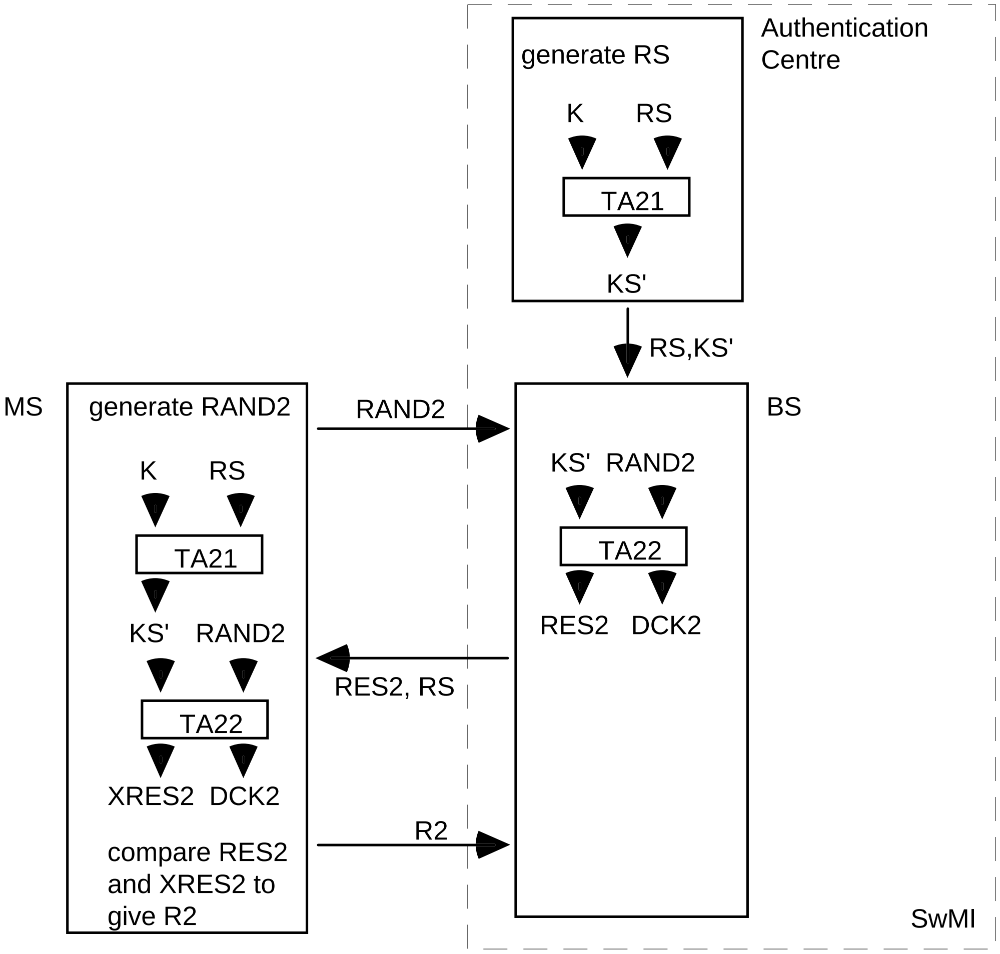


Figure 2: Authentication of the infrastructure by a user

4.1.4 Mutual authentication of user and infrastructure

Mutual authentication of user and infrastructure shall be achieved using a combined three pass mechanism. The algorithms and key K used shall be same as those used in the one way authentication described in the previous subclauses. The decision to make the authentication mutual shall be made by the first party to be challenged, not the initial challenging party. Thus mutual authentication shall be started as a one way authentication by the first challenging party, and shall be made mutual by the responding party.

If the first authentication in such a case fails, the second authentication shall be abandoned.

If the authentication was initiated by the SwMI, it shall use K and one random seed RS with algorithms TA11 and TA12 to generate a session key KS. It shall then send random challenge RAND1 to the MS together with random seed RS. The MS shall run TA11 to generate session key KS, and because the authentication is to be made mutual it shall also run algorithm TA12 to generate a second session key KS'. Both MS and SwMI shall run algorithm TA12; the MS then sends its response RES1 back to the SwMI. However, the MS also sends its mutual challenge RAND2 to the SwMI at the same time. The SwMI shall compare the response from the MS RES1 with its expected response XRES1, and because it has received a mutual challenge, it shall run TA12 to generate session key KS'. The SwMI shall then run TA22 to produce its response to the MS's challenge RES2. RES2 is sent to the MS, which shall also run TA22 to produce expected response XRES2. The MS shall compare RES2 with XRES2; and if the same, mutual authentication will have been achieved.

Algorithms TA12 and TA22 produce DCK1 and DCK2 respectively; these shall be combined in TB4 by both MS and SwMI to produce a DCK which has therefore been created as a result of challenges by both parties. The algorithm TB4 is described in subclause 4.2.1.

The process is shown in figure 3.

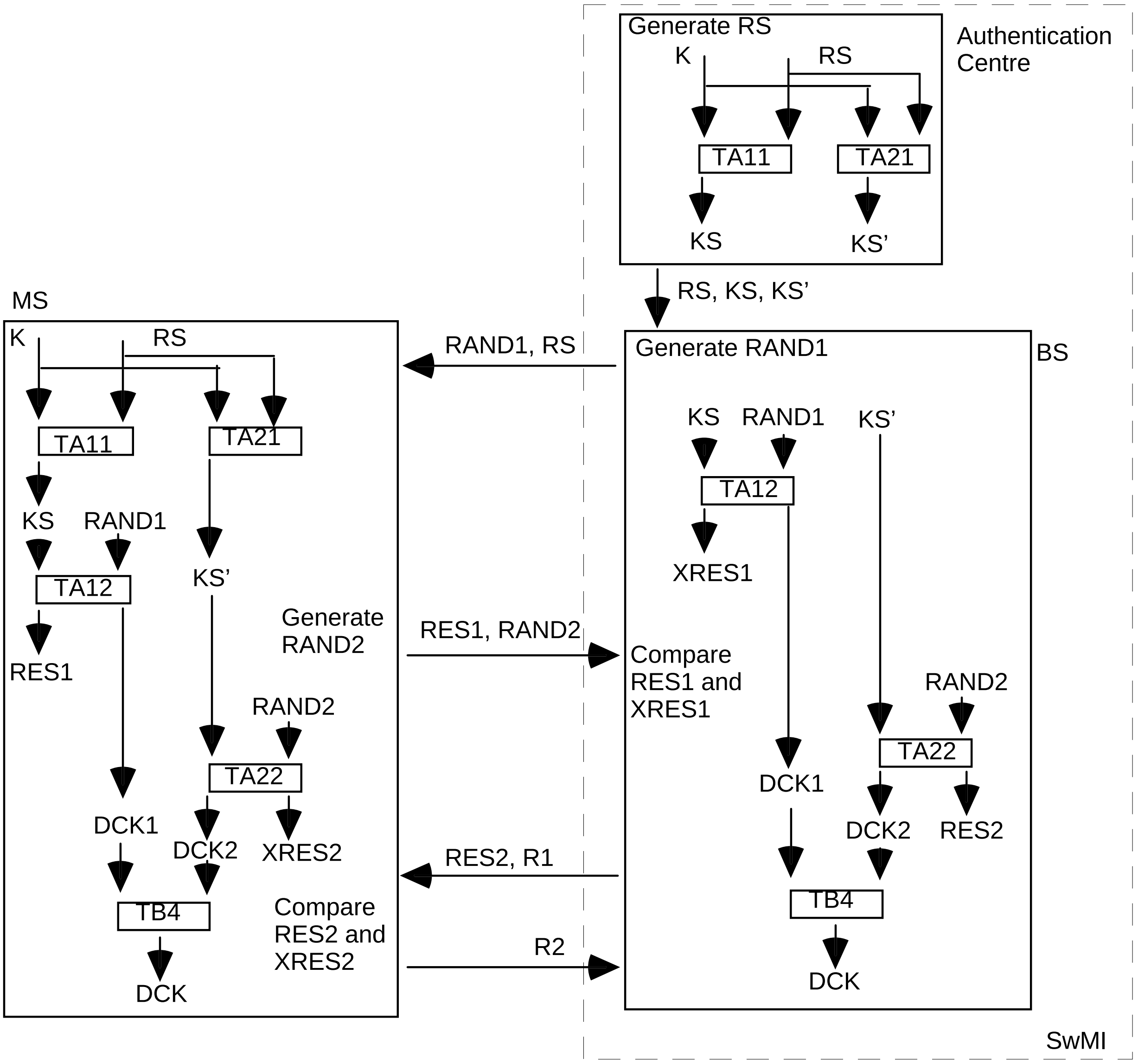


Figure 3: Mutual authentication initiated by SwMI

The mutual authentication process may also occur if a one way authentication is initiated by the MS, and then made mutual by the SwMI. In this case, the algorithms are the same, however the sequence is reversed as shown in figure 4.

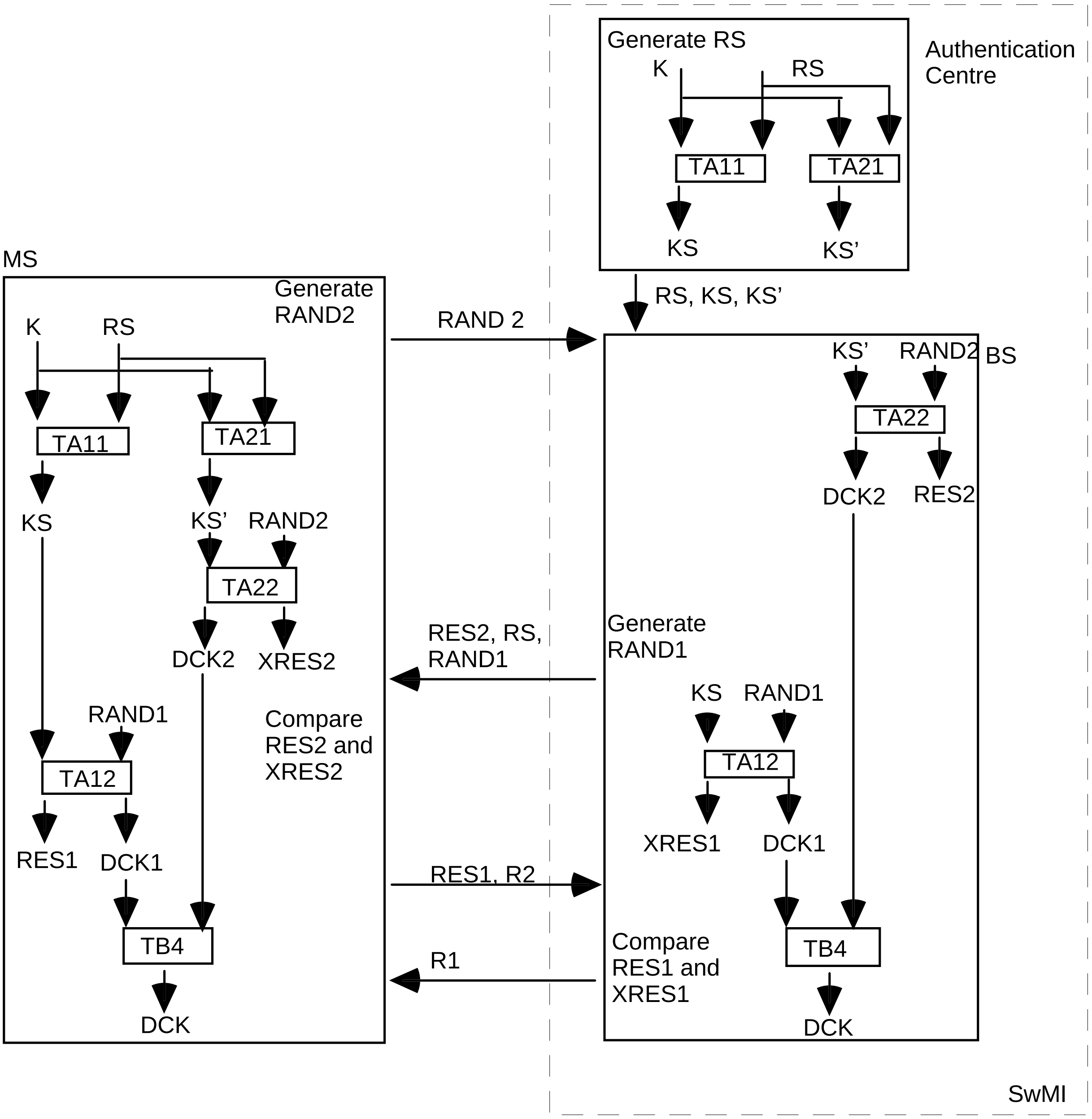


Figure 4: Mutual authentication initiated by MS

4.1.5 The authentication key

Users should be authenticated by a process that is carried out in the MS, as described in subclause 4.1.2. To provide against misuse of lost, or stolen, MS, and to authenticate the user to the MS, the user should be required to make an input before K is available and valid for use. K may be stored in a module, which may or may not be detachable, and the user may be required to make an input to this module, e.g. a personal identification number (PIN).

4.1.5.1 Generation of K

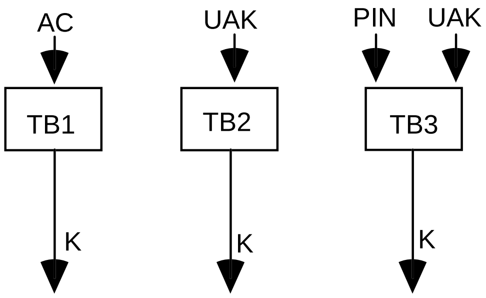


Figure 5: Generation of the authentication key

The generation of K shall be carried out using at least one of the following cases, summarized in figure 5:

1) K may be generated from an Authentication Code (AC) that is manually entered by the user. In this case AC shall be remembered by the user and should not normally be longer than a few digits. The procedure to generate K from AC is labelled TB1;

2) K may be generated from a User Authentication Key (UAK). In this case the UAK can be a random value of a desirable length (e.g. 128 bits). The procedure to generate K from UAK is labelled TB2;

3) K may be generated from both the UAK stored in a module and the PIN entered by the user. The procedure to generate K from UAK and PIN is labelled TB3. In this case the actual checking shall be carried out implicitly by the infrastructure through the authentication process.

4.1.6 Equipment authentication

The authentication of the TETRA Equipment Identity (TEI) is outside the scope of this ETS. However the protocol described in subclause 4.3 provides a mechanism whereby the BS may demand an MS to provide TEI in encrypted form as part of the registration exchange.

4.2 Air Interface key management mechanisms

The authentication exchange described in subclause 4.1 shall be linked to the exchange of cipher keys for use by the air interface encryption process described in clause 6.

Four types of key are managed over the air interface:

- the Derived Cipher Key (DCK);

- the Common Cipher Key (CCK);

- the Group Cipher Key (GCK);

- the Static Cipher Key (SCK).

4.2.1 The DCK

Successful authentication of the user or the infrastructure shall result in the generation of DCK1 or DCK2, respectively. Mutual authentication shall generate both DCK1 and DCK2.

The DCK shall be derived from its two parts DCK1 and DCK2 by the procedure TB4, as shown in figure 6. In case of unilateral authentication, either DCK1 or DCK2 shall be set to zero: DCK2=0 for an authentication of the user by the infrastructure; DCK1=0 for an authentication of the infrastructure by the user.

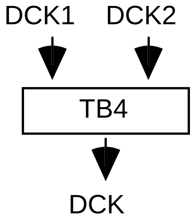


Figure 6: Derivation of the DCK from its two parts

In an authentication exchange the algorithm TB4 shall always be invoked in accordance with the rules for input given above. An authentication exchange shall always provide a new DCK, therefore at the end of an authentication exchange "old" versions of DCK1 or DCK2 shall be set to zero.

DCK may be used to protect voice, data, and signalling sequences between the infrastructure and an individual MS after successful authentication has taken place.

4.2.2 The GCK

The GCK shall be generated by the infrastructure and distributed to the MSs. GCK shall not be used directly by the air interface encryption unit. Within each LA the GCK shall be modified by CCK (see subclause 4.2.3) using algorithm TA71 to provide a Modified GCK (MGCK) for use on the air interface. The process is shown in figure 7.

If GCK is not defined for a group, CCK shall be used in place of MGCK. The value of MGCK shall be equal to that of CCK and algorithm TA71 shall not be invoked.

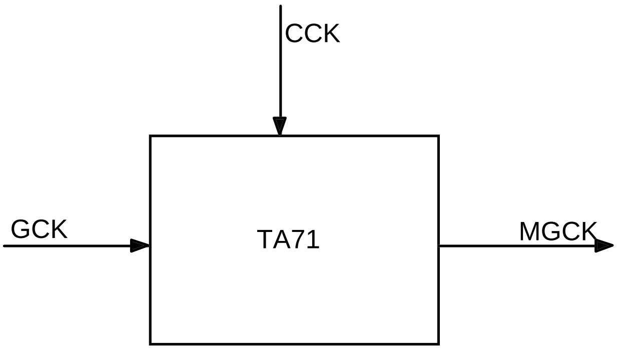


Figure 7: Generation of MGCK from GCK and CCK

Where the Supplementary Service - Dynamic Group Number Assignment (SS-DGNA) is used a GCK may be provided by an Over The Air Re-keying (OTAR) mechanism similar to that for CCK and SCK.

The GCK may be transmitted in encrypted form using algorithm TA81 and DCK as the sealing key. To allow the GCK to be decrypted by the MS, algorithm TA81 shall have an inverse TA82. To allow the MS to discover if GCK has been corrupted due to transmission errors or manipulation, TA81 may introduce some redundancy into the Sealed Group Cipher Key (SGCK). The algorithm TA81 may use the GTSI to which the GCK is linked, and the group key version number (GCK-VN), to provide this redundancy. The redundancy should be checked by TA82. A detected manipulation shall be indicated by setting the manipulation flag MF.

The process is summarized in figure 8.

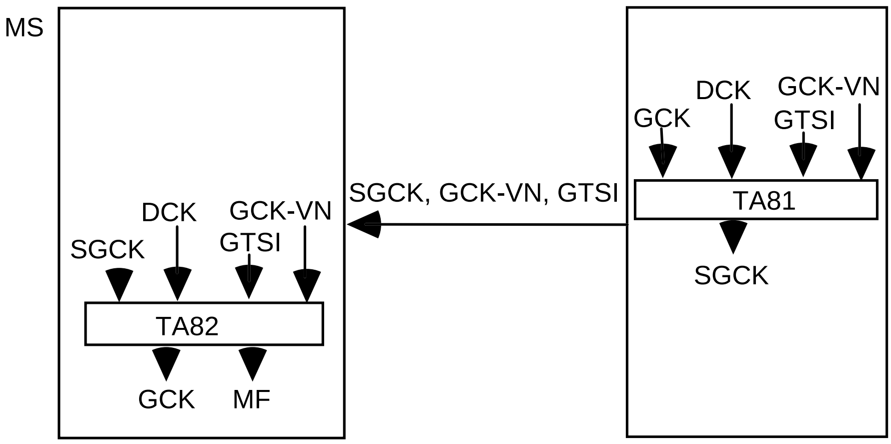


Figure 8: Distribution of a group cipher key

4.2.3 The CCK

K shall be individual to each ITSI and any key derived from it cannot be used for group addressed calls and signalling. A CCK should be used to provide confidentiality for these messages. If GCKs are defined for groups CCK shall be used as a GCK-modifier (see subclause 4.2.2) to further protect group addressed messages.

The CCK shall be generated by the infrastructure and distributed to the MSs. There shall be one such key for every Location Area (LA); a CCK may be used in more than one LA or there may be a distinct CCK for every LA in the system. The MS may request the CCK when registering in an LA. The CCK may then be transmitted in encrypted form using algorithm TA31 and DCK as the sealing key. To allow the CCK to be decrypted by the MS, algorithm TA31 shall have an inverse TA32. To allow the MS to discover if CCK has been corrupted due to transmission errors or manipulation, TA31 may introduce some redundancy into the Sealed Common Cipher Key (SCCK). The redundancy should be checked by TA32. A detected manipulation shall be indicated by setting the manipulation flag MF.

The infrastructure may change the CCK and distribute the new key to the MSs. For this purpose a CCK Identifier (CCK-id) shall be generated and distributed along with the key. CCK-id shall be incremented for each new key and shall be input to algorithms TA31 and TA32 to the effect that decryption of the correct CCK shall only be possible if the correct CCK-id has been received. CCK-id shall be referenced by one bit in the header of the encrypted message to select the active CCK. The value of this bit shall equal the value of the least significant bit of CCK-id. By checking that CCK-id of a newly distributed CCK has been increased, the MS may protect itself against replay of old keys.

The process is summarized in figure 9.

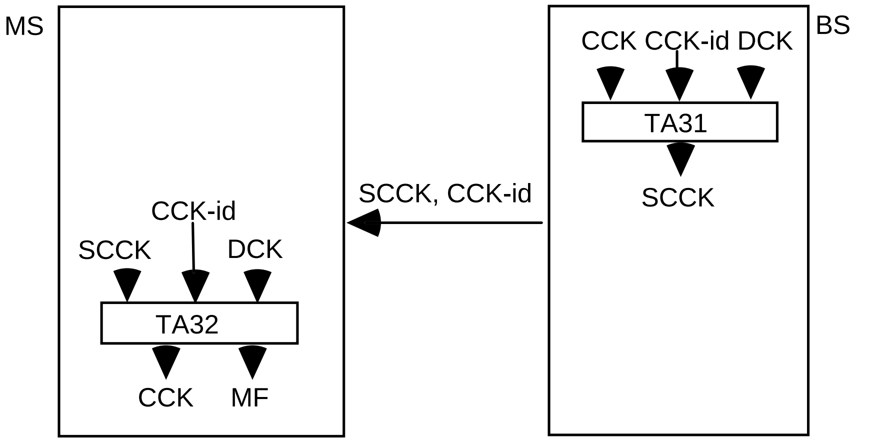


Figure 9: Distribution of a common cipher key

4.2.4 The SCK

To allow encrypted operation without prior authentication there shall be up to 32 SCKs available to each ITSI. SCK shall be a fixed value that should be known to the infrastructure and every MS. The SCKs are termed "static" because they shall not be generated or changed by the authentication exchange.

SCK shall be a member of an SCK set containing up to 32 keys, and each key shall be identified by its position in the SCK set (SCK number). Members of an SCK set may be shared amongst TETRA networks and so may be allocated in either the home network of the MS or by an external body representing more than one TETRA network.

SCKs may be protected for distribution in like manner to the CCK using algorithms TA51 and TA52.

An SCK shall be associated with two numbers: The SCK number (SCKN) shall address one of the 32 SCKs stored in a MS; The SCK Version Number (SCK-VN) shall identify the version of each of the 32 SCKs and shall be incremented for each new key. As with the CCK, SCK-VN is used to protect the distribution of the SCKs against replay. The SCKN is input to TA51 and output from TA52.

When distributing SCK by an OTAR mechanism (algorithms TA51 and TA52) a session key for OTAR (KSO) shall be used to protect the SCK in preference to the DCK. KSO shall be individual to each user and shall be derived from a user’s authentication key (K) and a random seed RSO with algorithm TA41.

NOTE: The OTAR mechanism described can only be used in systems for which a secret key K exists for each ITSI.

The result of the application of TA51 to SCK, SCK-VN, KSO and SCKN shall be a Sealed Static Cipher Key (SSCK). To allow recovery of SCK at the MS, SCK-VN and RSO shall be distributed together with SSCK.

For OTAR, SCKs may be generated in and distributed from any network entity. Two typical cases can be the following:

- SCKs may be generated in the same entity that stores the users' authentication keys, i.e. an authentication centre. This case is shown in figure 10.

- SCKs may be generated and distributed in a key distribution mobile. In this case, as shown in figure 11, the KSO shall be forwarded from the authentication centre to the MS in a secure way.

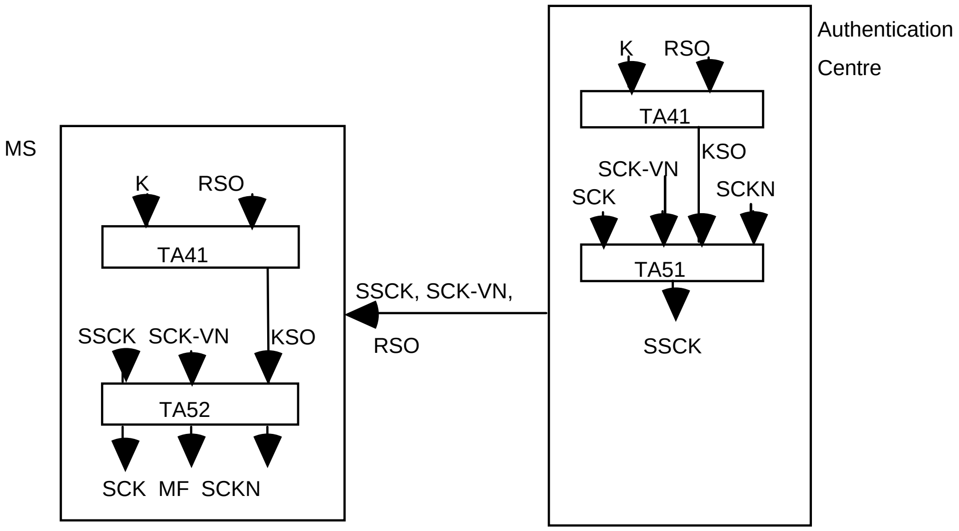


Figure 10: Distribution of SCK by an authentication centre

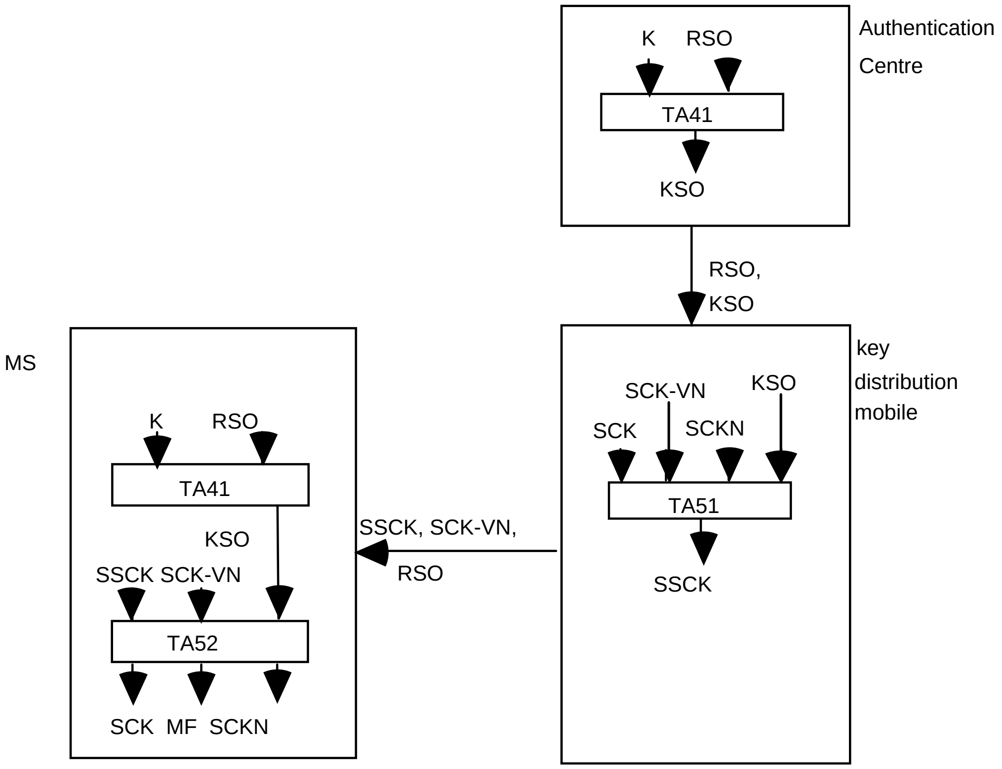


Figure 11: Distribution of SCK by a key distribution mobile

4.2.5 Encrypted Short Identity (ESI) mechanism

The ESI mechanism shall provide a means of protection of identities transmitted over the air interface. It operates in addition to, or as a replacement for, the Alias Short Subscriber Identity (ASSI) mechanism described in ETS 300 392-1 [1], clause 7.

NOTE: In standard TETRA addressing no alias addresses are associated with a group address in the home system. The ESI mechanism provides such an alias within a location area for all address types.

This subclause describes a mechanism that allows an MS to encrypt addresses. The mechanism is valid only for networks with air interface encryption applied. The mechanism shall be integrated with the use of CCK within a location area or with SCK for systems without authentication. Whenever encrypted signalling is used, the ESI shall be sent instead of the true identity. The mechanism uses algorithm TA61 as shown in figure 12.

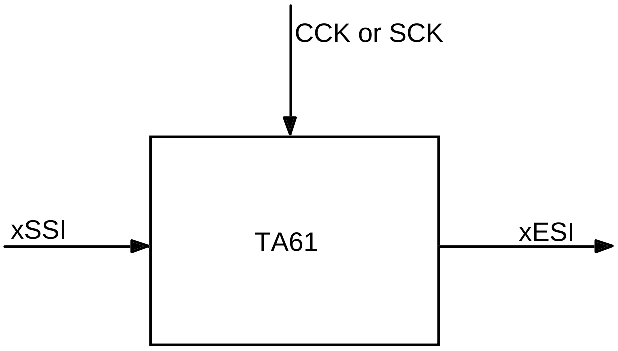


Figure 12: Generation of ESI from SSI and a cipher key

CCK is derived from algorithm TA32, and xSSI are all short addresses valid for the user (ISSI, GSSI, ASSI). The output xESI (IESI, GESI, AESI) shall be a cryptographic address. Only users in a location area with the correct values of CCK or SCK shall be able to identify messages addressed for their attention.

The bits incorporated in the MAC header to indicate encryption control shall also indicate application of ESI. Thus, if the bits are set to "0", encryption off, ESI shall not be used in that PDU, and the true SSI shall be transmitted. This enables a clear registration to be carried out with the MS's true identity visible. The use of signalling for AI encryption management is more fully described in subclause 6.1.5.2.

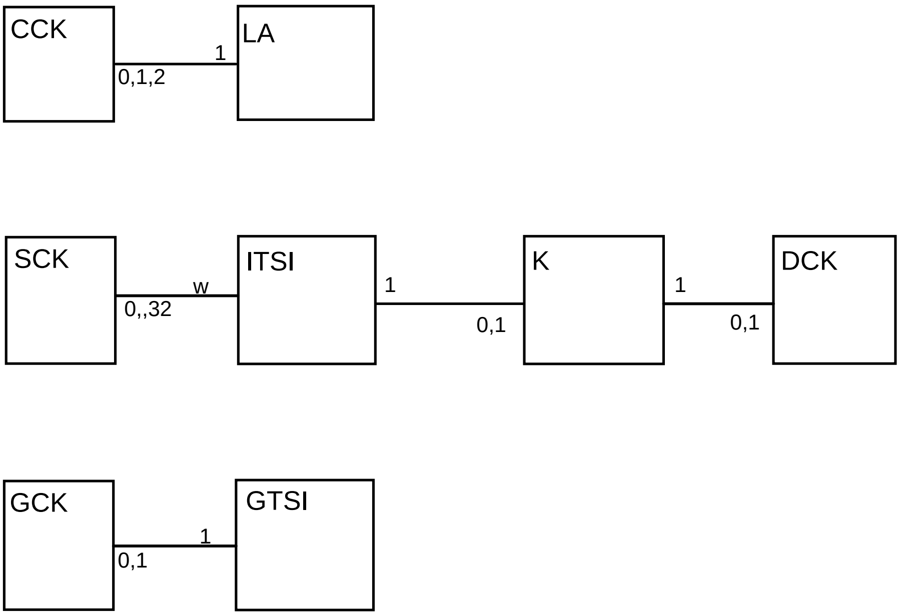
4.2.6 Summary of AI key management mechanisms

Table 1 summarizes the pre-conditions and lifetimes for each key.

Table 1 Cipher Key pre-conditions and lifetime

Key	Pre-condition	Lifetime
K	none	ITSI
DCK	authentication	Authentication period.
CCK	authentication	Not defined.
SCK	none	Not defined.
GCK	authentication	Not defined. Downloaded when using the Supplementary Service Dynamic Group Number Assignment (SS-DGNA).
NOTE: If OTAR is used for SCK, K is required as the key is sealed with a function of K.		

There is a fixed relationship between TETRA addresses and cipher keys shown in figure 13. The link between each entity describes a relationship "is associated with" and the numbers on the link define the form of this relationship. For example the ITSI-K relationship shows that for each ITSI there is zero or one K, and for each K there is only one ITSI.



NOTE 1: The SCK-ITSI relation allows 0 up to 32 keys to be associated with any ITSI but SCKs need not be shared among ITSIs.

NOTE 2: Only one CCK shall be in use at one time in an LA.

Figure 13: Mapping of Cipher Key and TETRA Address Relationships

4.3 Service description and primitives

4.3.1 Authentication primitives

At the TNMM Service Access Point (SAP), a specific service shall be provided to allow an application to initiate an authentication exchange and to receive its result. The MS-MM shall respond to an authentication demand from the SwMI. The primitives required shall be as follows:

- TNMM-AUTHENTICATE indication shall be used to report to the MS application the result of an authentication returned by the SwMI;

- TNMM-AUTHENTICATE confirm shall be used to confirm successful or failed authentication of the SwMI by the MS;

- TNMM-AUTHENTICATE request shall be used by the MS application to initiate an authentication of the SwMI;

- TNMM-AUTHENTICATE configure shall be used by the MS application to instruct the MM on the use of mutual authentication when responding to an authentication demand from the SwMI. This primitive shall also instruct MS-MM whether or not to include an authentication challenge when sending U-LOCATION UPDATE DEMAND to authenticate the SwMI when registering.

