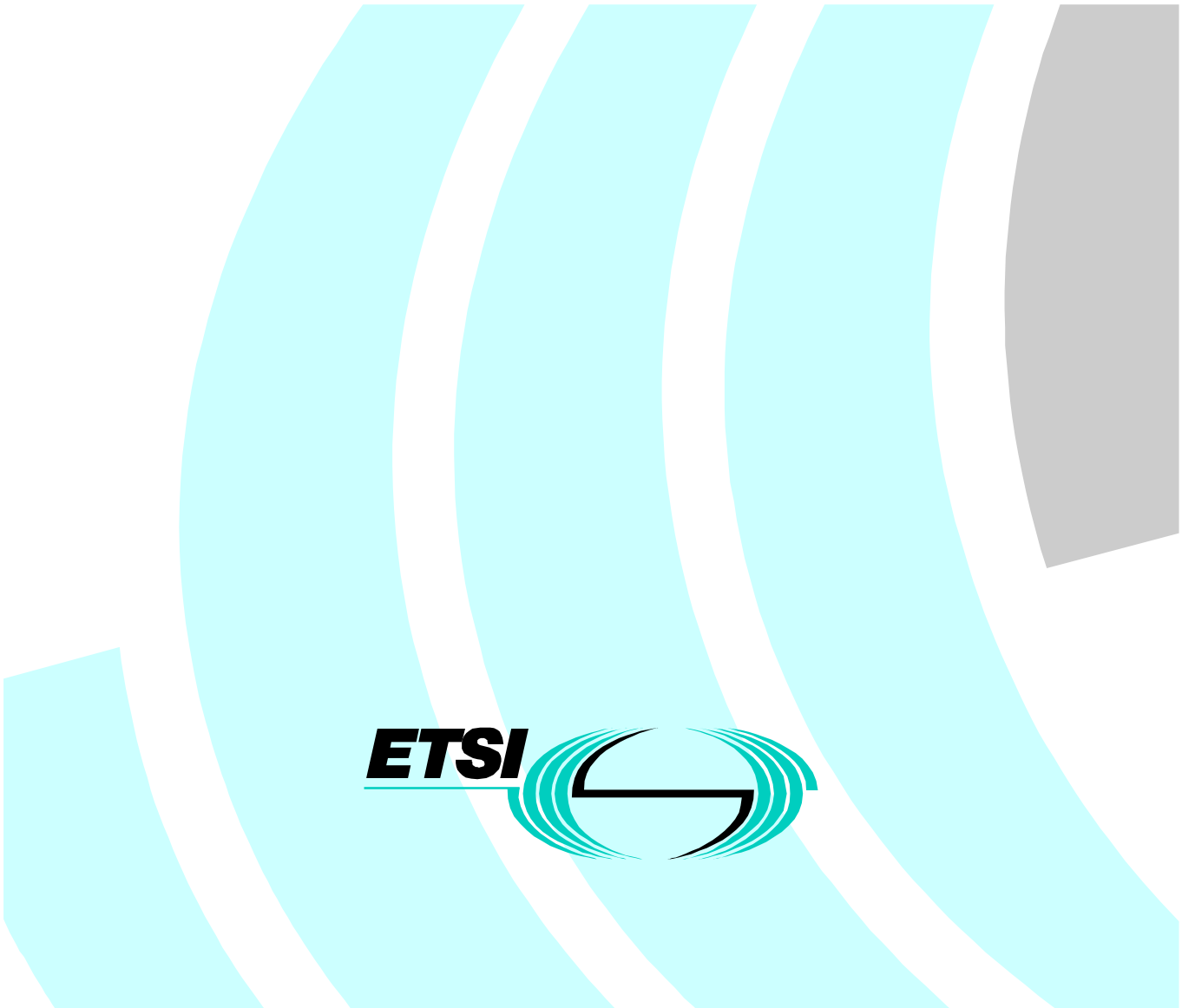
Final draft ETSI EN 300 392-7 V2.1.1 (2000-12)

European Standard (Telecommunications series)

Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security



Reference
REN/TETRA-06001-7

Keywords
TETRA, V+D, Security

ETSI

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

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

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

Important notice

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

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

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

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

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2000.
All rights reserved.

Contents

Intellectual Property Rights

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

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

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Project Terrestrial Trunked Radio (TETRA), and is now submitted for the Vote phase of the ETSI standards Two-step Approval Procedure.

The present document had been submitted to Public Enquiry as ETS 300 392-7 [3]. During the processing for Vote it was converted into an EN.

The present document is part 7 of a multi-part deliverable covering the Voice plus Data (V+D), as identified below:

Part 1: "General network design";

Part 2: "Air Interface (AI)";

Part 3: "Interworking at the Inter-System Interface (ISI)";

Part 4: "Gateways basic operation";

Part 5: "Peripheral Equipment Interface (PEI)";

Part 6: "Line connected Station (LS)";

Part 7: "Security";

Part 9: "General requirements for supplementary services";

Part 10: "Supplementary services stage 1";

Part 11: "Supplementary services stage 2";

Part 12: "Supplementary services stage 3";

Part 13: "SDL model of the Air Interface (AI)";

Part 14: "Protocol Implementation Conformance Statement (PICS) proforma specification";

Part 15: "TETRA frequency bands, duplex spacings and channel numbering".

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

1 Scope

The present document defines the Terrestrial 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.

The present document 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.

1.1 Security classes

TETRA security is defined in terms of class. Each class has associated features that are mandatory or optional and are summarized in table 1.

Table 1: Summary of Security features in TETRA by class

Class	Authentication	OTAR	Encryption	Enable-Disable	End-to-end
	Clause 4	**Clause 4**	**Clause 6**	**Clause 5**	**Clause 7**
1	O	-	-	M	O
2	O	O	M	M	O
3	M	M	M	M	O
NOTE:	M = Mandatory; O = Optional; - = Does not apply				

The present document describes a system in which all signalling and traffic within that system comply with the same security class. However signalling permits more than one security class to be supported concurrently within a SwMI, and movements between these classes are described in the present document. The SwMI shall control the state of AI encryption.

An MS may support one, several, or all security classes. Each cell may support at any one time one of the following options:

class 1 only;

class 2 only;

class 2 and class 1;

class 3 only; or

class 3 and class 1.

Class 2 and class 3 are not permitted to be supported at the same time in any cell.

1.2 Document layout

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 [4], 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 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 and keys for end-to-end confidentiality described.

The present document 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 the present document.

2 References

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

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

[1] ETSI ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

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

[3] ETSI ETS 300 392-7 (1996): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

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

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

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

[7] ETSI ETS 300 812: "Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM - ME) interface".

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

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document the following terms and definitions apply:

Authentication Code (AC): (short) sequence to be entered by the user into the MS that may be used in addition to the UAK to generate K with algorithm TB3

Authentication Key (K): 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 key within an LA and the protection against replay of old keys

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

cipher text: data produced through the use of encipherment. The semantic content of the resulting data is not available (see ISO 7498-2 [5])

class: see security class

Common Cipher Key (CCK): cipher key that is generated by the infrastructure to protect group addressed signalling and traffic. CCK is also used to protection of SSI identities (ESI) in layer 2

decipherment: reversal of a corresponding reversible encipherment (see ISO 7498-2 [5])

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

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

encipherment: cryptographic transformation of data to produce cipher text (see ISO 7498-2 [5])

Encryption Cipher Key (ECK): cipher key that is used as input to the encryption algorithm. This key is derived from one of SCK, DCK, MGCK or CCK and modified using an algorithm by the broadcast data of the serving cell

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

encryption state: encryption on or off

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

Extended Group Session Key for OTAR (EGSKO): cipher key used for distribution of keys to groups of users

Fallback SCK: key used by class 3 system when operating in class 2, for example in a fault or fallback situation

flywheel: 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): cipher key known by the infrastructure and MS to protect group addressed signalling and traffic. Not used directly at the air interface but modified by CCK or SCK to give a Modified Group Cipher Key (MGCK)

Group Session Key for OTAR (GSKO): cipher key used to derive EGSKO for the distribution of keys to groups of users

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

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

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

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

Location Area id (LA-id): unique identifier within a SwMI of a location area

Manipulation Flag (MF): used to indicate that a sealed cipher key (CCK, SCK or GCK) has been incorrectly recovered

Modified Group Cipher Key (MGCK): cipher key known by the infrastructure and MS to protect group addressed signalling and traffic that is composed algorithmically from either CCK and GCK, or SCK and GCK

Over The Air Re-keying (OTAR): method by which the SwMI can transfer secret keys securely to terminals

Personal Identification Number (PIN): entered by the user into the MS and used to authenticate the user to the MS

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

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

Random Challenge (RAND1, RAND2): random value generated by the infrastructure to authenticate a user or in an MS to authenticate the infrastructure, respectively

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

Random seed for OTAR (RSO): random value used to derive a session key for OTAR from a user's authentication key

Registered Area (RA): collection of location areas (LA) to which the MS may perform cell re-selection without need for explicit invocation of the registration protocol

Response (RES1, RES2): 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: collective term for the group of 32 SCK associated with each ITSI

Security class 1, 2 or 3: classification of terminal and SwMI encryption and authentication support. Class 1: no encryption, may use authentication; Class 2: SCK encryption, ESI with SCK, may use authentication; Class 3: DCK encryption, ESI with CCK, authentication

Sealed Common Cipher Key (SCCK): common cipher key cryptographically sealed with a particular user's derived cipher key

Sealed Group Cipher Key (SGCK): group cipher key cryptographically sealed with a particular user's derived cipher key

Sealed Static Cipher Key (SSCK): static cipher key cryptographically sealed with a particular user's secret key

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

Session Key for OTAR (KSO): derived from a user's authentication key and a random seed for OTAR. KSO is used to protect the transfer of the Static Cipher Key

Static Cipher Key (SCK): predetermined cipher key that may be used to provide confidentiality in class 2 systems with a corresponding algorithm

Synchronization value: sequence of symbols that is transmitted to the receiving terminal to synchronize the EKSG in the receiving terminal with the EKSG in the transmitting terminal. The sequence may also contain identification of end-to-end encryption algorithm and the used encryption key

synchronous stream cipher: 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: mathematical description of a cryptographic process used for either of the security processes authentication or encryption

time stamp: 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 the present document the following abbreviations apply:

AC	Authentication Code
AI	Air Interface
AS	Alias Stream
AESI	Alias Encrypted Short Identity
ASSI	Alias Short Subscriber Identity
BNCH	Broadcast Normal Channel
BS	Base Station
CC	Colour Code
CCK	Common Cipher Key
CCK-id	CCK identifier
CK	Cipher Key
CN	Carrier Number
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
DM-SCK	SCK used in Direct Mode operation
ECK	Encryption Cipher Key
EGSKO	Extended Group Session Key for OTAR
EKSG	End-to-end Key Stream Generator
EKSS	End-to-end Key Stream Segment
ESI	Encrypted Short Identity
F	Function
FACCH	Fast Associated Control Channel
FEC	Forward Error Correction
GCK	Group Cipher Key
GCKN	Group Cipher Key Number
GCK-VN	GCK-Version Number
GESI	Group Encrypted Short Identity
GSKO	Group Session Key OTAR
GSKO-VN	GSKO Version Number
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 for OTAR
KSS	Key Stream Segment
LA	Location Area
LA-id	Location Area identifier
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
OTAR	Over The Air Re-keying
PDU	Protocol Data Unit
PIN	Personal Identification Number
PT	Plain Text
RA	Registered Area
RAND1	RANDom challenge 1
RAND2	RANDom challenge 2
RES1	RESponse 1
RES2	RESponse 2
RS	Random Seed
RSO	Random Seed for OTAR
SACCH	Slow Associated Control Channel
SAP	Service Access Point
SCCK	Sealed Common Cipher Key
SCH	Signalling Channel
SCH/F	Full Slot Signalling Channel
SCH/HU	Half-slot Uplink Signalling Channel
SCH/HD	Half-slot Downlink Signalling Channel
SCK	Static Cipher Key
SCK-VN	SCK Version Number
SCKN	Static Cipher Key Number
SDU	Service Data Unit
SF	Synchronization Frame
SGCK	Sealed GCK
SGSKO	Sealed GSKO
SHSI	Stolen Half-Slot Identifier
SS	Synchronization Status
SSCK	Sealed SCK
SSI	Short Subscriber Identity
STCH	STealing CHannel
SV	Synchronization Value
SwMI	Switching and Management Infrastructure
TA	TETRA Algorithm (used with specific numeric algorithm identity e.g. TA31)
TCH	Traffic Channel
TCH/2.4	Traffic Channel for 2.4kbs circuit mode data
TCH/4.8	Traffic Channel for 4.8kbs circuit mode data
TCH/7.2	Traffic Channel for 7.2kbs circuit mode data
TEA	TETRA Encryption Algorithm (used with specific numeric algorithm identity e.g. TEA1)
TEI	TETRA Equipment Identity
TNMM	TETRA Network Mobility Management (refers to the SAP)
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

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

4.1 Air interface authentication mechanisms

4.1.1 Overview

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). The design of the SwMI is not specified, but some other entity such as a Base Station (BS) may carry out the authentication protocol on behalf of the Authentication Centre. This entity is assumed to be trusted by the SwMI and the authentication exchange proves knowledge given to this entity by the authentication centre. This knowledge shall be the session authentication key. This ensures that the authentication key K of the MS is never visible outside the Authentication Centre.

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 cipher keys over the air interface. The controlling party in all authentication exchanges shall be the SwMI.

The authentication process describes a confirmed 2-pass challenge-response protocol.

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

4.1.2 Authentication of a user

In this clause, 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 SwMI shall generate a random number as a challenge RAND1. The MS shall compute a response, RES1, and the SwMI shall compute an expected response, XRES1. A part of the derived cipher key shall be generated by this process, labelled DCK1. The SwMI 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.

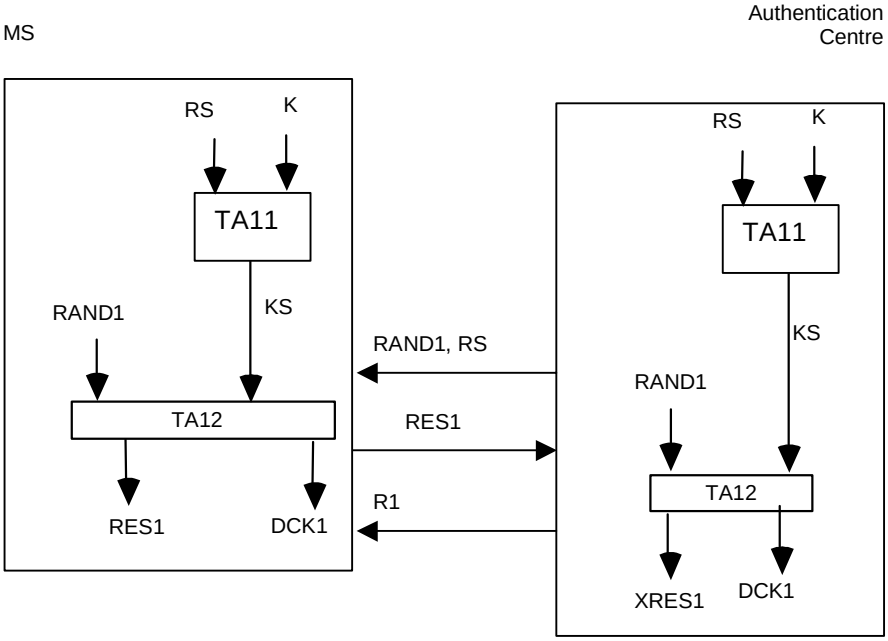


Figure 1: Authentication of a user by the infrastructure

DCK1 is not used in a system operating in class 1 and class 2.

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 clause 4.1.2 with the roles of the challenger and challenged reversed. The MS shall generate a challenge, RAND2, the SwMI shall generate an actual response, RES2, and the MS shall generate an expected response, XRES2. A part of the derived cipher key shall be generated by this process, labelled DCK2. The MS on receipt of RES2 from the SwMI 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.