Table 2: TNMM AUTHENTICATE service primitives

GENERIC NAME	Specific name	PARAMETERS
TNMM-AUTHENTICATE	indication	result , reason
TNMM-AUTHENTICATE	confirm	result
TNMM-AUTHENTICATE	request	
TNMM-AUTHENTICATE	configure	mutual authentication authenticate at registration

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

result =

success;
failure of MS authentication;
failure of SwMI authentication;

reason =

authentication pending;

mutual authentication =

never;
always;

authenticate at registration =

never;
always.

4.3.2 SCK transfer primitives

A service shall be provided to allow an application to receive new SCKs either on demand or initiated by the SwMI. The primitives required shall be as follows:

- TNMM-SCK indication shall be used to provide the MS application with the SCKN and SCK-VN of each key received;

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

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

Table 3: TNMM SCK service primitives

Generic name	Specific name	Parameters
TNMM-SCK	indication	SCKN, SCK-VN
TNMM-SCK	confirm	Result
TNMM-SCK	request	SCKN

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

result =

SCK received successfully;
SCK failed to decrypt;

SCKN =

1;
2;
3;
…
32;

SCK-VN =

0;
…
2^{16}-1.

4.3.3 GCK transfer primitives

A service shall be provided to allow an application to receive new GCKs either on demand or initiated by the SwMI. The primitives required shall be as follows:

- TNMM-GCK indication shall be used to provide the MS application with the GTSI and GCK-VN of each key received;

- TNMM-GCK confirm shall be used by the MS application to confirm that the key information received is acceptable, or provide the reject reasons if not;

- TNMM-GCK request shall be used to request the distribution of a new GCK. It shall contain the address (GTSI) for each GCK requested. More than one GCK may be requested in one transaction.

Table 4: TNMM GCK service primitives

GENERIC NAME	Specific name	PARAMETERS
TNMM-GCK	indication	GTSI, GCK-VN
TNMM-GCK	confirm	Result
TNMM-GCK	request	GTSI

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

result =

GCK received successfully;
GCK failed to decrypt;

GTSI =

0;
1;
2;
…
2^{48}-1;

GCK-VN =

0;
…
2^{16}-1.

4.4 Definition of protocols

4.4.1 Authentication state transitions

Figure 14 gives an overview of the received PDUs that result in a change of authentication state. It is assumed that the initial state is Not-Authenticated and that demands for authentication may also be made when parties are in an authenticated state.

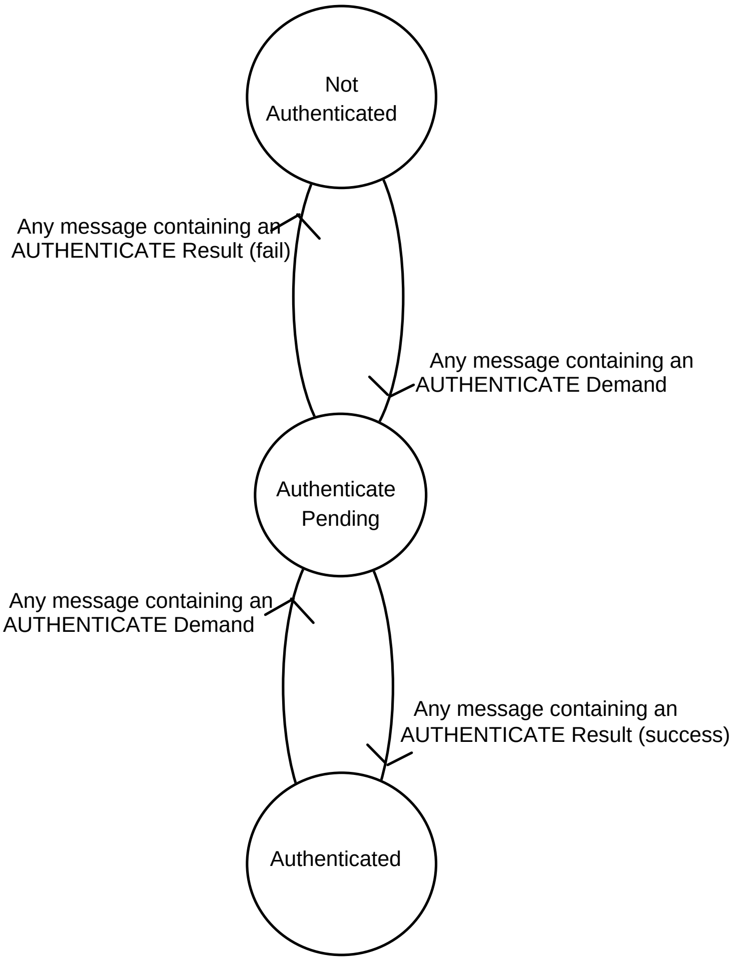

Not Authenticated
Any message containing an AUTHENTICATE Result (fail)
Any message containing an AUTHENTICATE Demand
Authenticate Pending
Any message containing an AUTHENTICATE Demand
Any message containing an AUTHENTICATE Result (success)
Authenticated

Figure 14: Authentication state transitions

4.4.2 Overview of authentication protocol

The air interface authentication protocol shall use the Mobility Management (MM) service of layer 3 in the TETRA protocol stack (see ETS 300 392-2 [2], clause 14).

An authentication exchange can be requested, either explicitly or as part of the registration procedure. It can be initiated by the MS or SwMI. The initiating side shall send an "AUTHENTICATION DEMAND" PDU that shall always be answered by the other side with an "AUTHENTICATION RESPONSE" PDU. Success or failure of the authentication shall be communicated by a specific "AUTHENTICATION RESULT" PDU.

The recipient of the first authentication demand may instigate mutual authentication by use of the mutual authentication indicator, and by sending its challenge together with the response to the first challenge. In this case, the response to this second challenge shall be sent together with the result of the first challenge. This mechanism saves signalling, as only one random seed RS is required, and the functions can be combined in PDUs requiring fewer transmissions at the air interface.

After a successful authentication exchange, both MS and SwMI shall replace both parts of the derived cipher key, DCK1 or DCK2, with the newly calculated values, and the derived cipher key DCK accordingly.

Descriptions of the protocol, together with Message Sequence Charts (MSCs), are given in subclauses 4.4.2.1 to 4.4.2.9. In each case the label in the MSC is mapped to a single statement in the text (if the same label appears on multiple diagrams the same text applies).

AUTHENTICATION DEMAND PDUs shall always be sent in clear. The further registration and authentication exchange is then carried out in clear until a new key has been derived and established. The exact point when encryption is switched on during authentication is shown in the message sequence charts for each case (subclauses 4.4.2.1 through 4.4.2.9).

NOTE 1: If an ASSI has been assigned the true SSI remains protected at the air interface in an authentication failure case.

NOTE 2: If an authentication fails and a valid DCK existed immediately prior to the authentication attempt the old DCK may be considered as still valid, or alternatively the parties may revert to clear.

The initiation of registration by an MS shall always be in clear.

In the MSCs given in subclauses 4.4.2.1 through 4.4.2.9 the position of the TNMM primitives is shown for information only.

4.4.2.1 Case 1: SwMI authenticates MS

D-AUTHENTICATION DEMAND shall contain RAND1+RS;
U-AUTHENTICATION RESPONSE shall contain RES1;
D-AUTHENTICATION RESULT shall contain R1.

The normal message sequence in this case shall be according to figure 15.

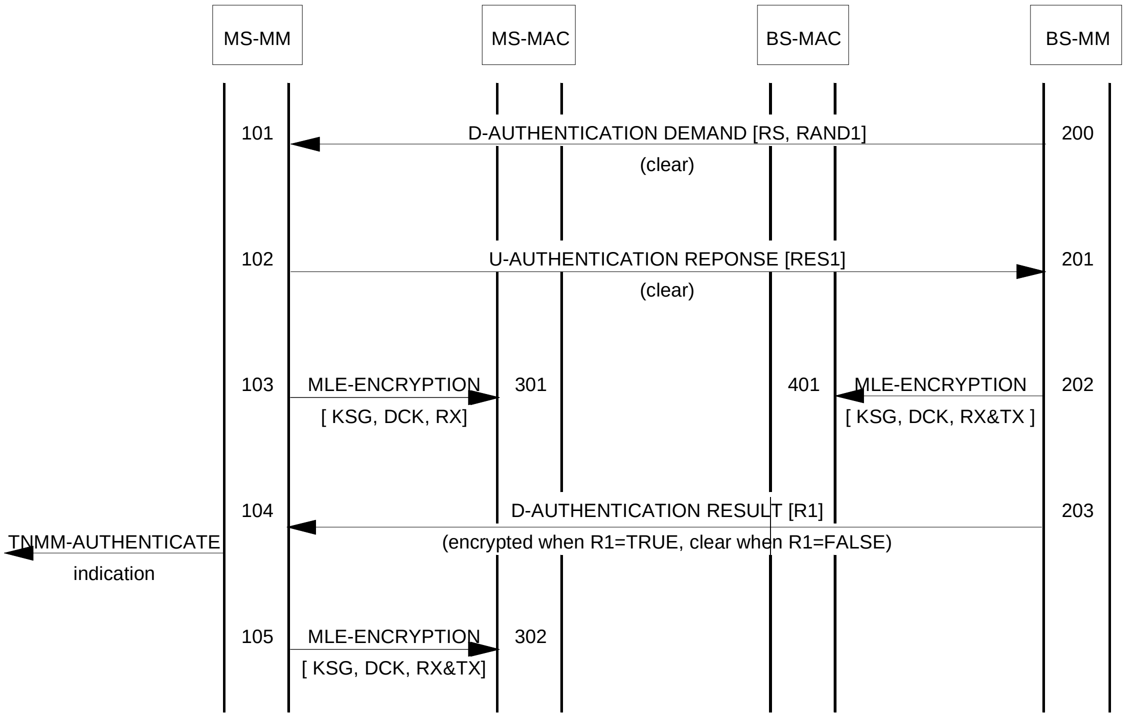


Figure 15: Authentication of MS by SwMI

200 BS-MM shall challenge MS-MM to authenticate by sending RS and RAND1. The SwMI shall also calculate XRES1 and DCK1 using algorithms TA11 and TA12 using RS and RAND1 as inputs.

101 MS-MM shall retrieve RS and RAND1 from the authentication challenge and shall run algorithms TA11 and TA12 to generate RES1 and DCK1. Since, in this case, the MS is configured for unilateral authentication, MS-MM shall run algorithm TB4 with DCK2=0 to generate DCK.

102 MS-MM shall respond to the authentication challenge by sending RES1 to BS-MM. Since the MS is not configured to mutually authenticate the SwMI, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESPONSE to be false and RAND2 shall not be included in this PDU.

103 MS-MM shall configure MS-MAC to receive with the newly calculated DCK.

301 MS-MAC shall be configured to receive with DCK.

201 BS-MM shall retrieve RES1 and compare it with the previously calculated XRES1 (as described in 200) to decide whether or not authentication was successful.

202 If the authentication was successful, and since the MS has not requested mutual authentication, BS-MM shall run algorithm TB4 with DCK2=0 to generate DCK and BS-MM shall configure BS-MAC to receive and transmit with the newly calculated DCK.

If the authentication was not successful, the SwMI shall continue to receive and transmit in clear or using the DCK in use before this authentication procedure was initiated.

401 BS-MAC shall be configured to receive and transmit with DCK.

203 BS-MM shall send the result R1 of the MS-MM authentication to MS-MM to indicate whether or not authentication was successful.

If authentication was successful, BS-MM shall set authentication result to TRUE and shall send D-AUTHENTICATION RESULT encrypted with the newly calculated DCK. Since, in this case, there is no mutual authentication, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESULT to be false and RES2 shall not be included in this PDU.

If authentication was not successful, BS-MM shall instead set authentication result to FALSE and shall send D-AUTHENTICATION RESULT in clear. The "Mutual authentication flag" in D-AUTHENTICATION RESULT shall be set to false and RES2 shall not be included in this PDU.

NOTE: The layer 2 acknowledgement to the preceding uplink message may be sent in clear, or may be encrypted. The timing of the acknowledgement and the setting of encryption parameters to ensure successful reception of this acknowledgement is outside the scope of this part of the ETS.

104 MS-MM shall retrieve R1.

If R1 indicates successful authentication, MS-MM shall run algorithm TB4 with DCK2=0 to obtain DCK.

If authentication was not successful, MS-MM shall not calculate DCK.

105 If authentication was successful, MS-MM shall configure MS-MAC to receive and transmit with the newly calculated DCK.

If authentication was not successful, the MS shall configure MS-MAC to receive and transmit in clear, or if the MS was using a DCK before this authentication procedure was started, the MS shall use this old DCK for subsequent signalling.

302 MS-MAC shall be configured to receive and transmit with DCK.

4.4.2.2 Case 2: MS authenticates SwMI

U-AUTHENTICATION DEMAND shall contain RAND2;
D-AUTHENTICATION RESPONSE shall contain RES2+RS;
U-AUTHENTICATION RESULT shall contain R2.

The normal message sequence in this case shall be according to figure 16.

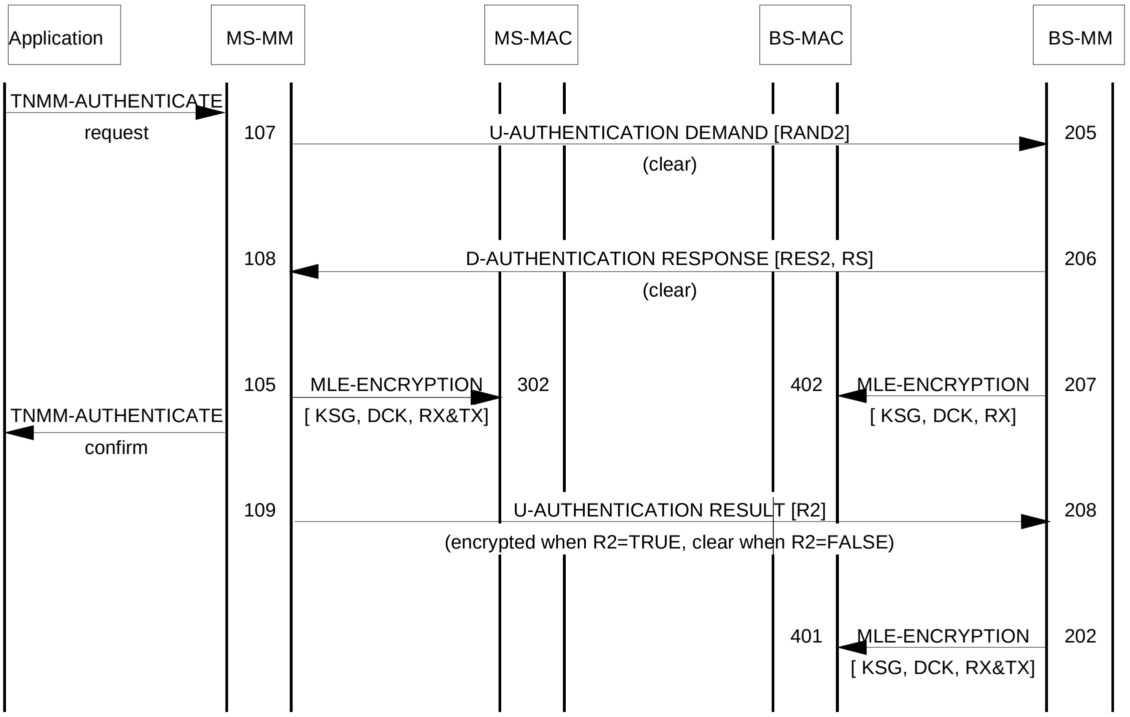


Figure 16: Authentication of the SwMI by the MS

107 MS-MM shall challenge BS-MM to authenticate by sending the challenge, RAND2.

205 BS-MM shall retrieve RAND2 and run algorithms TA21 and TA22 to generate RES2, and DCK2. Since, in this case, the SwMI is configured for unilateral authentication, BS-MM shall run TB4 with DCK1=0 to generate DCK.

206 BS-MM shall send the authentication response to MS-MM containing RES2 and RS. Since, in this case, the SwMI is not configured to mutually authenticate the MS, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESPONSE to be false and RAND1 shall not be included in this PDU.

207 BS-MM shall configure BS-MAC to receive with the newly calculated DCK.

402 BS-MAC shall be configured to receive with DCK.

108 MS-MM shall retrieve RES2 and RS, and run algorithms TA21 and TA22 to generate DCK2 and XRES2. MS-MM shall compare XRES2 and RES2 to decide whether or not authentication of the SwMI was successful.

If authentication was successful, and, since the SwMI has not requested mutual, MS-MM shall run algorithm TB4 with DCK1=0 to generate DCK.

If authentication was not successful, the MS should not attempt to calculate DCK.

105 If authentication was successful, MS-MM shall configure MS-MAC to receive and transmit with the newly calculated DCK.

If authentication was not successful, the MS shall configure MS-MAC to receive and transmit in clear, or if the MS was using a DCK before this authentication procedure was started, the MS shall use this old DCK for subsequent signalling.

302 MS-MAC shall be configured to receive and transmit with DCK.

109 MS-MM shall send the authentication result, R2, to BS-MM to indicate whether or not authentication was successful.

If authentication was successful, MS-MM shall send U-AUTHENTICATION RESULT encrypted with the newly calculated DCK. Since, in this case, there is no mutual authentication, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be false and RES1 shall not be included in this PDU.

If authentication was not successful, MS-MM shall send U-AUTHENTICATION RESULT in clear The "Mutual authentication flag" in U-AUTHENTICATION RESULT shall be set to false and RES1 shall not be included in this PDU.

208 BS-MM shall retrieve R2.

If R2 indicates successful authentication, BS-MM shall run algorithm TB4 DCK2=0 to generate DCK.

If authentication was not successful, BS-MM shall not calculate DCK.

202 If authentication was successful, BS-MM shall configure BS-MAC to receive and transmit with the newly calculated DCK.

If authentication was not successful, the SwMI shall configure BS-MAC to receive and transmit in clear or using the DCK in use before this authentication procedure was started by the MS.

401 BS-MAC shall be configured to receive and transmit with DCK.

4.4.2.3 Case 3: Mutual authentication initiated by SwMI

D-AUTHENTICATION DEMAND shall contain RAND1+RS,
U-AUTHENTICATION RESPONSE shall contain RES1+RAND2,
D-AUTHENTICATION RESULT shall contain RES2+R1,
U-AUTHENTICATION RESULT shall contain R2.

The normal message sequence in this case shall be according to figure 17.

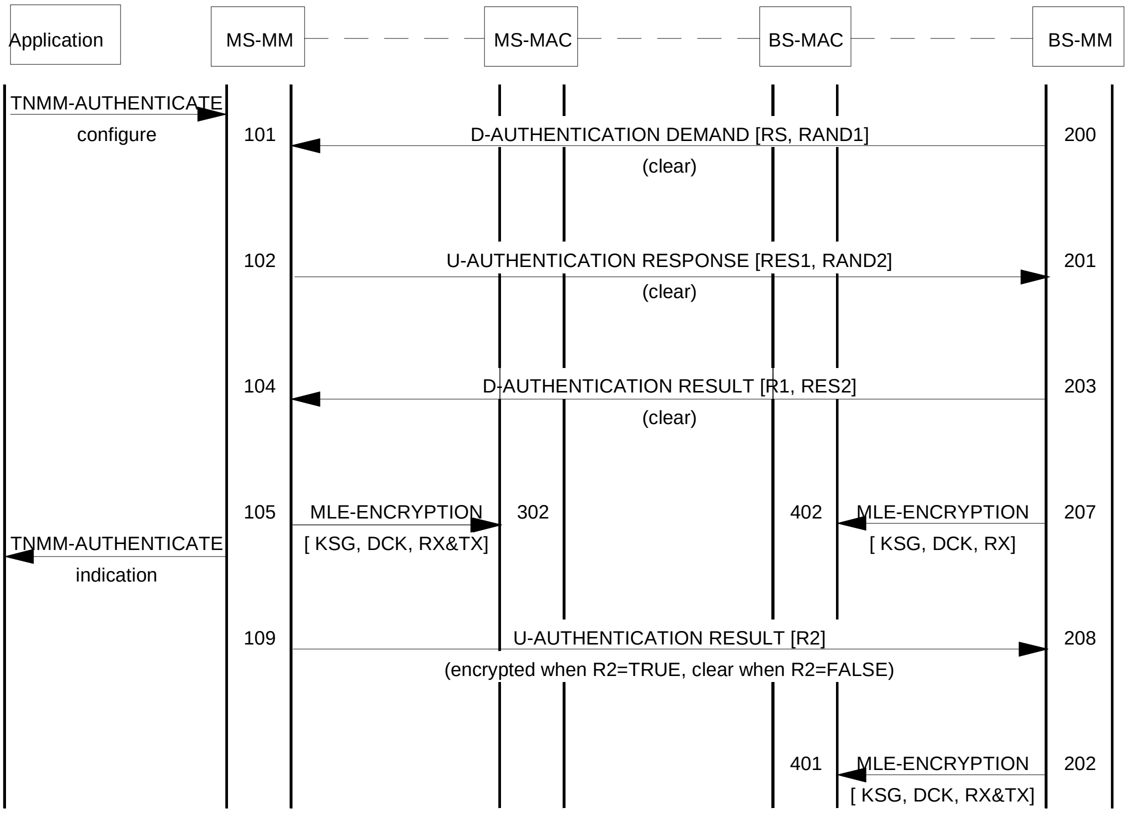


Figure 17: Mutual authentication initiated by SwMI

200 BS-MM shall challenge MS-MM to authenticate by sending RS and RAND1. The SwMI shall also calculate XRES1 and DCK1 using algorithms TA11 and TA12 and using RS and RAND1 as inputs.

101 MS-MM shall retrieve RS and RAND1 from the authentication challenge and shall run algorithms TA11 and TA12 to generate RES1 and DCK1. Since, in this case, the MS is configured to respond to authentication challenges from BS-MM with a mutual authentication, MS-MM should not calculate DCK since MS-MM does not yet have DCK2.

102 MS-MM shall respond to the authentication challenge by sending RES1 to BS-MM. Since, in this case, the MS is configured for mutual authentication, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESPONSE to be true and RAND2 shall be included in this PDU.

201 BS-MM shall retrieve RES1 and compare it with the previously calculated XRES1 (as described in 200) to decide whether or not authentication of the MS was successful.

If authentication of the MS was successful and, since, in this case, authentication is mutual, BS-MM shall also retrieve RAND2 from U-AUTHENTICATION RESPONSE and the SwMI shall generate DCK2 and RES2 using algorithms TA21 and TA22. BS-MM shall then run algorithm TB4 with DCK1 and DCK2 as inputs to generate DCK.

If authentication of the MS was not successful, BS-MM shall not calculate DCK2, RES2 or DCK.

203 BS-MM shall send the MS authentication result, R1 (success or failure), to MS-MM to indicate whether or not authentication of the MS was successful.

If authentication of the MS was successful, and, since the MS has requested mutual authentication, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESULT to be true and the response, RES2, shall be included in this PDU

If authentication of the MS was not successful, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESULT to be false and the response, RES2, shall not be included in this PDU.

207 If authentication of the MS was successful, BS-MM shall configure BS-MAC to receive with the newly calculated DCK.

If authentication of the MS was not successful, the SwMI shall continue to receive and transmit in clear, or if the SwMI was using a DCK before this authentication procedure was started the SwMI shall use this old DCK for subsequent signalling.

402 BS-MAC shall be configured to receive with DCK.

104 MS-MM shall retrieve R1.

If R1 indicates successful authentication, MS-MM shall retrieve RES2 and the MS shall run algorithms TA21 and TA22 to generate DCK2 and XRES2. MS-MM shall then compare XRES2 and RES2 to decide whether or not authentication of the SwMI was successful.

If authentication of the SwMI and MS were both successful, the MS shall run algorithm TB4 with DCK1 and DCK2 as inputs to give DCK.

If R1 does not indicate successful authentication of the MS, the MS shall not calculate DCK2 or XRES2.

If either authentication of the SwMI or of the MS was not successful, the MS should not attempt to calculate DCK.

105 If the MS and SwMI authentication were both successful, MS-MM shall configure MS-MAC to receive and transmit with the newly calculated DCK.

If either authentication of the SwMI or of the MS was not successful, the MS shall continue to receive and transmit in clear, if the MS was using a DCK before this authentication procedure was started the MS shall use this old DCK for subsequent signalling.

302 MS-MAC shall be configured to receive and transmit with DCK.

109 If authentication of the MS was successful as indicated by R1, MS-MM shall send the authentication result, R2, to BS-MM in U-AUTHENTICATION RESULT which shall be encrypted using the newly calculated DCK. Since this is the final stage of the mutual authentication procedure, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be false and RES1 shall not be included in this PDU.

If authentication of the MS was successful but authentication of the SwMI was not successful, MS-MM shall instead send U-AUTHENTICATION RESULT in clear to indicate the result, R2.

If authentication of the MS was not successful, MS-MM shall not send U-AUTHENTICATION RESULT.

208 BS-MM shall retrieve R2.

If R2 indicates successful authentication of the SwMI, the SwMI shall run algorithm TB4 with DCK1 and DCK2 as inputs to generate DCK.

If R2 does not indicate successful authentication of the SwMI, the SwMI shall not calculate DCK.

202 If the MS and SwMI authentication were both successful, BS-MM shall configure BS-MAC to receive and transmit with the newly calculated DCK.

If the either of the MS or SwMI authentication was not successful, BS-MM shall configure MS-MAC to receive and transmit in clear, or if the BS was using a DCK before this authentication procedure was started the BS shall use this old DCK for subsequent signalling.

401 BS-MAC shall be configured to receive and transmit with DCK.

4.4.2.4 Case 4: Mutual authentication initiated by MS

U-AUTHENTICATION DEMAND shall contain RAND2;
D-AUTHENTICATION RESPONSE shall contain RES2+RS+RAND1;
U-AUTHENTICATION RESULT shall contain RES1+R2;
D-AUTHENTICATION RESULT shall contain R1.

The normal message sequence in this case shall be according to figure 18.

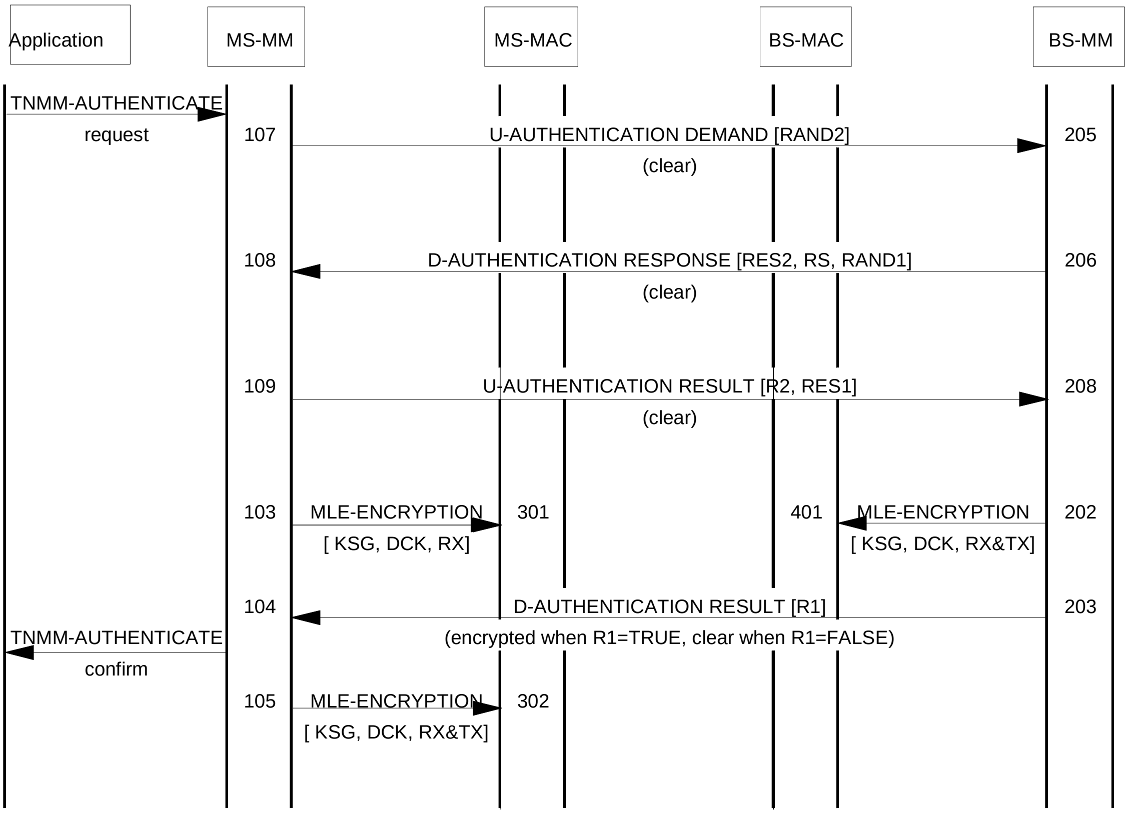


Figure 18: Mutual authentication initiated by MS

107 MS-MM shall challenge BS-MM (SwMI) to authenticate by sending the challenge, RAND2.

205 BS-MM shall retrieve RAND2 from the authentication challenge and run algorithms TA21 and TA22 to generate RES2 and DCK2. Since, in this case the SwMI is configured is configured to respond to authentication challenges from MS-MM with a mutual authentication, BS-MM should not calculate DCK since BS-MM does not yet have DCK1.

206 BS-MM shall respond to the authentication challenge by sending RES2 and RS to MS-MM. Since, in this case, the SwMI is configured for mutual authentication, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESPONSE to be true and RAND1 shall be included in this PDU.

108 MS-MM shall retrieve RES2 and RS, and run algorithms TA21 and TA22 to generate DCK2 and XRES2. MS-MM shall compare XRES2 and RES2 to decide whether or not authentication of the SwMI was successful.

If authentication of the SwMI was successful and, since, in this case, authentication is mutual, MS-MM shall also retrieve RAND1 from D-AUTHENTICATION RESPONSE and the MS shall generate DCK1 and RES1 using algorithms TA11 and TA12. MS-MM shall then run algorithm TB4 with DCK1 and DCK2 as inputs to generate DCK.

If authentication of the SwMI was not successful, MS-MM shall not calculate DCK1, RES1 or DCK.

109 MS-MM shall send the authentication result, R2 (success or failure), to BS-MM to indicate whether or not authentication of the SwMI was successful.

If authentication of the SwMI was successful, and, since the SwMI has requested mutual authentication, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be true and the response, RES1, shall be included in this PDU.

If authentication of the SwMI was not successful, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be false and the response, RES1, shall not be included in this PDU.

103 If the authentication of the SwMI was successful, MS-MM shall configure MS-MAC to receive with the newly calculated DCK.

If authentication of the SwMI was not successful, the MS shall continue to receive and transmit in clear or using the DCK in use before this authentication procedure was started by the MS.

301 MS-MAC shall be configured to receive with DCK.

208 BS-MM shall retrieve R2.

If R2 indicates successful authentication, BS-MM shall retrieve RES1 and the SwMI shall run algorithms TA11 and TA12 to generate DCK1 and XRES1. BS-MM shall then compare XRES1 and RES1 to decide whether or not authentication of the MS was successful (R1).

If authentication of the SwMI and MS were both successful, the SwMI shall run algorithm TB4 with DCK1 and DCK2 as inputs to generate DCK.

If R2 does not indicate successful authentication of the SwMI, the SwMI should not attempt to retrieve RES1 or calculate DCK1 or XRES1.

If either authentication of the SwMI or of the MS was not successful, the SwMI should not attempt to calculate DCK.

202 If the MS and SwMI authentication were both successful, BS-MM shall configure BS-MAC to receive and transmit with the newly calculated DCK.

If the either of the MS or SwMI authentication was not successful, BS-MM shall configure MS-MAC to receive and transmit in clear, or if the BS was using a DCK before this authentication procedure was started the BS shall use this old DCK for subsequent signalling.

401 BS-MAC shall be configured to receive and transmit with DCK.

203 If authentication of the SwMI was successful as indicated by R2, BS-MM shall send the authentication result, R1, using D-AUTHENTICATION RESULT which shall be encrypted using the newly calculated DCK. Since this is the final stage of the mutual authentication procedure, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESULT to be false and RES2 shall not be included in this PDU.

If authentication of the SwMI was successful but authentication of the MS was not successful, BS-MM shall send D-AUTHENTICATION RESULT in clear to indicate the result, R1.

If authentication of the SwMI was not successful, BS-MM shall not send D-AUTHENTICATION RESULT.

104 MS-MM shall retrieve R1.

If R1 indicates successful authentication of the MS, the MS shall run algorithm TB4 with DCK1 and DCK2 as inputs to give DCK.

If R1 does not indicate successful authentication of the MS, the MS shall not calculate DCK.

105 If the MS and SwMI authentication were both successful, MS-MM shall configure MAC to receive and transmit with the newly calculated DCK.

If either authentication of the SwMI or of the MS was not successful, the MS shall continue to receive and transmit in clear, if the MS was using a DCK before this authentication procedure was started the MS shall use this old DCK for subsequent signalling.

302 MS-MAC shall be configured to receive and transmit with DCK.

4.4.2.5 Case 5: SwMI authenticates MS during registration

U-LOCATION UPDATE DEMAND may contain CCK request;
D-AUTHENTICATION DEMAND shall contain RAND1+RS;
U-AUTHENTICATION RESPONSE shall contain RES1;
D-LOCATION UPDATE ACCEPT shall contain R1 (+ SCCK + CCK-id) (+ TEI request);
(U-TEI PROVIDE shall contain TEI).

The normal message sequence in this case shall be according to figure 19.