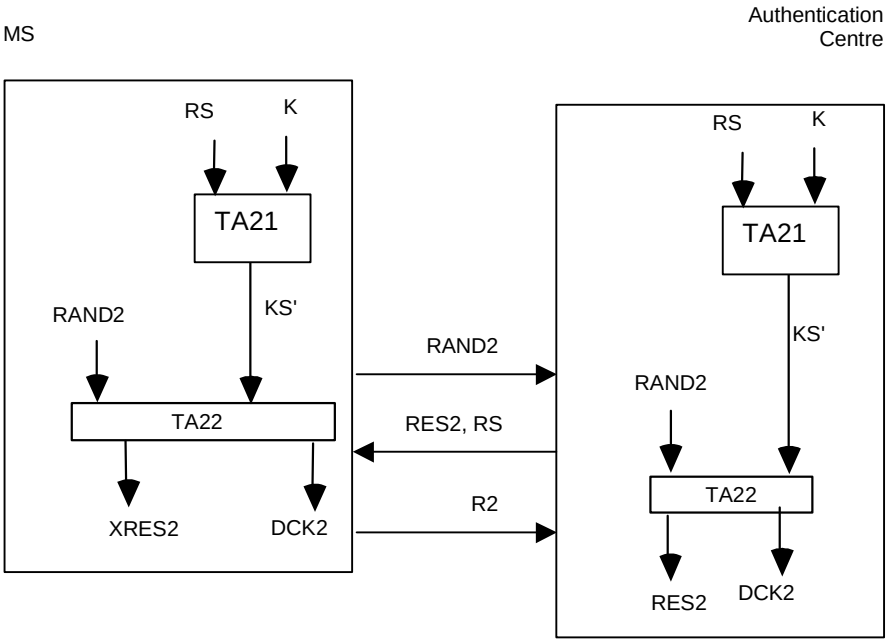


Figure 2: Authentication of the infrastructure by a user

DCK2 is not used in a system operating in class 1 and class 2.

4.1.4 Mutual authentication of user and infrastructure

Mutual authentication of user and infrastructure shall be achieved using a confirmed three pass mechanism. The algorithms and key K used shall be the same as those used in the one way authentication described in the previous clauses. 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 TA21 to generate the pair of session keys KS and 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 TA21 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 TA21 to generate session key KS' if it has not already done so. 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 clause 4.2.1.

The process is shown in figure 3.

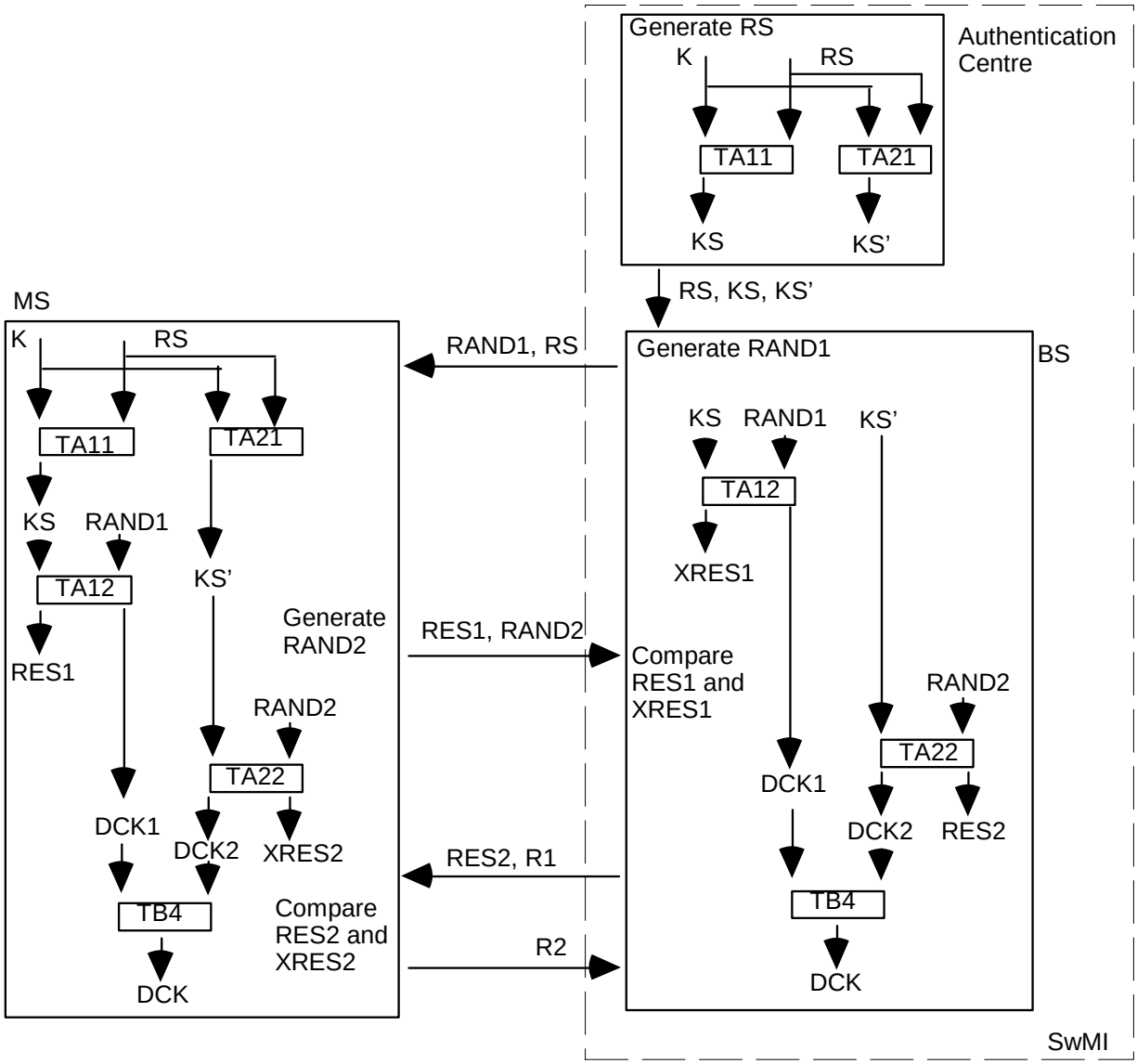


Figure 3: Mutual authentication initiated by SwMI

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.

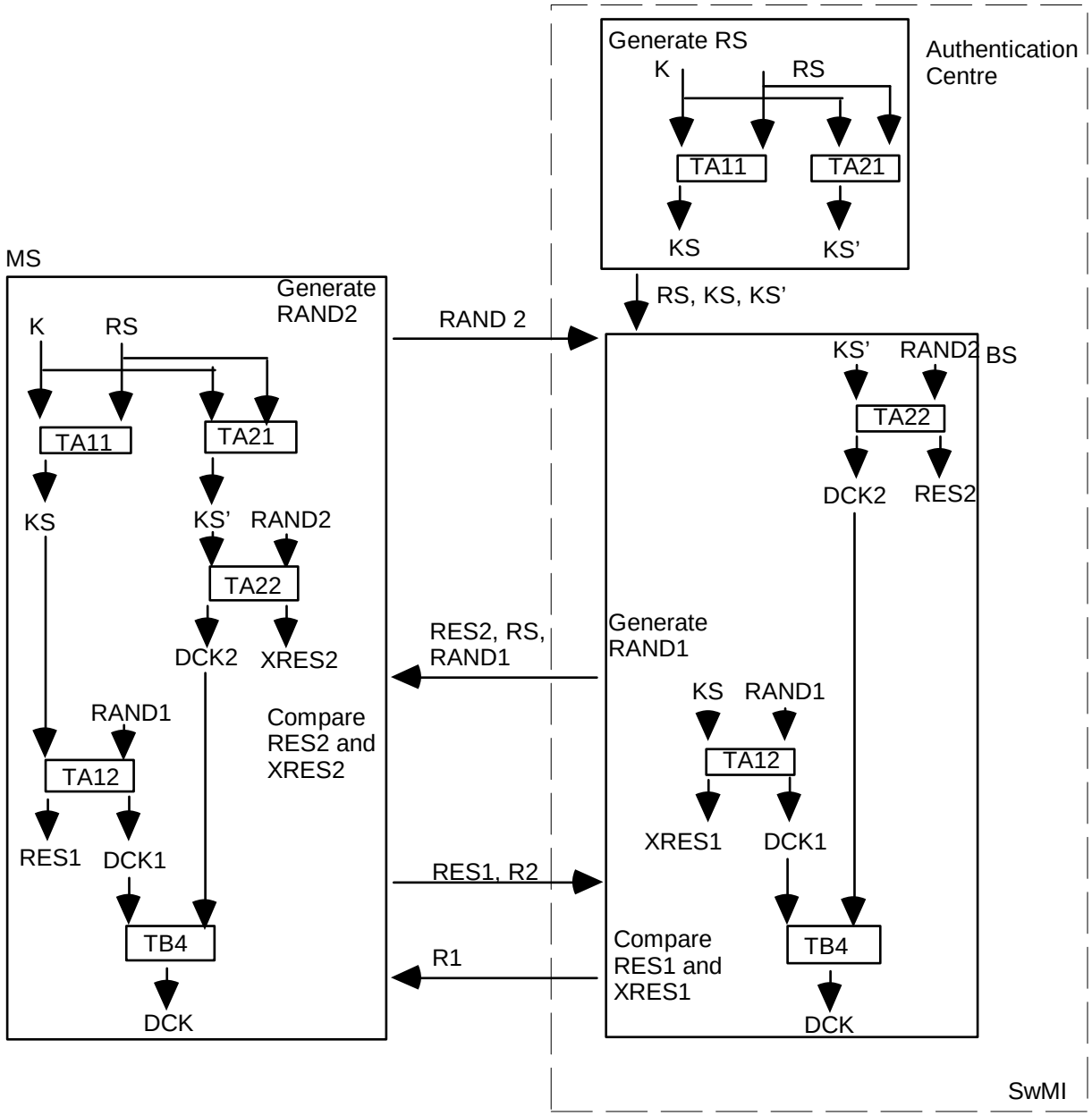


Figure 4: Mutual authentication initiated by MS

In class 1 and class 2 systems as DCK1 and DCK2 are not used algorithm TB4 to generate DCK should not be invoked.

4.1.5 The authentication key

The ITSI and its associated user should be authenticated by a process that is carried out in the MS, as described in clause 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 Making K available in an MS

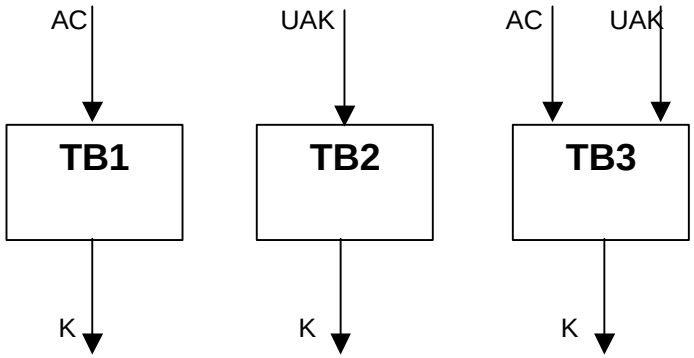


Figure 5: Making authentication key K available in an MS

K shall be made available by combining a user input and an algorithm 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) that may be stored in a module. 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 an AC entered by the user. The procedure to generate K from UAK and AC is labelled TB3. In this case the actual checking shall be carried out implicitly by the infrastructure through the authentication process.

If any of the input parameters are changed and K is altered as a result then the SwMI needs to have a harmonized change. A user shall not be able to change the input to the algorithm without harmonizing the change of input with the authentication centre in the SwMI. The present document does not describe a mechanism or protocol for such an information exchange.

4.1.6 Equipment authentication

The authentication of the TETRA Equipment Identity (TEI) is outside the scope of the present document. However the protocol described in clause 4.4 provides a mechanism whereby the BS may demand an MS to provide TEI as part of the registration exchange.

4.2 Air Interface key management mechanisms

Five 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 Group Session Key for OTAR (GSKO); and,
- the Static Cipher Key (SCK).

The ESI mechanism is also described in this clause. Exchange of DCK is linked to the authentication exchange described in clause 4.1. Clauses 4.2.2 through 4.2.4 describe over the air re-keying (OTAR) that is used to exchange the remainder of these keys.

4.2.1 The DCK

DCK applies only to class 3 cells.

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.

NOTE: Both the infrastructure and the terminal derive DCK during the authentication process.

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.

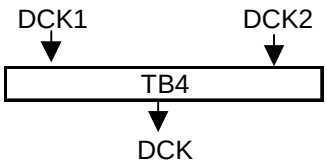


Figure 6: Derivation of the DCK from its two parts

In a successful authentication exchange the algorithm TB4 shall always be invoked in accordance with the rules for input given above.

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 known to the infrastructure and distributed to the MSs. GCK shall not be used directly by the air interface encryption unit. If used in a class 2 system, the GCK shall be modified by SCK (see clause 4.2.4) using algorithm TA71 to provide a Modified GCK (MGCK) for use on the air interface. In a class 3 system, within each LA the GCK shall be modified by CCK (see clause 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 the value of MGCK shall be equal to that of SCK (class 2 systems), or of CCK (class 3 systems) and algorithm TA71 shall not be invoked.

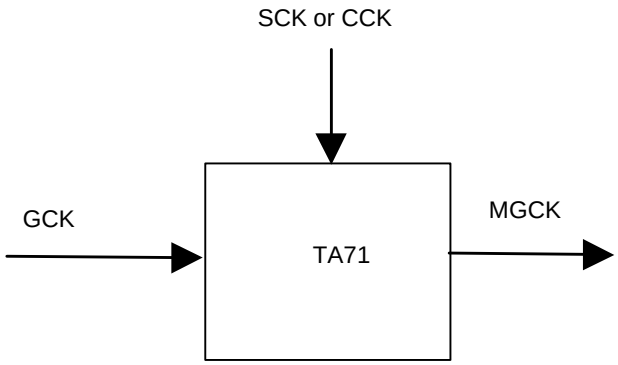


Figure 7: Generation of MGCK from GCK and CCK, or from GCK and SCK

One GCK may be associated with more than one group. A GCK Number (GCKN) associated with each GCK can be used to identify association with multiple groups. The values of GCKN should be unique between all MSs sharing the same sets of GCK. The association of GCK to groups may be changed by the OTAR service to allow automatic key management to take place.

If OTAR is used to transfer GCK it shall be transmitted in sealed form using algorithm TA81. When OTAR is used to distribute GCK to an individual a session key for OTAR (KSO) shall be used to protect the GCK. 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. 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 introduces some redundancy into the Sealed Group Cipher Key (SGCK). The algorithm TA81 uses the group key version number (GCK-VN) and the Group Cipher Key Number (GCKN), 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.

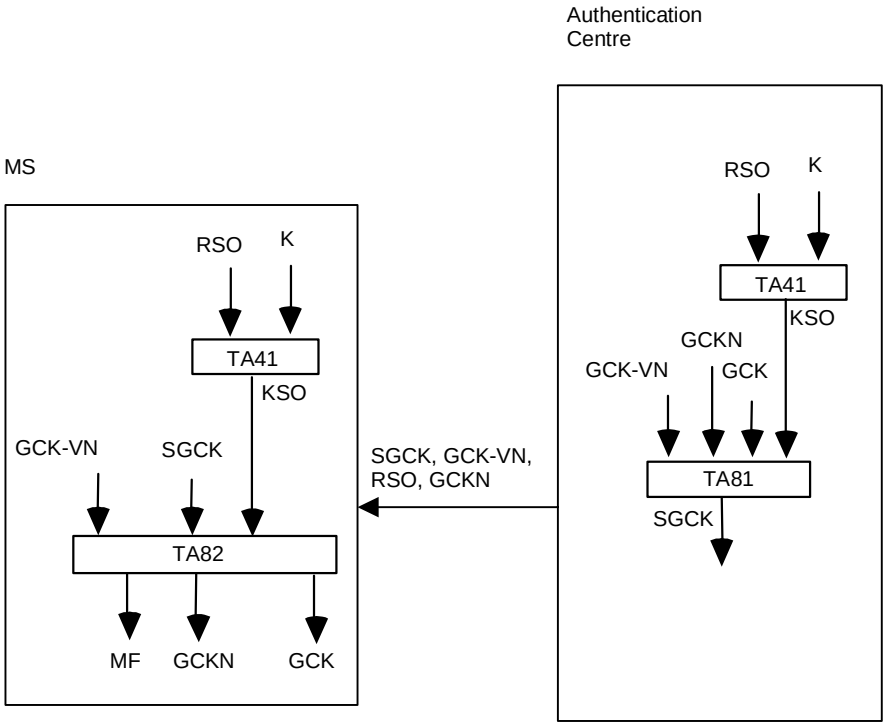


Figure 8: Distribution of a group cipher key to an individual

GCK may be used in partnership with the SCK (see clause 4.2.2) or with the CCK (see clause 4.2.3) to protect voice, data, and signalling sequences between the infrastructure and an MS when using group addresses.

GCK may also be distributed to groups using the mechanism described in 4.2.5.

4.2.3 The CCK

CCK applies only to class 3 cells.

CCK shall be used to give protection of voice, data, and signalling sequences between the infrastructure and an MS when using group addresses on the downlink either as a key modifier of GCK (see clause 4.2.2) or as a standalone key. In addition CCK shall be used to generate ESI as described in clause 4.2.5.

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 as part of the registration protocol, or at any other time as part of the CCK delivery protocol. 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 introduces 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.