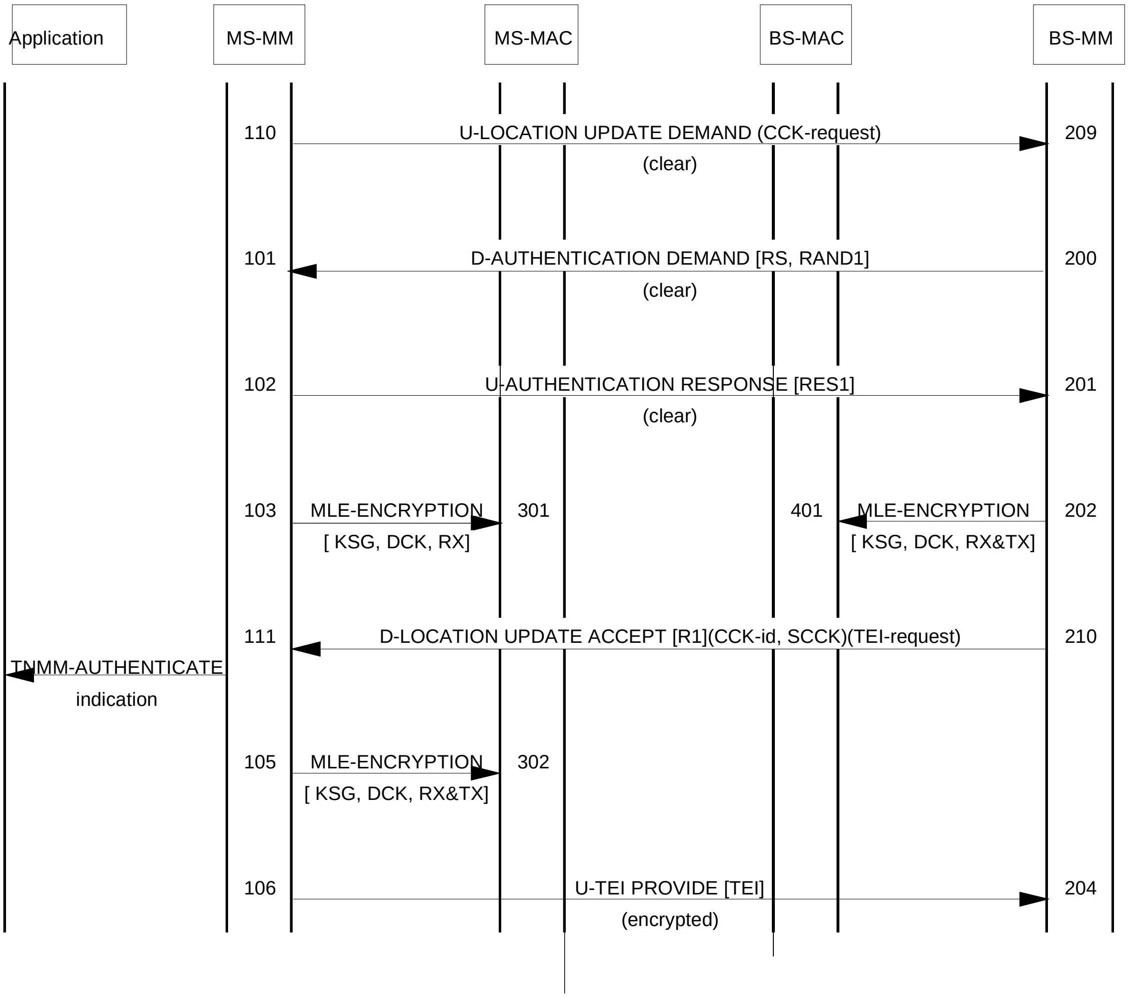


Figure 19: SwMI authentication of MS during registration procedure

110 MS-MM initiates registration. U-LOCATION UPDATE DEMAND may be sent by the MS as a result of one of the following registration scenarios:

- MS-initiated registration due to roaming (i.e. change of location area);
- user application initiated registration;
- MS-initiated registration due to migration after identity exchange with the SwMI;
- MS-initiated forward registration;
- after receiving D-LOCATION UPDATE COMMAND as part of SwMI-initiated registration.

In the case of migration which requires identity exchange with the SwMI, the MS shall not include an authentication challenge or CCK request in the first U-LOCATION UPDATE DEMAND of the procedure. The MS shall wait until it has received an SSI for use on the system (sent in D-LOCATION UPDATE PROCEEDING) and then include any authentication challenge in the second U-LOCATION UPDATE DEMAND which is sent using the visitor SSI allocated during identity exchange. Similarly, the SwMI shall not attempt to authenticate an MS when U-LOCATION UPDATE DEMAND is requesting an identity exchange, but only when the MS attempts registration with an ISSI or VASSI.

MS-MM may include the type 3 element "Authentication uplink" in U-LOCATION UPDATE DEMAND to request that the SwMI supplies the CCK for the location area with which the MS is attempting to register. Since, in this case, the MS is not configured to authenticate the SwMI during registration, the MS shall not include the random challenge, RAND2, in U-LOCATION UPDATE DEMAND.

209 Since, in this case, the SwMI is configured to authenticate an MS at registration, the SwMI shall initiate authentication of the MS as described by case 1 in subclause 4.4.2.1.

200 Refer to case 1 in subclause 4.4.2.1.

101 Refer to case 1 in subclause 4.4.2.1.

102 Refer to case 1 in subclause 4.4.2.1.

103 Refer to case 1 in subclause 4.4.2.1.

301 Refer to case 1 in subclause 4.4.2.1.

201 Refer to case 1 in subclause 4.4.2.1.

202 Refer to case 1 in subclause 4.4.2.1.

401 Refer to case 1 in subclause 4.4.2.1.

210 BS-MM shall inform MS-MM whether or not authentication was successful.

If authentication was successful and registration is to be accepted by the SwMI, BS-MM shall send D-LOCATION UPDATE ACCEPT encrypted with the newly calculated DCK. BS-MM shall include the "Authentication downlink" type 3 element in D-LOCATION UPDATE ACCEPT to convey R1. BS-MM may request MS-MM to supply the MS TEI by setting the "TEI request flag" in the "Authentication downlink" element. If the MS requested the CCK information in U-LOCATION UPDATE DEMAND, BS-MM shall include the "CCK information for current LA" in the "Authentication downlink" element.

NOTE 1: The SwMI should not ask the MS to supply its TEI unless the TEI can be sent using an encrypted PDU. The MS should not provide its TEI over the air interface in clear.

If authentication was not successful, BS-MM shall instead send D-LOCATION UPDATE REJECT in clear. D-LOCATION UPDATE REJECT shall contain a reject reason which shall indicate that authentication has failed.

111 If MS-MM receives D-LOCATION UPDATE ACCEPT, MS-MM shall retrieve R1 which should indicate successful authentication. If authentication has failed, the MS should receive D-LOCATION UPDATE REJECT.

If authentication was successful, MS-MM shall run algorithm TB4 with DCK2=0 to obtain DCK. If the MS requested CCK information in U-LOCATION UPDATE DEMAND, MS-MM shall retrieve the "CCK information for current LA" from the "Authentication downlink" element in D-LOCATION UPDATE ACCEPT.

If authentication was not successful, MS-MM shall not calculate DCK.

105 Refer to case 1 in subclause 4.4.2.1.

302 Refer to case 1 in subclause 4.4.2.1.

106 If authentication was successful and BS-MM requested the MS TEI in D-LOCATION UPDATE ACCEPT, MS-MM shall provide the MS TEI by sending U-TEI PROVIDE which shall contain the MS TEI and the address extension (MCC and MNC) for the MS so that the SwMI has the full ITSI of the MS.

NOTE 2: The BS should not ask the MS to supply its TEI unless encryption is on. The MS should not provide its TEI over the air interface in clear.

If authentication was not successful or the SwMI did not request the MS TEI in D-LOCATION UPDATE ACCEPT, U-TEI PROVIDE shall not be sent.

204 BS-MM shall retrieve the MS TEI from U-TEI PROVIDE. The BS may record the association of ITSI and TEI.

4.4.2.6 Case 6: MS authenticates SwMI during registration

U-LOCATION UPDATE DEMAND shall contain RAND2 (+ CCK-request);
D-AUTHENTICATION RESPONSE shall contain RES2+RS;
U-AUTHENTICATION RESULT shall contain R2;
D-LOCATION UPDATE ACCEPT may contain SCCK + CCK-id (+ TEI-request);
(U-TEI PROVIDE shall contain TEI).

The normal message sequence in this case shall be according to figure 20.

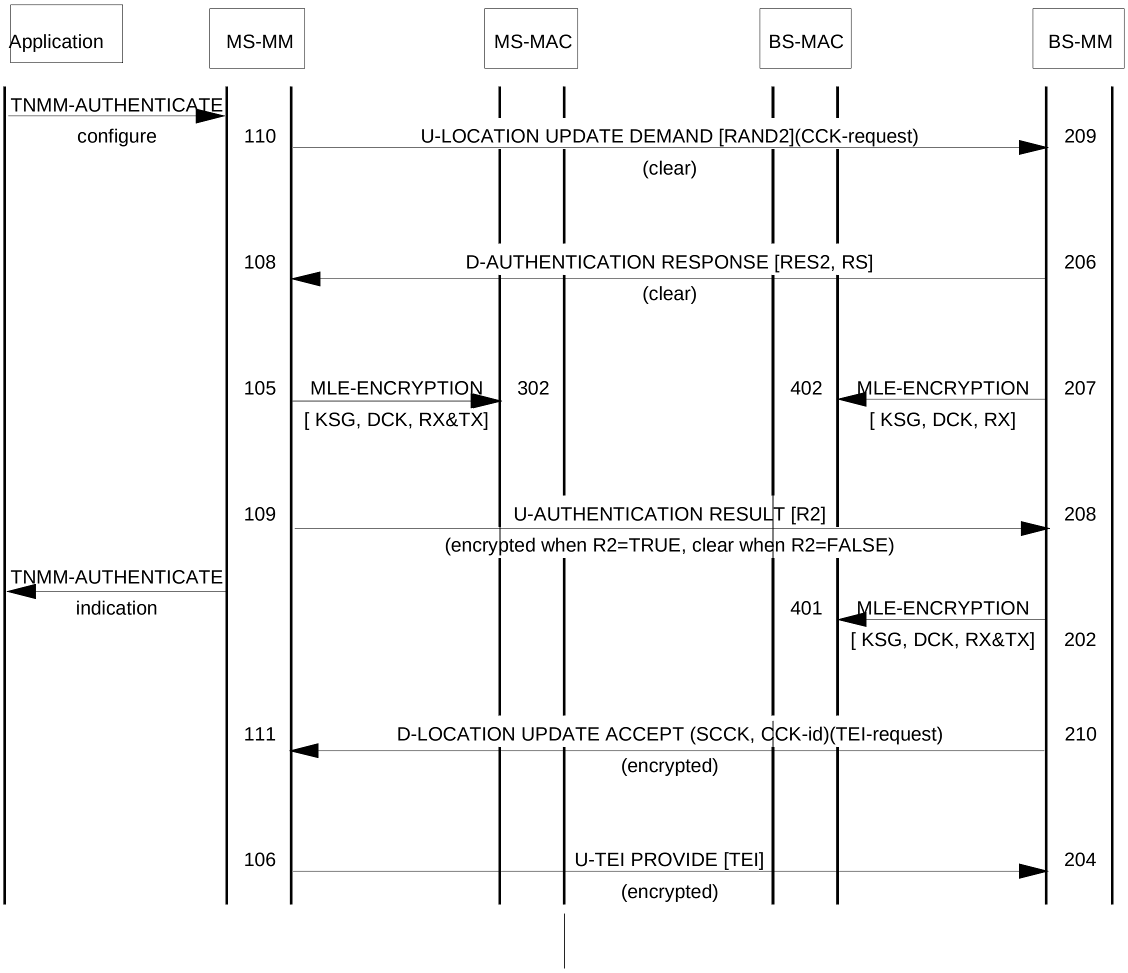


Figure 20: MS authentication of SwMI by the MS during registration

110 MS-MM initiates registration. U-LOCATION UPDATE DEMAND may be sent by the MS as a result of one of the following registration scenarios:

- MS-initiated registration due to roaming (i.e. change of location area);
- user application initiated registration;
- MS-initiated registration due to migration after identity exchange with the SwMI;
- MS-initiated forward registration;
- after receiving D-LOCATION UPDATE COMMAND as part of SwMI-initiated registration.

In the case of migration which requires identity exchange with the SwMI, the MS shall not include an authentication challenge or CCK request in the first U-LOCATION UPDATE DEMAND of the procedure. The MS shall wait until it has received an SSI for use on the system (sent in D-LOCATION UPDATE PROCEEDING) and then include any authentication challenge in the second U-LOCATION UPDATE DEMAND which is sent using the visitor SSI allocated during identity exchange. Similarly, the SwMI shall not attempt to authenticate an MS when U-LOCATION

UPDATE DEMAND is requesting an identity exchange, but only when the MS attempts registration with an ISSI or VASSI.

209 BS-MM shall retrieve RAND2 and run algorithms TA21 and TA22 to generate RES2 and DCK2. Since, in this case, the SwMI is not configured for mutual authentication, BS-MM shall run TB4 with DCK1=0 to generate DCK. If the MS has requested CCK information, BS-MM shall seal the CCK which is valid for the LA with which the MS is trying to register using algorithm TA41. CCK shall be sealed with newly calculated DCK. BS-MM shall then respond to the authentication request from the MS as described by case 2 in subclause 4.4.2.2.

206 Refer to case 2 in subclause 4.4.2.2.

207 Refer to case 2 in subclause 4.4.2.2.

402 Refer to case 2 in subclause 4.4.2.2.

108 Refer to case 2 in subclause 4.4.2.2.

105 Refer to case 2 in subclause 4.4.2.2.

302 Refer to case 2 in subclause 4.4.2.2.

109 Refer to case 2 in subclause 4.4.2.2.

208 Refer to case 2 in subclause 4.4.2.2.

202 Refer to case 2 in subclause 4.4.2.2.

401 Refer to case 2 in subclause 4.4.2.2.

210 If authentication was successful and registration is to be accepted by the SwMI, BS-MM shall send D-LOCATION UPDATE ACCEPT encrypted with the newly calculated DCK. BS-MM may include the "Authentication downlink" type 3 element in D-LOCATION UPDATE ACCEPT to request MS-MM to supply the MS TEI by setting the "TEI request flag". Since, in this case, the authentication procedure has already been completed, R1 element shall be set to "successful". If the MS requested the CCK information in U-LOCATION UPDATE DEMAND, BS-MM shall include the "CCK information for current LA" in the "Authentication downlink" element.

NOTE 1: The SwMI should not ask the MS to supply its TEI unless the TEI can be sent using an encrypted PDU. The MS should not provide its TEI over the air interface in clear.

If authentication was not successful, BS-MM should instead send D-LOCATION UPDATE REJECT in clear. D-LOCATION UPDATE REJECT shall contain a reject reason which shall indicate that authentication has failed.

111 If MS-MM receives D-LOCATION UPDATE ACCEPT, after completing authentication of the SwMI, MS-MM shall ignore R1. If authentication has failed, the MS should receive D-LOCATION UPDATE REJECT.

106 If authentication was successful and BS-MM requested the MS TEI in D-LOCATION UPDATE ACCEPT, MS-MM shall provide the MS TEI by sending U-TEI PROVIDE which shall contain the MS TEI and the address extension (MCC and MNC) for the MS so that the SwMI has the full ITSI of the MS.

NOTE 2: Tthe BS should not ask the MS to supply its TEI unless encryption is on. The MS should not provide its TEI over the air interface in clear.

If authentication was not successful or the SwMI did not request the MS TEI in D-LOCATION UPDATE ACCEPT, U-TEI PROVIDE shall not be sent.

204 BS-MM shall retrieve the MS TEI from U-TEI PROVIDE. The BS may record the association of ITSI and TEI.

4.4.2.7 Case 7: Mutual authentication initiated by MS during registration

U-LOCATION UPDATE DEMAND shall contain RAND2 (+ CCK-request);
D-AUTHENTICATION RESPONSE shall contain RES2+RS+RAND1;
U-AUTHENTICATION RESULT shall contain RES1+R2;
D-LOCATION UPDATE ACCEPT shall contain R1 (+ SCCK + CCK-id) (+ TEI-request);
(U-TEI PROVIDE shall contain TEI).

The normal message sequence in this case shall be according to figure 21.

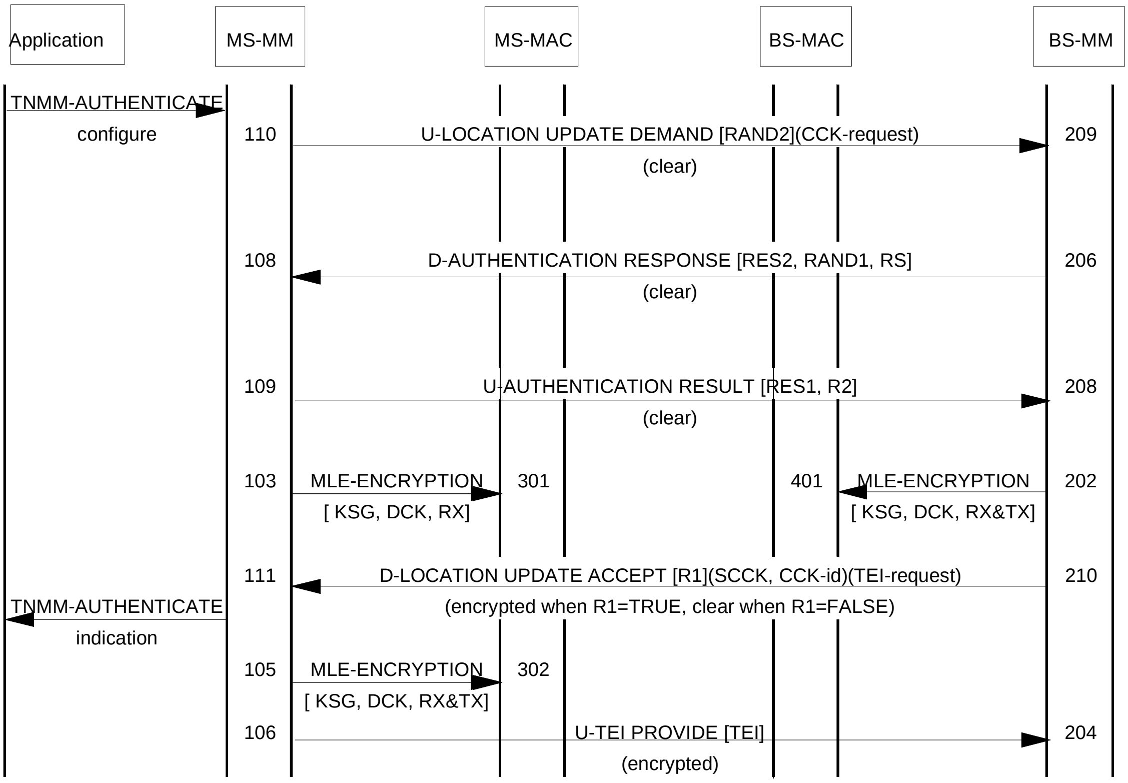


Figure 21: Mutual authentication started by the MS during registration

110 MS-MM initiates registration. U-LOCATION UPDATE DEMAND may be sent by the MS as a result of one of the following registration scenarios:

- MS-initiated registration due to roaming (i.e. change of location area);
- user application initiated registration;
- MS-initiated registration due to migration after identity exchange with the SwMI;
- MS-initiated forward registration;
- after receiving D-LOCATION UPDATE COMMAND as part of SwMI-initiated registration.

In the case of migration which requires identity exchange with the SwMI, the MS shall not include an authentication challenge or CCK request in the first U-LOCATION UPDATE DEMAND of the procedure. The MS shall wait until it has received an SSI for use on the system (sent in D-LOCATION UPDATE PROCEEDING) and then include any authentication challenge in the second U-LOCATION UPDATE DEMAND which is sent using the visitor SSI allocated during identity exchange. Similarly, the SwMI shall not attempt to authenticate an MS when U-LOCATION UPDATE DEMAND is requesting an identity exchange, but only when the MS attempts registration with an ISSI or VASSI.

Since, in this case, MS-MM is configured to authenticate the SwMI at registration, MS-MM shall include the type 3 element "Authentication uplink" in U-LOCATION UPDATE DEMAND and MS-MM shall include the random challenge, RAND2, in this element. MS-MM may request the SwMI to provide the CCK for the location area with which the MS is attempting to register by setting "CCK request flag" in the "Authentication uplink" element.

209 BS-MM shall retrieve RAND2 and run algorithms TA21 and TA22 to generate RES2 and DCK2. Since, in this case, the SwMI is configured for mutual authentication, BS-MM respond to the authentication request from the MS as described by case 4 in subclause 4.4.2.6.

206 Refer to case 4 in subclause 4.4.2.6.

109 Refer to case 4 in subclause 4.4.2.6.

103 Refer to case 4 in subclause 4.4.2.6.

301 Refer to case 4 in subclause 4.4.2.6.

208 Refer to case 4 in subclause 4.4.2.6.

202 Refer to case 4 in subclause 4.4.2.6.

401 Refer to case 4 in subclause 4.4.2.6.

210 If authentication of the MS was successful as indicated by R2, BS-MM shall inform MS-MM whether or not authentication of the SwMI was successful.

If authentication of the SwMI was successful and registration is to be accepted by the SwMI, BS-MM shall send D-LOCATION UPDATE ACCEPT encrypted with the newly calculated DCK. BS-MM shall include the "Authentication downlink" type 3 element in D-LOCATION UPDATE ACCEPT to convey R1. BS-MM may request MS-MM to supply the MS TEI by setting the "TEI request flag" in the "Authentication downlink" element. If the MS requested the CCK information in U-LOCATION UPDATE DEMAND, BS-MM shall include the "CCK information for current LA" in the "Authentication downlink" element.

If authentication of the SwMI or authentication of the MS was not successful, BS-MM shall instead send D-LOCATION UPDATE REJECT in clear. D-LOCATION UPDATE REJECT shall contain a reject reason which shall indicate that authentication has failed.

111 If MS-MM receives D-LOCATION UPDATE ACCEPT, MS-MM shall retrieve R1 which should indicate successful authentication. If authentication has failed, the MS should receive D-LOCATION UPDATE REJECT.

If authentication of the SwMI and MS were both successful, MS-MM shall run algorithm TB4 with to generate DCK with DCK1 and DCK2 as inputs. If the MS requested CCK information in U-LOCATION UPDATE DEMAND, MS-MM shall retrieve the "CCK information for current LA" from the "Authentication downlink" element in D-LOCATION UPDATE ACCEPT.

If authentication of the MS was not successful, MS-MM shall not calculate DCK.

105 Refer to case 4 in subclause 4.4.2.6.

302 Refer to case 4 in subclause 4.4.2.6.

106 If authentication of the MS and SwMI were both successful and BS-MM requested the MS TEI in D-LOCATION UPDATE ACCEPT, MS-MM shall provide the MS TEI by sending U-TEI PROVIDE which shall contain the MS TEI and the address extension (MCC and MNC) for the MS so that the SwMI has the full ITSI of the MS. Note that the BS should not ask the MS to supply its TEI unless encryption is on. The MS should not provide its TEI over the air interface in clear.

If authentication was not successful or the SwMI did not request the MS TEI in D-LOCATION UPDATE ACCEPT, U-TEI PROVIDE shall not be sent.

204 BS-MM shall retrieve the MS TEI from U-TEI PROVIDE. The BS may record the association of ITSI and TEI.

4.4.2.8 Case 8: SwMI rejects authentication demand from MS

The normal message sequence in this case shall be according to figure 22.

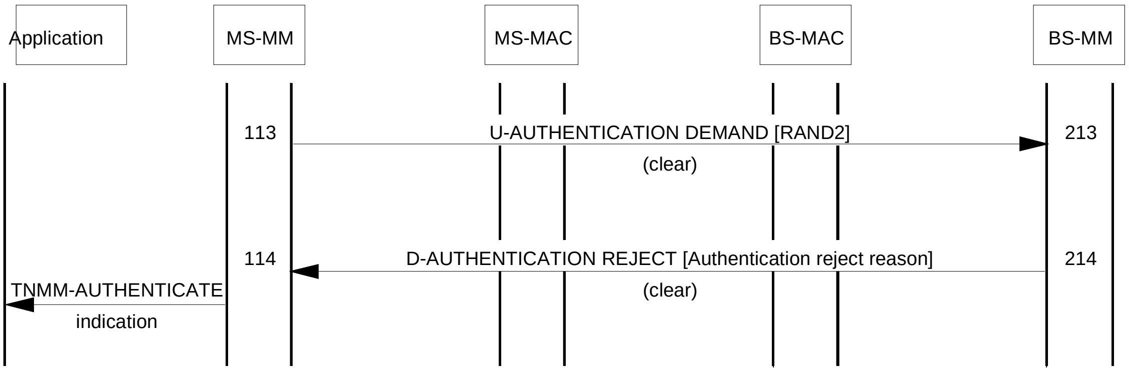


Figure 22: Authentication of MS as part of the registration procedure

113 The MS attempts to authenticate the SwMI by sending U-AUTHENTICATION DEMAND or by including the "Authentication uplink" type 3 element in U-LOCATION UPDATE DEMAND.

213 BS-MM receives an authentication challenge from the MS.

214 If the SwMI cannot support authentication, BS-MM shall respond to the authentication challenge with D-AUTHENTICATION REJECT. Note that if the SwMI responds to the authentication challenge with a mutual authentication, the MS shall not respond with U-AUTHENTICATION REJECT. If the MS initiates authentication of the SwMI, then the MS shall be able to support a mutual authentication request from the SwMI.

If the MS has sent an authentication challenge as part of a registration request (U-LOCATION UPDATE DEMAND) and the SwMI cannot support authentication because the MS has selected the wrong ciphering parameters in U-LOCATION UPDATE DEMAND, BS-MM shall reject the request by sending D-LOCATION UPDATE REJECT instead of D-AUTHENTICATION REJECT, which should also include a suggestion for what the ciphering parameters should be. This allows the MS to try again with the correct ciphering parameters.

114 MS-MM receives D-AUTHENTICATION REJECT and shall extract the reject reason which may be passed to the user application. If D-AUTHENTICATION REJECT is received in response to an authentication challenge embedded in U-LOCATION UPDATE DEMAND, MS-MM shall abandon the registration procedure. The MS may subsequently attempt to register with the SwMI without an authentication challenge.

4.4.2.9 Case 9: MS rejects authentication demand from SwMI

The normal message sequence in this case shall be according to figure 23.

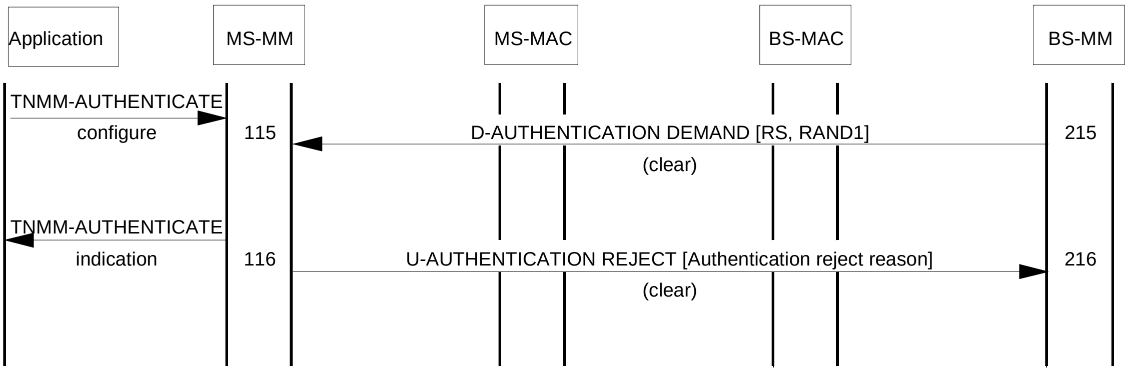


Figure 23: MS rejection of SwMI authentication demand

215 The SwMI attempts to authenticate the MS by sending D-AUTHENTICATION DEMAND.

NOTE: This may be sent in response to a registration request from the MS or it may be initiated by the SwMI.

115 MS-MM receives an authentication challenge from the MS.

116 If the MS cannot support authentication, MS-MM shall respond to the authentication challenge with U-AUTHENTICATION REJECT. If the MS responds to the authentication challenge with a mutual authentication, the SwMI shall not respond with D-AUTHENTICATION REJECT. If the SwMI initiates authentication of the MS, then the SwMI shall be able to support a mutual authentication request from the MS.

216 BS-MM receives U-AUTHENTICATION REJECT and shall extract the reject reason. If U-AUTHENTICATION REJECT is received in response to an authentication challenge which was sent as a result of an MS attempting to register (i.e. using U-LOCATION UPDATE DEMAND), BS-MM should respond with D-LOCATION UPDATE REJECT. This ensures that the SwMI does not allow an MS which cannot be authenticated to register on the network.

4.4.3 OTAR protocol functions - CCK

The CCK in use in a particular location area can be requested by the MS as part of the registration procedures (which may also include authentication) as described in subclause 4.3.7. However, the MS may also require CCK information at other times. For example, if an MS is about to select a LA in which it is already registered, it does not necessarily have the CCK information for that LA. The MS may wish to request the CCK information for that LA, either before or after selecting the new LA. A second example is where the SwMI indicates (by broadcasting the CCK-id in SYSINFO) that the CCK in use has changed and the MS does not yet have the new CCK. The MS needs a mechanism to ask the SwMI for the new CCK in use. Finally, the SwMI may wish to supply MSs currently registered in an LA with a new CCK (perhaps because it is about to change the CCK in use).

The distribution of CCK information can be done using the CCK OTAR mechanisms described in this subclause. The MS can request the CCK information for a particular LA (either the current LA or another LA in the system). The SwMI can then provide the CCK information for that LA which comprises of the CCK currently in use and the CCK which shall be used next. This means that the MS has the CCK information even if the SwMI changes the CCK in use in that LA.

Alternatively, the SwMI can provide the MS with the CCK information unsolicited for an LA. Again, the current CCK and the next one to be used are provided.

MS-initiated CCK OTAR can be combined with the announcement signalling during cell re-selection to allow the MS to get the CCK in use in a new LA before changing to that LA; this helps the MS to change between LAs with minimal disruption to any call in progress.

The MSCs and associated text in the following subclauses show the CCK OTAR scenarios

4.4.3.1 SwMI-initiated OTAR CCK provision and subsequent SYSINFO-initiated CCK change

This scenario shows how the SwMI can distribute new CCK information before it changes the CCK in use in a particular LA. When the SwMI changes the CCK in use, the MS already has the CCK information and can simply switch to using the new CCK without any additional signalling over the air interface.

The normal message sequence in this case shall be according to figure 24.

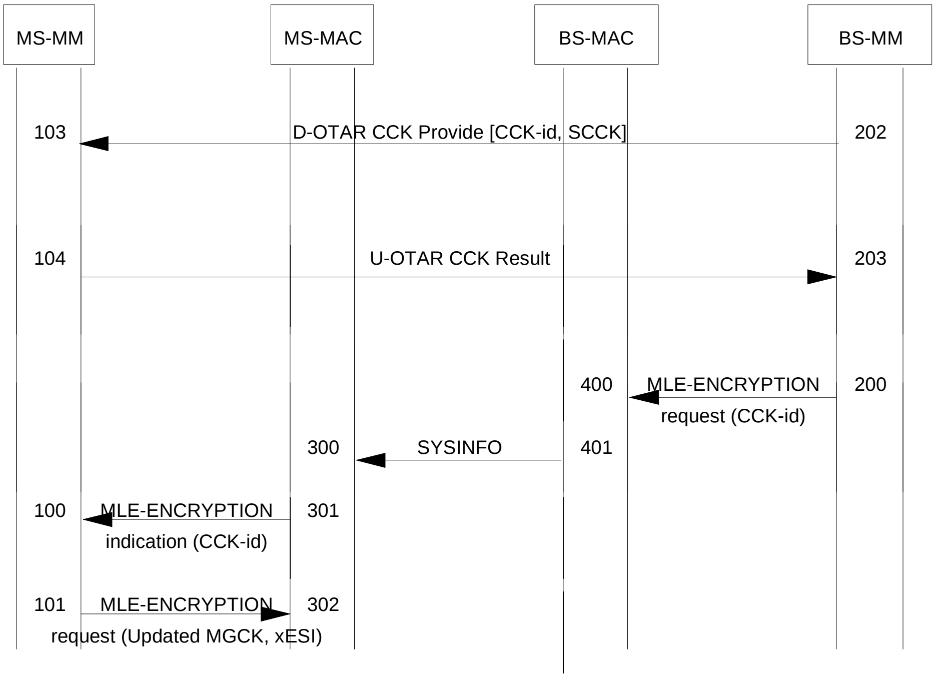


Figure 24: CCK change notified in MAC-SYSINFO broadcast

202 The SwMI may distribute CCK information to an MS by sending D-OTAR CCK Provide to that MS. D-OTAR Provide shall contain a "CCK provision indicator" which shall inform the MS about the scope of usage of the CCK information in this PDU. The provision indicator shall indicate if the CCK is for the current LA, for other LAs or for the entire system (i.e. all location areas for this SwMI). The "CCK provision indicator" element shall not indicate "No CCK in use or not known" for SwMI-initiated CCK OTAR.

D-OTAR CCK Provide shall include the CCK currently in use in the specified LA(s) and/or the CCK which shall be used next. If the SwMI is sending the CCK because it is about to change the CCK in use, the SwMI should include the future CCK and identifier element.

The SwMI may include the location area list element which shall indicate that the CCK information provided is valid for the listed LAs. These LAs may be in addition to the current LA as specified by the "CCK provision indicator" element.

103 The MS shall attempt to retrieve the sealed CCK(s) provided by the SwMI using algorithm TA32 with the CCK-id, SCCK and DCK as inputs. The MS shall then store the CCK(s) along with the applicable LAs as indicated by D-OTAR CCK Provide.