CCK is uniquely identified by the combination of LA-id and CCK-id. Within an LA the CCK-id shall increment by 1 on each change of CCK. Where a CCK applies to many LAs the CCK-id shall be the same in each LA.

The process is summarized in figure 9.

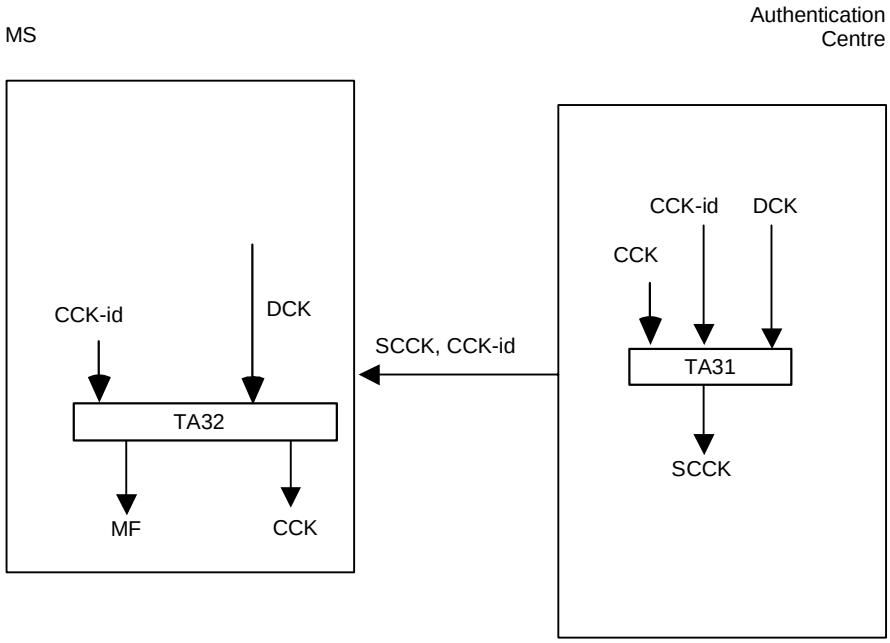


Figure 9: Distribution of a common cipher key

4.2.4 The SCK

SCK applies to class 2 cells and to Direct Mode operations (see ETS 300 396-6 [8]).

SCK shall be used to protect voice, data, and signalling sequences between the infrastructure and an individual MS in a class 2 cell. The SCK or the MGCK derived from the SCK (see clause 4.2.3) may be used to protect voice, data, and signalling sequences between the infrastructure and a group-addressed MS. 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 GCK 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. SCK-VN may be used to protect the distribution of the SCKs against replay. The method of determining a valid SCK-VN and therefore of identifying a replay is outside the scope of the present document. The SCKN is input to TA51 and output from TA52.

When distributing SCK to an individual by an OTAR mechanism (algorithms TA51 and TA52) a session key for OTAR (KSO) shall be used to protect the SCK. 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.

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 and SCKN at the MS, SCK-VN and RSO shall be distributed together with SSCK.

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

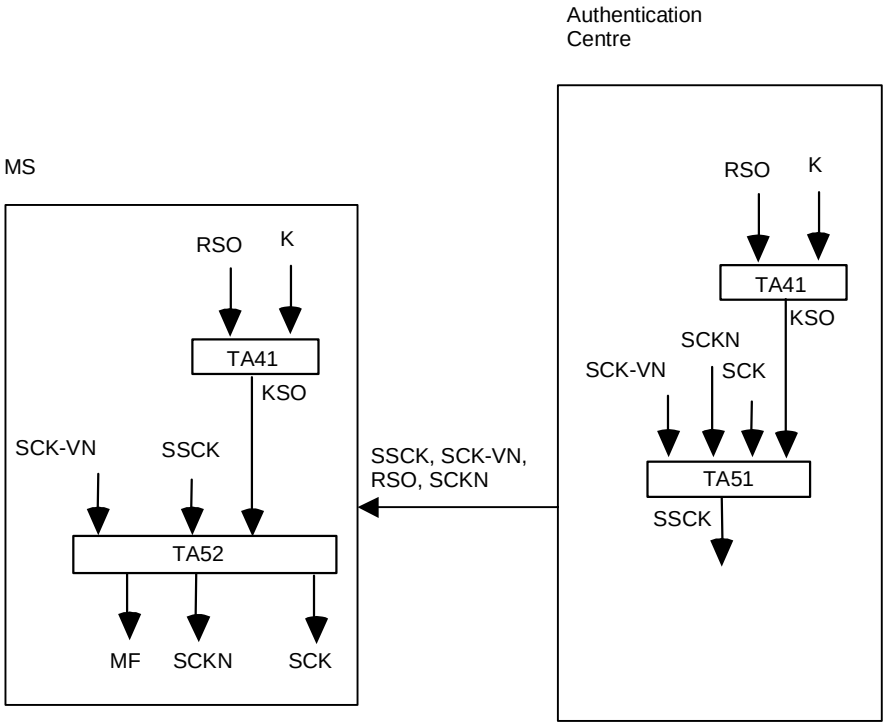


Figure 10: Distribution of SCK to an individual by an authentication centre

SCKs may be associated with one or more groups for encryption in DMO (see ETS 300 396-6 [8]). The OTAR service provided here may also be used to provide key management in DMO. The OTAR service allows a provided SCK to be associated with one or more groups in DMO and this does not apply to TMO. It also provides a means to change an SCK associated with one or more groups for the purposes of limiting the lifetime of a key, and for fleet management.

SCK may also be distributed to groups using the mechanism described in 4.2.5.

4.2.5 The GSKO

The OTAR mechanisms described in clauses 4.2.2 and 4.2.4 shall be used for distribution of GCK and SCK to individuals as identified by ITSI and by K. In some cases keys may need to be distributed to groups as identified by GTSI. In order to allow the sealing mechanisms described in clauses 4.2.2 and 4.2.4 to operate KSO shall be replaced by an Extended Group Session Key for OTAR (EGSKO) derived using algorithm TB7 from the Group Sealing Key for OTAR (GSKO).

GSKOs may be protected for distribution in like manner to the CCK but instead using algorithms TA91 and TA92.

When distributing GSKO by an OTAR mechanism (algorithms TA91 and TA92) a session key for OTAR (KSO) shall be used to protect the GSKO. 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 as for distribution of SCK and GCK. The GSKO has an associated version number, GSKO-VN which can be used for replay protection.

Algorithm TA91 is used with GSKO, KSO and GSKO-VN as inputs to produce a sealed key SGSKO for transmission to an MS. Recovery of GSKO from SGSKO is achieved using algorithm TA92 in conjunction with KSO and GSKO-VN as inputs. A manipulation flag MF provides assurance of correct recovery.

The process is summarized in figure 11.

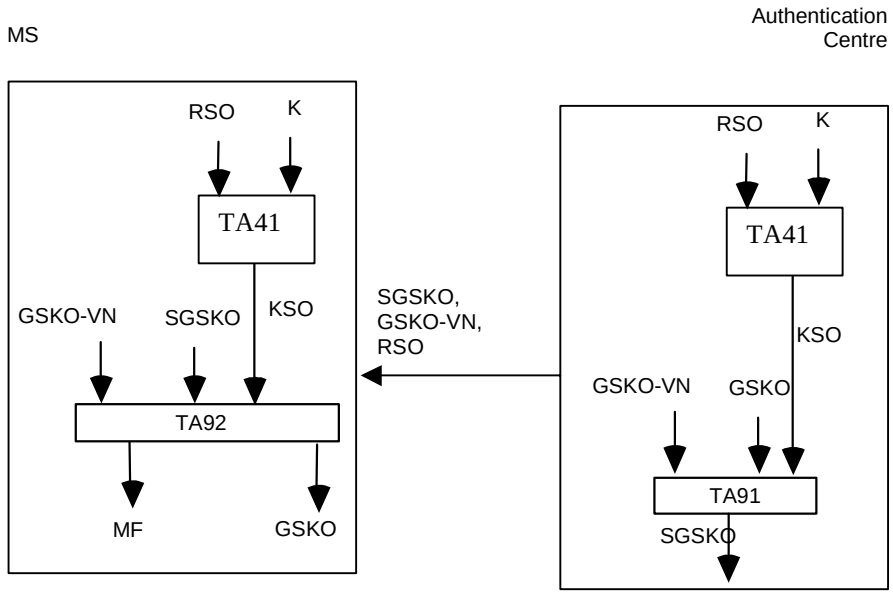


Figure 11: Distribution of GSKO by an authentication centre

4.2.5.1 SCK distribution to groups with OTAR

When distributing SCK to a group EGSKO shall be used in place of KSO as input to algorithms TA51 and TA52. Signalling shall indicate if the distributed SCK is sealed with EGSKO or KSO. In this case the mechanism shall be as shown in figure 10 with TA41 not invoked and KSO replaced by EGSKO.

EGSKO is derived from GSKO using algorithm TB7 as shown in figure 12.

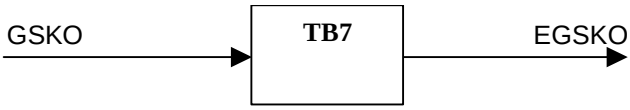


Figure 12: Generation of EGSKO using TB7

4.2.5.2 GCK distribution to groups with OTAR

When distributing GCK to a group EGSKO shall be used in place of KSO as input to algorithms TA81 and TA82. Signalling shall indicate if the distributed GCK is sealed with EGSKO or KSO. In this case the mechanism shall be as shown in figure 8 with TA41 not invoked and KSO replaced by EGSKO.

4.2.6 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 clause describes a mechanism that allows the encryption of the SSI segment of addresses used by layer 2. The event label and usage marker shall not be encrypted by this mechanism. 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 in cells of security class 3, or with SCK for cells of security class 2. Whenever encrypted signalling is used, the ESI shall be sent instead of the true identity. The mechanism uses algorithm TA61 as shown in figure 13.

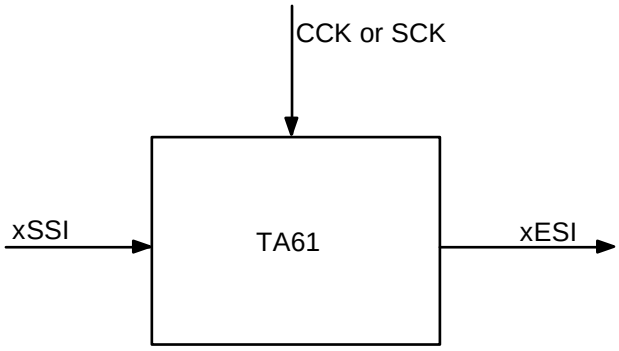


Figure 13: Generation of ESI from SSI and a cipher key

CCK is derived from algorithm TA32, and xSSI are all short addresses valid for the user (ISSI, GSSI, ASSI, V-ASSI, V-GSSI). The output xESI (IESI, GESI, AESI, V-AESI, V-GESI) 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 "00", 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 clause 6.4.

4.2.7 Encryption Cipher Key

The Encryption Cipher Key (ECK) shall be derived using algorithm TB5 from a selected CK. The CK shall be one of DCK, CCK, MGCK in class 3 cells, and shall be SCK or MGCK derived from SCK in class 2 cells. TB5 combines CK with CN, CC and LA identifier to produce ECK. This is to prevent attacks on the encryption process by replaying cipher text to eliminate the keystream, and to prevent keystream replay within the repeat period of the frame numbering system.

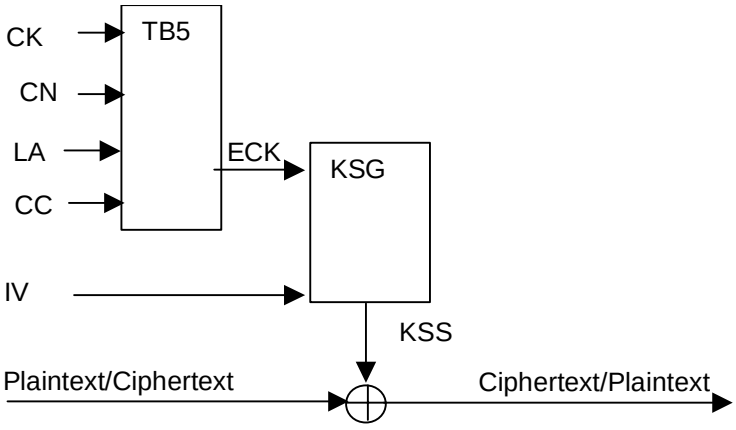


Figure 14: Use of TB5 to generate ECK

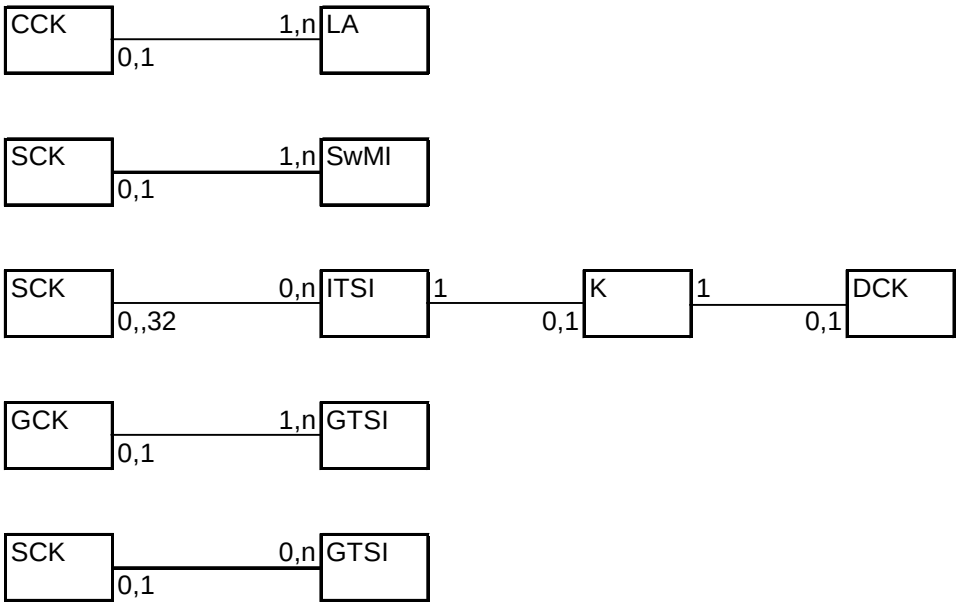
4.2.8 Summary of AI key management mechanisms

Table 2 summarizes the pre-conditions and lifetimes for each key.

Table 2: Cipher Key pre-conditions and lifetime

Key	Pre-condition	Lifetime
K	None	ITSI (note 1)
DCK	Authentication	Authentication period (note 3)
CCK	Authentication	Not defined (note 4)
SCK	None	Not defined (note 2)
GCK	None	Not defined (note 5)
MGCK	Authentication	As per CCK
GSKO	None	Not defined (note 5)
NOTE 1: If OTAR is used for SCK, K or GSKO is required. NOTE 2: K or GSKO is required for OTAR in class 2 and class 3. NOTE 3: In an MS DCK may be deleted on power down. NOTE 4: CCK may be deleted from the MS on power down. NOTE 5: Generally long life.		

Figure 15 shows the fixed relationship between TETRA addresses and cipher keys. 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: An ITSI may have 0, 1 or up to 32 SCKs associated with it.
NOTE 2: An SCK may be associated with 0,1 or many ITSIs (in the diagram "n" represents this).
NOTE 3: An LA may only use one CCK at any one time.
NOTE 4: A CCK may be used in more than one LA (represented by "n").
NOTE 5: An ITSI may have 0 or 1 key K.
NOTE 6: Key K shall only be associated with 1 ITSI.
NOTE 7: A SwMI shall only use one SCK at any one time (see also 6.5).
NOTE 8: An SCK may be used in more than one SwMI.
NOTE 9: A GCK may be associated with 1 or many GTSIs.
NOTE 10: A GTSI may have 0 or 1 GCK associated with it.
NOTE 11: An SCK may be associated with 0, 1 or many GTSIs for DMO only.
NOTE 12: A GTSI may have 0 or 1 SCK associated with it, or for DMO only many SCKs associated with it.

Figure 15: 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. It may also be used to configure the mutual authentication and registration behaviour of the MS.

Table 3: TNMM AUTHENTICATE service primitives

GENERIC NAME	Specific name	PARAMETERS
TNMM-AUTHENTICATE	indication	Result, reason
TNMM-AUTHENTICATE	confirm	Result
TNMM-AUTHENTICATE	request	Configure

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;

- configure =

  authenticate SwMI now;

  never mutually authenticate;

  always mutually authenticate;

  never authenticate during location update;

  always authenticate during location update;

  authenticate only in ITSI-Attach form of location update.