104 The MS shall report whether or not it accepts the supplied CCK(s) by sending U-OTAR CCK Result to the SwMI. If the MS was able to unseal the CCK, it shall accept the CCK. If the MS is unable to unseal the CCK, it shall reject the CCK using the "Provision result" element in U-OTAR CCK Result to report the reason for CCK rejection to the SwMI.

203 The SwMI shall retrieve the "Provision result" for the CCK(s) which it provided to the MS and may record whether or not the MS accepted the CCK(s). If the MS rejected one or both of the CCK(s) provided due to it not being able to decrypt the key, the SwMI may retry sending of D-OTAR CCK Provide one more time.

200 The SwMI may change the CCK in use in an LA by incrementing the CCK identifier in the SYSINFO broadcast for that LA. Before, doing this, the SwMI should ensure that all MSs currently registered in this LA have the new CCK. This requirement is very important since, if there are MSs which do not have the new CCK, the change of the CCK-id shall trigger those MSs to request the new CCK using the MS-initiated OTAR CCK procedure, which could result in a flood of signalling on the air interface.

The SwMI may provide the CCK to MSs before changing the CCK-id using the SwMI-initiated OTAR CCK procedure described in 202, 103, 104 and 203 above.

400 BS-MAC shall store the new CCK and shall begin to use that for all downlink transmission. The SwMI should synchronize the changeover to the new CCK with sending of SYSINFO on each channel. Since SYSINFO may be sent at different times on different logical channels (timeslots), the changeover to the new CCK may not be synchronized between those channels.

401 BS-MAC shall change the CCK-id in the SYSINFO broadcast to reflect the change of CCK. The SwMI shall also indicate this change in the 2-bit "Encryption mode" element in the MAC header of downlink PDUs.

NOTE: The SYSINFO initiated change of CCK is equivalent to, and co-ordinated with, changing the short CCK identifier in the MAC encryption information element.

300 MS-MAC shall recognize that the CCK in use has been changed by the SwMI as a result of the CCK-id in the SYSINFO broadcast being changed.

301 MS-MAC shall inform MS-MM of the new CCK-id.

100 If MS-MM already knows the CCK associated with new CCK-id, MS-MM shall run algorithm TA61 to generate new ESIs for all addresses. MS-MM shall also run algorithm TA71 to generate new MGCK(s) for all attached GTSIs. If MS-MM does know the CCK associated with the new CCK-id, MS-MM shall initiate an OTAR CCK exchange as described in the following subclause.

101 If MS-MM has the new CCK is use, it shall deliver the new CCK, the updated MGCK and xESI to MS-MAC. If MS-MM does not have the new CCK in use, MS-MAC will not be able to decrypt incoming PDUs until MS-MM has obtained the new CCK using MS-initiated OTAR CCK exchange.

302 MS-MAC shall store the new CCK and its associated CCK-id, the xESI and MGCK for decryption of subsequent downlink PDUs.

4.4.3.2 SYSINFO-initiated CCK change and MS-initiated OTAR CCK provision

This scenario shows SwMI changing the CCK in use in an LA. In this case, the MS does have the new CCK and so needs to use the OTAR CCK procedure to request the new CCK from the SwMI.

The normal message sequence in this case shall be according to figure 25.

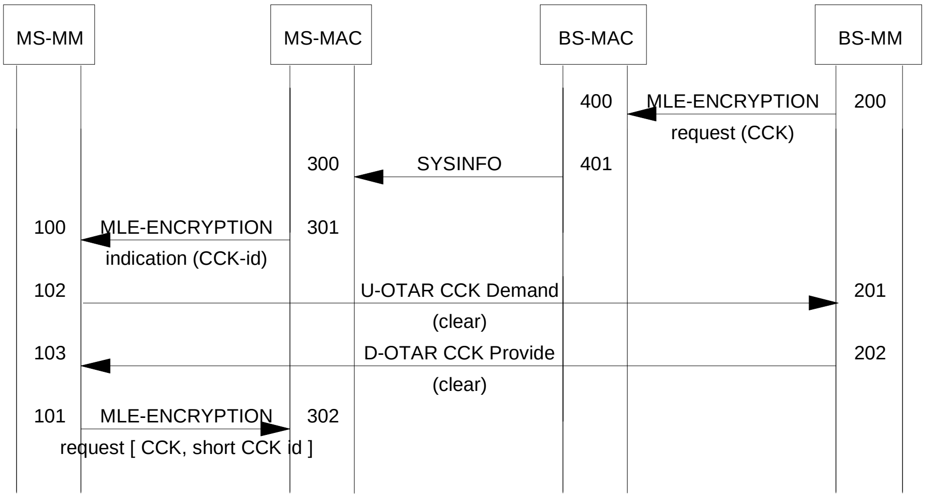

MS-MM
MS-MAC
BS-MAC
BS-MM
400
MLE-ENCRYPTION request (CCK)
200
300
SYSINFO
401
100
MLE-ENCRYPTION indication (CCK-id)
301
102
U-OTAR CCK Demand (clear)
201
103
D-OTAR CCK Provide (clear)
202
101
MLE-ENCRYPTION request [CCK, short CCK id]
302

Figure 25: CCK OTAR initiated by SYSINFO

200 As described in subclause 4.4.3.1.

400 As described in subclause 4.4.3.1.

401 As described in subclause 4.4.3.1.

300 As described in subclause 4.4.3.1.

301 As described in subclause 4.4.3.1.

100 Since, in this case, the MS does not have the new CCK (indicated by the CCK-id in SYSINFO), the MS shall initiate the OTAR CCK procedure. The MS shall perform this procedure using clear signalling since it does not have the CCK needed to encrypt the signalling.

102 MS-MM shall request the CCK for an LA be sending U-OTAR CCK Demand to BS-MM. The MS shall include in this PDU the LA for which the CCK is required. The LA may either be the same as that in which the MS is operating or it may be another LA in the coverage of the SwMI.

NOTE: The MS may send U-OTAR CCK Demand at any time to obtain CCK information for an LA; although, in this case, it is triggered by a change of CCK in the current LA, MS-MM also request the CCK at other times.

201 BS-MM shall retrieve the LA from U-OTAR CCK Demand and obtain the current and future CCK in use for that LA.

202 BS-MM shall respond to the OTAR CCK request from the MS by sending D-OTAR CCK Provide which shall include the current CCK and may include the future CCK for the LA which the MS has indicated in U-OTAR CCK Demand. The SwMI should also indicate in D-OTAR CCK Provide if the CCK for that LA is in use in other LAs or is in use throughout the SwMI.

103 The MS shall attempt to retrieve the sealed CCK(s) provided by the SwMI using algorithm TA32 with the CCK-id, SCCK and DCK as inputs. The MS shall then store the CCK(s) along with the applicable LAs as indicated by D-OTAR CCK Provide. In the case of the MS-initiated OTAR CCK procedure, MS-MM shall not respond to D-OTAR CCK Provide with U-OTAR CCK Result. If the MS was unable to decrypt either of the supplied CCKs, MS-MM should attempt to take appropriate action to obtain the information it needs to decrypt the keys.

101 Now that MS-MM has the new CCK is use, it shall run algorithm TA61 to generate new ESIs for all addresses and it shall also run algorithm TA71 to generate new MGCK(s) for all attached GTSIs. MS-MM shall then deliver the new CCK, the updated MGCK and xESIs to MS-MAC.

302 MS-MAC shall store the new CCK and its associated CCK-id, the xESI and MGCK for decryption of subsequent downlink PDUs.

4.4.3.3 MS-initiated OTAR CCK provision during cell re-selection announcement signalling

This scenario shows how the MS may combine an OTAR CCK request with cell re-selection announcement signalling. This procedure may be used as part of announced type 2 or announced type 3 cell re-selection. This reduces the amount of signalling needed during a cell change when the MS does not know the CCK in use in a new cell (which is part of a new LA) which it is about to select during a circuit mode call.

The normal message sequence in this case shall be according to figure 26.

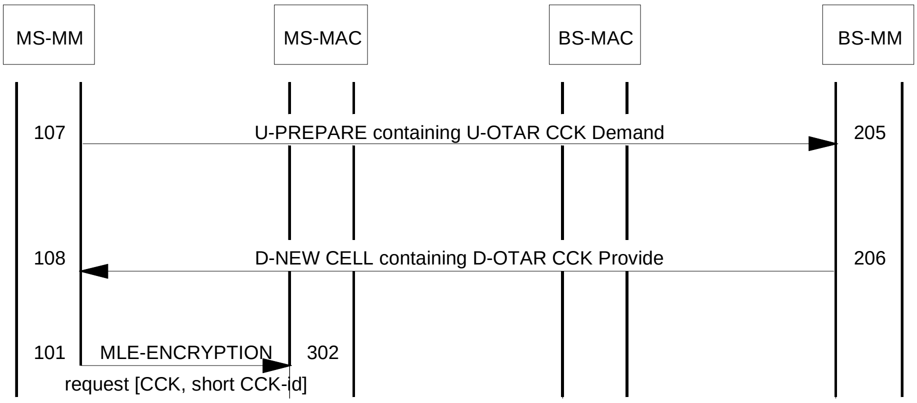

MS-MM
MS-MAC
BS-MAC
BS-MM
107
U-PREPARE containing U-OTAR CCK Demand
205
108
D-NEW CELL containing D-OTAR CCK Provide
206
101
MLE-ENCRYPTION
request [CCK, short CCK-id]
302

Figure 26: OTAR CCK during cell re-selection

107 In this case, the MS detects that it is to change to a new cell (which is part of new LA) during a circuit mode call. The MS does not have the CCK for that LA and so may combine the MLE announcement signalling with an OTAR CCK request.

If the MS chooses to invoke this procedure, MS-MM shall use the MLE-PREPARE request primitive to request that the MLE sends U-OTAR CCK Demand to be carried by the MLE U-PREPARE PDU. MS-MM shall include, in U-OTAR CCK Demand, the LA for which the CCK is required; in this case, the LA should be the one which the MS is about to select.

205 BS-MM shall retrieve the LA from U-OTAR CCK Demand and obtain the current and future CCK in use for that LA.

206 BS-MM shall respond to the request from the MS by sending D-OTAR CCK Provide which shall be carried by the MLE D-NEW CELL PDU. D-OTAR Provide shall include the current CCK and may include the future CCK for the LA which the MS has indicated in U-OTAR CCK Demand. The SwMI may also indicate, in D-OTAR CCK Provide, if the CCK(s) provided is in use in other LAs or is in use throughout the SwMI.

108 The MS shall retrieve D-OTAR CCK Provide from the D-NEW CELL PDU and MLE shall select the new cell as described by the cell re-selection procedures in ETS 300 392-2 [1], clause 18. The MS shall attempt to retrieve the sealed CCK(s) provided by the SwMI using algorithm TA32 with the CCK-id, SCCK and DCK as inputs. The MS shall then store the CCK(s) along with the applicable LAs as indicated by D-OTAR CCK Provide. In the case of the MS-initiated OTAR CCK procedure, MS-MM shall not respond to D-OTAR CCK Provide with U-OTAR CCK Result. If the MS was unable to decrypt either of the supplied CCKs, MS-MM should attempt to take appropriate action to obtain the information it needs to decrypt the keys after changing to the new cell.

101 Now that MS-MM has the new CCK is use, it shall run algorithm TA61 to generate new ESIs for all addresses and it shall also run algorithm TA71 to generate new MGCK(s) for all attached GTSIs. MS-MM shall then deliver the new CCK, the updated MGCK and xESIs to MS-MAC.

302 MS-MAC shall store the new CCK and its associated CCK-id, the xESI and MGCK for decryption of subsequent downlink PDUs.

4.4.4 OTAR protocol functions - SCK

One or several SCKs may be distributed to the MS using the "D-OTAR SCK Provide" PDU. The provision may be started automatically by the SwMI or in response to a request from the MS using the "U-OTAR SCK Demand" PDU. These two cases are described by the MSCs and protocol description in the following subclauses.

4.4.4.1 MS requests provision of SCK(s)

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.

The normal message sequence in this case shall be according to figure 27.

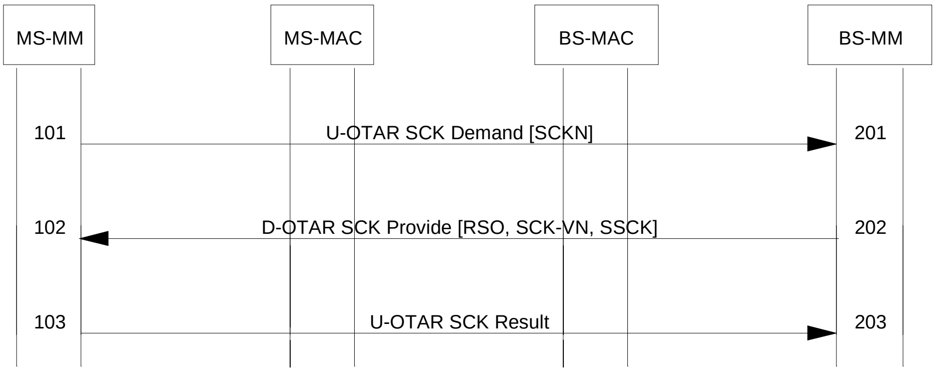


Figure 27: SCK delivery initiated by MS

101 The MS may request up to four SCKs in each SCK OTAR transaction. When the MS requests distribution of SCKs, MS-MM shall set the "Number of SCKs requested" element in the U-OTAR SCK Demand PDU to be equal to the number of keys demanded. The following list of SCK numbers shall indicate the number of each SCK which is being requested by the MS. There shall be as many "SCK number" elements in the PDU as were indicated by the "Number of SCKs requested" element.

201 BS-MM shall retrieve the SCKNs requested by the MS and shall obtain the SCKs and corresponding SCK-VNs identified by each SCKN. The SwMI shall also generate a random seed, RSO, used as one input to TA41 that generates KSO to encrypt the key information. The SwMI shall then seal each of the SCKs by running algorithms TA41 and TA51, using the SCK, SCK-VN and RSO as inputs.

202 The "D-OTAR SCK Provide" PDU shall be sent by the SwMI to provide the MS with the SCK information it has requested. For each SCK, BS-MM shall send SCKN, SCK-VN and the sealed SCK. The "Number of SCKs provided" element shall have a value equal to the number of SCKs provided within the PDU (which may be up to four). If the SwMI is unable to provide any requested SCKs, it shall omit those SCKs from the "D-OTAR SCK Provide" PDU, reducing the value of the "Number of keys provided" element. Therefore, the indication that certain requested SCKs are not available shall be implicit and not explicit by this mechanism.

BS-MM shall also send the random seed, RSO, in D-OTAR SCK Provide which is used to generate a session key used in the key encryption process.

102 MS-MM shall retrieve the SSCK(s) and corresponding SCKN(s) and SCK-VN(s) supplied in D-OTAR SCK Provide and the random seed, RSO. The MS shall then attempt to decrypt the SCK(s) using algorithms TA41 and TA52 with SSCK, SCK-VN and RSO as inputs.

103 If the SwMI has provided one or more SCKs in D-OTAR SCK Provide, MS-MM shall respond using U-OTAR SCK Result to indicate to the SwMI whether each SCK provided was accepted or the MS failed to decrypt the key. For each SCK which the SwMI has provided, MS-MM shall include an "SCK number and result" element. The "Number of SCKs requested" element in this PDU shall correspond to the number of results which are included in the PDU.

The MS shall only accept or reject the keys that it receives. If D-OTAR SCK Provide indicates that the SwMI has not provided any SCKs in response to the MS request, the MS shall not send U-OTAR SCK Result.

203 If BS-MM has supplied one or more SCKs, BS-MM shall expect to receive U-OTAR SCK Result. BS-MM shall retrieve the provision result for each of the SCKs which it has provided. If the MS fails to decrypt any of the SCKs, the SwMI may record this information.

4.4.4.2 SwMI provides SCK(s) to MS

This scenario shows the case where the SwMI provides one or more SCK(s) to an MS without the MS first requesting SCK provision. The SwMI may initiate this procedure at any time.

The normal message sequence in this case shall be according to figure 28.

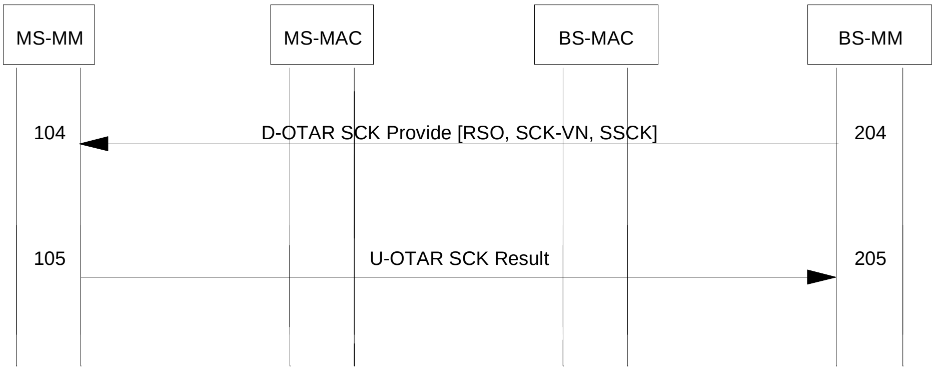


Figure 28: SCK delivery initiated by SwMI

204 When the SwMI wishes to download one or more SCKs to an MS, BS-MM shall obtain the SCKs and corresponding SCK-VNs and SCKNs. The SwMI shall generate a random seed, RSO, used as input to TA41 to generate KSO that is used to encrypt the key information. The SwMI shall then seal each of the SCKs by running algorithms TA41 and TA51, using the SCK, SCK-VN and RSO as inputs.

The "D-OTAR SCK Provide" PDU shall be sent by the SwMI to provide the MS with the SCK information. For each SCK, BS-MM shall send SCKN, SCK-VN and the sealed SCK, SSCK. The "Number of SCKs provided" element shall have a value equal to the number of SCKs provided within the PDU (which may be up to four). When the SwMI initiates SCK provision, it shall not set the "Number of keys provided" element to a value of zero.

BS-MM shall also send the random seed, RSO, in D-OTAR SCK Provide which is used to generate a session key used in the key encryption process.

104 MS-MM shall retrieve the SCK(s) supplied in D-OTAR SCK Provide and the random seed, RSO. The MS shall then attempt to decrypt the SCK(s) using algorithms TA41 and TA52 with SSCK, SCK-VN and RSO as inputs.

105 MS-MM shall respond to the key provision using U-OTAR SCK Result to indicate to the SwMI whether each SCK provided was accepted or the MS failed to decrypt the key. For each SCK which the SwMI has provided, MS-MM shall include an "SCK number and result" element. The "Number of SCKs requested" element in this PDU shall correspond to the number of results which are included in the PDU.

205 BS-MM shall expect to receive U-OTAR CCK Result. BS-MM shall retrieve the provision result for each of the SCKs which it has provided. If the MS fails to decrypt any of the SCKs, the SwMI may record this information.

4.4.5 OTAR protocol functions - GCK

A GCK may be distributed to the MS using the "D-OTAR GCK Provide" PDU. The provision may be started automatically by the SwMI or in response to a request from the MS using the "U-OTAR GCK Demand" PDU. These two cases are described by the MSCs and protocol description in the following subclauses.

4.4.5.1 MS requests provision of GCK

This scenario shows the case where the MS requests provision of a GCK for a group. The MS may initiate this procedure at any time.

The normal message sequence in this case shall be according to figure 29.

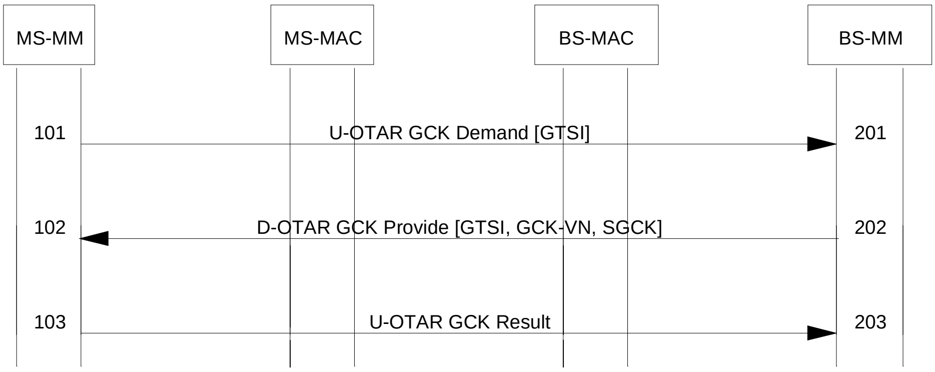


Figure 29: GCK delivery initiated by MS

101 The MS may request up the GCK for a particular group by sending U-OTAR GCK Demand to the SwMI. When the MS sends U-OTAR GCK Demand, MS-MM shall set the GSSI to be equal to the group number for which the GCK is requested. If the group has an MCC and/or MNC which is different to that for the current SwMI, MS-MM shall also include the "Address extension" element in the PDU. This ensures the SwMI has the full GTSI of the group requested.

201 BS-MM shall retrieve the GSSI and, if present in the PDU, the address extension. If the PDU does not include the address extension, the SwMI shall assume that it is equal to its own MCC and MCC. The SwMI shall obtain the GCK and corresponding GCK-VN corresponding to the GTSI of the group indicated by the MS. The SwMI shall run algorithm TA81 to generate the sealed GCK, SGCK, using GCK, GTSI, GCK-VN and the DCK for the requesting MS as inputs.

202 The "D-OTAR GCK Provide" PDU shall be sent by the SwMI to provide the MS with the GCK information it has requested. D-OTAR GCK Provide shall include the SGCK and GCK-VN as well as the GSSI of the group for which the GCK is being provided. The "Address extension" shall be included if the MCC and/or MNC of the group is different to that of the SwMI sending the PDU. Otherwise the address extension shall not be included.

If the SwMI is unable to provide the requested GCK, it shall omit the "GCK key and identifier" element from D-OTAR GCK Provide. This shall implicitly indicate to the MS that the requested GCK is not available.

102 MS-MM shall retrieve the GSSI and address extension, if present, from D-OTAR GCK Provide. MS-MM shall attempt to retrieve the GCK supplied in the D-OTAR GCK Provide.

If D-OTAR GCK Provide contains a "GCK key and identifier", the MS shall then attempt to decrypt the GCK using algorithm TA82 with SGCK, GTSI, GCK-VN and the DCK for the MS as inputs.

If D-OTAR GCK Provide does not contain a "GCK key and identifier", the MS shall assume that the key cannot be provided by the SwMI. The MS may report this to the user application.

103 If the SwMI has a GCK in D-OTAR GCK Provide, MS-MM shall respond using U-OTAR GCK Result to indicate to the SwMI whether the GCK was accepted by the MS. MS-MM shall include the GCK-VN, GSSI and, if needed, the address extension. MS-MM shall also include a provision result which shall inform the SwMI about the result of the GCK provision.

If D-OTAR GCK Provide does not include a "GCK key and identifier" element, the MS shall not send U-OTAR GCK Result.

203 If BS-MM has supplied a SGCK, BS-MM shall expect to receive U-OTAR GCK Result. BS-MM shall retrieve the provision result for the GCK which it has provided. If the MS fails to decrypt the GCK, the SwMI may record this information.

4.4.5.2 SwMI provides GCK to MS

This scenario shows the case where the SwMI provides a GCK to an MS without the MS first requesting GCK provision. The SwMI may initiate this procedure at any time.

The normal message sequence in this case shall be according to figure 30.

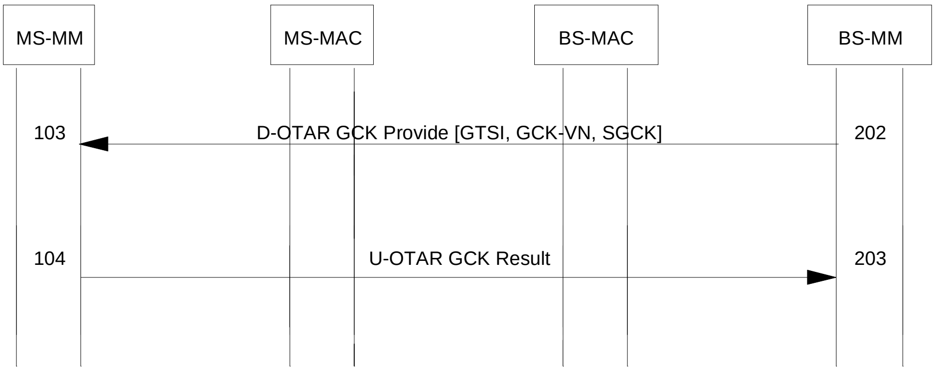


Figure 30: GCK delivery initiated by SwMI

204 When the SwMI wishes to download a GCK to an MS, BS-MM shall obtain the GCK and corresponding GCK-VN for the group corresponding to a GTSI. The SwMI shall run algorithm TA81 to generate the sealed GCK, SGCK, using GCK, GTSI, GCK-VN and the DCK for the MS to which the SwMI is going to send the GCK as inputs.

The D-OTAR GCK Provide PDU shall be sent by the SwMI to provide the MS with the GCK information. D-OTAR GCK Provide shall include the SGCK and GCK-VN as well as the GSSI of the group for which the GCK is being provided. The "Address extension" shall be included if the MCC and/or MNC of the group is different to that of the SwMI sending the PDU. Otherwise the address extension shall not be included. When the SwMI initiates GCK provision, it shall always include the "GCK key and identifier" element in the D-OTAR GCK Provide PDU.

104 MS-MM shall retrieve the SGCK supplied in D-OTAR GCK Provide. The MS shall then attempt to decrypt the GCK using algorithm TA82 with SGCK, GTSI, GCK-VN and the DCK for the MS as inputs.

105 MS-MM shall respond to the key provision using U-OTAR GCK Result to indicate to the SwMI whether GCK was accepted by the MS. MS-MM shall include the GCK-VN, GSSI and, if needed, the address extension. MS-MM shall also include a provision result which shall inform the SwMI about the result of the GCK provision.

205 BS-MM shall expect to receive U-OTAR GCK Result. BS-MM shall retrieve the provision result for the GCK which it has provided. If the MS fails to decrypt the GCK, the SwMI may record this information.

4.4.6 PDU descriptions

The PDUs detailed within this subclause shall be visible at the Um reference point (see ETS 300 392-1 [1], clause 5).

The general format of the PDU is defined according to table 5.

The elements shall be transmitted in the order specified by the table with the top element being transmitted first (before interleaving). The content of an information element is represented by a binary value and the most significant bit of that binary value shall be transmitted first (before interleaving). The coding of each element is specified in subclause 4.3.10.

Table 5: PDU layout

Information element	Length	Value	Remark
PDU Type	4		
Type 1 element (1)	varies		See definitions below.
Type 1 element (2)	varies		See definitions below.
…etc.	…etc.		…etc.
Type 1 element (n)	varies		See definitions below.
Optional bit (O-bit)	1	0	No optional type 2 or type 3 elements follow
		1	Optional type 2 or type 3 elements follow
Presence bit (P-bit) (1)	1	0	The type 2 element (1) is not present
		1	The type 2 element (1) is present.
Type 2 element (1)	varies		See definitions below.
Presence bit (P-bit) (2)	1	0	The type 2 element (2) is not present
		1	The type 2 element (2) is present.
Type 2 element (2)	varies		See definitions below.
…etc.	…etc.		…etc.
Presence bit (P-bit) (n)	1	0	The type 2 element (n) is not present
		1	The type 2 element (n) is present.
Type 2 element (n)	varies		See Type 2 element (1)
More bit (M-bit) (1)	1	0	No type 3 elements follow
		1	Type 3 elements follow
Type 3 Element Identifier (1)	4		See definitions below.
Length indicator (1)	11	0	Reserved for possible future use.
		$1\text{-}2047_{10}$	Length of the following type 3 Element in bits:
Type 3 Element (1)	varies		See definitions below.
More bit (M-bit) (2)	1	0	No more type 3 elements follow
		1	More type 3 elements follow
Type 3 Element Identifier (2)	4		See definitions below.
Length indicator (2)	11	0	Reserved for possible future use.
		$1\text{-}2047_{10}$	Length of the following type 3 Element in bits:
Type 3 Element (2)	varies		See definitions below.
…etc.	…etc.		…etc.
More bit (M-bit) (n)	1	0	No more type 3 elements follow
		1	More type 3 elements follow
Type 3 Element Identifier (n)	4		See definitions below.
Length indicator (n)	11	0	Reserved for possible future use.
		$1\text{-}2047_{10}$	Length of the following type 3 Element in bits:
Type 3 Element (n)	varies		See definitions below.
More bit (M-bit) (n+1) = 0	1	0	Last M-bit (Least Significant Bit in the PDU) = 0

The element type defines the encoding rule applied to an element.

- Type 1 elements shall be placed within the PDU in a fixed order as specified in the PDU description tables. The elements shall have fixed lengths as specified in the length column or variable lengths as indicated by a preceding length element. Each Type 1 element shall either be a mandatory element or conditional to a mandatory element. Type 1 elements shall be placed before any Type 2 or Type 3 elements in the PDU. The last Type 1 element shall be followed by an O-bit. When the PDU contains any Type 2 or Type 3 elements the O-bit shall set to 1. When the PDU does not contain any Type 2 or Type 3 elements the O-bit shall be set to 0.

- Type 2 elements are either optional or conditional to an optional element and shall be placed within the PDU in a fixed order as specified in the PDU description tables. There shall be one P-bit preceding each Type 2 optional element specified for the PDU to indicate presence of that element. The P-bit shall indicate either "Type 2 element present" or "Type 2 element not present". Type 2 elements shall have fixed lengths as specified in the length column of the PDU description tables. Type 2 elements shall be placed after all Type 1 elements and before any Type 3 elements in the PDU.

- Type 3 elements are optional and shall be placed within the PDU in numerical order as specified within the "Type 3 Element Identifier" element. Type 3 Elements shall be placed after any Type 1 and Type 2 elements. If there are any Type 3 elements specified for the PDU an M-bit shall follow the Type 1 and Type 2 elements. The M-bit shall indicate either "Type 3 element to follow" or "no Type 3 element to follow". If there are Type 3 elements to follow, they shall be preceded by a "Type 3 Element Identifier" element and a "Length Indicator" element in that order. A further M-bit shall follow the Type 3 element and after the last Type 3 element included the M-bit shall be set to 0 to indicate "no Type 3 element to follow". Type 3 element coding can contain sub-elements which can be either of Type 1, 2 or 3.

The following rules shall apply for decoding of the PDU:

```
DO for all possible Type 1 elements
IF element is not a conditional element
    THEN DECODE Type 1 element
    ELSE DECODE conditional Type 1 element if indicated
END DO
DECODE O-bit
IF O-bit set to "No Optional Elements present"
    THEN END of PDU decoding
    ELSE
    DO for all possible Type 2 elements
        DECODE P-bit
        IF P-bit set to "Present"
            THEN DECODE Type 2 element AND
            IF element points to conditional element(s)
                THEN DECODE indicated conditional element(s), END IF
        IF P-bit not set "Present"
            THEN pass also elements conditional on that element
    END DO
    WHILE M-bit set to "More Type 3 elements follows"
        DECODE Type 3 element
    END WHILE
END of PDU decoding.
```

NOTE: There is only one P-bit common for a type 2 optional element and any element(s) conditional on the first element. In that case the conditional element(s) follow immediately the first element (without a P-bit between them).

The information contained in the following PDU description tables corresponds to the following key:

Length:	-	length of the element in bits;
Type:	-	element type (1, 2, or 3) as defined above;
C/O/M:	-	conditional/optional/mandatory information in the PDU;
Remark:	-	comment.

NOTE: The preceding text has been taken (copied) from ETS 300 392-2 [2], subclause 14.7 and this reference is to be considered the normative source.

There shall be 11 PDUs defined at the air interface some of which shall have subtypes as shown in table 6.

Table 6: AIR INTERFACE PDUs and related sub-types

Air Interface PDU	Sub-type
D-AUTHENTICATION DEMAND	-
D-AUTHENTICATION RESPONSE	-
D-AUTHENTICATION RESULT	-
D-AUTHENTICATION REJECT	-
U-AUTHENTICATION DEMAND	-
U-AUTHENTICATION RESPONSE	-
U-AUTHENTICATION RESULT	-
U-AUTHENTICATION REJECT	-
D-OTAR	SCK Provide
	CCK Provide
	GCK Provide
U-OTAR	CCK Demand
	CCK Result
	SCK Demand
	SCK Result
	SCK Reject
	GCK Demand
	GCK Result
U-TEI PROVIDE	-

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.

4.4.6.1 D-AUTHENTICATION DEMAND

Shall be used by the infrastructure to initiate an authentication of the MS.

Direction: SwMI to MS
Service used: MM
Response to: U-LOCATION UPDATE DEMAND or none
Response expected: U-AUTHENTICATION RESPONSE

Table 7: D-AUTHENTICATION DEMAND PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0001_2
Random challenge [RAND1]	80	1	M	
Random seed [RS]	80	1	M	
Proprietary element		3	O	

4.4.6.2 D-AUTHENTICATION RESPONSE

Shall be used by the infrastructure to respond to an authentication demand from the MS.

Direction:	SwMI to MS
Service used:	MM
Response to:	U-AUTHENTICATION DEMAND
Response expected:	U-AUTHENTICATION RESULT

Table 8: D-AUTHENTICATION RESPONSE PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	1000_2
Random seed [RS]	80	1	M	
Response value [RES2]	32	1	M	
Mutual authentication flag	1	1	M	
Random challenge [RAND1]	80	1	C	note
Proprietary element		3	O	
NOTE: RAND1 is conditional on the Mutual authentication flag element. RAND1 shall be present if Mutual authentication flag = 1. Otherwise, RAND1 shall not be present in the PDU.				

4.4.6.3 D-AUTHENTICATION RESULT

Shall be used by the infrastructure to report the result of an MS authentication to the MS.