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 4: TNMM SCK service primitives

Generic name	Specific name	Parameters
TNMM-SCK	indication	SCKN, SCK-VN, GTSI
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;

  SwMI Unable to provide SCK;

- 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 GCKN, optionally the GTSI, and GCK-VN of the 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 either the address (GTSI) for the GCK requested or the GCKN for the GCK requested..

Table 5: TNMM GCK service primitives

GENERIC NAME	Specific name	PARAMETERS
TNMM-GCK	Indication	GTSI, GCK-VN, GCKN
TNMM-GCK	Confirm	Result
TNMM-GCK	Request	GTSI, GCKN

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

- result =

  GCK received successfully;

  GCK failed to decrypt;

  SwMI Unable to provide GCK;

- GTSI =

  01;

  2;

  …;

  2^{48}-1;

NOTE: The SSI part of GTSI cannot take the values "000000_{16}" and "$FFFFFF_{16}$"

- GCK-VN =

  0;

  …;

  2^{16}-1.

- GCKN =

  0;

  1;

  2;

  …;

  2^{16}-1;

4.3.4 GSKO transfer primitives

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

- TNMM-GSKO indication shall be used to provide the MS application with the GSKO-VN of each key received;
- TNMM-GSKO 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-GSKO request shall be used to request the distribution of a new Group Session Key for OTAR.

Table 6: TNMM GSKO service primitives

Generic name	Specific name	Parameters
TNMM-GSKO	indication	GSKO-VN
TNMM-GSKO	confirm	Result
TNMM-GSKO	request	

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

- result =

  GSKO received successfully;

  GSKO failed to decrypt;

  SwMI Unable to provide GSKO;

- GSKO-VN =

  0;

  …;

  2^{16}-1.

4.4 Authentication protocol

4.4.1 Authentication state transitions

Figures 16 and 17 give an overview of the received PDUs that result in a change of authentication state.

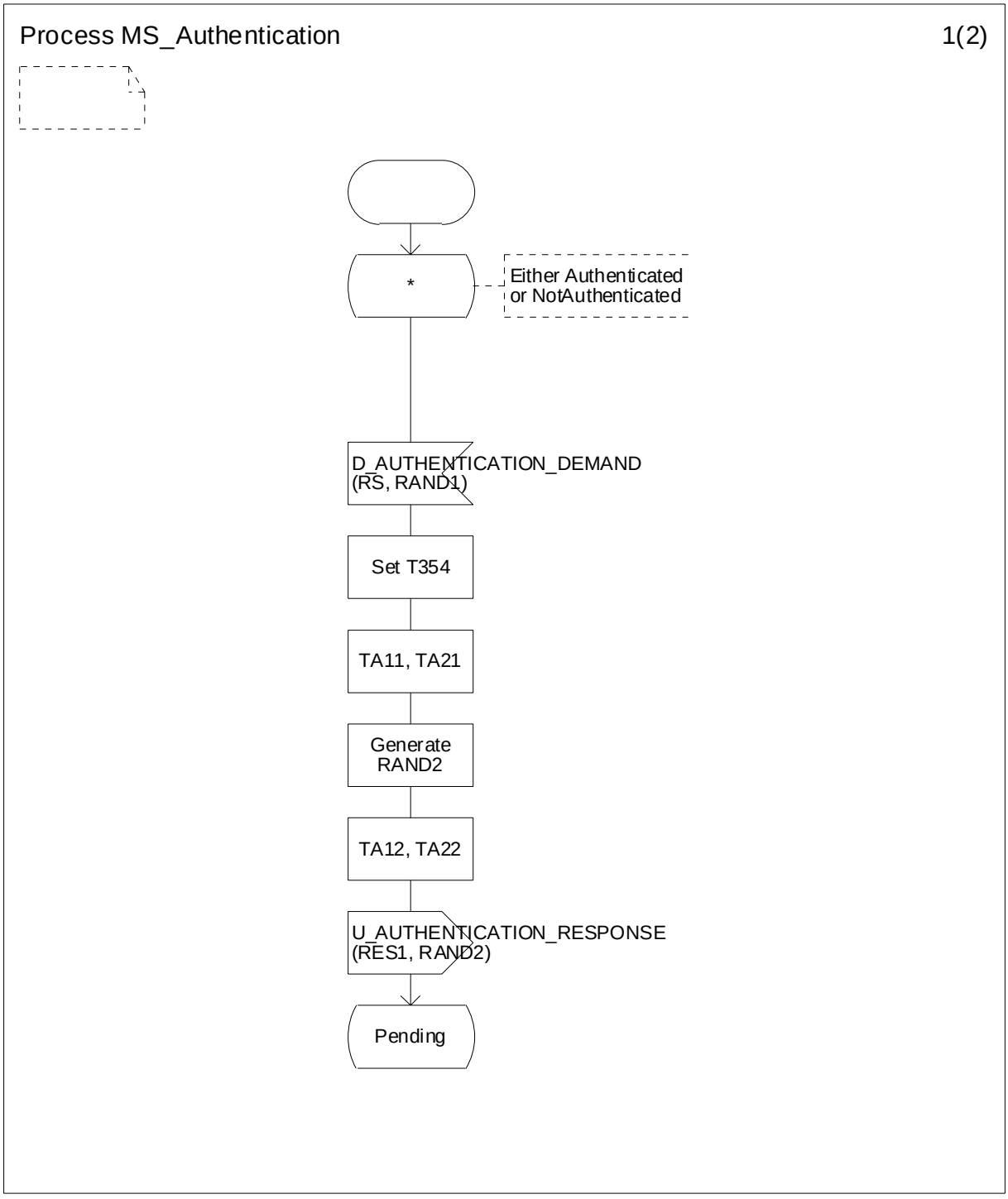


Figure 16: SDL process diagram for MS authentication (page 1 of 2)

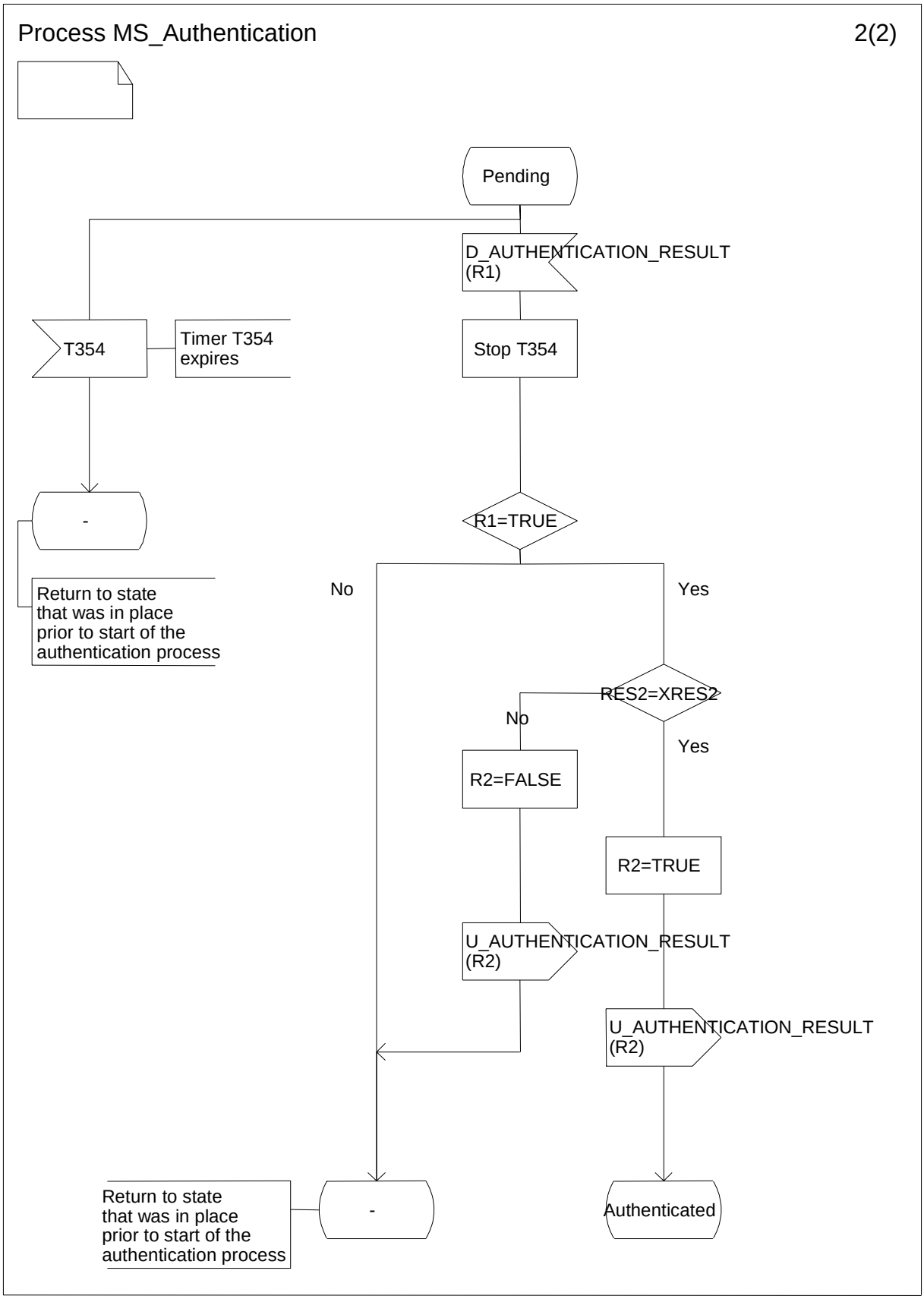


Figure 17: SDL process diagram for MS authentication (page 2 of 2)

4.4.1.1 Description of authentication states

The following states are defined in the preceding figures and have the meaning described here:

Authenticated: The MS has performed a successful authentication sequence. In class 3 cells DCK has been calculated and made available for use by the MAC;

NotAuthenticated: The MS has not yet been authenticated. In this state for class 3 cells, and for class 2 and class 1 cells in which authentication is required, the SwMI should offer only those MM services required to allow registration;

Pending: An authentication sequence has begun and not yet completed.

If a new authentication is started then any existing authentication state machine shall be terminated.

4.4.2 Authentication protocol sequences and operations

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

The following statements outline the dynamic requirements described by the protocol:

- if the authentication procedure fails to complete within time T354 the authenticating parties shall each revert to the security state (key) that was in place prior to the start of the authentication procedure;
- if DCK is to be used for AI encryption then CCK shall be used for ESI and to generate MGCK (class 3 cell);
- if authentication is performed during a U-plane transmission the DCK change shall take place according to the criteria given in clause 4.5.5.1;
- authentication should be carried out using a previously established encryption key where possible (changeover of DCK may be applied at the points shown in the MSCs of this clause).
- the encryption state (clear or encrypted) and the used cipher key shall not be changed during location update signalling. The change (if required) shall be made when both the authentication sequence has been completed and the location update has been accepted. The synchronization of parameter change in the SwMI and the MS will follow the same mechanism as in clause 4.5.5.1 change of DCK.

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 either an "AUTHENTICATION RESPONSE" or an "AUTHENTICATION REJECT" 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.

If the mutual authentication flag is set then the recipient knows to use DCK1 and DCK2 as input to TB4. If the mutual authentication flag is not set then TB4 is run with the "other" DCKx set to zero as stated as 4.2.1. Thus if MS to SwMI authentication is followed by MS to SwMI authentication there will be a DCK from the first (setting DCK2 to zero) and a later new DCK (setting DCK1 to zero). If the mutual authentication flag is used and the authentication made mutual as described above and in 4.1.4 then DCK is an algorithmic combination of DCK1 and DCK2.

In class 3 cells 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. In class 1 and class 2 cells DCK1 and DCK2 can be discarded.

The authentication timer T354 shall always be less than or equal in value to the registration timer T351 (see EN 300 392-2 [2], clause 16.11.1.1). When T354 is running only authentication signalling shall be accepted by MS-MM and BS-MM. When authenticating during registration the value of T354 shall be the same as T351 and as such only one timer needs to be invoked.

When T354 expires the MS and SwMI shall revert to the state that existed prior to the initiating authentication challenge.

4.4.2.1 MSCs for authentication

This clause presents Message Sequence Charts (MSCs) for the authentication protocol to enable the mechanisms described in clause 4.1.

Case	Title	Figure number
1	SwMI authenticates MS	18
2	MS authenticates SwMI	19
3	Authentication initiated by SwMI and made mutual by the MS	20
4	Authentication initiated by MS and made mutual by the SwMI	21
5	SwMI rejects authentication demand from MS	22
6	MS rejects authentication demand from SwMI	23

NOTE: In the MSCs where the timer T354 is explicitly shown it is shown as being terminated by the MS-MM process and not as having expired.

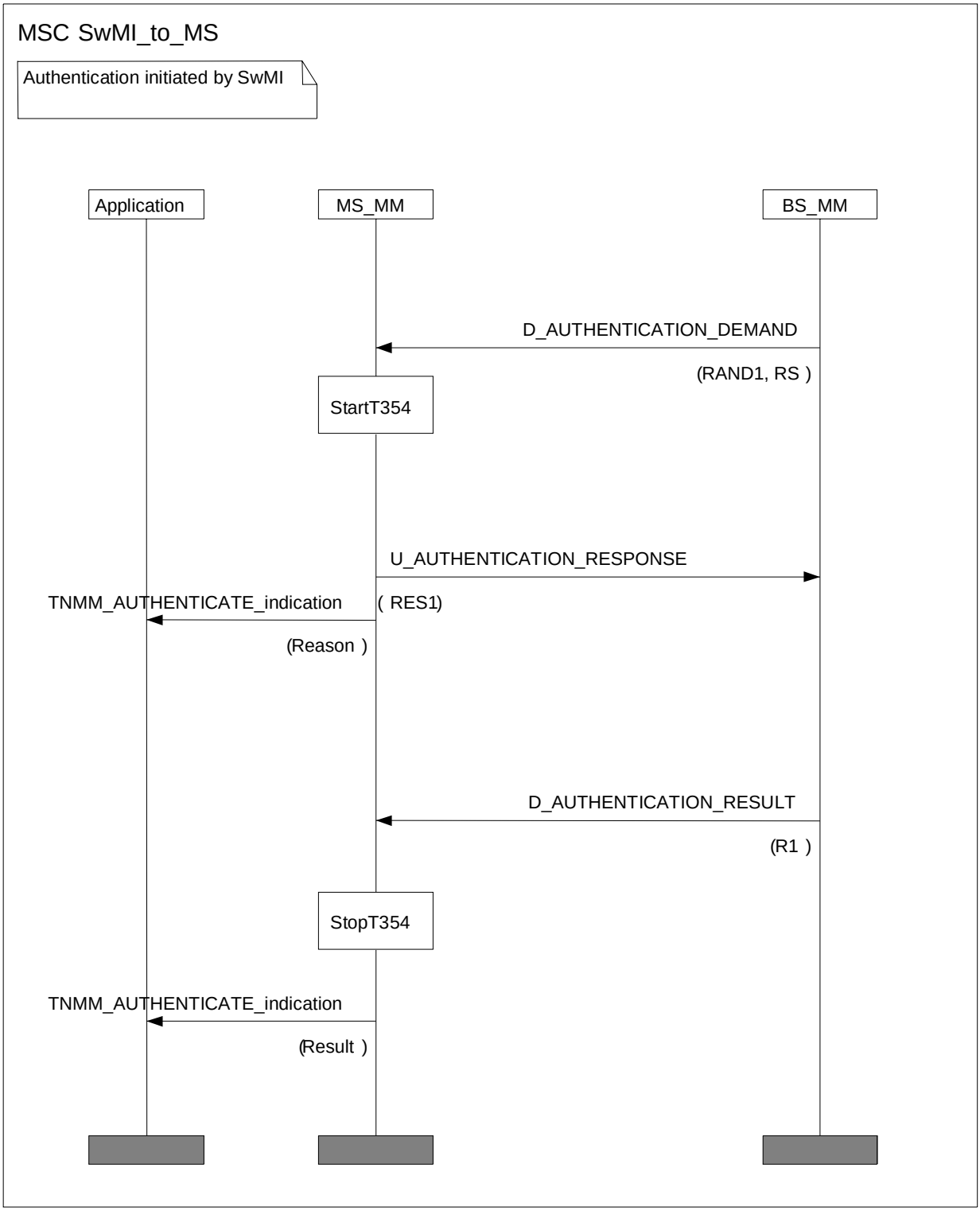


Figure 18: Authentication of MS by SwMI

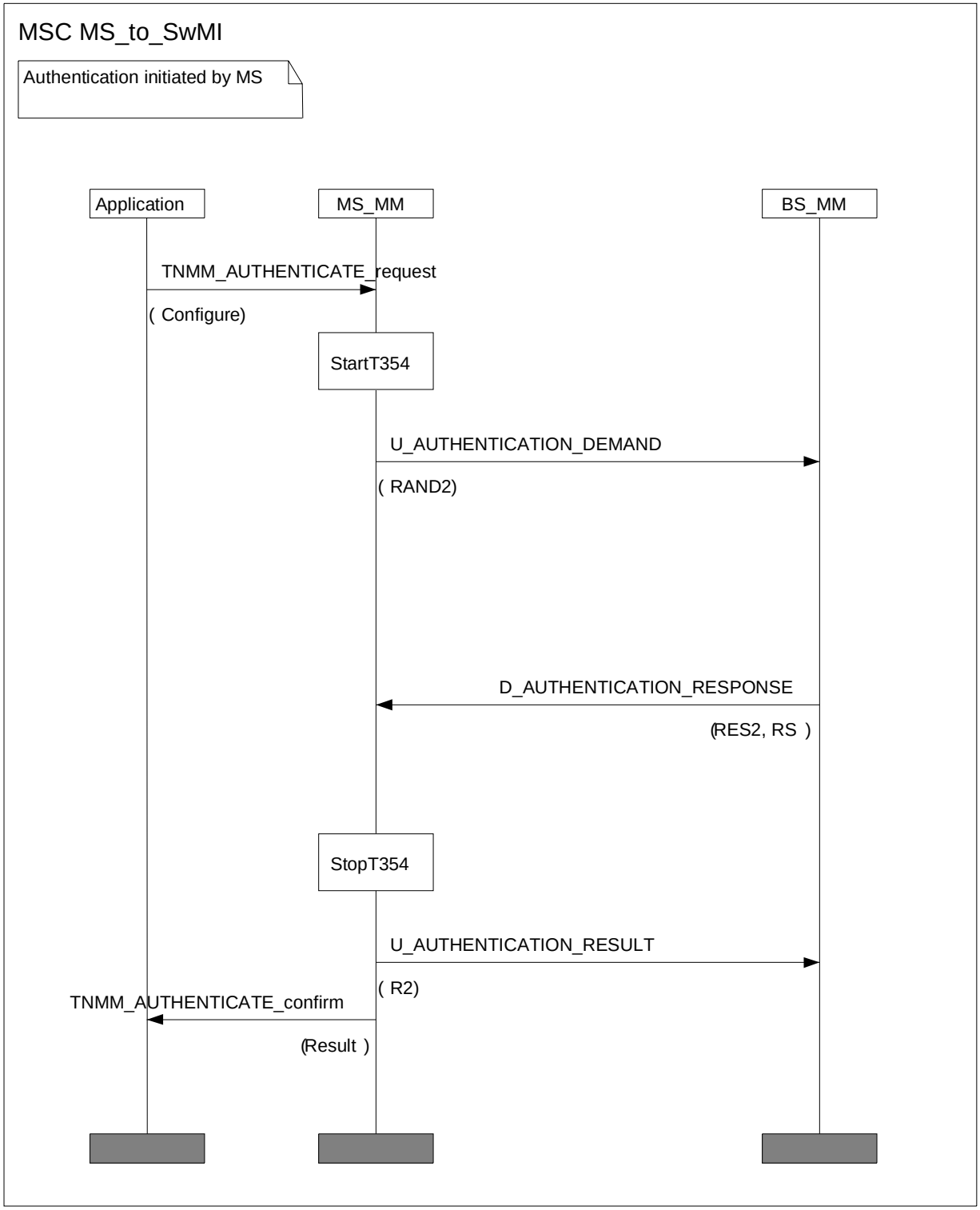


Figure 19: Authentication of the SwMI by the MS

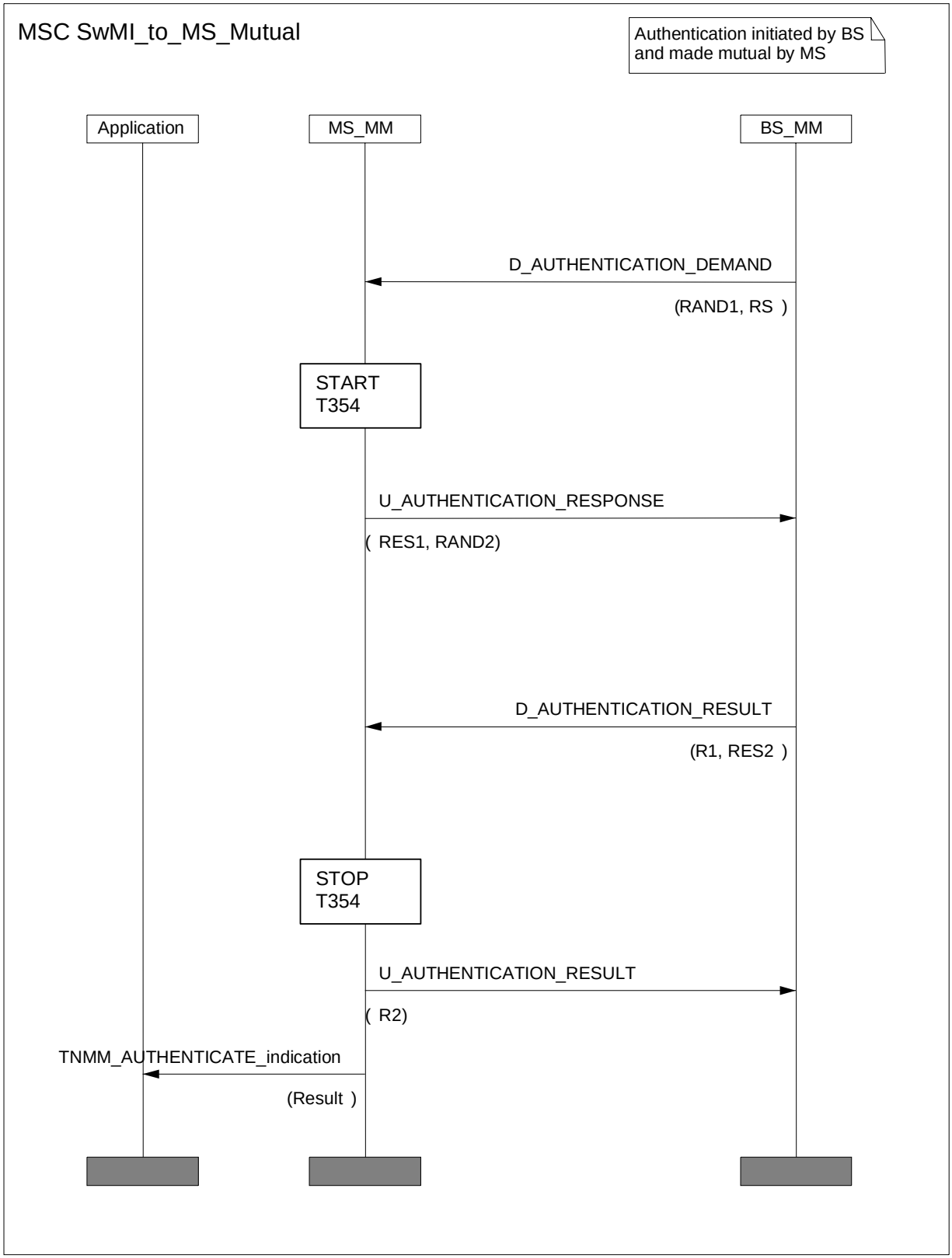


Figure 20: Authentication initiated by SwMI and made mutual by the MS

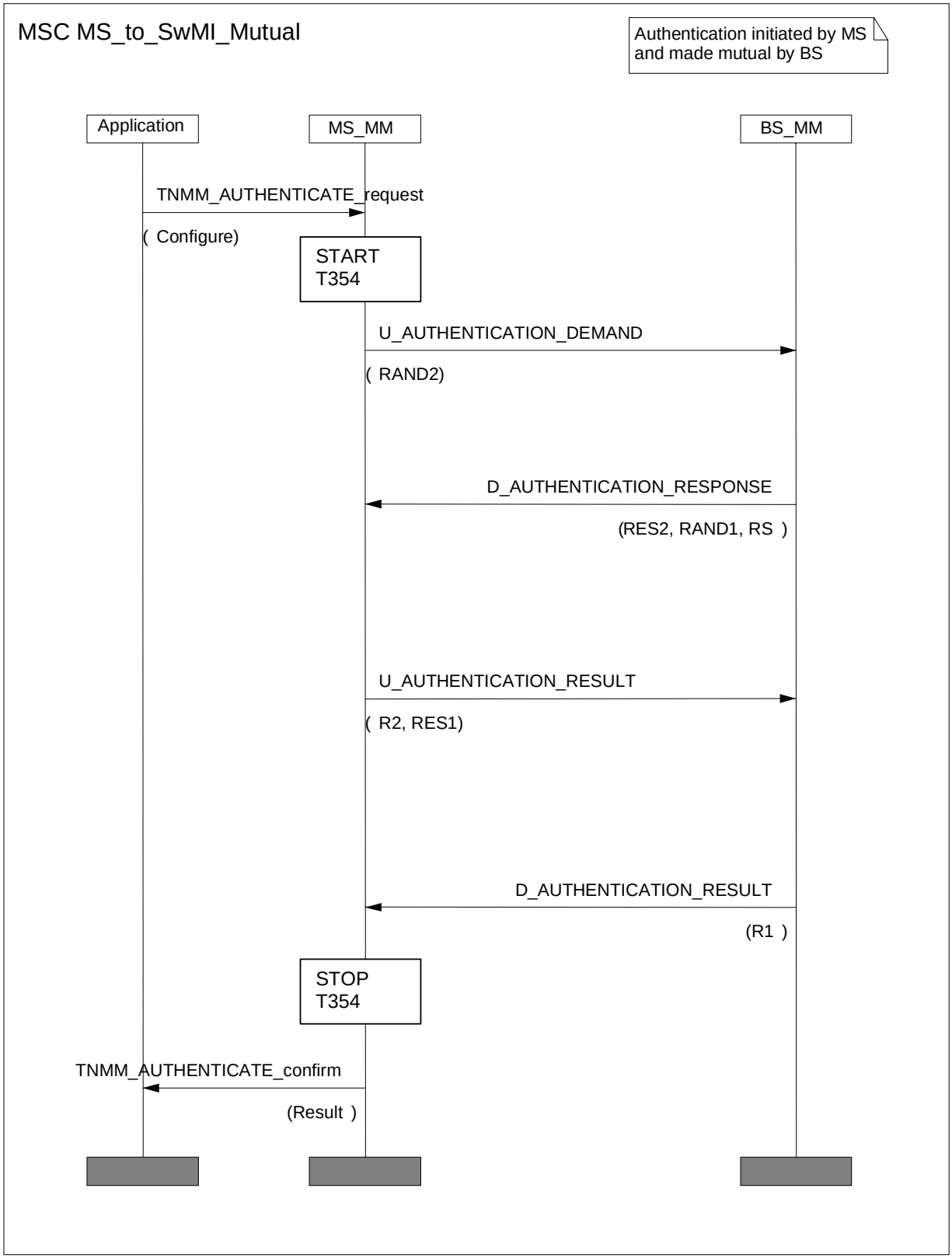


Figure 21: Authentication initiated by MS and made mutual by the SwMI

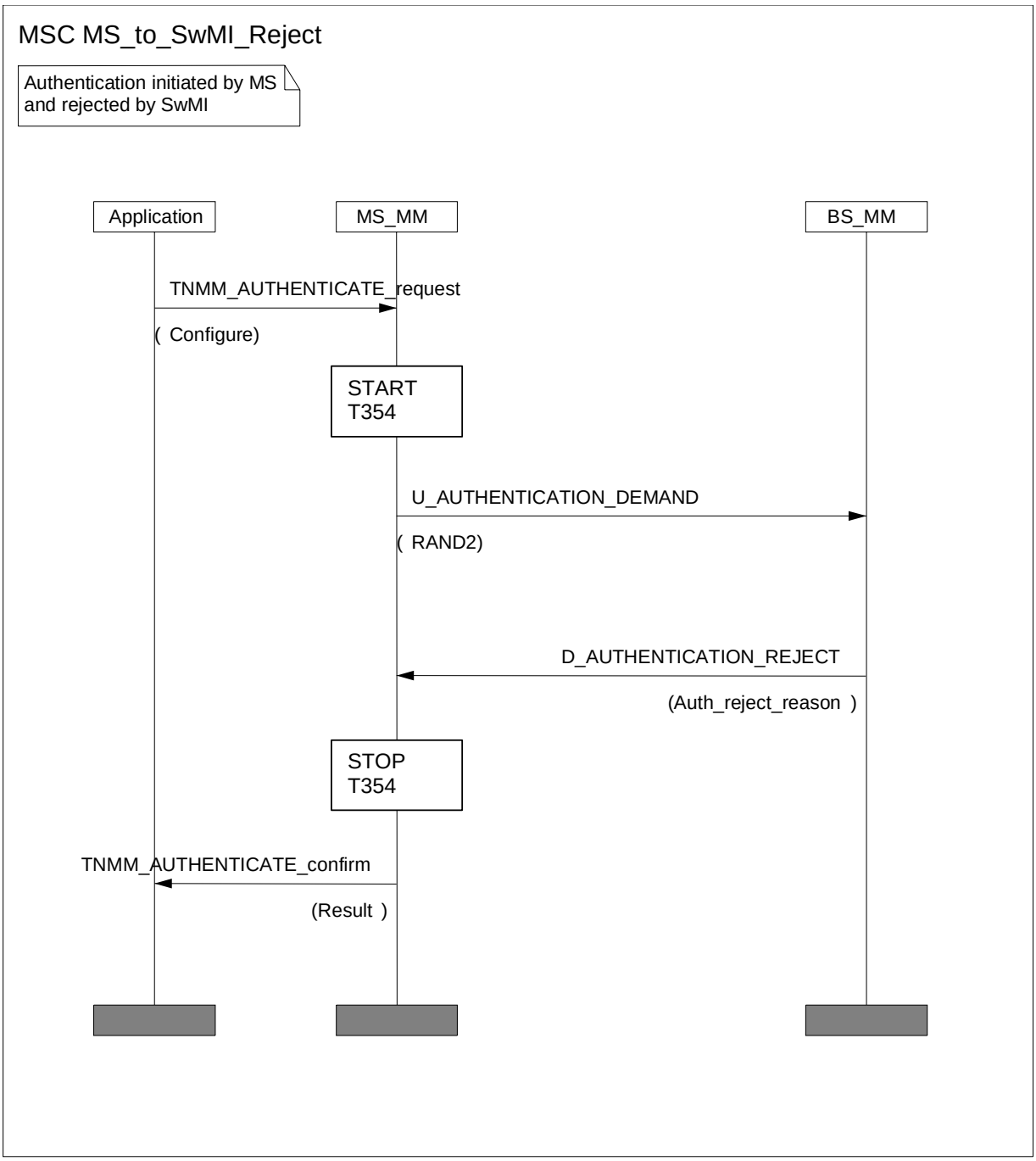


Figure 22: Authentication initiated by MS and rejected by SwMI

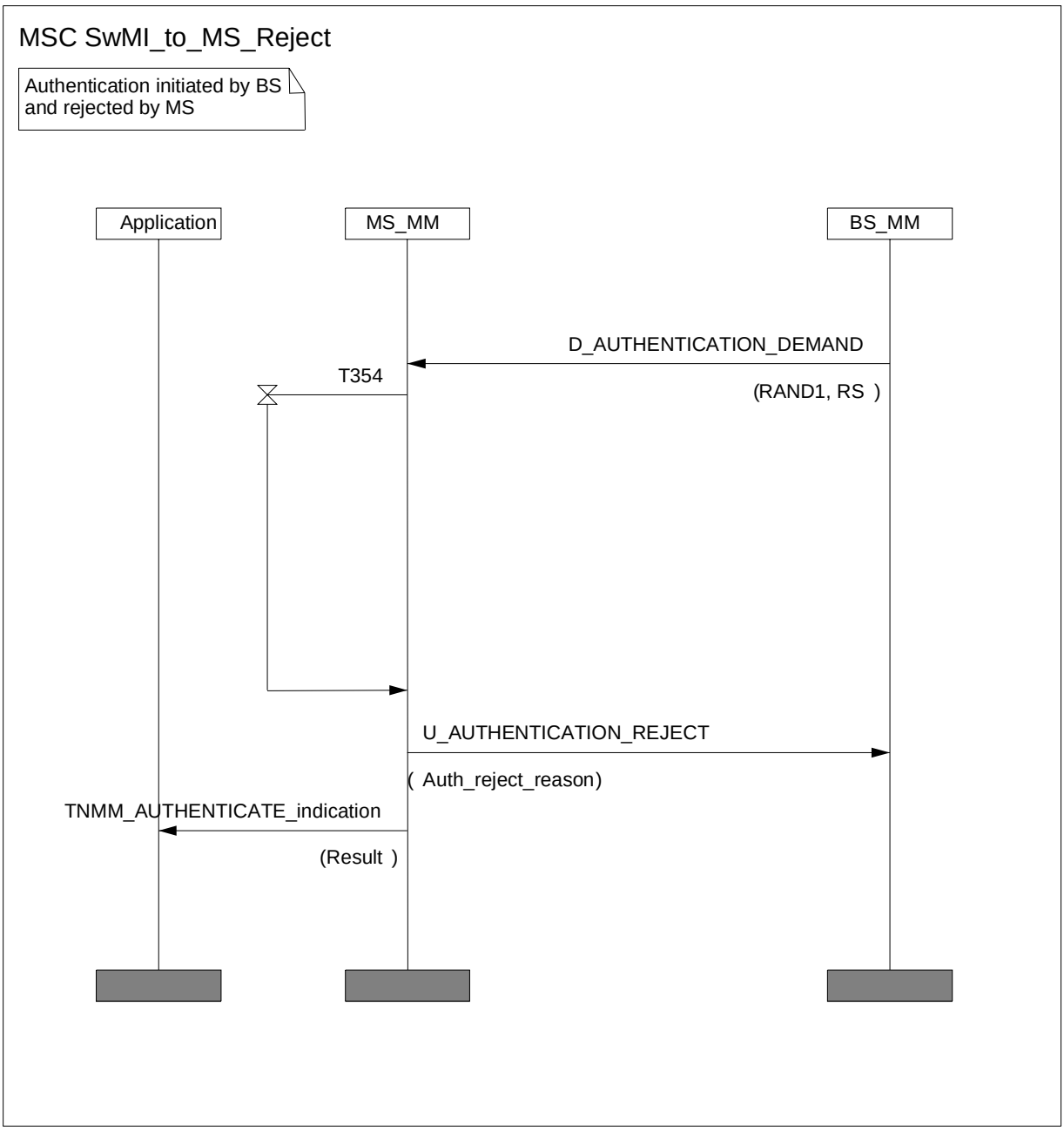


Figure 23: Authentication initiated by SwMI and rejected by MS

4.4.2.2 MSCs for authentication Type-3 element

The type-3 PDU elements Authentication-uplink and Authentication-downlink allow authentication and CK key exchange to be initiated by the MS. The SwMI then is able to provide the CK for the current LA (of which the serving cell is a member) to the registering MS.