Direction:	SwMI to MS
Service used:	MM
Response to:	U-AUTHENTICATION RESPONSE or U-AUTHENTICATION RESULT
Response expected:	U-AUTHENTICATION RESULT or none

Table 9: D-AUTHENTICATION RESULT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	1110_2
Authentication result [R1]	1	1	M	
Mutual authentication flag	1	1	M	
Response Value [RES2]	32	1	C	note
Proprietary element		3	O	
NOTE: RES2 is conditional on the Mutual authentication flag element. RES2 shall be present if Mutual authentication flag = 1. Otherwise, RES2 shall not be present in the PDU.				

4.4.6.4 D-AUTHENTICATION REJECT

Shall be used by the infrastructure to report to the MS any rejection of an authentication demand.

Direction:	SwMI to MS
Service used:	MM
Response to:	U-AUTHENTICATION DEMAND
Response expected:	none

Table 10: D-AUTHENTICATION REJECT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0010_2
Authentication reject reason	3	1	M	

4.4.6.5 U-AUTHENTICATION DEMAND

Shall be used by the MS to initiate an authentication of the BS/SwMI.

Direction:	MS to SwMI
Service used:	MM
Response to:	none
Response expected:	D-AUTHENTICATION RESPONSE

Table 11: U-AUTHENTICATION DEMAND PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0100_2
Random challenge [RAND2]	80	1	M	
Proprietary element		3	O	

4.4.6.6 U-AUTHENTICATION RESPONSE

Shall be used by MS-MM to respond to an authentication demand from the SwMI of the MS.

Direction:	MS to SwMI
Service used:	MM
Response to:	D-AUTHENTICATION DEMAND
Response expected:	D-AUTHENTICATION RESULT

Table 12: U-AUTHENTICATION RESPONSE PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0000_2
Response Value [RES1]	32	1	M	
Mutual authentication flag	1	1	M	
Random challenge [RAND2]	80	1	C	note
Proprietary element		3	O	
NOTE: RAND2 is conditional on the Mutual authentication flag element. RAND2 shall be present if Mutual authentication flag = 1. Otherwise, RAND2 shall not be present in the PDU.				

4.4.6.7 U-AUTHENTICATION RESULT

Shall be used by MS-MM to report the result of an authentication of the BS/SwMI.

Direction:	MS to SwMI
Service used:	MM
Response to:	D-AUTHENTICATION RESULT or D-AUTHENTICATION RESPONSE
Response expected:	D-AUTHENTICATION RESULT or none

Table 13: U-AUTHENTICATION RESULT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0110_2
Authentication result [R2]	1	1	M	
Mutual authentication flag	1	1	M	
Response Value [RES1]	32	1	C	note
Proprietary element		3	O	
NOTE: RES1 is conditional on the Mutual authentication flag element. RES1 shall be present if Mutual authentication flag = 1. Otherwise, RES1 shall not be present in the PDU.				

4.4.6.8 U-AUTHENTICATION REJECT

Shall be used by the MS to report to the infrastructure any rejection of an authentication demand.

Direction:	MS to SwMI
Service used:	MM
Response to:	D-AUTHENTICATION DEMAND
Response expected:	none

Table 14: U-AUTHENTICATION REJECT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	1010_2
Authentication reject reason	3	1	M	

4.4.6.9 D-OTAR CCK Provide

Shall be used by the infrastructure to provide CCK to an MS.

Direction:	SwMI to MS
Service used:	MM
Response to:	U-OTAR CCK Demand or none
Response expected:	U-OTAR CCK Result or none

Table 15: D-OTAR CCK Provide PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0000_2
OTAR sub-type	3	1	M	CCK Provide
CCK Provision Indicator	2	1	M	
CCK and Identifier (current)	136	2	O	CCK details currently in use
CCK and Identifier (future)	136	2	O	CCK details for future use
Location area list		2	O	
Proprietary element		3	O	

4.4.6.10 D-OTAR SCK Provide

Shall be used by the infrastructure to provide SCK to an MS.

Direction:	SwMI to MS
Service used:	MM
Response to:	U-OTAR SCK Demand or none
Response expected:	U-OTAR SCK Result

Table 16: D-OTAR SCK Provide PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0000_2
OTAR sub-type	3	1	M	SCK Provide
Random seed	80	1	M	
Number of SCKs provided	3	1	M	
SCK key and identifier	141	1	C	note
Proprietary element		3	O	
NOTE: 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.				

4.4.6.11 D-OTAR GCK Provide

Shall be used by the infrastructure to provide GCK to an MS.

Direction:	SwMI to MS
Service used:	MM
Response to:	U-OTAR GCK Demand or none
Response expected:	U-OTAR GCK Result

Table 17: D-OTAR GCK Provide PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU type	4	1	M	0000_2
OTAR sub-type	3	1	M	GCK Provide
GSSI	24	1	M	
Address extension	24	2	O	
GCK key and identifier	136	2	O	
Proprietary element		3	O	

4.4.6.12 U-OTAR CCK Demand

Shall be used by MS-MM to request CCK for a location area from the SwMI.

Direction:	MS to SwMI
Service used:	MM
Response to:	none
Response expected:	D-OTAR CCK Provide

Table 18: U-OTAR CCK Demand PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0101_2
OTAR sub-type	3	1	M	CCK Demand
Location Area	14	1	M	
Proprietary element		3	O	

4.4.6.13 U-OTAR CCK Result

Shall be used by MS-MM to explicitly accept or reject some or all of the CCKs provided by the SwMI.

Direction:	MS to SwMI
Service used:	MM
Response to:	D-OTAR CCK Provide
Response expected:	none

Table 19: U-OTAR CCK Result PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0101_2
OTAR sub-type	3	1	M	CCK Result
Provision result (current CCK)	3	1	M	Provision result for CCK currently in use - note
Provision Result (future CCK)	3	1	M	Provision result for CCK to be use in the future - note
Proprietary element		3	O	
NOTE: If the MS did not receive a current or future CCK in the D-OTAR Provide PDU, then the MS shall set the corresponding provision result to be equal to 000_2 - CCK accepted.				

4.4.6.14 U-OTAR SCK Demand

Shall be used by the MS to request SCK from the SwMI.

Direction: MS to SwMI
Service used: MM
Response to: none
Response expected: D-OTAR SCK Provide

Table 20: U-OTAR SCK Demand PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0101_2
OTAR sub-type	3	1	M	SCK Demand
Number of SCKs requested	2	1	M	
SCK number (SCKN)	5	1	C	note
Proprietary element		3	O	
NOTE: 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.				

4.4.6.15 U-OTAR SCK Result

Shall be used by MS-MM to explicitly accept or reject the SCKs provided by the SwMI.

Direction: MS to SwMI
Service used: MM
Response to: D-OTAR SCK Provide
Response expected: none

Table 21: U-OTAR SCK Result PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0101_2
OTAR sub-type	3	1	M	SCK Result
Number of SCKs requested	2	1	M	
SCK number and result	8	1	C	note
Proprietary element		3	O	
NOTE: 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.				

4.4.6.16 U-OTAR GCK Demand

Shall be used by the MS to request a GCK from the SwMI.

Direction: MS to SwMI
Service used: MM
Response to: none
Response expected: D-OTAR GCK Provide

Table 22: U-OTAR GCK Demand PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0101_2
OTAR sub-type	2	1	M	GCK Demand
GSSI	24	1	M	
Address Extension	24	2	O	
Proprietary element		3	O	

4.4.6.17 U-OTAR GCK Result

Shall be used by MS-MM to explicitly accept or reject a GCK provided by the SwMI.

Direction:	MS to SwMI
Service used:	MM
Response to:	D-OTAR GCK Provide
Response expected:	none

Table 23: U-OTAR GCK Result PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0101_2
OTAR sub-type	2	1	M	GCK Result
GCK Version Number	16	1	M	
Provision result (GCK)	3	1	M	
GSSI	24	1	M	
Address Extension	24	2	O	
Proprietary element		3	O	

4.4.6.18 U-TEI PROVIDE

Shall be used by MS-MM to inform the SwMI of its terminal equipment identifier.

Direction:	MS to SwMI
Service used:	MM
Response to:	D-LOCATION UPDATE ACCEPT
Response expected:	none

Table 24: U-TEI PROVIDE PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	1001_2
TEI	60	1	M	
Address extension	24	1	M	
Proprietary element		3	O	

4.4.7 MM PDU type 3 information elements coding

The authentication mechanisms may be combined with the normal and SwMI-initiated registration procedures as shown in MSC scenarios earlier in clause 4. Therefore, type 3 elements are defined which carry the authentication information and which can be appended to the MM registration PDUs. These type 3 elements shall be as defined in this subclause.

4.4.7.1 Authentication uplink

This type 3 element shall be appended to U-LOCATION UPDATE DEMAND when the MS combines a registration request with a request to authenticate the SwMI or when the MS requests the CCK information for the current LA.

Direction:	MS to SwMI
MM PDU:	U-LOCATION UPDATE DEMAND
Response to:	D-LOCATION UPDATE COMMAND or none
Response expected:	D-AUTHENTICATION RESPONSE

Table 25: Authentication uplink element contents

Information Element	Length	Type	C/O/M	Remark
CCK request flag	1	1	M	
Random challenge [RAND2]	80	2	O	

4.4.7.2 Authentication downlink

This type 3 element shall be appended to D-LOCATION UPDATE ACCEPT to inform the MS about the result of an authentication procedure which has been combined with registration and/or to request that an MS supplies its TEI and/or to supply the MS with CCK information for the current cell.

Direction:	SwMI to MS
MM PDU:	D-LOCATION UPDATE ACCEPT
Response to:	U-AUTHENTICATION RESPONSE
Response expected:	none

Table 26: Authentication downlink element contents

Information Element	Length	Type	C/O/M	Remark
Authentication result [R1]	1	1	M	
TEI request flag	1	1	M	
CCK information for current LA	138	2	O	

4.4.8 PDU Information elements coding

The encoding of the elements for the PDUs described in subclause 4.3.8 is given in the following subclauses. The most significant bit of the values shown in the tables is transmitted first.

4.4.8.1 Address extension

The address extension element is used to indicate the full TSI address as defined below:

Table 27: Address extension element contents

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

4.4.8.2 Authentication result

Authentication result indicates the success or failure of an authentication. If the authentication fails, this element gives the reason for failure.

Table 28: Authentication result element contents

Information element	Length	Value	Remark
Authentication Result [R1 or R2]	1	0	Authentication failed
		1	Authentication successful or no authentication currently in progress

4.4.8.3 Authentication reject reason

Authentication reject reason indicates why a demand for authentication is rejected.

Table 29: Authentication reject reason element contents

Information element	Length	Value	Remark
Authentication reject reason	3	000_2	Authentication not supported
		others	Reserved

4.4.8.4 CCK identifier

The CCK identifier (CCK-id) is the numerical value associated with a version number of a common cipher key.

Table 30: CCK Identifier element contents

Information element	Length	Value	Remark
CCK Identifier	16	Any	

4.4.8.5 CCK key and identifier

The CCK key and identifier element is defined as below:

Table 31: CCK key and identifier element contents

Information Element	Length	Type	C/O/M	Remark
CCK identifier (CCK-id)	16	1	M	
Sealed CCK (SCCK)	120	1	M	

4.4.8.6 CCK information for current LA

The CCK information element is defined as below:

Table 32: CCK information element contents

Information Element	Length	Type	C/O/M	Remark
CCK provision indicator	2	1	M	
CCK Identifier (CCK-id)	16	1	C	note
Sealed CCK (SCCK)	120	1	C	note
NOTE: The CCK-id and SCCK elements shall only be present if CCK provision indicator = 10_2 or 11_2				

4.4.8.7 CCK provision indicator

The CCK indicator element indicates the scope of usage of a CCK. This element can indicate that no CCK is in use in the location area and also whether the CCK is unique to one or more location areas or is system wide.

Table 33: CCK provision indicator element contents

Information element	Length	Value	Remark
CCK provision indicator	2	00_2	No CCK in use or CCK not known
		01_2	CCK provided for this LA
		10_2	CCK provided for other LAs - note 1
		11_2	System wide CCK provided - note 2
NOTE 1: If this value is used, there should be a location are list in the PDU to indicate which LAs the CCK is provided for. NOTE 2: This value indicates that the CCK in being used in all LAs covered by the SwMI.			

4.4.8.8 CCK request flag

The CCK request flag is used to ask the SwMI to send the CCK in use in the current location area.

Table 34: CCK request flag element contents

Information element	Length	Value	Remark
CCK request flag	1	0	No CCK requested
		1	CCK requested

4.4.8.9 GCK key and identifier

The CCK key and identifier element is defined as below:

Table 35: GCK key and identifier element contents

Information Element	Length	Type	C/O/M	Remark
GCK version number	16	1	M	
Sealed GCK (SGCK)	120	1	M	

4.4.8.10 GCK version number

The GCK version number shall be used in the GCK OTAR mechanism to uniquely identify a key.

Table 36: GCK version number element contents

Information element	Length	Value	Remark
GCK-VN	16	any	

4.4.8.11 GSSI

The group address to which a GCK is associated. For a full definition see ETS 300 392-1 [1], clause 7.

Table 37: GSSI element contents

Information element	Length	Value	Remark
GSSI	24	any	

4.4.8.12 Location area list

The location area list element provides a list of location areas.

Table 38: Location area list element contents

Information Element	Length	Type	C/O/M	Remark
Number of location areas	4	1	M	
Location area	14	1	C	note
NOTE: The Location area element shall be repeated as many times as indicated by the Number of location areas element				

4.4.8.13 Location area

A location area in a TETRA network. For a full definition see ETS 300 392-2 [2], clause 16.

Table 39: Location area element contents

Information element	Length	Value	Remark
Location area	14	any	

4.4.8.14 Mobile country code

The mobile country code of a TETRA network. For a full definition see ETS 300 392-1 [1], clause 7.

Table 40: Mobile country code element contents

Information element	Length	Value	Remark
Mobile country code	10	any	

4.4.8.15 Mobile network code

The mobile network code of a TETRA network. For a full definition see ETS 300 392-1 [1], clause 7.

Table 41: Mobile network code element contents

Information element	Length	Value	Remark
Mobile network code	14	any	

4.4.8.16 Mutual authentication flag

The Mutual Authentication Identifier is used to indicate whether or not the PDU is part of a mutual authentication exchange between the MS and SwMI.

Table 42: Mutual authentication flag element contents

Information element	Length	Value	Remark
Mutual authentication flag	1	0	Mutual authentication = FALSE
		1	Mutual authentication = TRUE

4.4.8.17 Number of location areas

The Number of location areas element indicates how many location area elements there are to follow in the PDU.

Table 43: Number of location areas element contents

Information element	Length	Value	Remark
Number of location areas	4	000_2	Reserved
		001_2 to 111_2	1 to 15 location areas

4.4.8.18 Number of SCKs provided

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

Table 44: 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

4.4.8.19 Number of SCKs requested

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

Table 45: Number of SCKs requested element contents

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

4.4.8.20 OTAR sub-type

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

Table 46: OTAR sub-type element contents

Information element	Length	Value	Remark
OTAR sub-type	3	000_2	CCK Demand (uplink) or CCK Provide (downlink)
		001_2	CCK Result
		010_2	SCK Demand (uplink) or SCK Provide (downlink)Reject
		011_2	SCK Result
		100_2	GCK Demand (uplink) or GCK Provide (downlink)Reject
		101_2	GCK Result
		110_2	Reserved
		111_2	Reserved

4.4.8.21 PDU type

The PDU type indicates the MM PDU type for the authentication and OTAR PDUs. The PDU types in the following table are taken from the unused or security-reserved values of PDU type in the MM protocol. For more details, see ETS 300 392-2 [1], clause 16.

Table 47: PDU type element contents

Information element	Length	Value	Downlink Assignment	Uplink Assignment
PDU Type	4	0000_2	D-OTAR	U-AUTHENTICATION RESPONSE
		0001_2	D-AUTHENTICATION DEMAND	
		0010_2	D- AUTHENTICATION REJECT	
		0011_2	D-DISABLE	
		0100_2	D-ENABLE	U-AUTHENTICATION DEMAND
		0101_2		U-OTAR
		0110_2		U-AUTHENTICATION RESULT
		1000_2	D- AUTHENTICATION RESPONSE	
		1001_2		U-TEI PROVIDE
		1010_2		U-AUTHENTICATION REJECT
		1011_2		U-DISABLE STATUS
		1110_2	D-AUTHENTICATION RESULT	

NOTE: Values not shown on both uplink and downlink are assigned to other PDU types, which are given in ETS 300 392-2, [2], subclause 16.10.39.

4.4.8.22 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.

4.4.8.23 Provision result

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

Table 48: 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 KN
		011_2 to 111_2	Reserved

4.4.8.24 Random challenge

The random challenge is an 80 bit number used as the input to the authentication algorithm, from which a response is calculated.

Table 49: Random challenge element contents

Information element	Length	Value	Remark
Random challenge [RAND1 or RAND2]	80	Any	

4.4.8.25 Reject cause

The reject cause element is defined in clause 16 of ETS 300 392-2 [1] for the MM PDU, D-LOCATION UPDATE REJECT. The following table gives additional reject causes which are defined by the security protocol which is incremental upon the MM protocol.

Table 50: Reject cause element contents

Information element	Length	Value	Remark
Reject cause	5	00000_2 to 10001_2	Used for MM protocol -see ETS 300 392-2 [1], clause 16
		10010_2	Ciphering required
		10011_2	Authentication failure
		10100_2 to 11111_2	Reserved

4.4.8.26 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 and OTAR processes. Only one random seed is used per D-OTAR PDU, irrespective of the number of keys contained in the PDU. It is only provided from SwMI to MS.

Table 51: Random seed element contents

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

4.4.8.27 Response value

The response value is the value returned by the challenged party, calculated from the random challenge.

Table 52: Response value element contents

Information element	Length	Value	Remark
Response Value (RES1 or RES2)	32	Any	

4.4.8.28 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 53: SCK version number element contents

Information element	Length	Value	Remark
SCK version number	16	Any	

4.4.8.29 SCK key and identifier

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

Table 54: 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	

4.4.8.30 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 55: 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

4.4.8.31 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 56: 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	

4.4.8.32 Sealed Key

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

Table 57: Sealed Key element contents

Information element	Length	Value	Remark
Sealed Key	120	Any	

4.4.8.33 TEI

This is the terminal equipment identifier of the MS. For a full definition see ETS 300 392-1 [1], clause 7.

Table 58: TEI contents

Information element	Length	Value	Remark
Terminal equipment identifier	60	Any	

4.4.8.34 TEI information

This is the terminal equipment identifier and address extension of the MS. For a full definition see ETS 300 392-1 [1], clause 7.

Table 59: TEI information contents

Information Element	Length	Type	C/O/M	Remark
Terminal equipment identifier	60	1	M	
Address extension	24	1	M	

4.4.8.35 TEI request flag

This bit indicates whether the MS should supply the TEI.

Table 60: TEI request flag contents

Information element	Length	Value	Remark
TEI request flag	1	0	Do not supply TEI
		1	Supply TEI

4.4.8.36 Type 3 element identifier

The type 3 element identifier indicates the MM type 3 element to be used in the MM PDUs for authentication and OTAR purposes. The type 3 element identifiers in the following table are taken from the reserved values of type 3 element identifier defined in the MM protocol. For more details, see ETS 300 392-2 [1], clause 16.

Table 61: Type 3 element identifier element contents

Information element	Length	Value	Remarks
Type 3 element identifier	4	0100_2	Proprietary
		1001_2	Authentication uplink
		1010_2	Authentication downlink
		1011_2	Reserved for any future specified type 3 element
		1100_2	Reserved for any future specified type 3 element
		1101_2	Reserved for any future specified type 3 element
		1110_2	Reserved for any future specified type 3 element
		1111_2	Reserved for any future specified type 3 element

4.5 Boundary conditions for the cryptographic algorithms and procedures

In the following the symbol |XYZ| shall be used to denote the length of the parameter XYZ. If the length of a parameter can vary, |XYZ| denotes the range between the shortest and the longest possible values for XYZ.

TA11: Shall be used to compute KS from K and RS. The algorithm shall have the following properties:

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

Output: Bit string of length |KS|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and the Output (even if the details of the algorithm are known).

TA21: Shall be used to compute the KS’ from K and RS. The algorithm shall have the following properties:

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

Output: Bit string of length |KS’|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and the Output (even if the details of the algorithm are known).

TA12: Shall be used to compute (X)RES1 as well as DCK1 from KS and RAND1. The algorithm shall have the following properties:

Input 1: Bit string of length |KS|;
Input 2: Bit string of length |RAND1|;

Output 1: Bit string of length |(X)RES1|;
Output 2: Bit string of length |DCK1|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 or Output 2 from the knowledge of Input 2 and Output 1 (even if the details of the algorithm are known).

TA22: Shall be used to compute (X)RES2 as well as DCK2 from KS' and RAND2. The algorithm shall have the following properties:

Input 1: Bit string of length |KS'|;
Input 2: Bit string of length |RAND2|;

Output 1: Bit string of length |(X)RES2|;
Output 2: Bit string of length |DCK2|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 or Output 2 from the knowledge of Input 2 and Output 1 (even if the details of the algorithm are known).

TA31: Shall be used to compute SCCK from CCK, CCK-id and DCK. The algorithm shall have the following properties:

Input 1: Bit string of length |CCK|;
Input 2: Bit string of length |CCK-id|;
Input 3: Bit string of length |DCK|;

Output: Bit string of length |SCCK|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and the Output, provided that Input 3 is unknown (even if the details of the algorithms are known).

TA32: Shall be used to compute CCK from SCCK, CCK-id and DCK. The algorithm shall have the following properties:

Input 1: Bit string of length |SCCK|;
Input 2: Bit string of length |DCK|;
Input 3: Bit string of length |CCK-id|;

Output 1: Bit string of length |CCK|;
Output 2: Boolean.

The algorithm should be designed such that it is difficult to find for a fixed Input 2 a value for Input 1 and Input 3 that results in Output 2 assuming the value "FALSE", provided that Input 2 is unknown (even if the details of the algorithms are known). Moreover, it shall be difficult to derive (parts of) Input 2 from the observation of various matching values of other inputs and outputs (known plain text attack).

TA41: Shall be used to compute KSO from K and RSO. The algorithm shall have the following properties:

Input 1: Bit string of length |K|;
Input 2: Bit string of length |RSO|;

Output 1: Bit string of length |KSO|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from knowledge of input 2 and the output (even if details of the algorithm are known).

TA51: Shall be used to compute SSCK from SCK, SCKN, SCK-VN, and KSO. The algorithm shall have the following properties:

Input 1: Bit string of length |SCK|;
Input 2: Bit string of length |SCK-VN|;
Input 3: Bit string of length |KSO|;
Input 4: Bit string of length |SCKN|;

Output: Bit string of length |SSCK|.

The algorithms should be designed such that it is difficult to infer any information about Input 1 or Input 4 from the knowledge of Input 2 and the Output, provided that Input 3 is unknown (even if the details of the algorithm are known).

TA52: Shall be used to compute SCK and SCKN from SSCK, SCK-VN and KSO. The algorithm shall have the following properties:

Input 1: Bit string of length |SSCK|;
Input 2: Bit string of length |KSO|;
Input 3: Bit string of length |SCK-VN|;

Output 1: Bit string of length |SCK|;
Output 2: Boolean;
Output 3: Bit string of length |SCKN|.

The algorithm should be designed such that it is difficult to find for a fixed Input 2 values for Input 1 and Input 3 that result in Output 2 assuming the value FALSE, provided that Input 2 is unknown (even if the details of the algorithm are known). Moreover, it shall be difficult to derive (parts of) Input 2 from the observation of various matching values of other inputs and outputs (known plain text attack).

TA61: Shall be used to compute xESI from xSSI and either SCK or CCK. The algorithm shall have the following properties:

Input 1: Bit string of length |CCK|;
Input 2: Bit string of length |SSI|;

Output 1: Bit string of length |ESI|.

The algorithm should be designed such that it is difficult to infer any knowledge of Input 1 from observation of various matching values of other inputs and outputs. Further it should be difficult to infer any knowledge of Input 2 from observation of various matching values of other inputs and outputs. Moreover, for a fixed input 1 different values of Input 2 shall always give different values of the output.

TA71: Shall be used to compute MGCK from GCK and CCK. The algorithm shall have the following properties:

Input 1: Bit string of length |GCK|;
Input 2: Bit string of length |CCK|;

Output 1: Bit string of length |MGCK|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from knowledge of input 2 and the output (even if details of the algorithm are known), and also designed such that it is difficult to infer any information about Input 2 from knowledge of input 1 and the output (even if details of the algorithm are known).

TA81: Shall be used to compute SGCK from GCK, GTSI, GCK-VN and DCK. The algorithm shall have the following properties:

Input 1: Bit string of length |GCK|;
Input 2: Bit string of length |GCK-VN|;
Input 3: Bit string of length |DCK|;
Input 4: Bit string of length |GTSI|;

Output: Bit string of length |SGCK|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2, Input 4 and the Output, provided that Input 3 is unknown (even if the details of the algorithms are known).

TA82: Shall be used to compute GCK from SGCK, GCK-VN, GTSI and DCK. The algorithm shall have the following properties:

Input 1: Bit string of length |SGCK|;
Input 2: Bit string of length |DCK|;
Input 3: Bit string of length |GCK-VN|;
Input 4: Bit string of length |GTSI|;

Output 1: Bit string of length |CCK|;
Output 2: Boolean.

The algorithm should be designed such that it is difficult to find for a fixed Input 2 values for Input 1, Input 3 and Input 4 that result in Output 2 assuming the value "FALSE", provided that Input 2 is unknown (even if the details of the algorithms are known). Moreover, it shall be difficult to derive (parts of) Input 2 from the observation of various matching values of other inputs and outputs (known plain text attack).

TB1: Shall be used to compute K from AC. The algorithm shall have the following properties:

Input: Bit string of length |AC|;

Output: Bit string of length |K|.

The algorithm should be designed such that the Output is dependent on every bit of the Input.

TB2: Shall be used to compute K from UAK. The algorithm shall have the following properties:

Input: Bit string of length |UAK|;

Output: Bit string of length |K|.

The algorithm should be designed such that the Output is dependent on every bit of the Input.

TB3: Shall be used to compute K from UAK and PIN. The algorithm shall have the following properties:

Input 1: Bit string of length |PIN|;
Input 2: Bit string of length |UAK|;

Output: Bit string of length |K|.

The algorithm should be designed such that the Output is dependent on every bit of both Inputs.

TB4: Shall be used to compute DCK from DCK1 and DCK2. The algorithm shall have the following properties:

Input 1: Bit string of length |DCK1|;
Input 2: Bit string of length |DCK2|;

Output: Bit string of length |DCK|.

The algorithm should be designed such that the Output is dependent on every bit of both Inputs.

4.6 Dimensioning of the cryptographic parameters

Table 62: Dimensioning of cryptographic parameters

Abbreviation	No. of Bits
AC	16 - 32
CK	80
CCK	80
CCK-id	16
DCK1	80
DCK2	80
DCK	80
ESI	24
GCK	80
GCK-VN	16
GTSI	48
K	128
KS	128
KS’	128
KSO	128
MF	1
MGCK	80
PIN	16 - 32
RAND1	80
RAND2	80
RES1	32
RES2	32
RS	80
RSO	80
SCCK	120
SCK	80
SCKN	5
SCK-VN	16
SGCK	120
SSCK	120
SSI	24
UAK	128
XRES1	32
XRES2	32

4.7 Summary of the cryptographic processes

A summary of the authentication mechanisms explained in the previous subclauses is given in figure 31. Only the paths where keys are generated by an algorithm are shown and only the CCK option for generating MGCK from GCK is shown.

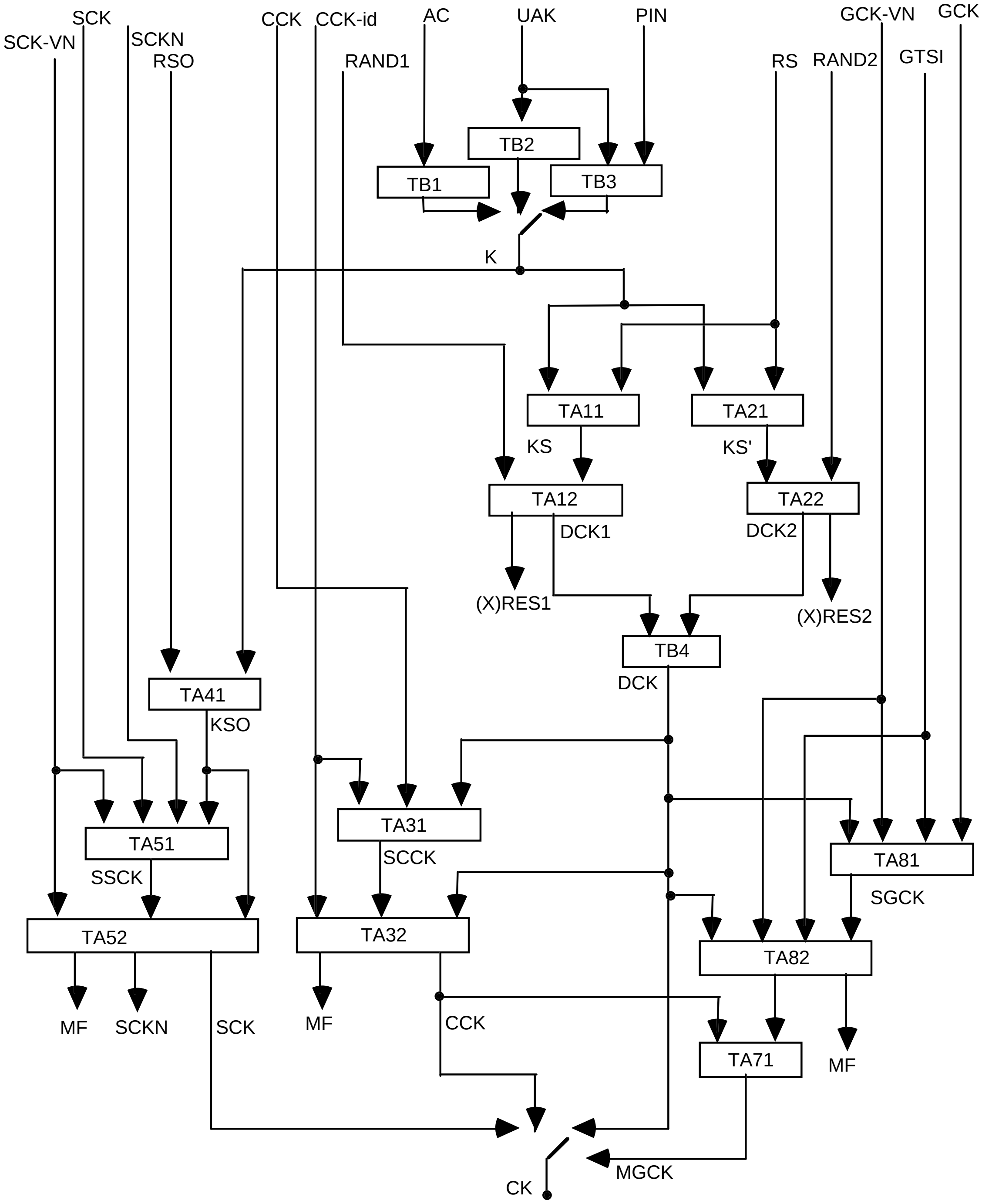


Figure 31: Overview of air interface authentication and key management

5 Secure enable and disable mechanism

5.1 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 32. 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 300 392-1 [1], clause 7.