The CK key being requested in the Authentication-uplink shall be qualified by the security class field in the ciphering parameters, i.e:

- if the MS requests the CK in the Authentication-uplink, and the ciphering parameters indicate security class 2, then the SwMI shall infer that the MS is requesting the SCK;
- if the MS requests the CK in the Authentication-uplink, and the ciphering parameters indicate security class 3, then the SwMI shall infer that the MS is requesting the CCK.

When the SwMI provides CK information in the Authentication-downlink, the SwMI may provide additional CK material as well as that originally requested in the Authentication-uplink, i.e:

- if the MS requests the CCK in the Authentication-uplink, the SwMI may provide the CCK and the SCK in the Authentication-downlink;
- if the MS requests the SCK in the Authentication-uplink, the SwMI may provide the SCK and the CCK in the Authentication-downlink.

The Authentication-downlink may also contain a demand for the MS to provide its TEI. It is recommended that this option is used only if encryption is applied (i.e. in class 2 and class 3 systems).

In class 3 systems using authentication in combination with location update using the type-3 elements described the new DCK cannot be used until the location update protocol has been successfully completed.

This clause shows the message sequence charts for the following cases:

- MS initiated location update request with embedded CK request and SwMI CK provision;
- MS initiated location update request with embedded Authentication challenge;
- SwMI initiated TEI provision request.

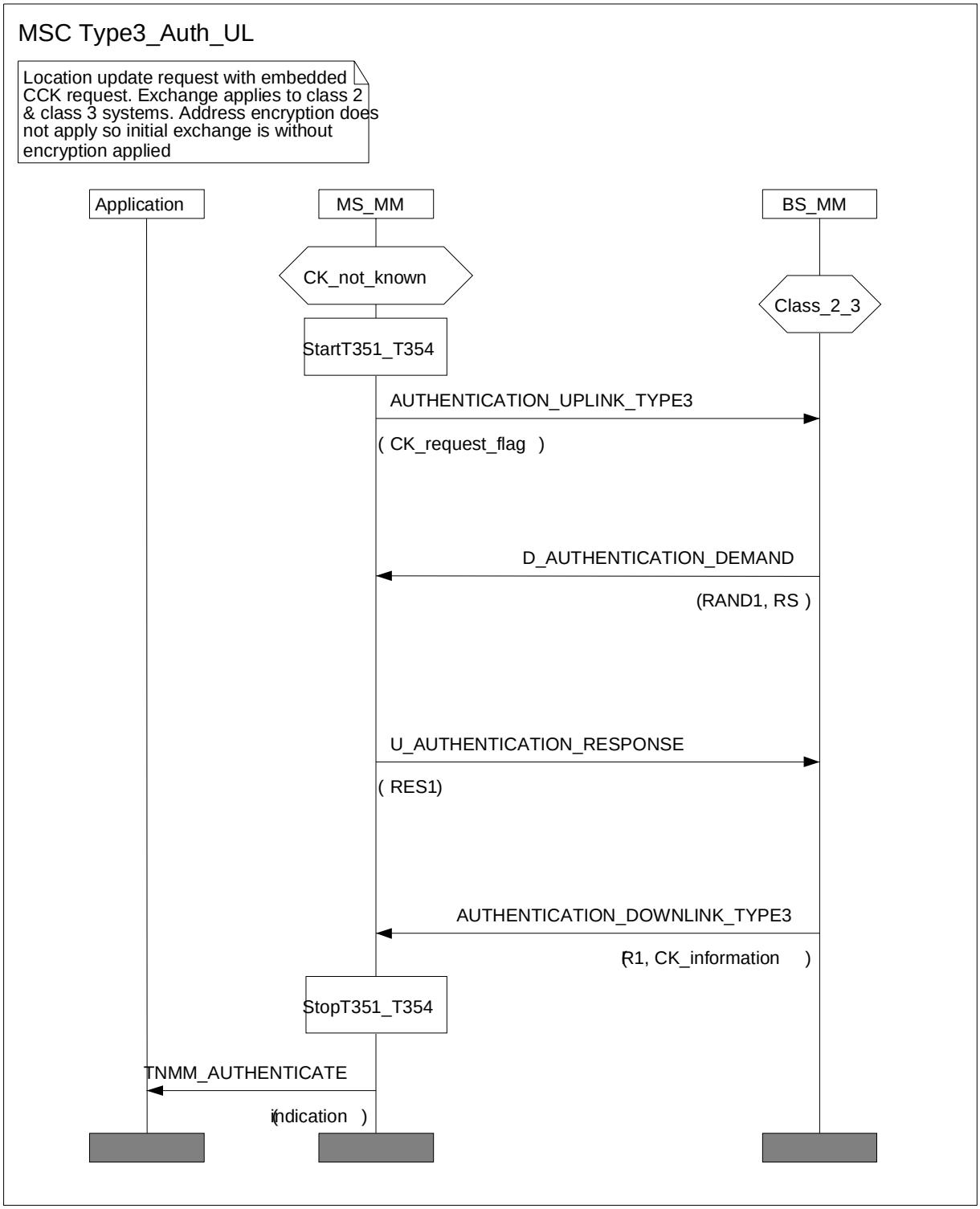


Figure 24: CK provision request during location update with authentication applied by SwMI

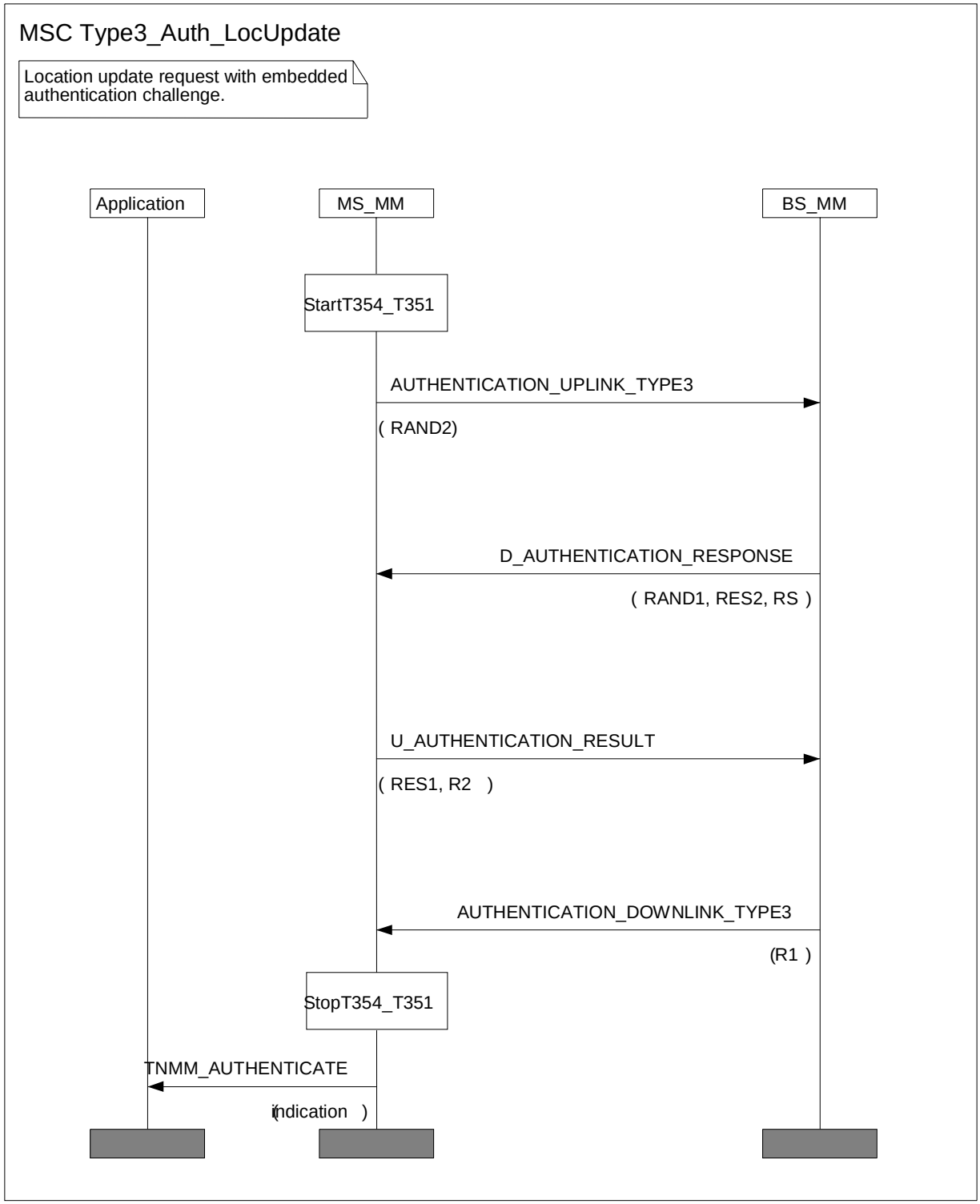


Figure 25: Location update request with embedded authentication challenge

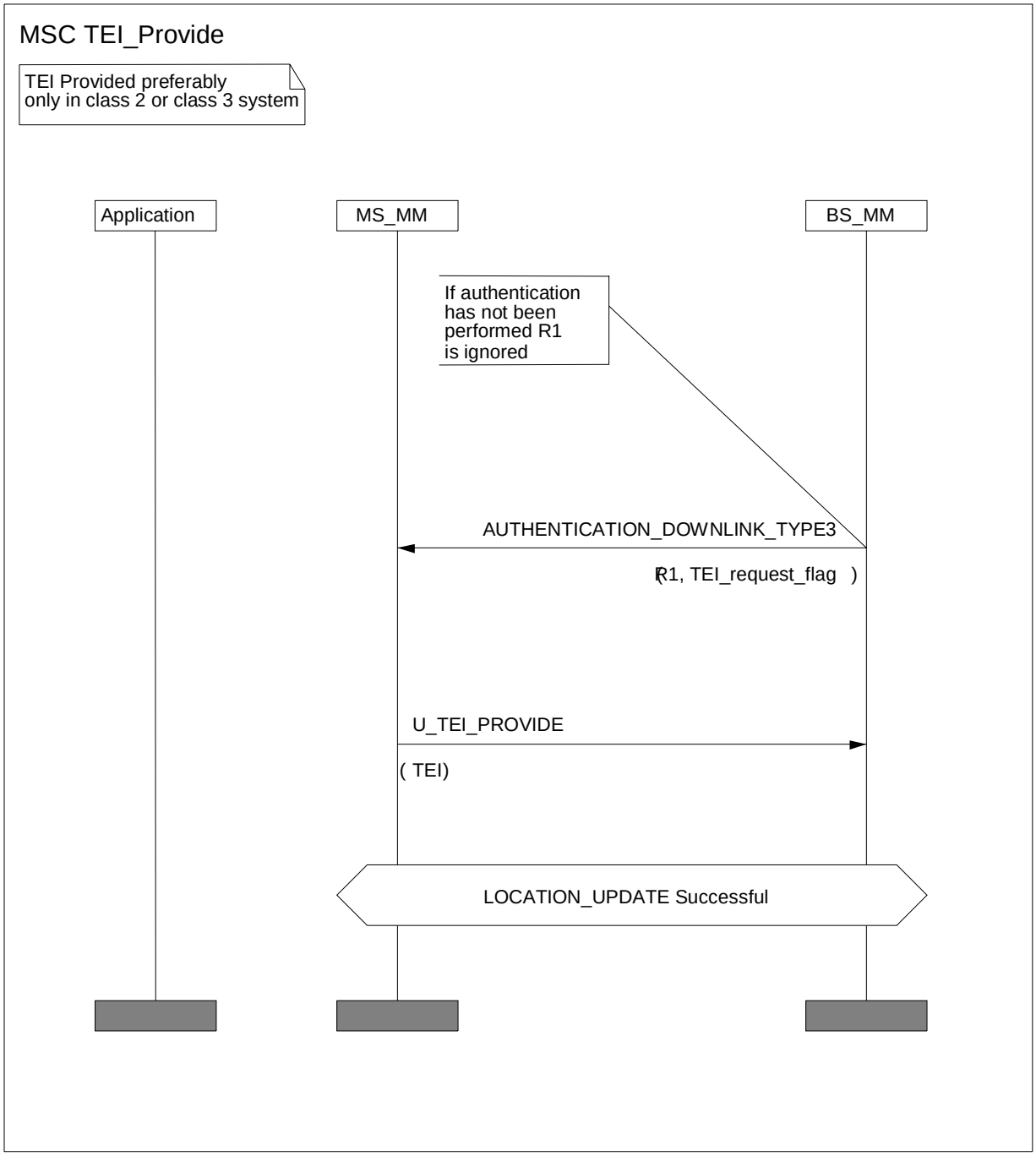


Figure 26: TEI Provision in class 2 or 3 system

4.4.2.3 Control of authentication timer T354 at MS

Where authentication occurs embedded within a registration exchange then timer T351 (registration timer) shall be treated as T354 (authentication timer) and the rules below shall not be followed but overridden by the rules for T351 found in EN 300 392-2 [2].

The timer shall be started under the following conditions:

- on sending of U-AUTHENTICATION DEMAND;
- on receipt of D-AUTHENTICATION DEMAND; and,
- on sending of U-LOCATION UPDATE DEMAND containing an Authentication challenge in the type-3 element "Authentication uplink". In this case the value of T354 shall be the same as T351 and only one of these timers needs to be started.

The timer shall be stopped (cancelled) under the following conditions:

- on receipt of D-AUTHENTICATION RESULT for SwMI initiated unilateral authentication, and for authentication initiated by the MS but made mutual by the SwMI;
- on sending of U-AUTHENTICATION RESULT for MS initiated unilateral authentication, and for authentication initiated by the SwMI but made mutual by the MS;
- on sending of U-AUTHENTICATION REJECT;
- on receipt of D-AUTHENTICATION REJECT; and
- on receipt of D-LOCATION UPDATE ACCEPT containing the type-3 element "Authentication downlink".

NOTE: The behaviour of T354 in the SwMI has to be set to ensure correct MS operation.

4.5 OTAR Protocols

4.5.1 CCK delivery - protocol functions

The CCK delivery functions described in this clause shall only apply to class 3 mobiles and cells.

CCK is a cipher key linked to the use of Air Interface encryption with DCK. This clause describes the key management protocols used to support the algorithms and mechanisms described in clause 4.2.3. CCK is required prior to enabling encrypted air interface services on a cell as it is linked to the ESI mechanism used for layer 2 addressing (see clause 4.2.6).

CCK shall be delivered over the air interface using the mechanisms and protocols described in this clause, and by the registration and authentication procedures defined in clause 4.4.2.

When scanning a cell prior to registration an MS shall receive the CCK-id and LA-id of the CCK in use on that cell in the SYSINFO broadcast. If the CCK so identified is not known to the MS it shall request the CCK either through its current serving cell or at the new cell using the protocols defined in the present document.

The SwMI can deliver to all registered users a CCK for future use.

When delivering a CCK the SwMI shall indicate the LAs for which the CCK is valid. This may be in the form of a list of LAs, a bit mask of LA identities, a range of LA identities, or it may be applied to all LAs. When sending CCK by a list the list shall include the corresponding LA identity.

The LA selector and mask mechanism is intended to find if the CCK applies to the current LA. To achieve this the mask is logically ANDed with the LA-id received from the SwMI in the broadcast parameters. If the result is equal to the selector, then CCK is valid for the current LA-id.

The CCK may be provided explicitly by the SwMI using the "D-OTAR CCK Provide" PDU, the "D-OTAR NEWCELL" PDU, or may be provided during the registration procedure using the MM type 3 element "Authentication downlink".

An MS may explicitly request a CCK from the SwMI using the "U-OTAR CCK Demand" PDU, or the "U–OTAR PREPARE PDU", or CCK may be requested during the registration procedure using the MM type 3 element "Authentication uplink".

When an MS is authenticated and requests CCK within the location update seqeuence, then the DCK that is generated in the authentication exchange shall be used to seal the provided CCK(s).

4.5.1.1 SwMI-initiated CCK provision

This scenario shows how the SwMI can distribute new CCK information. The SwMI can initiate CCK provision at any time. The SwMI may provide the CCK of the current cell or the CCK of any other cell. The LAs for which the CCK is valid are always identified in the D-OTAR CCK Provide PDU in the CCK information element.

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

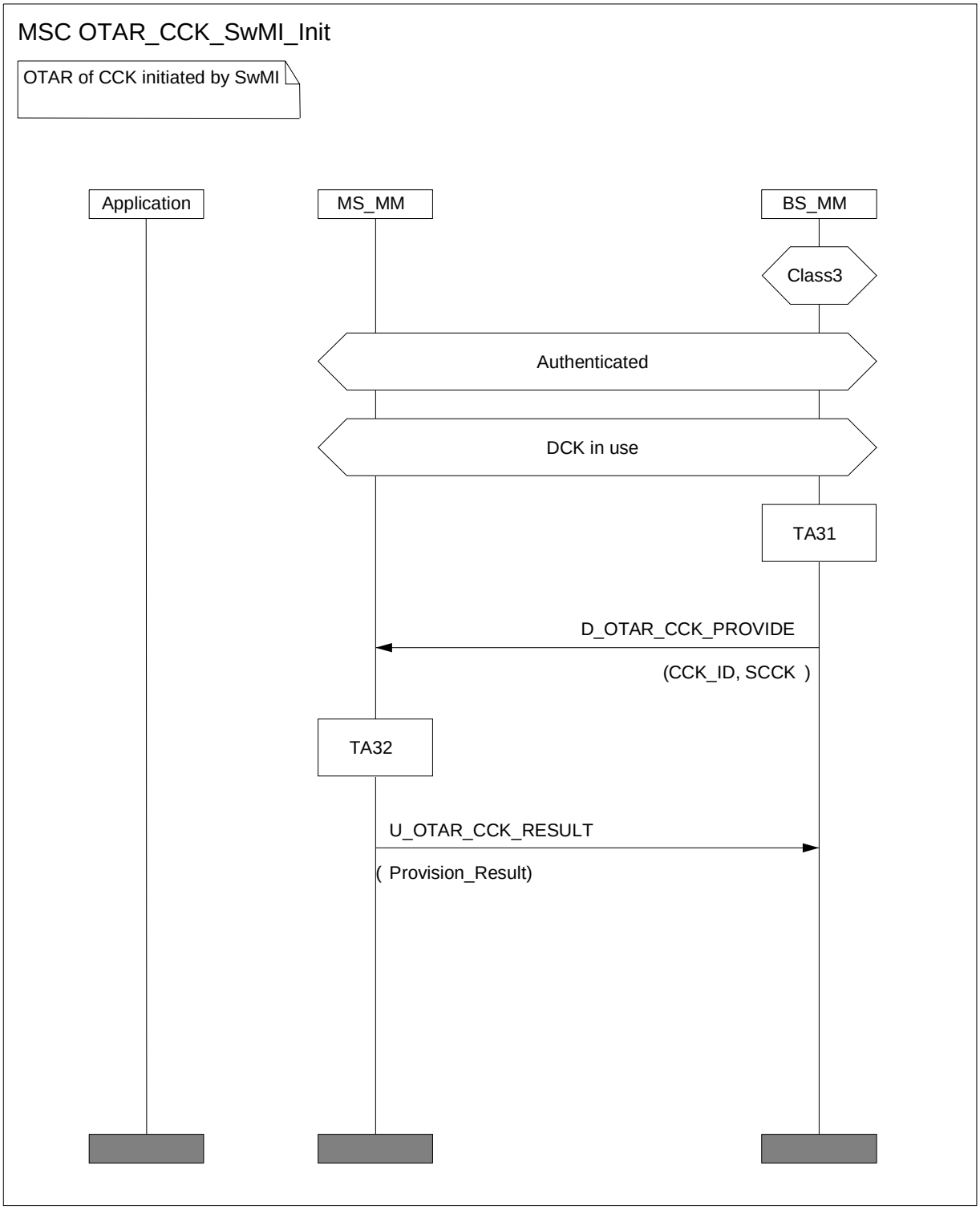


Figure 27: SwMI-initiated CCK provision

4.5.1.2 MS-initiated CCK provision with U-OTAR CCK Demand

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

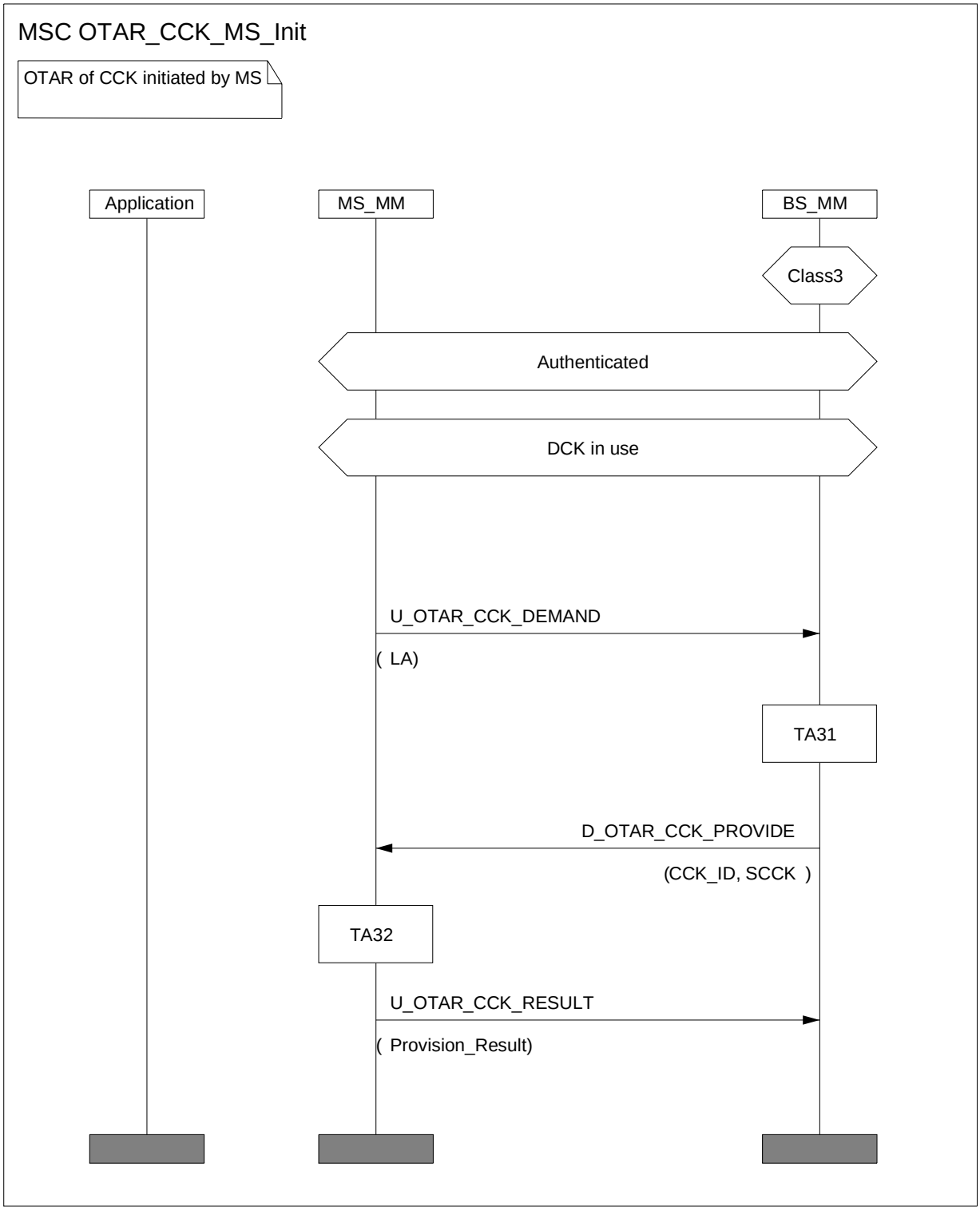


Figure 28: MS-initiated CCK provision

4.5.1.3 MS-initiated CCK provision with announced cell reselection

Whilst the primary use of the U-PREPARE PDU is to allow call restoration when moving between cells it may also be used by an MS to request the CCK for the new cell, or to forward register to a new cell using the announced type 1 cell re-selection mechanism. In order to support encrypted cell change to class 3 cells the U-PREPARE PDU may carry an U-OTAR CCK Demand PDU.

For announced type 1 cell reselection where the CCK of the new cell is required two options exist:

1) MS forced to register:

   the CK request for CCK information shall be sent in the U-LOCATION UPDATE DEMAND PDU carried by the U-PREPARE PDU;

2) MS not forced to register:

   the CCK request shall be sent in the U-OTAR CCK Demand PDU carried by the U-PREPARE PDU.

Case 1: New cell is in same LA and same registered area

MS shall assume that the current values of CCK and DCK will be valid on new cell. U-PREPARE shall contain no MM PDUs.

Case 2: New cell is in different LA but same registered area

Before roaming to a new cell the MS may request the CCK of the new cell from its current serving cell by sending U-OTAR CCK with LA = LA of new cell. The U-OTAR CCK Demand PDU may be sent in the U-PREPARE PDU, in case MS is allowed to make the announced cell re-selection. The MS shall assume that DCK is valid in the new cell.

The SwMI shall supply the CCK of the requested LA using the D-OTAR CCK Provide PDU, which may be contained in the D-NEW CELL PDU, or it may inform the MS that provision is not possible.

Case 3: New cell is in different LA and different registered area

For roaming between cells of class 3 only using announced type 1 cell reselection, the MS shall send U–PREPARE with U-LOCATION UPDATE DEMAND and CK request for CCK information (if needed). If the new cell accepts the registration the SwMI shall ensure that the new serving cell, and the LA to which it belongs, has DCK of the roaming ITSI. The acceptance of the registration shall be contained in D-NEW-CELL containing D–LOCATION UPDATE ACCEPT and the CCK information of the new cell if requested.

For roaming to cells of class 3 only using announced type 2 cell reselection, the MS may send U-PREPARE with a CCK request (using U-OTAR CCK Demand). If the new cell accepts the cell reselection the MS shall assume that the new serving cell, and the LA to which it belongs, has DCK of the roaming ITSI. The acceptance of the cell reselection shall be contained in D-NEW-CELL which, if requested, may contain the CCK information of the new cell (using D-OTAR CCK Provide).

See also clause 6.6 for change of class on moving between cells.

4.5.2 OTAR protocol functions - SCK

Up to four 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 clauses.

4.5.2.1 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 29 that shows the invocation of algorithms at each of MS and BS to satisfy the request.