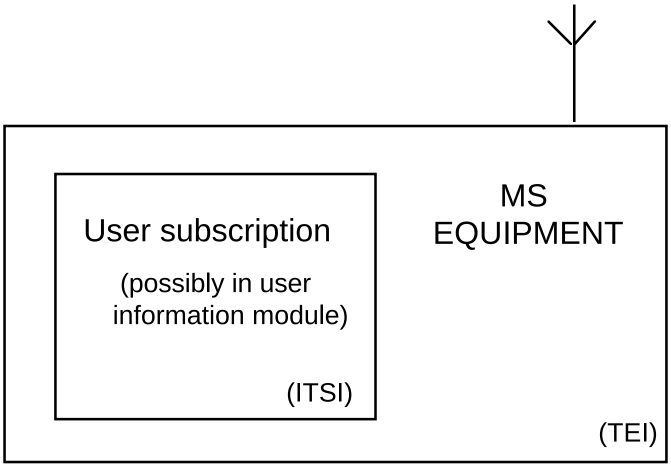
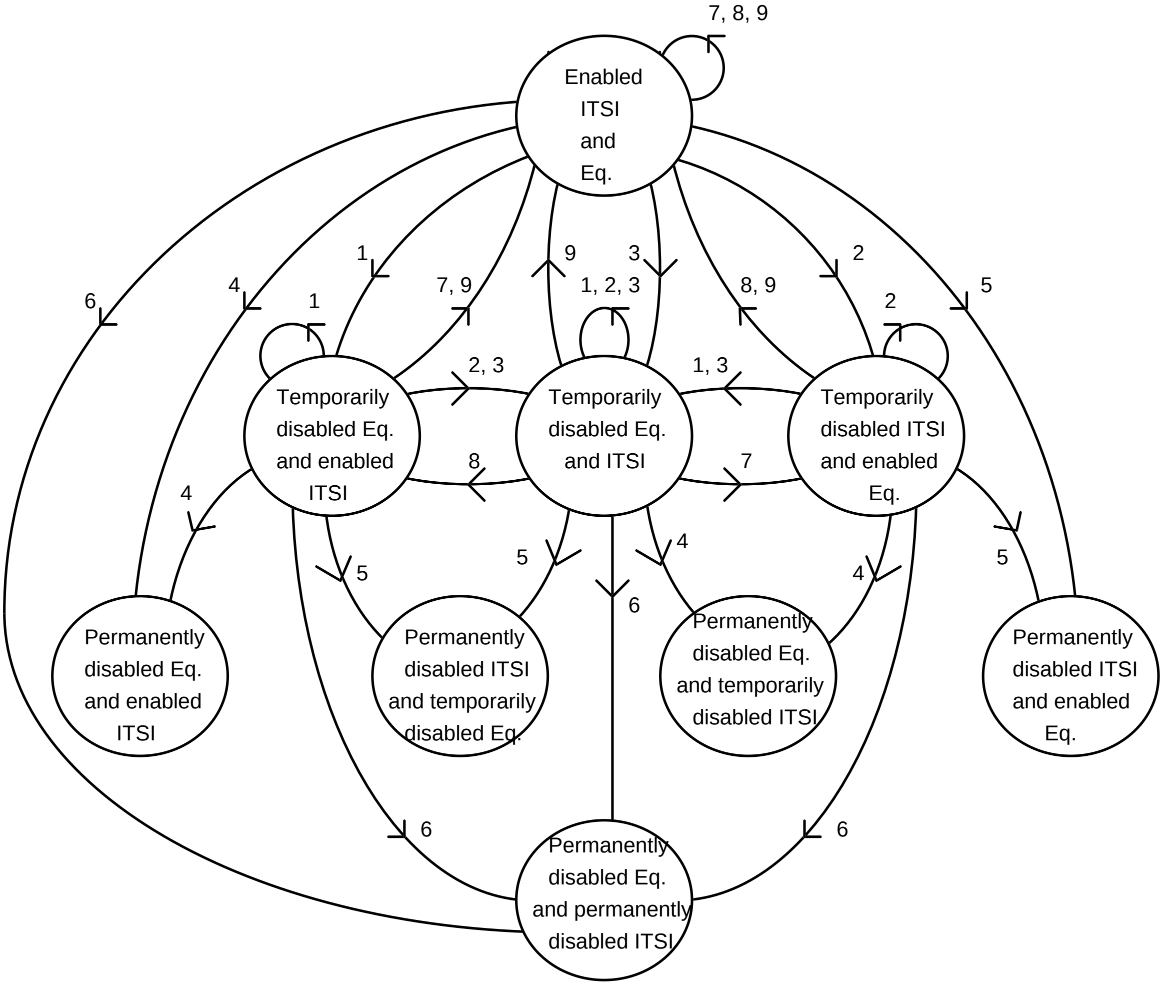


Figure 32: Relationship of TEI and ITSI in MS

5.2 Enable/disable state transitions

The state diagram in figure 33 shows all possible enabled and disabled states of one pair of MS equipment and ITSI. This diagram does not show state transitions due to separation of ITSI from, or fitting of ITSI into, an MS equipment.


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

KEY:

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 33: State transitions of enable/disable mechanism

5.3 Mechanisms

There are six possible transactions necessary for the enable/disable procedure which allow disable and enable of the MS equipment, the users' subscription, or both. These are detailed in subclauses 5.3.1 to 5.3.6. All transactions should be carried out with air interface encryption applied to avoid visibility of the TEI at the air interface.

The state of the MS when either equipment or subscription are temporarily or permanently disabled shall follow the descriptions in ETS 300 392-2 [2], clauses 15 and 16. Wherever the state of the MS is described as enabled or disabled in this subclause, the definition of operation in ETS 300 392-2 [2] shall apply. The mechanisms described in this subclause shall replace those described in ETS 300 392-2 [2], clauses 15 and 16.

The disable and enable mechanisms can be applied with different security levels: specifically, they can be applied with or without air interface encryption in place, and can be applied with or without authentication. Each MS should implement a disable and enable mechanism that requires the same level of security as that of its home encrypted SwMI type. The encrypted SwMI types are listed in table 82. An MS should be disabled by a disable mechanism of equal or greater security to that in use in its home system, but should not be disabled by a lesser security mechanism. For example if the home system implements encryption by SCK and no authentication (SwMI type 2), the MS should accept disable requests from SwMI types 2 to 4. If the home SwMI of the MS employs authentication, the MS should not accept enable or disable requests without authentication. Further, if the home SwMI of the MS employs authentication, the MS shall not accept enable or disable requests from its home SwMI without authentication.

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 5.3.4 to 5.3.6. Equipment or subscriptions that have been permanently disabled shall not be enabled by these mechanisms.

5.3.1 Disable of MS equipment

The MS equipment shall be disabled by the SwMI 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.

5.3.2 Disable of MS subscription

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

5.3.3 Disable an MS subscription and equipment

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

5.3.4 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.

5.3.5 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.

5.3.6 Enable an MS equipment and subscription

The MS equipment and subscription shall be enabled by signalling addressed to both ITSI and TEI, and shall be enabled whether the subscription or equipment has previously been disabled, or both. Equipment, or 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 utilising any of the mechanisms described in subclauses 5.3.1, 5.3.2 and 5.3.3. However, to re-enable an MS the SwMI shall use the corresponding mechanism or a mechanism including it. Therefore, an MS temporarily disabled using the mechanism described in subclause5.3.1 shall only be enabled using the mechanisms described in subclause 5.3.4 or subclause 5.3.6; an MS disabled by the mechanism described in subclause 5.3.2 shall only be enabled by the mechanisms described in subclause 5.3.5 or subclause 5.3.6; and an MS disabled by the mechanism described in subclause 5.3.3 shall only be enabled by the mechanism described in subclause 5.3.6.

5.4 Enable/disable protocol

5.4.1 General case

All signalling should be directed to an MS by ITSI: this implies that the SwMI should already know the ITSI/TEI binding where necessary, for example by obtaining ITSI-TEI mapping at registration. If the SwMI supports authentication, it should authenticate the MS to ensure that it is obtaining a response from the correct MS. The MS should also authenticate the SwMI when possible to validate the instruction. The authentication protocol and PDUs are contained in clause 4.

The TEI when included in PDUs is not protected by any specific cryptographic sealing mechanism. It should therefore only be provided when encryption parameters have been established, and air interface encryption is operating on a system as described in clause 6.

5.4.2 Specific protocol exchanges

The normal message exchanges for the various cases shall be according to subclauses 5.4.2.1 through 5.4.2.4.

5.4.2.1 Disabling an MS using authentication

The protocol is shown in figure 34 and described below. For more details on the authentication protocols used as part of the disable procedure, see subclauses 4.4.2.1, 4.4.2.3, and 4.4.2.9 which show SwMI authentication of the MS and SwMI-initiated mutual authentication scenarios. The authentication protocol described in these subclauses shall also be valid here.

If authentication is to be used as part of the disable procedure, the MS and SwMI should mutually authenticate each other.

The SwMI shall send a D-DISABLE intent to the MS addressed to its individual SSI. The "Equipment disable" and "Subscription disable" elements shall indicate whether the equipment or subscription or both are to be disabled. If the subscription is to be disabled, the "Address extension" element shall be present; and if the equipment is to be disabled, the "TEI" element shall be present. The D-DISABLE intent shall indicate whether the disabling is temporary or permanent by setting the "Disabling type" element appropriately. Since, in this case, the SwMI is configured to authenticate the MS before disabling, D-DISABLE intent shall also contain the "Authentication challenge" element to authenticate the MS.

After sending the D-DISABLE intent, the SwMI shall switch off air interface encryption for its transmitter using the MLE-ENCRYPTION primitive.

On receipt of the request, the MS shall also switch off air interface encryption for its transmitter using the MLE-ENCRYPTION primitive.

If the TEI and/or address extension is included in D-DISABLE intent and they match those of the MS and, if authentication is supported by the MS, it shall then send a U-AUTHENTICATION RESPONSE to the SwMI containing the response to the SwMI's challenge. The MS may also mutually authenticate the SwMI by including a random challenge in U-AUTHENTICATION RESPONSE.

NOTE: The MS should mutually authenticate the SwMI during the disabling procedure if authentication is supported by the MS.

If the TEI and/or address extension is included in D-DISABLE intent and either of these does not match those of the MS, the MS shall respond to D-DISABLE intent with U-DISABLE STATUS which shall indicate that the disabling attempt has failed due to mismatch of the TEI and/or address extension.

If authentication is not supported by the MS, it shall instead send U-AUTHENTICATION REJECT to the SwMI in response to D-DISABLE intent. The SwMI may then send D-DISABLE intent again, this time without the "Authentication challenge element" to attempt to disable the MS without authentication as described in subclause 5.4.2.2.

On receiving U-AUTHENTICATION RESPONSE, the SwMI shall send a D-AUTHENTICATION RESULT with the result of the SwMI's authentication of the MS. If the MS has requested mutual authentication, the SwMI shall also include its response to the MS challenge in D-AUTHENTICATION RESULT.

The MS shall load the new ciphering parameters established by the authentication exchange for receive and transmit to the MLE using the MLE encryption primitive, and the BS shall load these parameters for receive only.

If mutual authentication is in progress, the MS shall then send a U-AUTHENTICATION RESULT containing the result of the MS's authentication of the SwMI. The BS shall then load the new ciphering parameters to the MLE for receive and transmit using the MLE ENCRYPTION primitive.

If the MS has not previously requested mutual authentication, and D-AUTHENTICATION RESULT indicates that the SwMI has successfully authenticated the MS, the MS shall send U-DISABLE STATUS to inform the SwMI of the result of the disable procedure, which should be successful if authentication was successful. If successful disabling is indicated in U-DISABLE STATUS, the TEI and address extension shall be included in this PDU.

If mutual authentication is in progress and U-AUTHENTICATION RESULT indicates that the MS authentication of the SwMI was successful, the SwMI shall send a D-DISABLE confirm PDU using the new encryption parameters to confirm the disabling command. D-DISABLE confirm shall include the same parameters as the previously sent D-DISABLE intent, except that D-DISABLE confirm shall not include an "Authentication challenge" element.

The MS shall reply with a U-DISABLE STATUS PDU (indicating that disabling was successful), in which it shall send its TEI together with the address extension to the SwMI. The "Equipment status" and "Subscription status" elements shall indicate the new state of the MS; note that it is possible that an MS already disabled by one means may subsequently be disabled by the other, hence these elements may not correspond to the desired status of the "Disable subscription" and "Disable equipment" elements in the D-DISABLE PDUs.

The MS shall then comply with the request, and disable itself, sending an MLE-CLOSE req primitive from MM to MLE to prevent the MS from taking part in calls, and sending a TNMM-DISABLING ind primitive to the user application.

Once temporarily disabled, the MS may still respond to further disable requests, for example to be disabled by TEI when already disabled by ITSI, or responding to a duplicate request. If permanently disabled, the MS shall not respond to further signalling.

If the MS is to be permanently disabled MS-MM shall send an MLE-DEACTIVATE primitive.

Note that the authentication establishes a new DCK, and this new DCK shall be passed to the MAC in the MS by using the MLE_ENCRYPTION primitive once it is derived. This results in the D-DISABLE confirm and U-DISABLE STATUS being sent to the SwMI with the new DCK.

If the either authentication fails, the MS shall ignore the request and instead the recovery procedure following failed authentication shall apply. This is described in subclause 4.3.2.

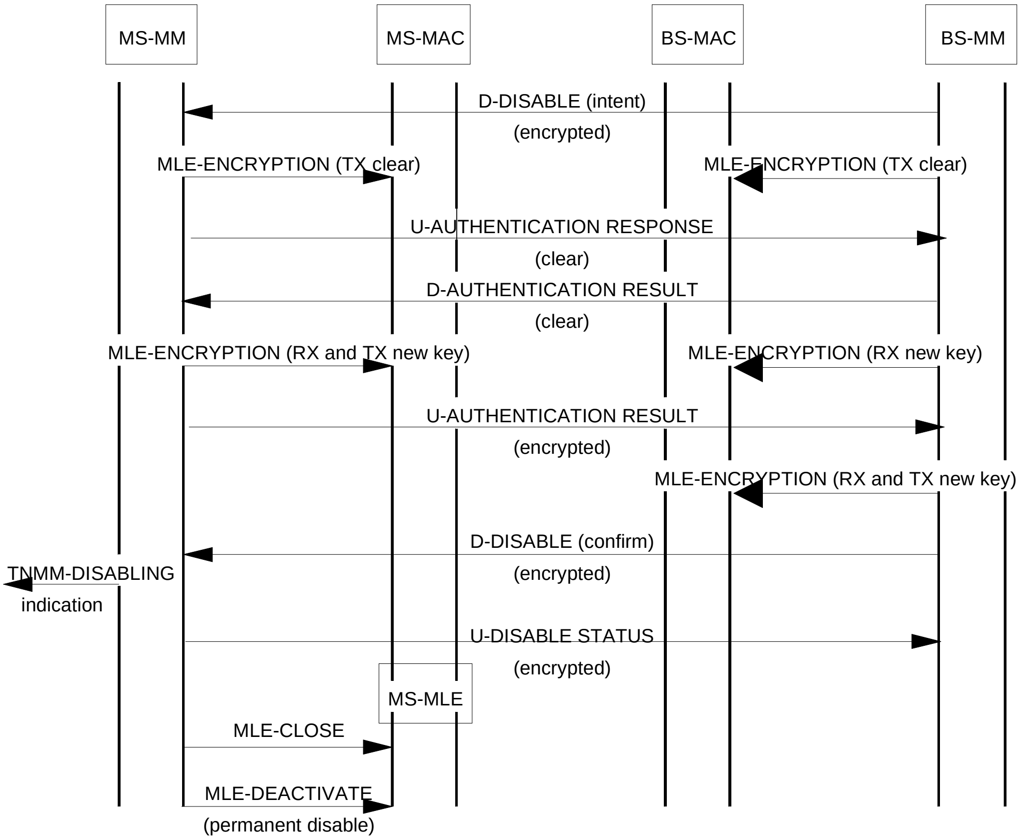


Figure 34: Disabling an MS with authentication

5.4.2.2 Disable an MS without authentication

The protocol is shown in figure 35 and described below.

The SwMI shall send a D-DISABLE intent to the MS addressed to its individual SSI. The "Equipment disable" and "Subscription disable" elements shall indicate whether the equipment or subscription or both is to be disabled. If the subscription is to be disabled, the "Address extension" element shall be present; and if the equipment is to be disabled, the "TEI" element shall be present. The D-DISABLE intent shall indicate whether the disabling is temporary or permanent by setting the "Disabling type" element appropriately. Since, in this case, the SwMI is not configured to authenticate the MS before disabling, no authentication challenge shall be included in D-DISABLE intent.

If the MS is configured to respond to such a request without authentication, it shall respond with a U-DISABLE STATUS PDU to indicate whether or not disabling was successful.

If disabling was successful, U-DISABLE STATUS shall include the TEI and address extension elements.

If disabling was not successful, the MS shall use the "Enable/disable result" element to indicate the reason for disabling failure, i.e. mismatch of one or both of address extension and TEI, or the MS requires authentication before disabling is accepted. In the case of disabling failure, the address extension and TEI shall not be included in U-DISABLE STATUS. If U-DISABLE STATUS indicates disabling failure due to the MS need for authentication, the SwMI should repeat the D-DISABLE intent PDU, but including an authentication challenge.

In all cases, the "Equipment status" and "Subscription status" elements in U-DISABLE STATUS shall indicate the new state of the MS; note that it is possible that an MS already disabled by one means may subsequently be disabled by the other, hence this may not correspond to the desired status of the "Disable equipment" and "Disable subscription" elements in the D-DISABLE intent PDU.

Both D-DISABLE intent and U-DISABLE STATUS PDUs shall be sent with encryption, if applied, switched on.

If temporarily disabled, the MS may still respond to further disable requests, for example to be disabled by TEI when already disabled by ITSI, or responding to a duplicate request. If permanently disabled, the MS shall not respond to further signalling.

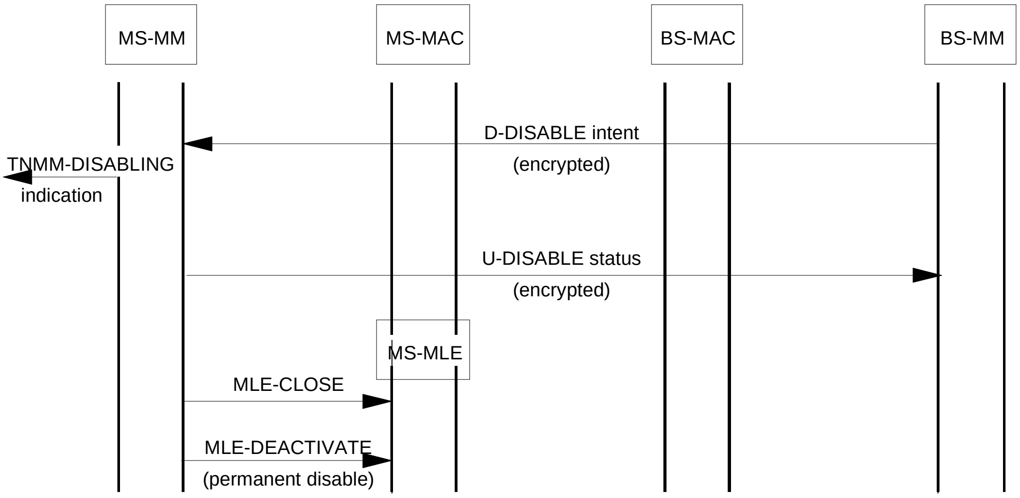


Figure 35: Disable of MS without authentication

5.4.2.3 Enable an MS using authentication

The protocol is shown in figure 36 and described below. For more details on the authentication protocols used as part of the enable procedure, see subclauses 4.4.2.1 and 4.4.2.3, 4.4.2.9 which show SwMI authentication of the MS and SwMI-initiated mutual authentication scenarios. The authentication protocol described in these subclauses shall also be valid here.

If authentication is to be used as part of the enable procedure, the MS and SwMI should mutually authenticate each other.

The SwMI shall send a D-ENABLE intent to the MS addressed to its individual SSI. The "Equipment enable" and "Subscription enable" elements shall indicate whether the equipment or subscription is to be re-enabled, or both. If the subscription is to be enabled, the "Address extension" element shall be present; and if the equipment is to be enabled, the "TEI" element shall be present. An enable from permanent disable shall not be permitted as the MS may only be enabled after a temporary disabling. Since, in this case, the SwMI is configured to authenticate the MS before enabling, D-ENABLE intent shall also contain the "Authentication challenge" element to authenticate the MS.

Once the SwMI has sent the D-ENABLE intent, it shall switch off air interface encryption for its transmitter using the MLE-ENCRYPTION primitive.

On receipt of the request, the MS shall also switch off encryption for its transmitter using the MLE-ENCRYPTION primitive.

If the TEI and/or address extension is included in D-ENABLE intent and they match those of the MS and, if authentication is supported by the MS, it shall then send a U-AUTHENTICATION RESPONSE to the SwMI containing the response to the SwMI’s challenge. The MS may also mutually authenticate the SwMI by including a random challenge in U-AUTHENTICATION RESPONSE.

NOTE: The MS should mutually authenticate the SwMI during the enabling procedure if authentication is supported by the MS.

If the TEI and/or address extension is included in D-ENABLE intent and either of these does not match those of the MS, the MS shall respond to D-ENABLE intent with U-DISABLE STATUS which shall indicate that the enabling attempt has failed due to mismatch of the TEI and/or address extension.

If authentication is not supported by the MS, it shall instead send U-AUTHENTICATION REJECT to the SwMI in response to D-ENABLE intent. The SwMI may then send D-ENABLE intent again, this time without the "Authentication challenge element" to attempt to enable the MS without authentication as described in subclause 5.4.2.4.

On receiving U-AUTHENTICATION RESPONSE, the SwMI shall send a D-AUTHENTICATION RESULT with the result of the SwMI's authentication of the MS. If the MS has requested mutual authentication, the SwMI shall also include its response to the MS challenge in D-AUTHENTICATION RESULT.

The MS shall load the new ciphering parameters established by the authentication exchange for receive and transmit to the MLE using the MLE encryption primitive, and the BS shall load these parameters for receive only.

If mutual authentication is in progress, the MS shall then send a U-AUTHENTICATION RESULT containing the result of the MS's authentication of the SwMI. The BS shall then load the new ciphering parameters to the MLE for receive and transmit using the MLE ENCRYPTION primitive.

If the MS has not previously requested mutual authentication, and D-AUTHENTICATION RESULT indicates that the SwMI has successfully authenticated the MS, the MS shall send U-DISABLE STATUS to inform the SwMI of the result of the enable procedure, which should be successful if authentication was successful. If successful enabling is indicated in U-DISABLE STATUS, the TEI and address extension shall be included in this PDU

If mutual authentication is in progress and U-AUTHENTICATION RESULT indicates that the MS authentication of the SwMI was successful, the SwMI shall then send a D-ENABLE confirm PDU using the new encryption parameters to confirm the enabling command. D-ENABLE confirm shall include the same parameters as the previously sent D-ENABLE intent, except that D-ENABLE confirm shall not include an "Authentication challenge" element.

The MS shall reply with U-DISABLE STATUS (indicating that enabling was successful), in which it shall include its TEI together with the address extension to the SwMI. The "Equipment status" and "Subscription status" elements shall indicate the new state of the MS which may or may not correspond to the requested status, depending whether the enabling corresponded to previous disabling or not.

If the both "status" elements had been set to indicate "enabled", the MS shall enable itself, sending an MLE-OPEN req primitive from MM to MLE to enable the MS and sending a TNMM-ENABLING ind primitive to the user application to allow the application to be enabled also. If the enabling request did not correspond fully to a previous disabling, the "status" elements shall indicate that some disabling is not cleared, and the MLE shall not be opened.

The authentication establishes a new DCK, and this new DCK shall be passed to the MAC in the MS by using the MLE_ENCRYPTION primitive once it is derived. This results in the D-DISABLE confirm and the U-DISABLE STATUS being sent to the SwMI with the new DCK.

If the authentication fails, the MS shall ignore the request and instead the recovery procedure following failed authentication shall apply. This is described in subclause 4.3.2.

If the MS is configured not to accept enabling requests, or if the transaction fails because the TEI and/or address extension supplied by the SwMI (if any) does not match that of the MS, the MS shall respond with a U- DISABLE STATUS immediately indicating this mismatch; the protocol therefore follows that described in subclause 5.4.2.4.

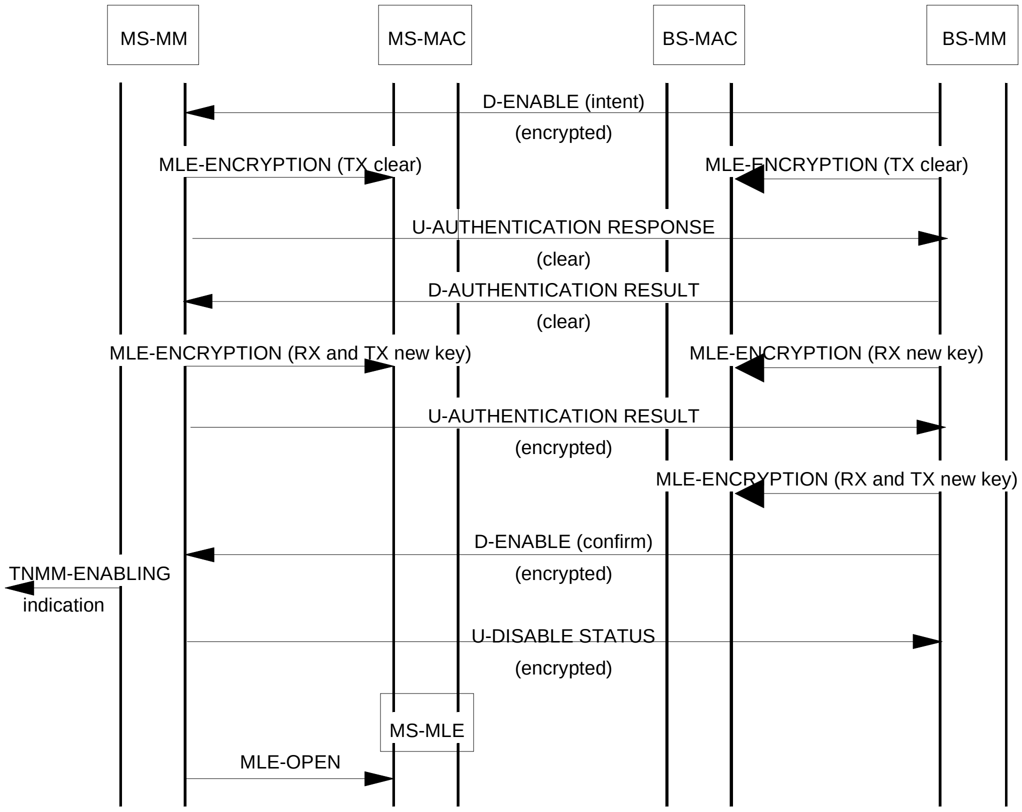


Figure 36: Enabling an MS with authentication

5.4.2.4 Enable an MS without authentication

The protocol is shown in figure 37 and described below.

The SwMI shall send a D-ENABLE intent to the MS addressed to its individual SSI. The "Equipment enable" and "Subscription enable" elements shall indicate whether the equipment or subscription or both is to be re-enabled. If the subscription is to be enabled, the "Address extension" element shall be present; and if the equipment is to be enabled, the "TEI" element shall be present. An enable from permanent disable shall not be permitted as the MS may only be enabled after a temporary disabling. Since, in this case, the SwMI is not configured to authenticate the MS before disabling, no "Authentication challenge" element shall be included in D-ENABLE intent.

If the MS is configured to respond to such a request without authentication, it shall respond with a U-DISABLE STATUS PDU to indicate whether or not enabling was successful,

If enabling was successful, U-DISABLE STATUS shall include the TEI and address extension elements.

If enabling was not successful, the MS shall use the "Enable/disable result" element to indicate the reason for enabling failure, i.e. mismatch of one or both of address extension and TEI, or the MS requires authentication before enabling is accepted. In the case of enabling failure, the address extension and TEI shall not be included in U-DISABLE STATUS. If U-DISABLE STATUS indicates enabling failure due to the MS need for authentication, the SwMI should repeat the D-ENABLE intent PDU, but including an authentication challenge.

In all cases, the "Equipment status" and "Subscription status" elements shall indicate the new state of the MS which may or may not correspond to the requested status, depending whether the enabling corresponded to previous disabling or not.

Both D-ENABLE intent and U-DISABLE STATUS PDUs shall be sent with encryption, if applied, switched on.

If the both "status" elements had been set to indicate "enabled", the MS shall enable itself, sending an MLE-OPEN req primitive from MM to MLE to enable the MS and sending a TNMM-ENABLE ind primitive to the user application to allow the application to be enabled also. If the enabling request did not correspond fully to a previous disabling, the "status" elements shall indicate that some disabling is not cleared, and the MLE shall not be opened.

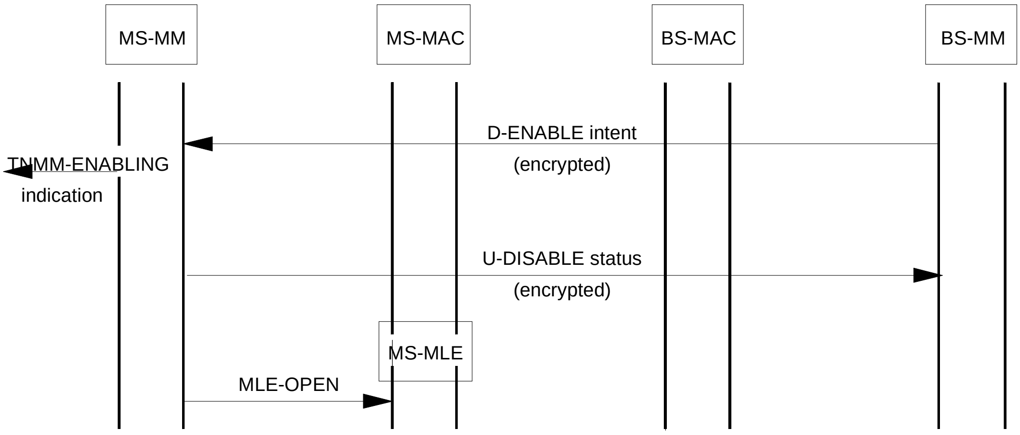


Figure 37: Enabling an MS without authentication, or failure of enable request

5.4.3 MM service primitives

MM shall provide indication to the user application when the MS has been disabled or enabled. The primitives that shall be provided are detailed in the following subclauses.

5.4.3.1 TNMM-DISABLING primitive

TNMM-DISABLING indication primitive shall be used as an indication to the user application that a temporary or permanent disabling of the MS is ordered.

The parameters shall be as defined in table 63:

Table 63: Parameters for the primitive TNMM-DISABLING indication

Parameter	Indication
Enable/disable status	M

5.4.3.2 TNMM-ENABLING primitive

TNMM-ENABLING indication primitive shall be used as an indication to the user application that the temporary disabling of the MS is cancelled.

The parameters shall be as defined in table 64:

Table 64: Parameters for the primitive TNMM-ENABLING indication

Parameter	Indication
Enable/disable status	M

The parameters in the primitives may take the following values:

Parameter name	Values / Options
Enable/disable status	Enabled
	Equipment temporary disabled
	Equipment permanently disabled
	Subscription temporary disabled
	Subscription permanently disabled
	Equipment and subscription temporary disabled
	Equipment and subscription permanently disabled

5.4.4 MM PDUs structures and contents

The PDUs described here replace PDUs described in ETS 300 392-2 [2], subclause 16.9.2, as follows:

D-DISABLE and D-ENABLE retain the same type values, however the PDU structures shall change as described below;

U-DISABLE STATUS uses a previously reserved value (1011_2).

5.4.4.1 D-DISABLE

Message:	D-DISABLE
Response to:	-
Response expected:	U-DISABLE STATUS or U-AUTHENTICATION RESPONSE
Short description:	The message is sent by the Infrastructure to indicate that the mobile station shall be disabled (permanently or temporarily)

Table 65: D-DISABLE contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0011_2
Intent/Confirm	1	1	M	Intent or confirm
Disabling type	1	1	M	Temporary or permanent
Equipment disable	1	1	M	Disable equipment
TETRA Equipment Identity	60	1	C	Present if equipment disable = 1
Subscription disable	1	1	M	Disable subscription
Address Extension	24	1	C	Present if Subscription disable = 1
Authentication challenge	160	2	O	
Proprietary		3	O	

5.4.4.2 D-ENABLE

Message:	D-ENABLE
Response to:	-
Response expected:	U-DISABLE STATUS or U-AUTHENTICATION RESPONSE
Short description:	The message is sent by the Infrastructure to indicate that the mobile station shall be enabled after a disable.

Table 66: D-ENABLE contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0100_2
Intent/Confirm	1	1	M	Intent or confirm
Equipment enable	1	1	M	Enable of equipment
TETRA Equipment Identity	60	1	C	Present if equipment enable = 1
Subscription enable	1	1	M	Enable of subscription
Address Extension	24	1	C	Present if Subscription disable =1
Authentication challenge	160	2	O	
Proprietary		3	O	

5.4.4.3 U-DISABLE STATUS

Message:	U-DISABLE STATUS
Response to:	D-DISABLE or D-ENABLE
Response expected:	None
Short description:	The message is sent by the mobile station to inform the infrastructure of its response to an enable or disable request and its resulting status.

Table 67: U-DISABLE STATUS contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	1011_2
Equipment status	2	1	M	Indicates disabled state of equipment
Subscription status	2	1	M	Indicates disabled state of subscription
Enable/Disable result	2	1	M	
Address Extension	24	1	C	Present only if enable/disable result = 000_2
TETRA Equipment Identity	60	1	C	Present only if enable/disable result = 000_2
Proprietary		3	O	

5.4.5 MM Information elements coding

5.4.5.1 Address extension

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

Table 68: Address Extension element contents

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

5.4.5.2 Authentication challenge

The Authentication Challenge element shall contain the random seed and random challenge from the SwMI to the MS if authentication is to be used in the enable or disable procedure.

Table 69: Authentication challenge element contents

Information sub element	Length	Type	Remark
Random challenge RAND1	80	1	
Random seed RS	80	1	

5.4.5.3 Disabling type

The purpose of the Disabling Type element shall be to indicate which of the disabling types (i.e. temporary or permanent) is requested.

Table 70: Disabling Type element contents

Information element	Length	Value	Remark
Disabling Type	1	0	Temporary
		1	Permanent

5.4.5.4 Enable/Disable result

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

Table 71: Enable/Disable result element contents

Information element	Length	Value	Remark
Enable/Disable result	3	000_2	enable/disable successful
		001_2	enable/disable failure, address extension mismatch
		010_2	enable/disable failure, TEI mismatch
		011_2	enable/disable failure, TEI and address extension mismatch
		100_2	enable/disable failure, authentication is required
		others	reserved

5.4.5.5 Equipment disable

The purpose of the equipment disable element shall be to indicate whether the equipment is to be disabled.

Table 72: Equipment disable element contents

Information element	Length	Value	Remark
Equipment disable	1	0	Equipment not to be disabled
		1	Equipment to be disabled

5.4.5.6 Equipment enable

The purpose of the Equipment enable element shall be to indicate whether the equipment is to be Enabled.

Table 73: Equipment enable element contents

Information element	Length	Value	Remark
Equipment enable	1	0	Equipment not to be enabled
		1	Equipment to be enabled

5.4.5.7 Equipment status

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

Table 74: 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

5.4.5.8 Intent/confirm

The purpose of the Intent/confirm element shall be to indicate whether the enable or disable command is the first intent, always used with or without authentication, or the confirmation once successful authentication has been carried out .

Table 75: Intent/confirm element contents

Information element	Length	Value	Remark
Intent/confirm	1	0	Intent
		1	Confirm

5.4.5.9 PDU Type

The PDU type. (The table modifies the definitions given in ETS 300 392-2 [2], subclause 16.10.39).

Table 76: PDU Type element contents

Information element	Length	Value	Downlink Assignment	Uplink Assignment
PDU Type	4	0011_2	D-DISABLE	
		0100_2	D-ENABLE	
		1011_2		U-DISABLE STATUS

NOTE: Values not shown on both uplink and downlink are assigned to other PDU types, which are given in ETS 300 392-2, [2], subclause 16.10.39, and as given in subclause 4.4.8.21 of this part of the ETS.

5.4.5.10 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.

5.4.5.11 Subscription disable

The purpose of the Subscription disable element shall be to indicate whether the subscription is to be disabled.

Table 77: Subscription disable element contents

Information element	Length	Value	Remark
Subscription disable	1	0	Subscription not to be disabled
		1	Subscription to be disabled

5.4.5.12 Subscription enable

The purpose of the Subscription enable element shall be to indicate whether the subscription is to be enabled.

Table 78: Subscription enable element contents

Information element	Length	Value	Remark
Subscription enable	1	0	Subscription not to be enabled
		1	Subscription to be enabled

5.4.5.13 Subscription status

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

Table 79: 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

5.4.5.14 TETRA equipment identity

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

Table 80: TETRA Equipment Identity element contents

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

6 Air Interface (AI) encryption

6.1 General principles

AI encryption shall provide confidentiality on the radio link between MS and BS.

The intention of this ETS is to describe a system in which all calls within that system are in the same AI encryption state and in which only one KSG is in use in the system. However signalling permits more than one KSG and more than one state to be supported. The SwMI shall control the state of AI encryption.

AI operates by combining the output of a Key Stream Generator (KSG) with the contents of messages to be transmitted across the air interface. Both control and traffic (speech or data) information can be encrypted. The encryption process shall take place in the upper Medium Access Control (MAC) layer of the TETRA protocol stack.

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

The headers for each MAC PDU shall not be encrypted with the exception of some elements of MAC-RESOURCE and MAC-END PDUs as defined in 6.1.6.2. This shall enable an MS to determine which messages are destined for it, the PDU type, the encryption state of the PDUs, and so determine which of these messages require decryption for further action. It shall also enable a BS to identify the individual MS or group involved in communication, and so select the appropriate key.

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

Each MS should hold a secret key which is used to determine the cipher key used by the KSG. Additionally, a common key should be used to modify the cipher key used for group addressed signalling. The BS shall have knowledge of all cipher keys in use by all individual MSs and all groups that are registered at that BS, or in the location area of which the BS is a part.

The KSG shall form an integral part of an MS or BS.

Air interface encryption shall be a separate function to the end-to-end encryption service described in clause 7. Information that has already been encrypted by the end-to-end service may be encrypted again by the air interface encryption function. Where TETRA provides for clear or encrypted circuit mode services in ETS 300 392-1 [1], clause 8, these shall be independent of air interface encryption; thus a circuit mode service invoked without end-to-end encryption may still be encrypted over the air interface.

6.1.1 Key Stream Generator (KSG)

Encryption shall be realized using an encryption algorithm implemented in a KSG.

The KSG shall have two inputs, an Initial Value (IV) and a cipher key. These parameters shall be as specified in subclause 6.1.4. 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 a TCH/7,2 unprotected traffic channel.

6.1.2 Encryption mechanism

The key stream bits shall be modulo 2 added (XORed) with plain text bits in data, speech and control channels to obtain encrypted cipher text bits, with the exception of the MAC header bits and fill bits. KSS(0) shall be XORed with the first transmitted bit of the first TM-SDU, and so on. There shall be one exception to this procedure which occurs when the MAC header includes channel allocation element data. This is described in subclause 6.1.6.2.

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.

On the control channel, the MAC may perform PDU association, where more than one PDU may be transmitted within one slot. These PDUs may be addressed to different identities. The MAC headers themselves may be of varying lengths. To allow for this, the KSS shall be restarted at the commencement of each SDU; the KSS that encrypts each SDU should be different provided that the SDUs within one slot are addressed to different identities, because the KSSs should be produced with different keys.

This mechanism shall apply in all control channel cases, including in the case of half slots on downlink or uplink.

Figure 38 illustrates the process where each PDU occupies one complete timeslot. Figure 39 illustrates the process with PDU association within one timeslot.

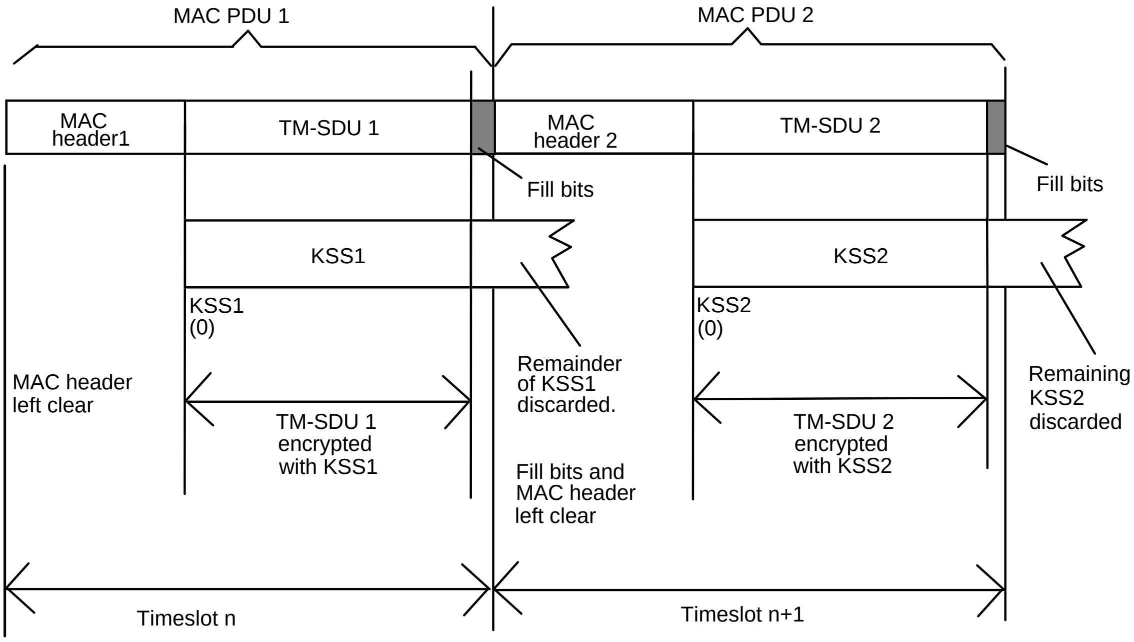
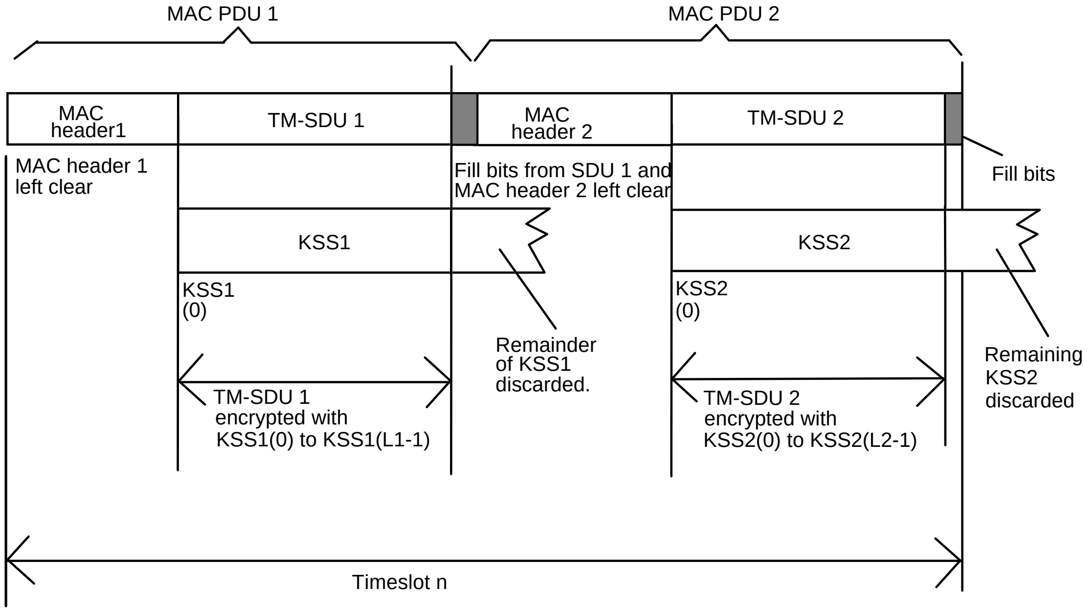


Figure 38: Allocation of KSS to encrypt MAC PDUs


MAC PDU 1
MAC PDU 2
MAC header1
TM-SDU 1
MAC header 2
TM-SDU 2
MAC header 1 left clear
Fill bits from SDU 1 and MAC header 2 left clear
Fill bits
KSS1
KSS2
KSS1 (0)
KSS2 (0)
Remainder of KSS1 discarded.
Remaining KSS2 discarded
TM-SDU 1 encrypted with KSS1(0) to KSS1(L1-1)
TM-SDU 2 encrypted with KSS2(0) to KSS2(L2-1)
Timeslot n

NOTE: Length of TM-SDU 1 is L1, length of TM-SDU 2 is L2

Figure 39: Allocation of KSS to encrypt MAC PDUs with PDU Association

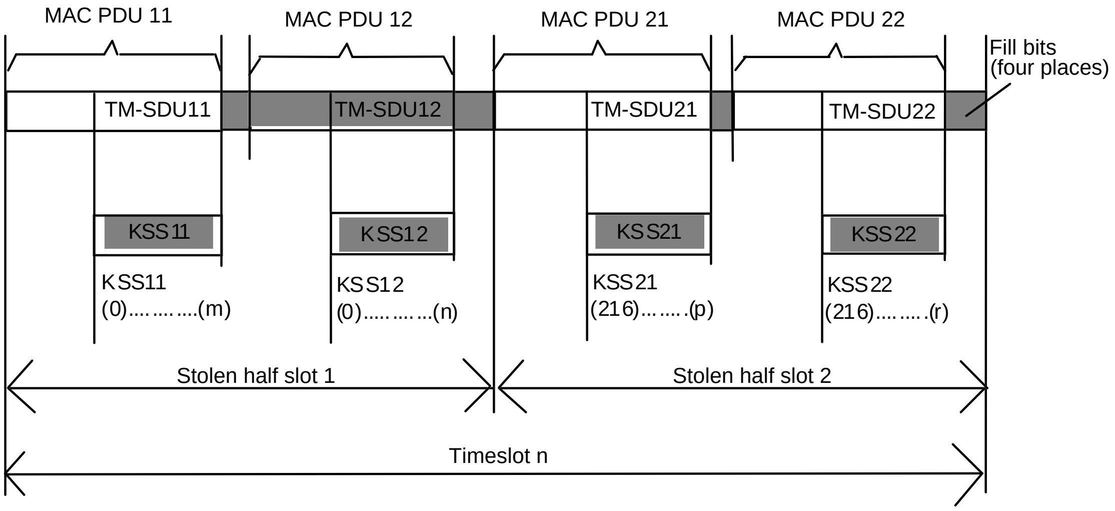
In the case of traffic channels, where one half or both halves of a timeslot are stolen for either C-Plane or U-plane signalling, the mechanism shall be as described below. This mechanism shall apply on both uplink and downlink. The keystream used to encrypt information in each half slot shall be generated separately by taking the maximum length keystream (432 bits) and dividing it into two equal parts.

The TM-SDU of the first half slot shall be encrypted with KSS(0,…,215). The TM-SDU of the second half slot shall be encrypted with KSS(216,…,431). If the encrypted contents of the first half slot have a length of less than 216 bits, the remainder of the KSS up to KSS(215) shall be discarded. The second half slot shall then use keystream from 216 on, discarding any remaining keystream should the second half slot require less than 216 bits.

Should either half slot be used with PDU association, the keystream shall be restarted to encrypt subsequent PDUs as in the control channel case described above. In the first half slot, the keystream shall be restarted from KSS(0), and in the second half slot, the keystream shall be restarted from KSS(216).

In the case where only one half slot is stolen, associated SDUs in the first half slot shall be encrypted using keystream from KSS(0) and the traffic in the second half slot shall be encrypted using keystream from KSS(216) onwards.

This process is illustrated in figure 40.



NOTE: KSS11(m+1) onwards discarded
KSS12(n+1) onwards discarded
KSS21(0) to KSS21(215) and KSS21(p+1) onwards discarded
KSS22(0) to KSS22(215) and KSS22(r+1) onwards discarded

Figure 40: Allocation of KSS to encrypt MAC PDUs when half slots are stolen

To avoid replay of key stream, the following should be avoided where PDU association takes place:

- Control channel: sending more than one SDU addressed to the same identity within one slot.
- Traffic channel: sending more than one SDU addressed to the same identity within one stolen half slot.
-

Sub-slots are described in ETS 300 392-2 [2], subclause 4.5.2.

6.1.3 KSG numbering and selection

There shall be at least one TETRA standard algorithm. Air interface signalling shall identify which algorithm is in use (see table 81). Migration should only be possible if there is agreement between operators on the algorithm used.

The values 0000_2 to 0111_2 of KSG-id used in signalling shall be reserved for the TETRA standard algorithms (see also ETS 300 392-2 [2], subclause 16.10.29).

Table 81: KSG Number element contents

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

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

6.1.4 Interface parameters

6.1.4.1 Initial Value (IV)

The IV shall be used to initialize the KSG at the start of every slot. The IV shall be a value 29 bits long represented as IV(0)….IV(28) based on the frame numbering system, which is defined by, and broadcast from the BS, where IV(0) shall be the least significant bit and IV(28) the most significant bit of IV.

The composition of the IV shall be as follows:

the first two bits IV(0) and IV(1) shall correspond to the slot number, and shall take values from 0 to 3, where value 0 corresponds to slot 1, and value 3 corresponds to slot 4. IV(0) shall be the least significant bit of the slot number (ETS 300 392-2 [2], subclause 9.3.5);

the next five bits IV(2) to IV(6) shall correspond to the frame number, and shall take values from 1 (00001 binary) to 18 (10010 binary). IV(2) shall correspond to the least significant bit of the frame number (ETS 300 392-2 [2], subclause 9.3.6);

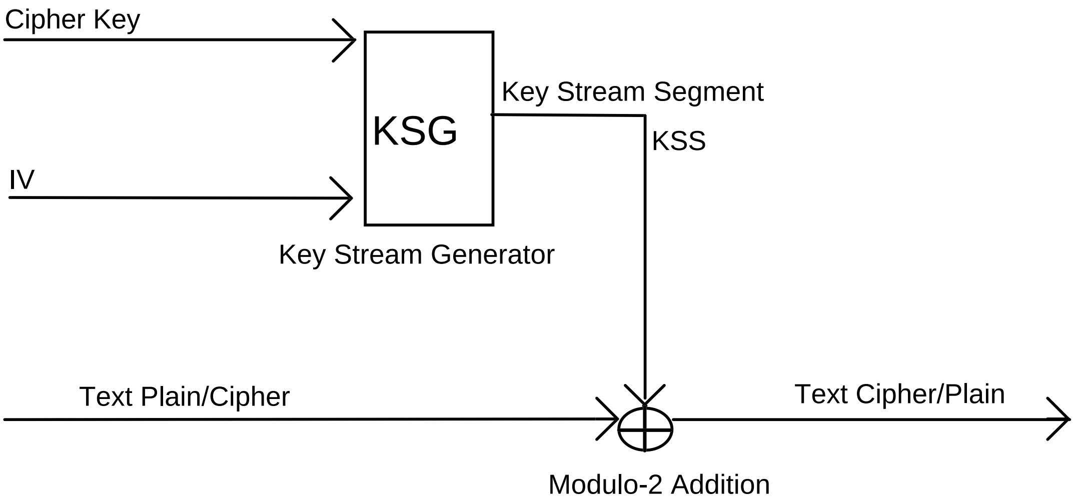
the next six bits IV(7) to IV(12) shall correspond to the multiframe number, and shall take values from 1 (00001 binary) to 60 (111100 binary). IV(7) shall correspond to the least significant bit of the multiframe number (ETS 300 392-2 [2], subclause 9.3.7);

the next 15 bits IV(13) to IV(27) shall correspond to the first 15 bits of an extension that numbers the hyper-frames. These can take all values from 0 to 32768. IV(13) shall correspond to the least significant bit of the hyper-frame numbering extension (ETS 300 392-2 [2], subclause 9.3.8);

the final bit, IV(28), shall be given the value 0 for downlink transmissions, and shall be given the value 1 for uplink transmissions.

6.1.4.2 Cipher Key

The ciphering process shall be as shown in figure 41. A cipher key shall be used in conjunction with a KSG to generate a key stream for encryption and decryption of information at the MAC layer. It can be considered a binary vector of 80 bits, labelled CK(0) … CK(79). The cipher key used for encryption and decryption of the uplink may be different from the cipher key used for encryption and decryption of the downlink, as described in subclause 6.1.5.



NOTE: IV at MS is received from the frame number broadcast. IV at BS is locally generated and broadcast to MS.

Figure 41: Speech and control information encryption

6.1.5 Use of cipher keys

The cipher keys and their allocation are described in subclauses 4.2.1 to 4.2.4.

The header of MAC PDUs transmitted over the air interface shall contain indications of the key in use.

The SCK should be used to encrypt individual and group addressed signalling on a SwMI that does not employ authentication. It may also be used with the identity encryption system to conceal identities in use at the air interface within a SwMI. Only one SCK may be in use within a SwMI at any one time.

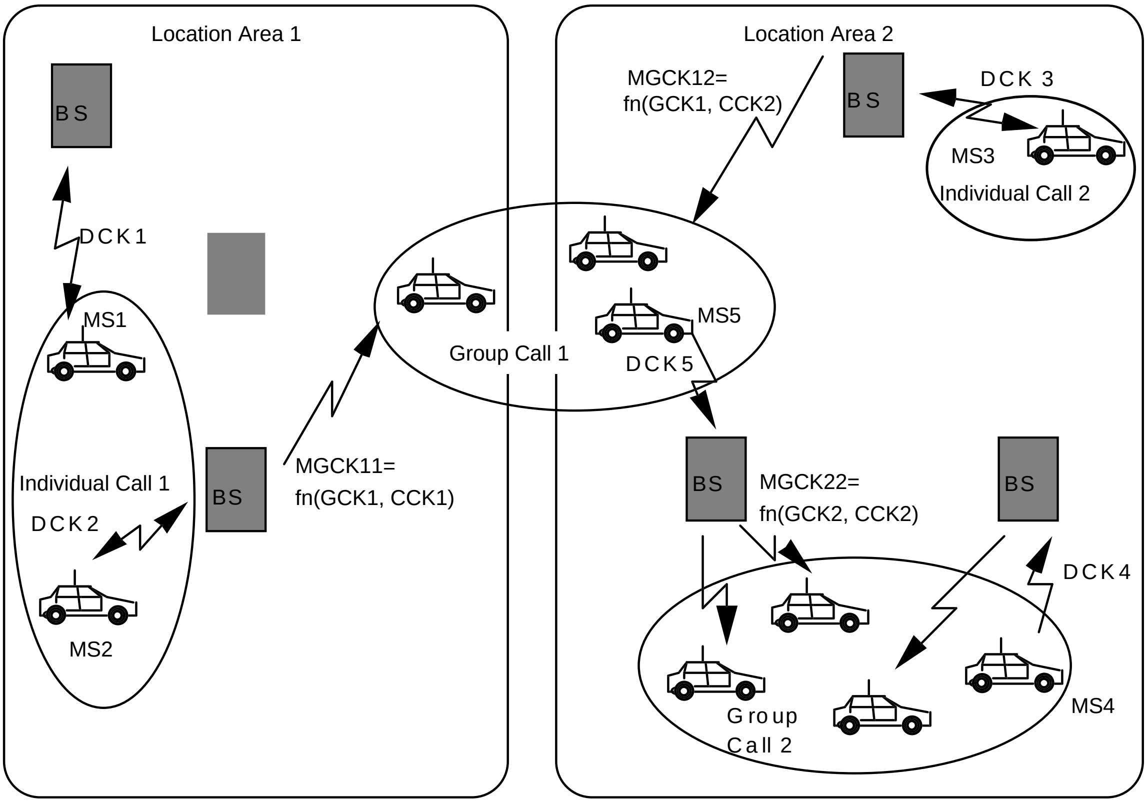
The DCK may be used to encrypt all signalling and traffic sent from an MS to the SwMI, and to encrypt individually addressed signalling and traffic sent from the SwMI to the MS.

A GCK may be associated with a single group address at any time.

The CCK shall be used as a key modifier to produce the MGCK which shall be used to encrypt group addressed signalling and traffic. It shall also be used in conjunction with the identity encryption system to protect all identities used with encryption within an LA. An MS may store the CCKs in use in more than one LA to ease cell re-selection.

If GCK is not defined, or not present, CCK shall be used in place of MGCK. The value of MGCK shall be equal to that of CCK and algorithm TA71 shall not be invoked.

The use of the different cipher keys is illustrated in figure 42.



BS = Base Station
MS = Mobile Station

DCK = Derived Cipher Key
CCK = Common Cipher Key
GCK = Group Cipher Key
MGCK = Modified Group Cipher Key

Figure 42: Illustration of cipher key use

The usage of the different key types within a SwMI depends on the prearranged encrypted SwMI type. These are described in subclause 6.1.5.1.

6.1.5.1 Encrypted SwMI types

Table 82 sets out the types of encrypted SwMI possible, and their attributes concerning encryption, authentication and concealment of identity. The concealment of identity is described in subclause 4.2.5.

Each TETRA SwMI should correspond to one of the types set out in the table, and knowledge of the type should be known to each MS that wishes to utilize that SwMI by pre-arrangement.

Table 82: Encrypted SwMI types and use of cipher keys

SwMI type	MS knows new cell CCK	Authenti-cation	Normal encryption mode	Identity conceal at cell change	Identity conceal in normal use	Encryption state at cell change
1	N/A	Optional	Clear	None or ASSI	None or ASSI	Clear
2	N/A	Optional	SCK (one only)	Yes (SCK)	Yes (SCK)	Encrypted (SCK)
3a	No	Yes	DCK/ CCK-GCK	None or ASSI	Yes (CCK)	Clear
3b	Yes	Yes	DCK/ CCK-GCK	Yes (new cell CCK)	Yes (CCK)	Encrypted (DCK)

In all SwMI types registration shall be carried out in clear. The identity used during registration may be the ASSI defined by an earlier registration.

Referring to table 82, the SwMI types are described in text below:

Type 1. No encryption shall be used. Authentication should be optional. Identities may be concealed after registration by the alias addressing system, described in ETS 300 392-2 [2], subclause 16.4, and in ETS 300 392-1 [1], clause 7.

Type 2. SCK shall be used within the system for all encryption. Encryption shall be applied following registration. At cell change subsequent to the initial registration, the SCK shall be used with the identity encryption mechanism to conceal the MS identity. This SwMI type permits an MS to negotiate the SCK in use during registration.

Type 3: Authentication shall be used to establish a DCK. The DCK shall be used by the MS to obtain the relevant CCK(s). The MS shall use the CCK as a key modifier to establish the keys to use in downlink group addressed transmissions in conjunction with the GCK. Initial registration shall be carried out in clear. Within an LA, one CCK shall be in use at a time.

If the MS cannot obtain the CCK in use in the new cell (case 3a), cell re-selection shall be carried out in clear. This is necessary as the CCK is used to encrypt and decrypt the MS ISSI sent at the air interface if the cell re-selection is encrypted.

If the MS can obtain the CCK for the new cell (case 3b), either by requesting from the old cell, or knowing that there is a system wide CCK in use, the cell change may be carried out in encrypted mode using the CCK with the encrypted short identity mechanism to conceal the ISSI, and the DCK for encryption of the location update PDUs. The SwMI shall either obtain the DCK for the MS in the new cell, or it shall force the MS to authenticate and establish a new DCK before further communication takes place.

If an MS and SwMI load different keys from each other, the receiving party will decode messages incorrectly. This will cause erroneous operation. The result of this, and any corrective action put in place to prevent errors, for example attempting a re-authentication to establish new keys, is outside the scope of the ETS.

NOTE: For any SwMI type, emergency calls may be made without authentication.

6.1.5.2 Identification of cipher keys

The encryption mode element (two bits) in the header of the downlink MAC-RESOURCE PDU shall be used for air interface encryption management, and shall indicate whether encryption is in use, and if so, which is the current key in use.

NOTE: This replaces the definition in ETS 300 392-2 [2], subclause 21.4.2.2.

The values of these two bits shall be assigned on the downlink for group addressed signalling as follows:

00_2 = No encryption;
01_2 = SCK is in use;
10_2 = Short CCK-id = "0" is in use;
11_2 = Short CCK-id = "1" is in use.

The values of these bits shall be assigned on the downlink for individually addressed signalling as follows:

00_2 = No encryption;
01_2 = SCK is in use;
10_2 = Short CCK-id = "0", and DCK is in use;
11_2 = Short CCK-id = "1", and DCK is in use.

This mechanism shall not be used to select between multiple CCKs in use at the same time within a LA. It shall only be used as a means of selecting a new key within a LA once this new key has been communicated to all registered MSs.

To prevent attacking by replaying a previous key, the CCK shall be identified by a longer CCK-id which shall be sent to an MS together with the CCK. The CCK-id can be selected independently for each location area by the SwMI. If the SwMI replaces a CCK in a location area, CCK-id shall be incremented by 1. SwMI and MS shall use the CCK with the highest number, the least significant bit of which matches the least significant bit of the encryption mode element in the MAC header when the most significant bit of this element is set to indicate CCK in use.

One bit of uplink signalling MAC PDU headers shall be reserved for air interface encryption. This shall indicate whether the contents of the PDU are encrypted or not.

This bit shall take one of the following values:

0 = Encryption off;
1 = Encryption on.

If it is desired to change the DCK in use by an MS, this should be achieved by the normal authentication process; and as both BS and MS are involved in the process and have knowledge that it has occurred, it shall not be necessary to include a key identifier in the uplink header.

The encryption mode element shall also indicate the state of the MAC header encryption mechanism as described in subclause 6.1.6.2, and the encrypted short identity mechanism described in subclause 4.2.5.

6.1.5.3 Change of CCK in an LA

A change of CCK in use in an LA shall be synchronized such that all MS using CCK (alone or as a modifier of GCK) change at the same time. However if a call is in progress at the time that the BS/SwMI changes the CCK in use that call shall continue to use the old CCK until either the call is cleared, or when indicated by the BS in the signalling.

There shall be two supporting mechanisms for the display of CCK-id in the air interface protocol: SYSINFO broadcast containing the CCK-id; some MAC headers containing a short version of the CCK-id. Both shall indicate the current CCK in use. A change in the short CCK-id value in the MAC header shall indicate that CCK-id has been incremented.

The SwMI/BS should change the broadcast CCK-id and the MAC header short CCK-id at the same time in one LA. When the SwMI applies the BNCH broadcast pattern as defined in ETS 300 392-2 [2], subclause 9.2.3.2, then for some timeslots the short CCK-id may change before a SYSINFO PDU is sent.

The SwMI should change the short CCK-id according to the CCK-id in the SYSINFO PDU as soon as it has sent a SYSINFO containing the changed (incremented) CCK-id in the associated control channel that the MSs are obliged to listen to.

MS-MM shall be responsible for the CCK management functions.

Subclause 4.4.3 describes the CCK distribution protocol. The MM should provide to the MAC layer at least the CCK, which is indicated by the SYSINFO broadcast element CCK-id, and the next CCK as soon as it is available to the MS. MM shall issue the CCKs to the MAC using the MLE ENCRYPTION request primitive. The associated CCK-id shall be provided together with each CCK. MM shall indicate to the MAC which CCK-id is currently broadcast in the SYSINFO message.

NOTE 1: This ETS does not define how many CCKs can or need to be stored at the same time in an MS for later use in addition to the two CCKs required by the protocol.

Upon reception of a currently broadcast CCK-id from the MM the MAC shall discard all CCKs indicated by an older CCK-id. The MAC shall also discard the CCK it is currently using, when it receives a MAC header indicating that the short CCK-id value is not the same as the least significant bit in the currently used CCK-id. The MAC shall then start to apply the CCK as indicated by the currently broadcast CCK-id or by the short version of it. In the latter case the MAC shall assume that the CCK-id value has been incremented by one.

NOTE 2: The described protocol is independent for each location area and a MS should not assume that CCKs are changing at the same time in all location areas.

Figure 43 describes how the MS shall change the currently used CCK. This shall be as described in subclause 4.4.3.

NOTE 3: The SYSINFO initiated change of CCK is equivalent to, and co-ordinated with, changing the short CCK identifier in the MAC encryption information element.

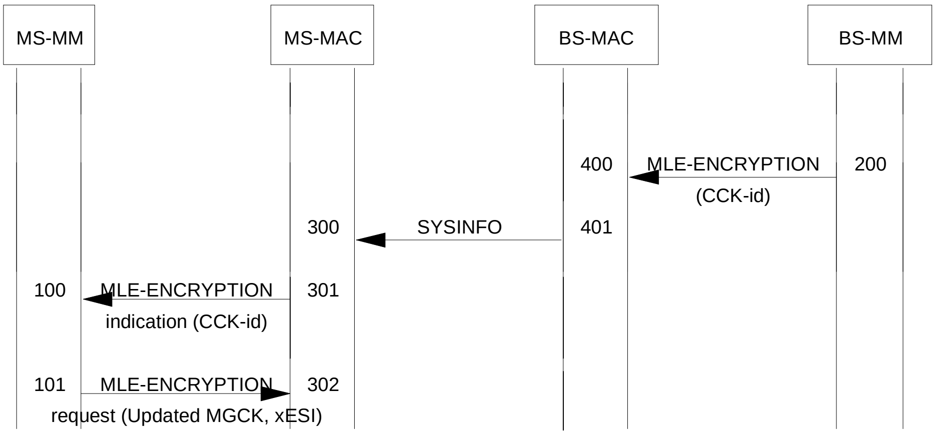


Figure 43: CCK change notified in MAC-SYSINFO broadcast

6.1.6 Data to be encrypted

6.1.6.1 Downlink control channel requirements

Certain control messages shall not be encrypted on the downlink, as they may be used by MSs prior to establishment of encryption parameters:

all messages sent to the MAC via the TMB-SAP;

D-NWRK-BROADCAST shall always be sent in clear;

broadcast messages where the destination SSI is set to all "1"s may be sent either in clear or with encryption applied. The encryption state of the message shall be indicated by the encryption mode element of the downlink MAC-RESOURCE PDU.

All remaining messages originating from higher layers shall be encrypted if a channel has been switched to encrypted operation.

6.1.6.2 Encryption of MAC header elements

When encryption is enabled some of the MAC header shall be considered by the encryption unit as belonging to the TM-SDU. The following rules apply when the encryption is on:

- in the MAC-RESOURCE PDU (see ETS 300 392-2 [2], subclause 21.4.3.1) all information from the channel allocation flag element shall be encrypted. The channel allocation flag shall be included in the data to be encrypted;
-
- in the downlink MAC-END PDU (see ETS 300 392-2 [2], subclause 21.4.3.3) all information from the channel allocation element flag element shall be encrypted. The channel allocation flag shall be included in the data to be encrypted.
-

The encryption process shall be accomplished in the same manner as is used to encrypt TM-SDUs, i.e. the modulo 2 addition of a key stream, where the key stream shall be generated as a function of frame numbering and cipher key relevant to the addressed party or parties. Therefore, if this information is sent to an individual MS, it shall be encrypted using the DCK relevant to that MS. If it is sent to a group, it shall be encrypted using the MGCK for that group. If it is sent to all MS's registered on that site or if there is no GCK for that group, it should be encrypted using the CCK for the LA.

The KSG shall be initialized as described in subclause 6.1.4.1 using the frame and slot numbering system.

To avoid a key stream repeat, the encrypted PDU should not be sent in the same time slot as another PDU encrypted with the same key.

6.1.7 Traffic channel encryption control

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

Traffic channels do not incorporate a separate MAC header in the same way as control channels. Instead, the entire channel is used for traffic data. Therefore on a traffic channel, the SDU that is encrypted is the entire contents of the transmitted slot.

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 (see ETS 300 392-2 [2], subclauses 14.5.1.4 and 14.5.2.4).

NOTE: Encryption state is either on or off.

Encryption of control and traffic (speech/data) channels shall be switched on and off only by the SwMI.

If an MS is unable to decrypt incoming information as a result of a mismatch of encryption parameters the MS may initiate a change of encryption parameters by making an authentication request.

Encryption mode control is achieved by an exchange of MM PDUs at registration. The PDU exchange shall allow switching both from clear to encrypted mode and the reverse.

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

6.2 Mobility procedures

6.2.1 General requirements

The cell selection procedures are defined in ETS 300 392-2 [2], subclause 18.3.4.

The transfer of security information should be made entirely within the TETRA network and should not involve any unprotected transmission on the air interface, this is especially true when transferring the cipher key. If this protected transfer is impossible then a new cipher key shall be established, requiring re-authentication.

Ciphering may be interrupted and the cell change may be in clear, this is described later in this subclause.

When an MS moves between LAs, it may still retain the CCK in use in the previous LA. This may permit the MS to move back without the need to obtain the CCK again.

The MS shall assume that the SwMI shall transfer its current DCK to the new cell within the network and shall use the same DCK in the new cell. If the SwMI is unable to do this, it shall require the MS to re-authenticate and establish a new DCK.

To facilitate mobility, each CCK sent to an MS shall be sent together with an identifier of the LA or cell in which that CCK is in use.

6.2.2 Mobility within a location area

When the MS needs to move between cells, it shall obtain the CCK for the new cell. If the new cell is within the same LA, the CCK in use shall be the same.

6.2.3 Mobility between location areas

The following methods shall be possible to achieve mobility between location areas:

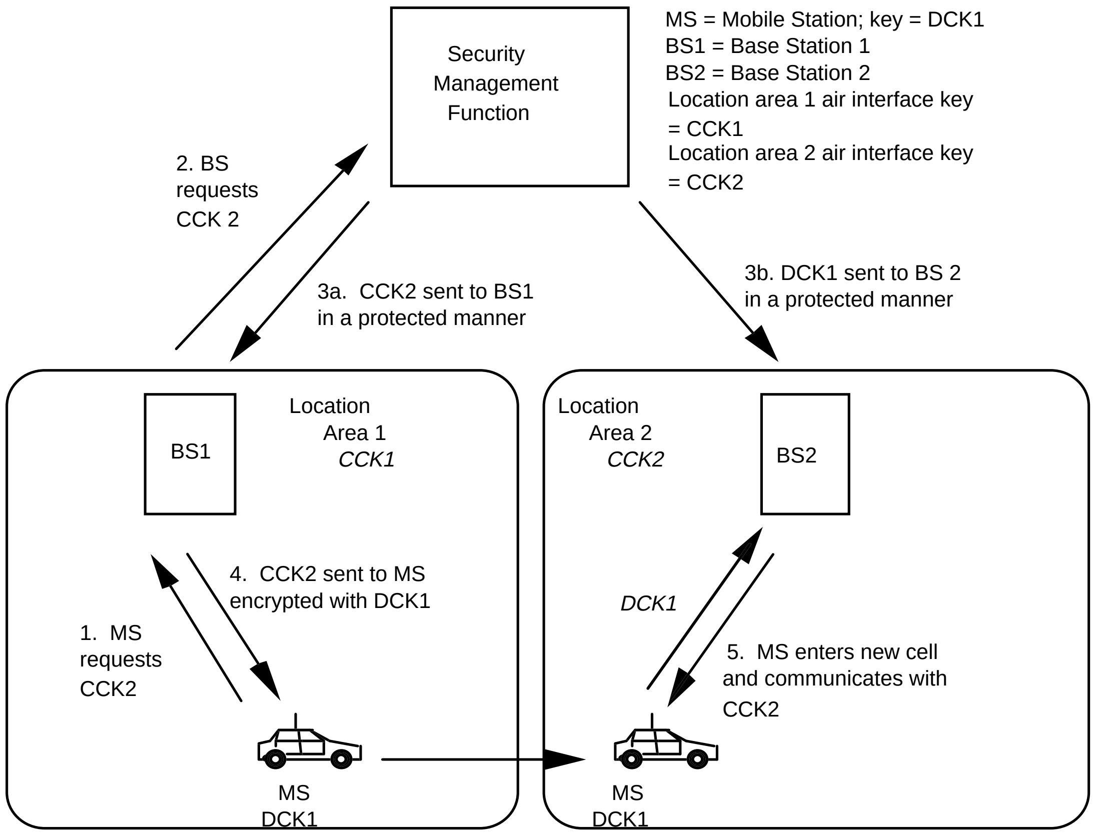
- the MS may request the CCK in use in the new area before leaving the old area by U-OTAR (see subclause 4.4.3);

- the MS may be given the new CCK in the new area without registration in the new cell using U-OTAR;

- the MS may be required to register in the new area, and obtain the new CCK.

If the SwMI is unable to transfer the old DCK of the MS, the MS shall authenticate and generate a new DCK. The latter case is likely to prevent a seamless handover from taking place.

If key data is to be exchanged between MS and BS, it shall be encrypted using the DCK of the MS to protect the data over the air interface. Figure 44 illustrates this process.


Security
Management
Function
MS = Mobile Station; key = DCK1
BS1 = Base Station 1
BS2 = Base Station 2
Location area 1 air interface key = CCK1
Location area 2 air interface key = CCK2
2. BS requests CCK 2
3a. CCK2 sent to BS1 in a protected manner
3b. DCK1 sent to BS 2 in a protected manner
BS1
Location Area 1
CCK1
Location Area 2
CCK2
BS2
4. CCK2 sent to MS encrypted with DCK1
1. MS requests CCK2
DCK1
5. MS enters new cell and communicates with CCK2
MS
DCK1
MS
DCK1

NOTE: In step 3b, DCK1 needs to be sent to all base stations in the new location area, unless DCK is changed by authentication.

Figure 44 Transfer of key between cells as mobile roams

When the new cell is known before the old cell is relinquished the MS may request the CCK in use in the new cell. This may be sent by the BS in the old cell, encrypted with the DCK of the MS. Alternatively, the CCK can be sent to the MS in the new cell. At the same time, the DCK in use by the MS in the old cell may be sent to BSs in the new cell in a protected manner within the SwMI. A call in process need not then be interrupted by the requirement to authenticate and obtain new keys. This requires that the SwMI should be able to transfer keys over its internal links in a protected manner.

Once the MS has transferred to the new cell the old DCK may be retained, or alternatively the authentication procedure shall be followed, and a new DCK generated.

If the new cell is not known and the MS is not yet registered in the new cell, the MS shall be required to register in the new cell. In this case the SwMI shall either transfer the MS's existing DCK to the new cell, or require the MS to authenticate and establish a new DCK. If the MS does not have the CCK for the new cell, the MS may request the CCK as part of the registration procedure or the announced cell re-selection procedure as described in clause 4.

6.2.4 Cell change with uninterrupted ciphering

A cell change may be carried out with uninterrupted ciphering provided that a registration or authentication is not required to take place without encryption applied.

This can occur:

on a change to another cell;

wherever key transfer is possible within the SwMI between cells in a protected manner.

The MS can be given the CCK for the new cell before cell transfer. The new cell can also be sent the DCK of the MS.

6.3 Air interface encryption protocol

6.3.1 General

The security procedure in the MS shall be controlled by MM, which may indicate its security state to the MS application by the TNMM SAP. The application in the MS shall not however change the security state; this shall only be performed by the SwMI.

The air interface 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;

exchange the encryption mode control messages to synchronize encryption.

The protocol shall involve layers and sub-layers of layer 3 (Mobility Management (MM) and Mobile Link Entity (MLE)), and of layer 2 (Logical Link Control (LLC) and (MAC)) of the TETRA protocol stack.

6.3.1.1 Positioning of encryption process

The encryption process itself shall be located in the upper part of the MAC layer, which itself is the lower part of layer 2. Situating the encryption process at this point, prior to channel coding at the transmitting end and after channel decoding at the receiving end, enables the MAC headers to be left unencrypted. This allows the appropriate channel coding to be used, and enables receiving parties to determine the applicability of a message received over air for them, and so enables them to apply the correct key for the decryption process. Figure 45 illustrates this interconnection:

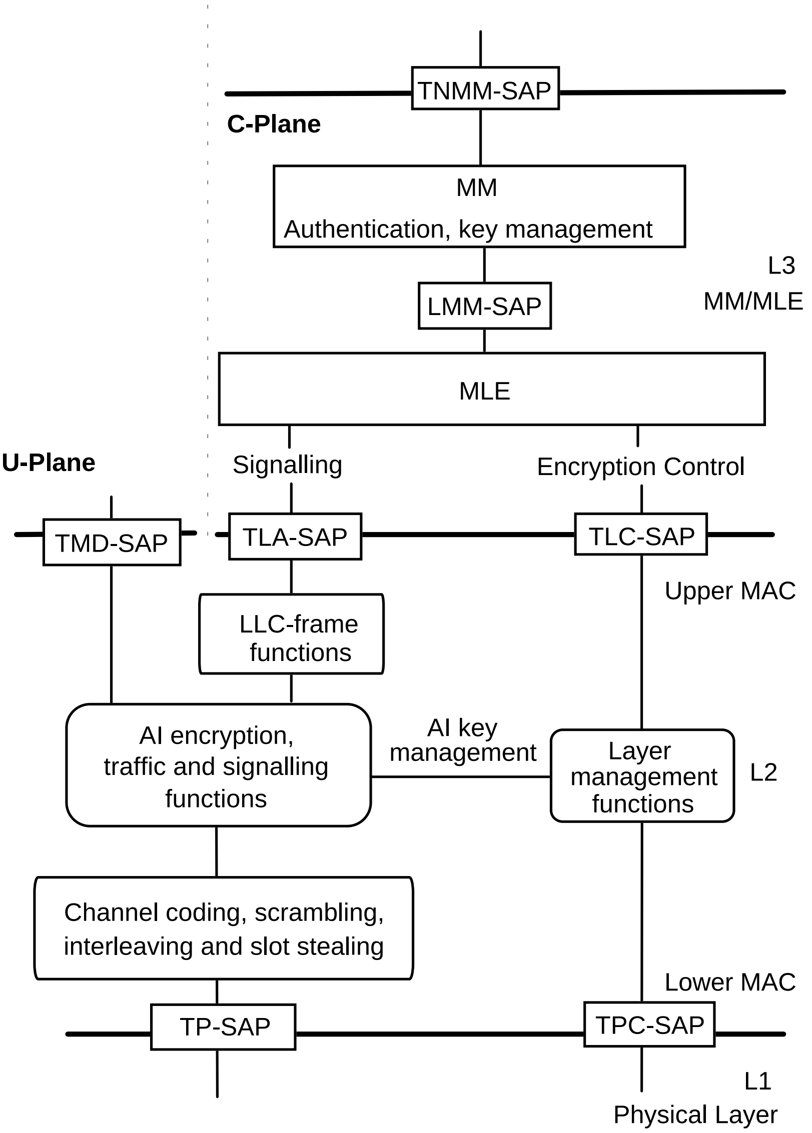


Figure 45: Relationship of security functions to layers functions in MS

6.3.1.2 Operation of encryption process

The encryption process shall be controlled in the TETRA protocol stack by MM. The SwMI shall administer the encryption process.

A network should operate in only one encryption state as described in subclause 6.1.5.1. A network should not support mixed SwMI types. The encrypted SwMI type should be advised prior to registration to all MSs intending to access the network.

At registration, the MS shall exchange encryption parameters with the SwMI using the Location Update PDU exchange. Once keys have been established, MM may initiate the encryption process by passing the encryption parameters to the MAC by using the MLE-ENCRYPTION request primitive.

If rejection occurs due to a mismatch in encryption parameters, MM may change the parameters and may try a new registration attempt. In this case, PDUs shall be sent from the SwMI to the MS-MM forcing a re-registration procedure with new encryption parameters set. If the re-registration is successful, MM shall pass the new encryption parameters to the MAC using the MLE-ENCRYPTION request primitive as before. Examples of the registration protocol sequences are given in subclause 4.4.2.

If the MS has only one set of encryption parameters which are rejected by the SwMI, MS-MM shall attempt to establish a clear connection.

The encryption state shall not be changed without following the registration procedure. For optimum security, the authentication procedure should also be followed where implemented prior to a change of encryption state.

NOTE: For any SwMI type, emergency calls may be made without authentication and may allow a change of encryption state without registration.

6.3.2 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 300 392-2 [2]. The primitives that are passed between the layers are also described.

6.3.2.1 Mobility Management (MM)

TNMM SAP: the encryption control procedure shall only be invoked by the SwMI using the registration procedure. The MS-MM may indicate its current state, or a change of state, to the MS application.

The primitive TNMM-REGISTRATION shall contain the parameter "Encryption control" to enable/disable the encryption process, and the parameter "KSG number".

Table 83: TNMM-REGISTRATION parameters (c.f. ETS 300 392-2 [2], subclause 15.3.3.7)

Parameter	Request	Indication	Confirm
Registration Status	-	M	M
Registration Reject Cause (note 1)	-	C	-
Registration Type	M	-	-
Location Area (note 2)	C	-	-
MCC (note 3)	C	-	-
MNC (note 3)	C	-	-
ISSI or ASSI or USSI (note 4)	M	-	-
Group identities	-	O	O
Group identity request	O	-	-
Group identity attach/detach mode	O	O	O
Group identity report	O	-	-
Encryption control	M	M	M
KSG number	-	O	O

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

NOTE 1: Shall be present if Registration Status = "failure"

NOTE 2: Shall be present if Registration Type = "No new ITSI - forward registration"

NOTE 3: Shall be present if Registration Type = "New ITSI" or Registration Type = "No new ITSI - forward registration"

NOTE 4: A previously established and valid ASSI may be used to prevent exposure of the ITSI at registration.

6.3.2.2 Mobile Link Entity (MLE)

At the LMM SAP the following MLE services shall be provided to MM:

loading of keys;

start and stop ciphering.

These services shall be achieved by passing information to the MAC layer using the MLE-ENCRYPTION request primitive. The MAC shall indicate to MM the current CCK-id that is received in the broadcast SYS-INFO PDU.

Table 84: MLE-ENCRYPTION parameters

Parameter	Request	Indication
Key download type	M	-
KSG Number (note 1)	O	-
SCK (note 2)	C	-
DCK (note 2)	C	-
CCK (note 2)	C	-
CCK-id (notes 2, 4)	C	M
MGCK (note 2)	C	-
GTSI (note 3)	C	-
xSSI (note 5)	C	-
Cipher usage (note 1)	O	-

Key: M = Mandatory; C = Conditional; O = Optional
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.
NOTE 3: Provided if MGCK downloaded.
NOTE 4: CCK-id supplied in indication.
NOTE 5: This is the SSI associated with the DCK when DCK is downloaded.

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

Key download type =

no keys downloaded;
SCK;
DCK, xSSI pair;
CCK, CCK-id pair;
MGCK, GTSI pair.

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;
RX;
RX and TX.

6.3.2.3 Layer 2

The layer 2 service shall be to load keys and start and stop the ciphering as required by the MM/MLE request. The MAC shall also be responsible for applying the correct key depending on the identity placed in the header of each MAC PDU. This is described in ETS 300 392-2 [2], clause 21.

The corresponding MLE-ENCRYPTION request and indication should be passed through the LLC in a transparent way by using TL-ENCRYPTION request and indication respectively at the TLC-SAP, the boundary between the MLE and LLC. Similarly, the LLC should exchange the TM-ENCRYPTION request and indication at the TMC-SAP, the boundary between the LLC and the MAC.

The MAC shall indicate to MM/MLE the CCK-id of the current CCK in use in the LA.

Encryption shall be performed in the upper MAC before FEC and interleaving.

6.3.3 Protocol functions

Each functional entity in the protocol stack shall communicate with its peer entity using a defined protocol; for example the MM entity in the MS communicates with its peer MM entity in the SwMI. The incorporation of encryption at the air interface requires additional functions to be added to some of the functional entities of the protocol stack. These functions shall be as described in the following subclauses.

6.3.3.1 MM

The protocol functions for air interface security shall be the following:

ciphering type elements shall be contained in the U- and D- LOCATION UPDATE PDUs. A negotiation for ciphering types shall be performed in a re-registration if the parameters are not acceptable;

MM shall perform a re-registration if the SwMI requires a change in the encryption parameters including on-off control of encryption.

6.3.3.2 MLE

No encryption functionality shall be added to the MLE protocol. The management SAP (TLC-SAP) should be used inside the MS to deliver the new ciphering parameters to the MAC and to receive an indication of a change in the short CCK-id from the MAC.

6.3.3.3 LLC

No encryption functionality shall be added to the LLC protocol. The management SAP (TLC-SAP) should be used inside the MS to deliver the new ciphering parameters to the MAC and to receive an indication of a change in the short CCK-id from the MAC.

6.3.3.4 MAC

The MAC shall indicate to MM a change in the CCK-id broadcast in MAC SYSINFO.

6.3.4 PDUs for cipher negotiation

Ciphering elements shall be contained in the U_LOCATION_UPDATE-DEMAND, and the D_LOCATION_UPDATE-REJECT PDUs to permit negotiation of encryption parameters. These PDUs are described in ETS 300 392-2 [2], subclause 16.9.

The definition of reject cause from ETS 300 392-2 [2], subclause 16.10.42, is extended as follows:

Table 85: Reject Cause element contents

Information element	Length	Value	Remark
Reject Cause	5	10010_2	Ciphering required

The MS-MM may suggest initial encryption parameters in the U-LOCATION UPDATE DEMAND PDU. The MS-MM shall assume that these parameters are acceptable and inform the MAC to use these parameters with the MLE-Encryption primitive. If the parameters are not acceptable the BS-MM shall reject them using the D-LOCATION-UPDATE REJECT with reject cause set to one of:

- no cipher KSG;
- identified cipher KSG not available;
- requested cipher key not available;
- identified cipher key not available;
- ciphering required.

If the encryption parameters are rejected the MS-MM shall use MLE-ENCRYPTION to inform the MAC to modify the parameters in accordance with the D-LOCATION UPDATE REJECT reject cause.

If the reject cause is "ciphering required" the MS may choose a set of parameters and send a new U-LOCATION UPDATE DEMAND or it may initiate the authentication process using the U-AUTHENTICATE DEMAND exchange described in subclause 4.4.6.

7 End-to-end encryption

7.1 Introduction

End-to-end encryption algorithms and key management are outside the scope of this ETS. This clause describes a standard mechanism for synchronization of the encryption system that shall be employed when using a synchronous stream cipher. The mechanism also permits transmission of encryption related and other signalling information. The mechanism shall apply only to U-plane traffic. The method described shall use the Stealing Channel, STCH, for synchronization during transmission (see ETS 300 392-2 [2], subclause 23.8.4).

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

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

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

7.2 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 46. This demonstrates the symmetry of transmitter and receiver with each side having common encryption units.

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

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

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

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

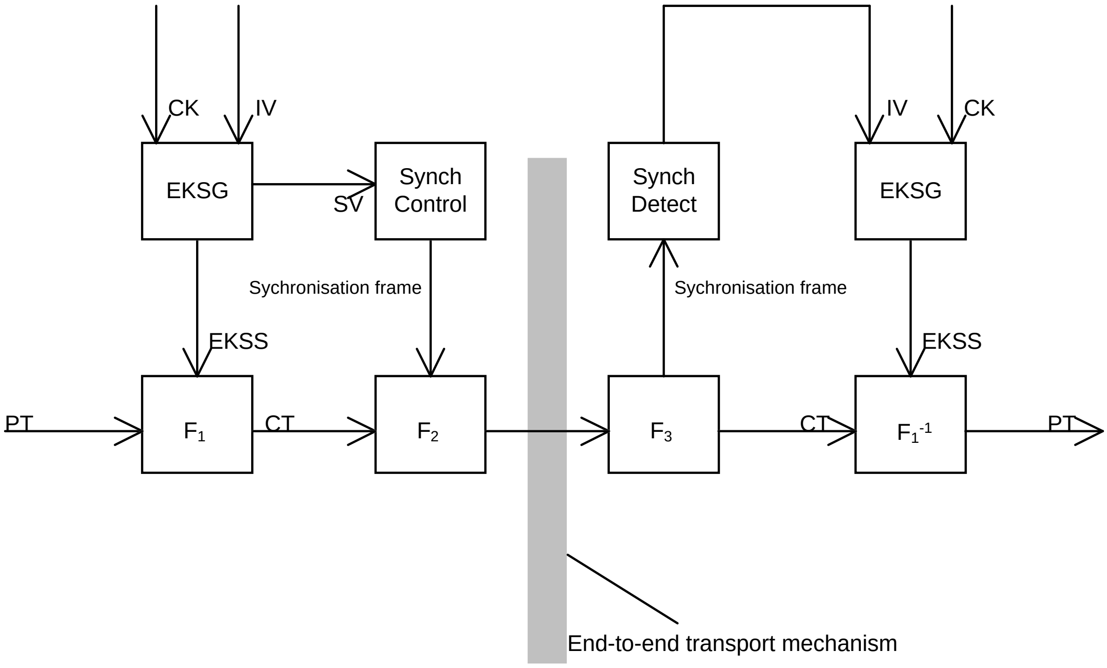


Figure 46: Functional diagram of voice encryption and decryption mechanisms.

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).

7.2.1 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.

7.3 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.

7.4 Exchange of information between encryption units

Two different cases shall be identified by an appropriate MAC header (see subclause 7.4.2):

- synchronization information in clear; or

- encrypted information.

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

7.4.1 Synchronization of encryption units

In figure 46 the processing blocks "synchronization control" and "synchronization detect" and their associated functions F_2 and F_3 shall provide the means of synchronising 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 300 392-2 [2], subclause 23.8.4).

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

The frame stealing shall make use of the TMD-UNITDATA primitive to address the MAC (request) and to inform the U-plane (indication). The parameters for this primitive shall be modified from the definition given in ETS 300 392-2 [2], subclause 20.4.4.1.2 to that shown in table 86.

Table 86: Modified definition of parameters used in the TMD-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 TMD-REPORT primitive modified from the definition given in ETS 300 392-2 [2]. Subclause 20.4.4.1.1 to that shown in table 87.

Table 87: Modified definition of parameters used in the TMD-REPORT primitive

Parameter	Indication	Remark
Half slot synchronization	C	
TCH type & interleaving depth	C	
Number of slots per TDMA frame	C	Only valid for report type Call-info
Encryption on / off flag	C	
User device	C	Reserved
Report	M	CALL_INFO, START_TX, STOP_TX, HALF_SLOT_STOLEN

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

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

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

7.4.2 Encrypted information between encryption units

In figure 42, other signalling information may be exchanged in encrypted form from a transmitting encryption unit to receiving encryption units. This is also shown in figure 50.

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 (see subclause 7.4.1 and ETS 300 392-2 [2], subclause 23.8.4).

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

The frame stealing shall make use of the TMD-UNITDATA primitive to address the MAC (request) and to inform the U-plane (indication). The parameters for this primitive shall be modified from the definition given in ETS 300 392-2 [2], subclause 20.4.4.1.2, to that shown in table 86.

Further communication from MAC to the U-plane shall use the TMD-REPORT primitive modified from the definition given in ETS 300 392-2 [2], subclause 20.4.4.1.1, to that shown in table 87.

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.

7.4.3 Transmission

The encryption control unit shall intercept TMD-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 TMD-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 88 should be followed, however no more than four half-slots should be stolen per second.

Table 88: Maximum average frequency of stealing

HIS	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 TMD-UNITDATA request. On receipt of a TMD-UNITDATA request that indicates a stolen frame the MAC shall generate the appropriate training sequence for the air interface to allow the receiving BS to recognize a stolen frame.

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

Figure 47 gives an example for determining the points of time of transmitting a new SV by the "sync-control" process. Transmission of a new SV may be forced after a period of 1 second after the last transmission of an SV. More SVs may be transmitted to improve reliability of synchronization and to allow for late entry.

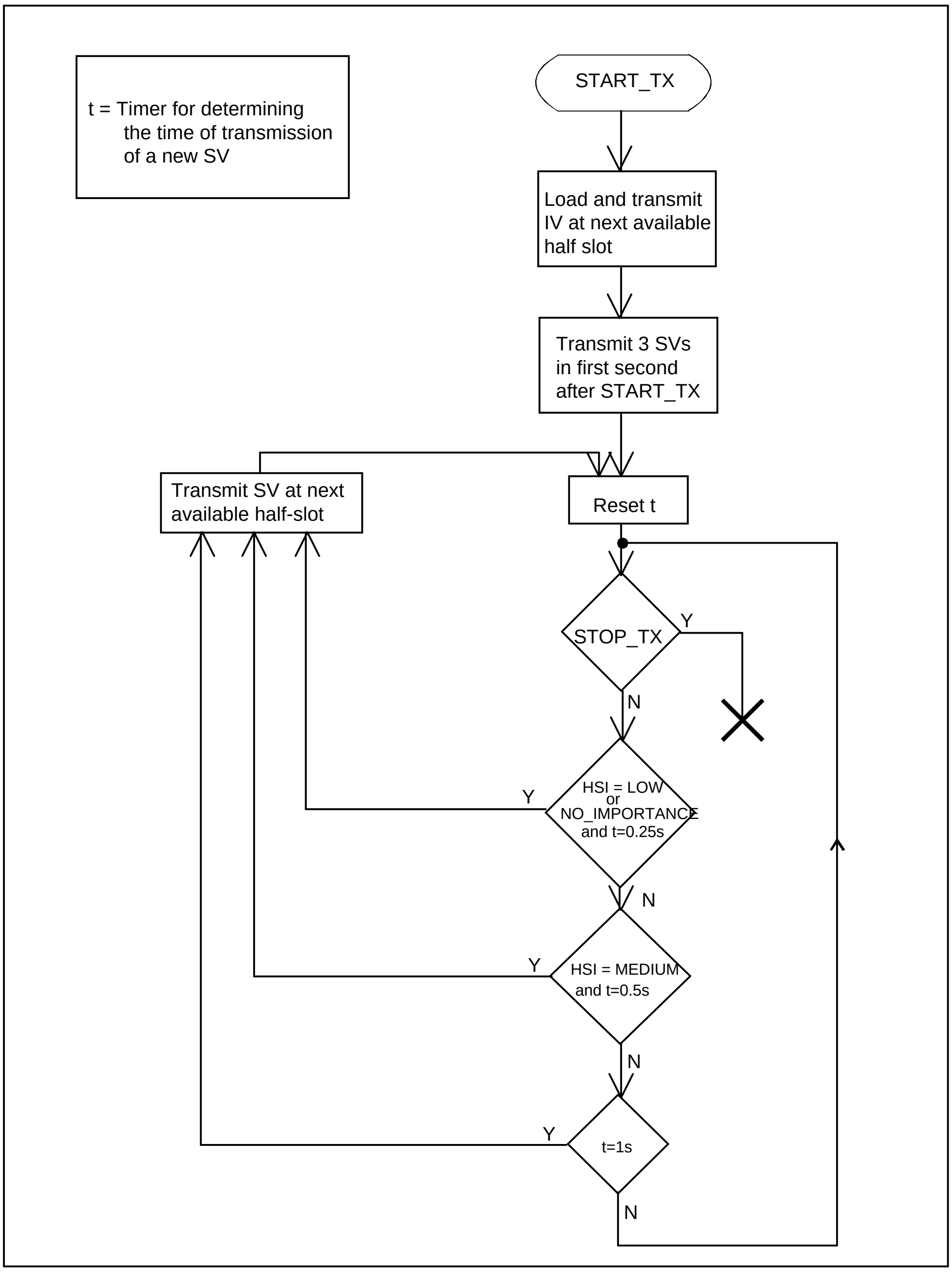

t = Timer for determining the time of transmission of a new SV
START_TX
Load and transmit IV at next available half slot
Transmit 3 SVs in first second after START_TX
Transmit SV at next available half-slot
Reset t
STOP_TX
Y
N
HSI = LOW or NO_IMPORTANCE and t=0.25s
Y
N
HSI = MEDIUM and t=0.5s
Y
N
t=1s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

Figure 47: Flow chart of the transmitter "sync-control" process.

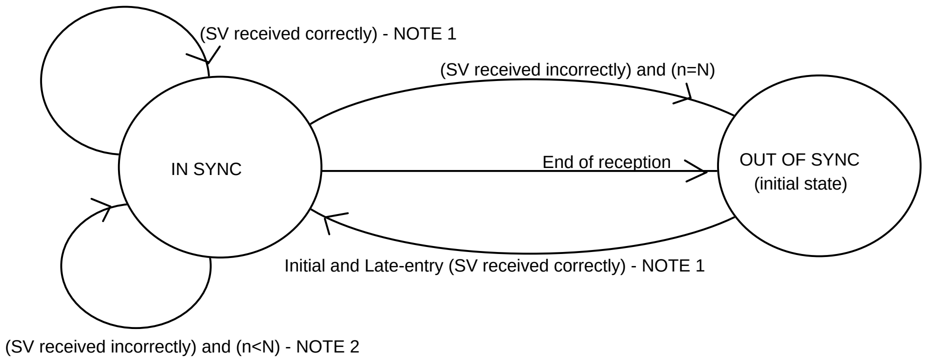
7.4.4 Reception

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

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

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

A state diagram of an example sync detect process is given in figure 48.


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

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

Figure 48: State diagram of the "sync-detect" process in the receiver.

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

7.4.5 Stolen frame format

The format of a stolen frame (half-slot) shall be as defined in table 89:

Table 89: Stolen frame format (half-slot)

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

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

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

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

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

Table 90: 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.

7.5 Location of security components in the functional architecture

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

In figure 49 the end-to-end encryption unit shall lie between the Traffic Source/Sink and TMD-SAP. The traffic source/sink may be a speech codec (see ETS 300 395-1 [5]), or any circuit mode data unit.

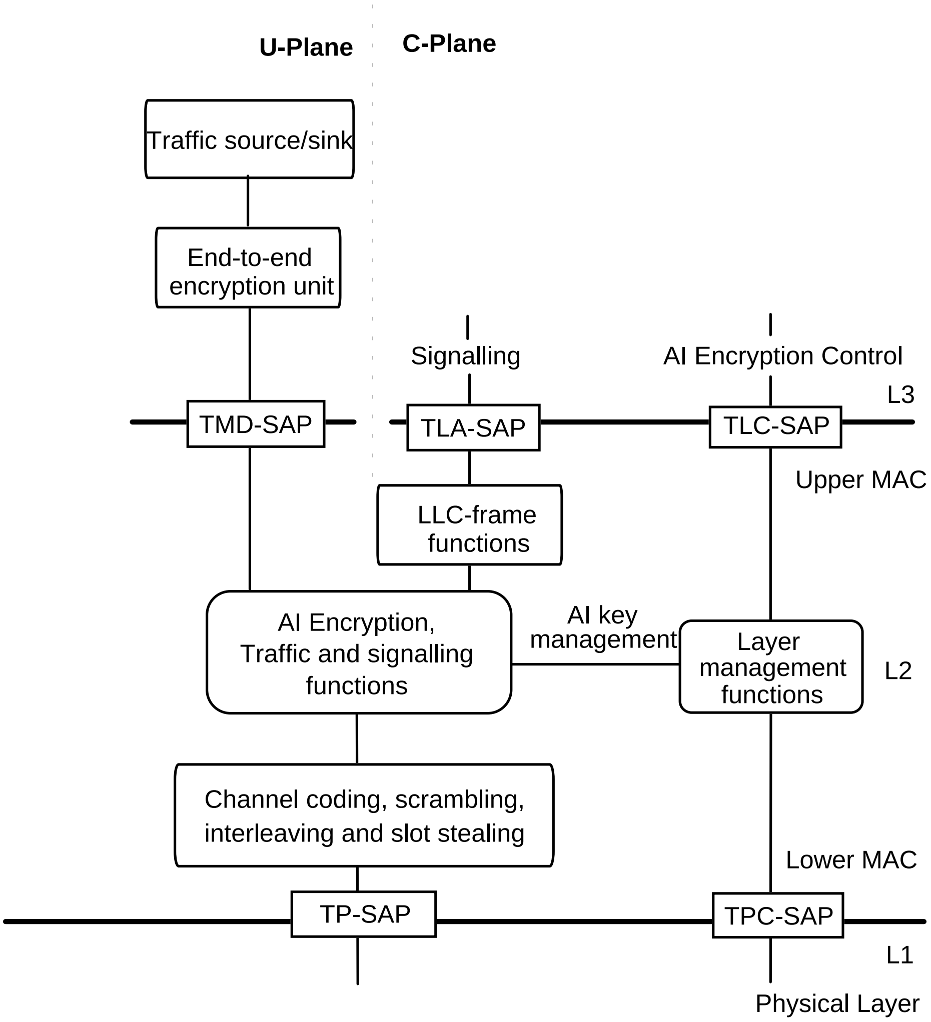


Figure 49: Position of end-to-end encryption unit in MS

The services offered on the U-Plane side, as shown in figure 49, may be further expanded in figure 50.

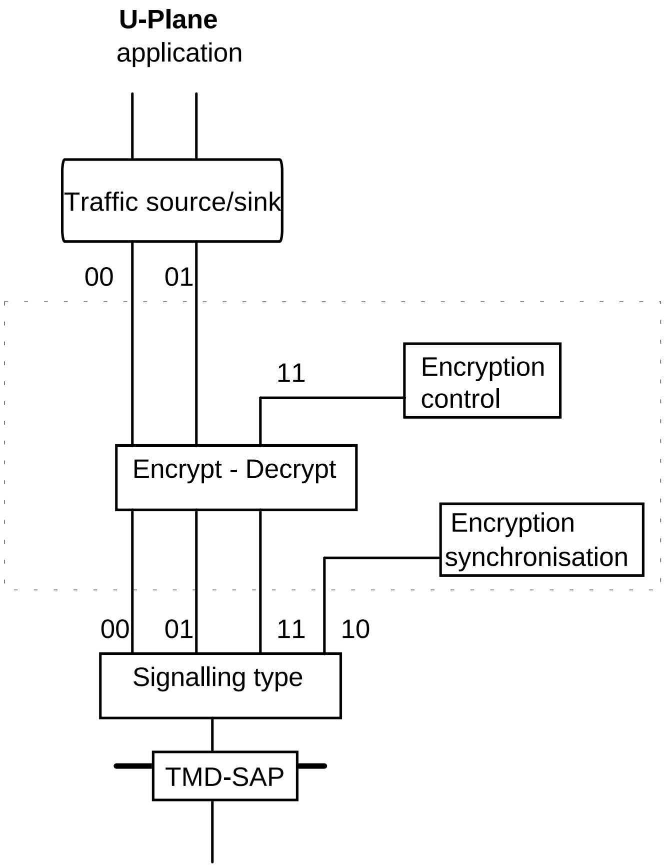


Figure 50: Functional model of the encryption unit

7.6 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 (SDS) with user defined data content. The key management message should include the following parameters:

- encryption key number;
- encryption unit identity;
- sealed encryption key.

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

The definition of user defined data type 4, given in ETS 300 392-2 [2], subclause 14.8.52 shall be replaced by the definition given in table 91:

Table 91: User defined data-4 element contents

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

History

Document history			
September 1995	Public Enquiry	PE 92:	1995-09-25 to 1996-01-19
September 1996	Vote	V 111:	1996-09-23 to 1996-11-15