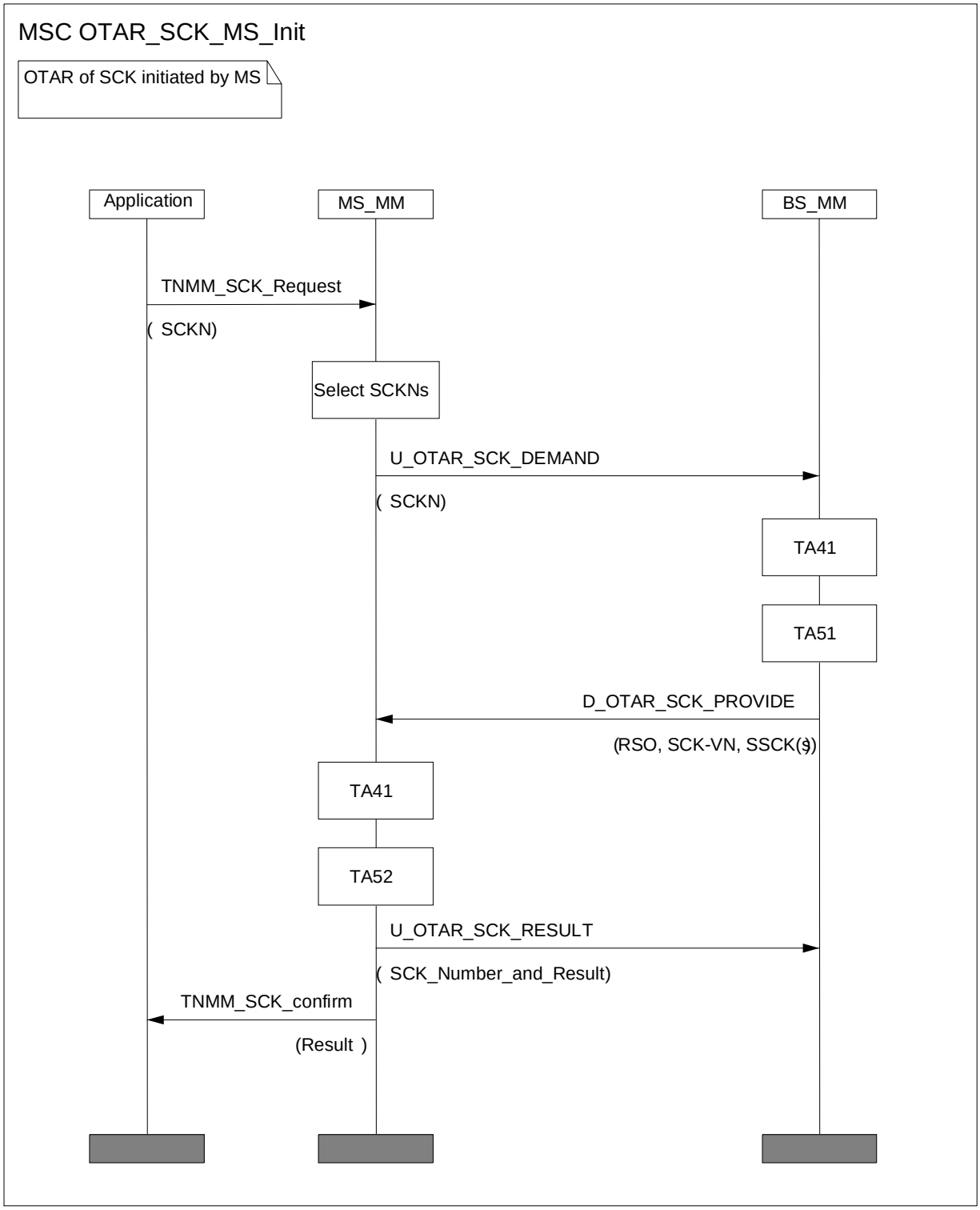


Figure 29: SCK delivery initiated by MS to an individual

4.5.2.2 SwMI provides SCK(s) to individual 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 30.

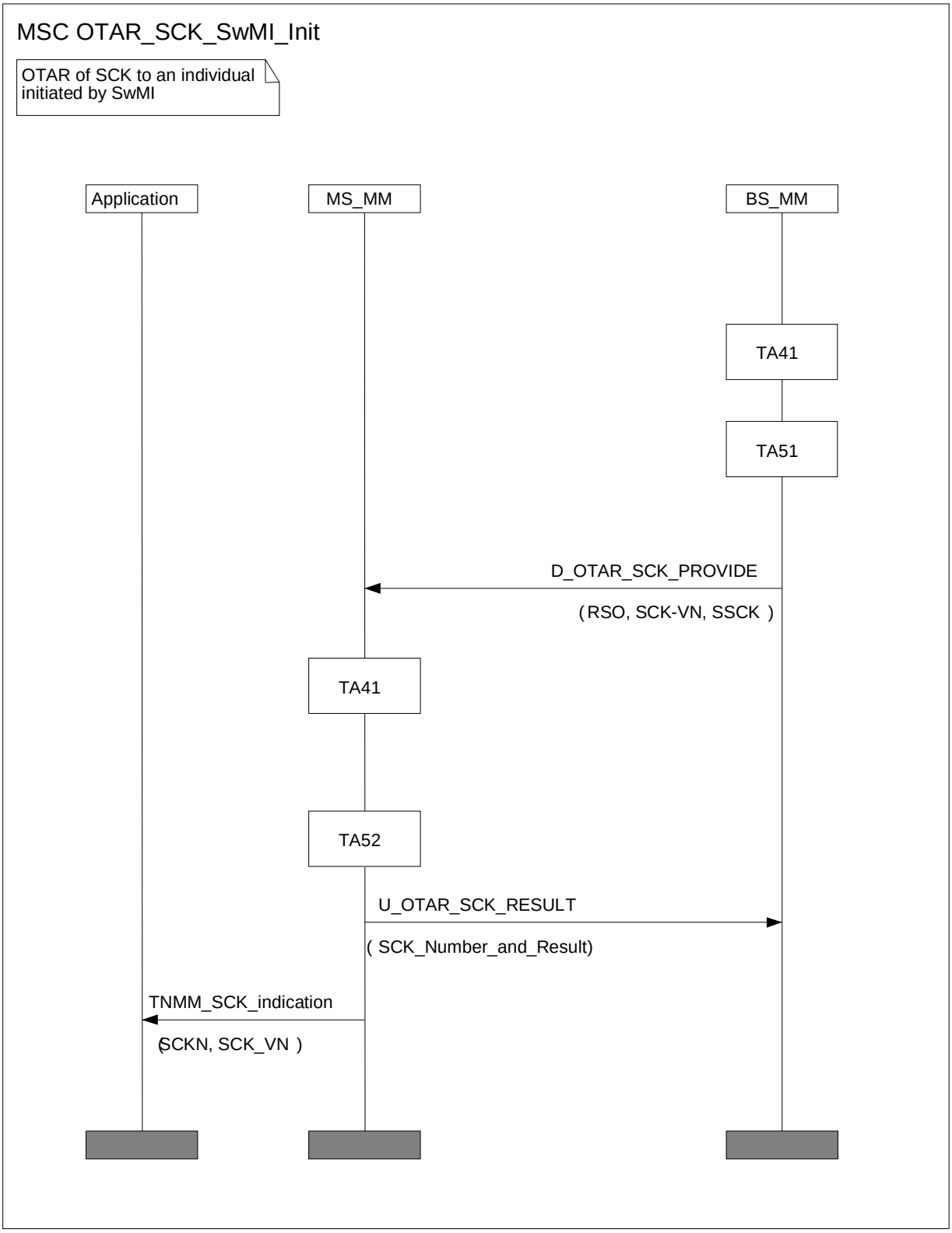


Figure 30: SCK delivery to an individual initiated by SwMI

4.5.2.3 SwMI provides SCK(s) to group of MSs

In the case of group addressed delivery of SCK, BS_MM and MS_MM shall not run TA41, but shall use EGSKO as input to TA51 and TA52. The U-OTAR SCK RESULT shall be sent from MS to SwMI following the expiry of random timer T371. T371 is started on reception of the D-OTAR SCK PROVIDE.

T371 is a timer with a value randomized to fall within the range 1s and 65535s (18,2 hours). The MS shall select a value in this range when setting T371. When T371 expires the MS shall wait a further random number of random access signalling slots before sending the U-OTAR SCK RESULT PDU. The procedure for randomly selecting the signalling slot shall follow the procedure for "Choosing from a new access frame" as defined in EN 300 392-2 [2] clause 23.5.1.4.6.

This scenario shows the case where the SwMI provides one or more SCK(s) to a group of MSs identified by GTSI. The SwMI may initiate this procedure at any time.

The normal message sequence in this case shall be according to figure 31.

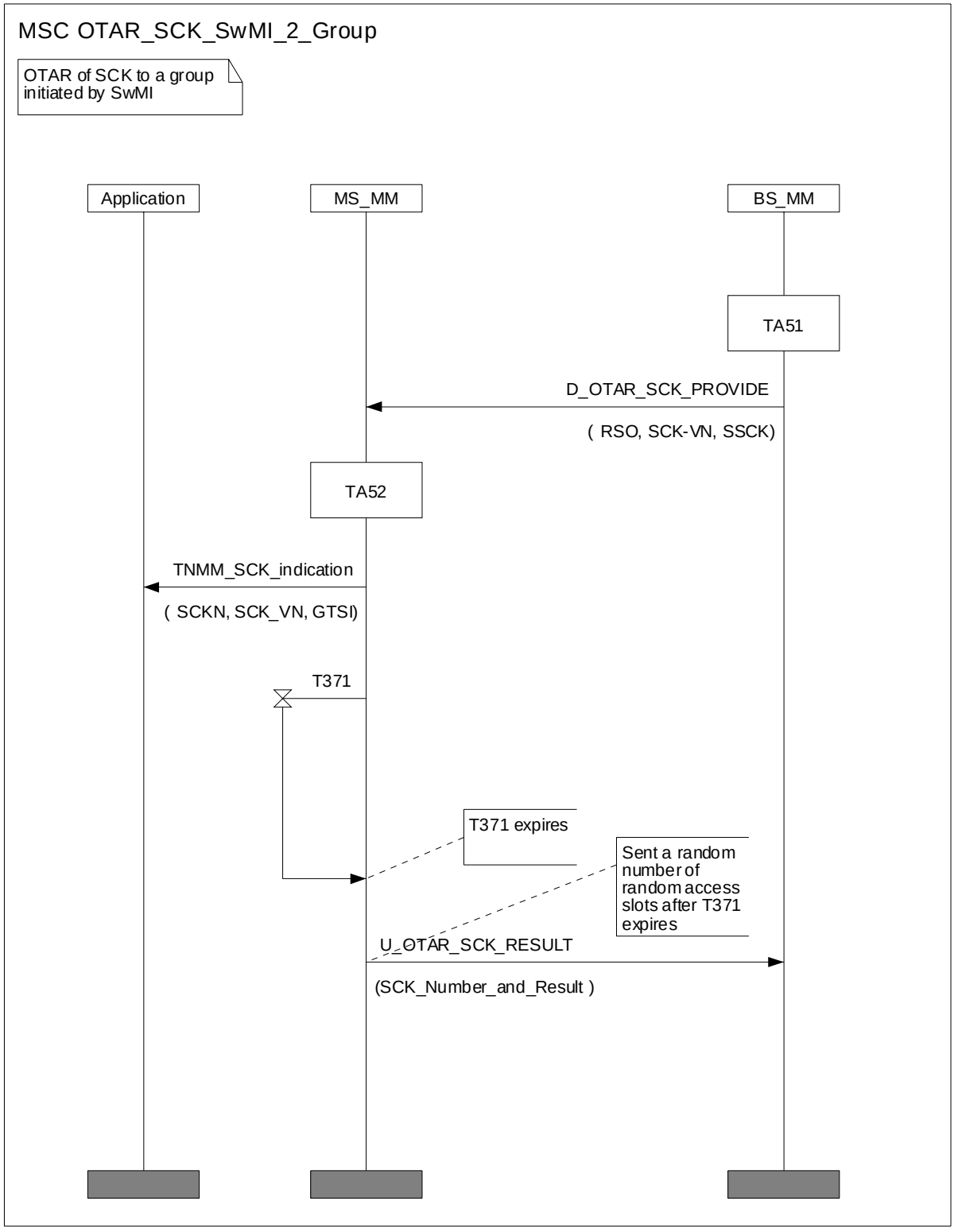


Figure 31: SCK delivery to a group initiated by SwMI

4.5.3 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 clauses.

4.5.3.1 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 MS may request GCK either by GCKN, or by GTSI. In each case the SwMI shall generate RSO and KSO, the latter shall be used to seal the key.

The normal message sequence in this case shall be according to figure 32.

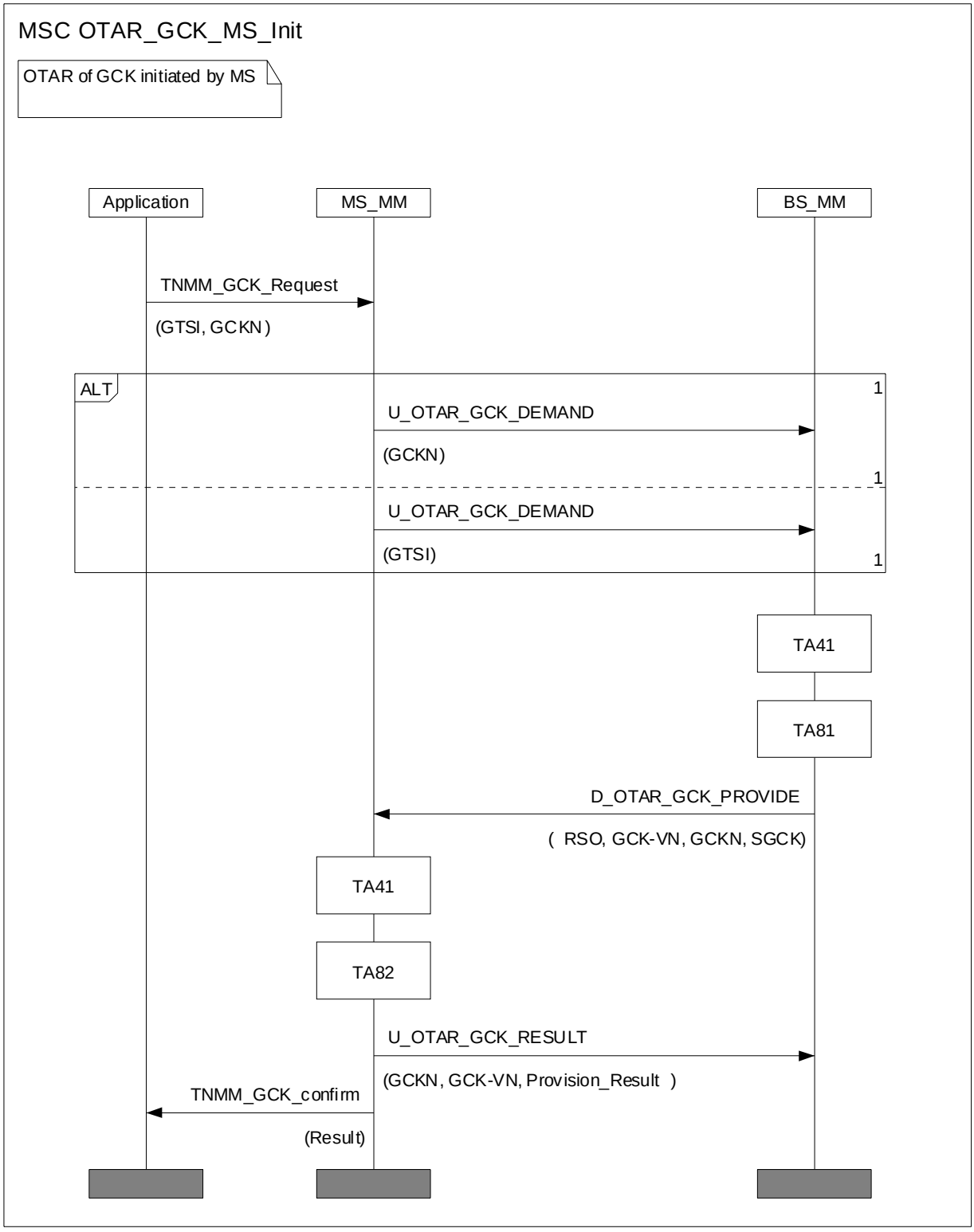


Figure 32: GCK delivery initiated by MS to an individual

4.5.3.2 SwMI provides GCK to an individual 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 GCK shall not be enabled until after the D-CK CHANGE DEMAND PDU has been received.

The normal message sequence in this case shall be according to figure 33.

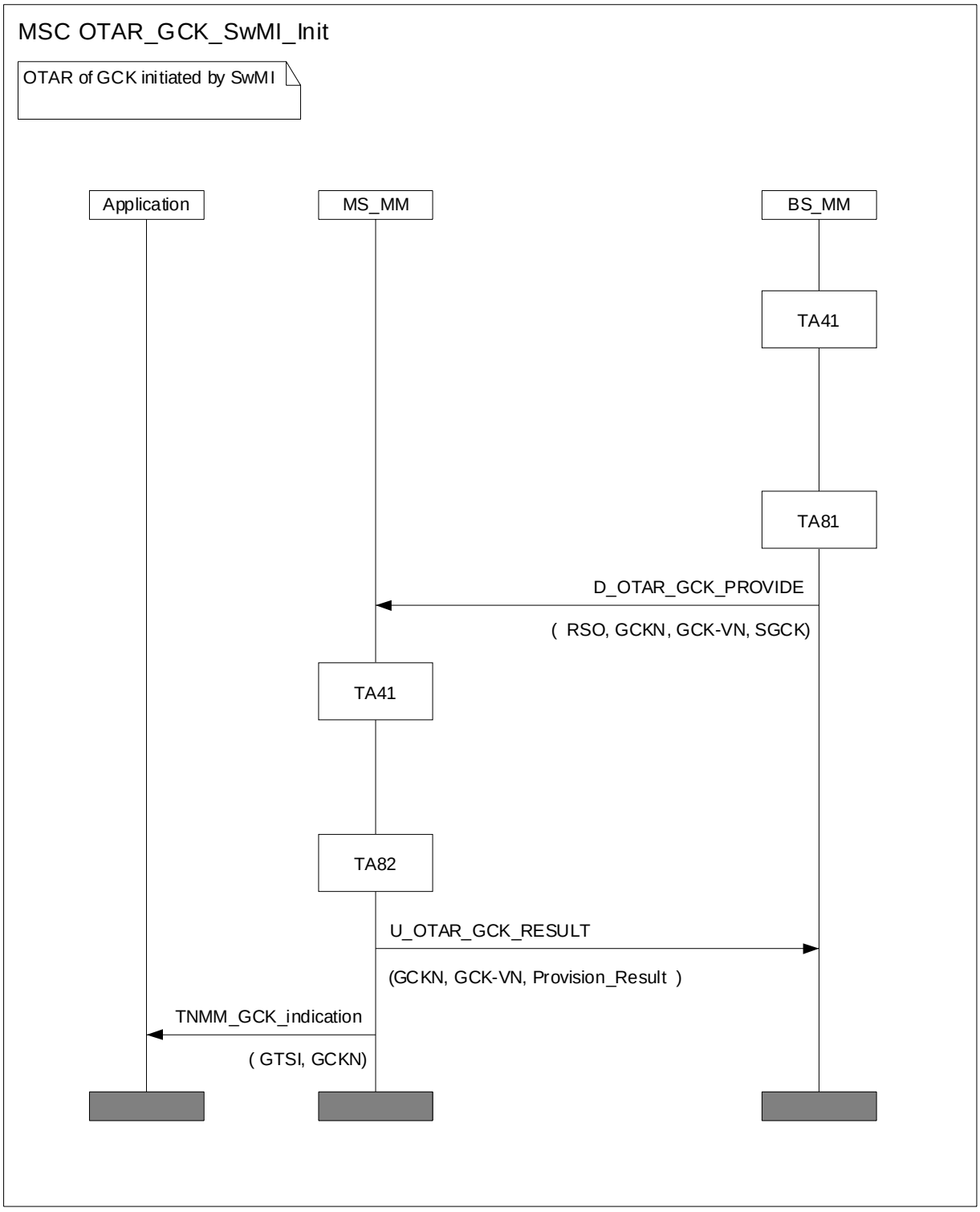


Figure 33: GCK delivery initiated by SwMI to an individual

4.5.3.3 SwMI provides GCK to a group of MSs

In the case of group addressed delivery of GCK, BS_MM and MS_MM shall not run TA41, but shall use EGSKO as input to TA81 and TA82. The U-OTAR GCK RESULT shall be sent from MS to SwMI following the expiry of random timer T371. T371 is started on reception of the D-OTAR GCK PROVIDE.

T371 is a timer with a value randomized to fall within the range 1s and 65535s (18,2 hours). The MS shall select a value in this range when setting T371. When T371 expires the MS shall wait a further random number of random access signalling slots before sending the U-OTAR GCK RESULT PDU. The procedure for randomly selecting the signalling slot shall follow the procedure for "Choosing from a new access frame" as defined in EN 300 392-2 [2] clause 23.5.1.4.6.

The normal message sequence in this case shall be according to figure 34.

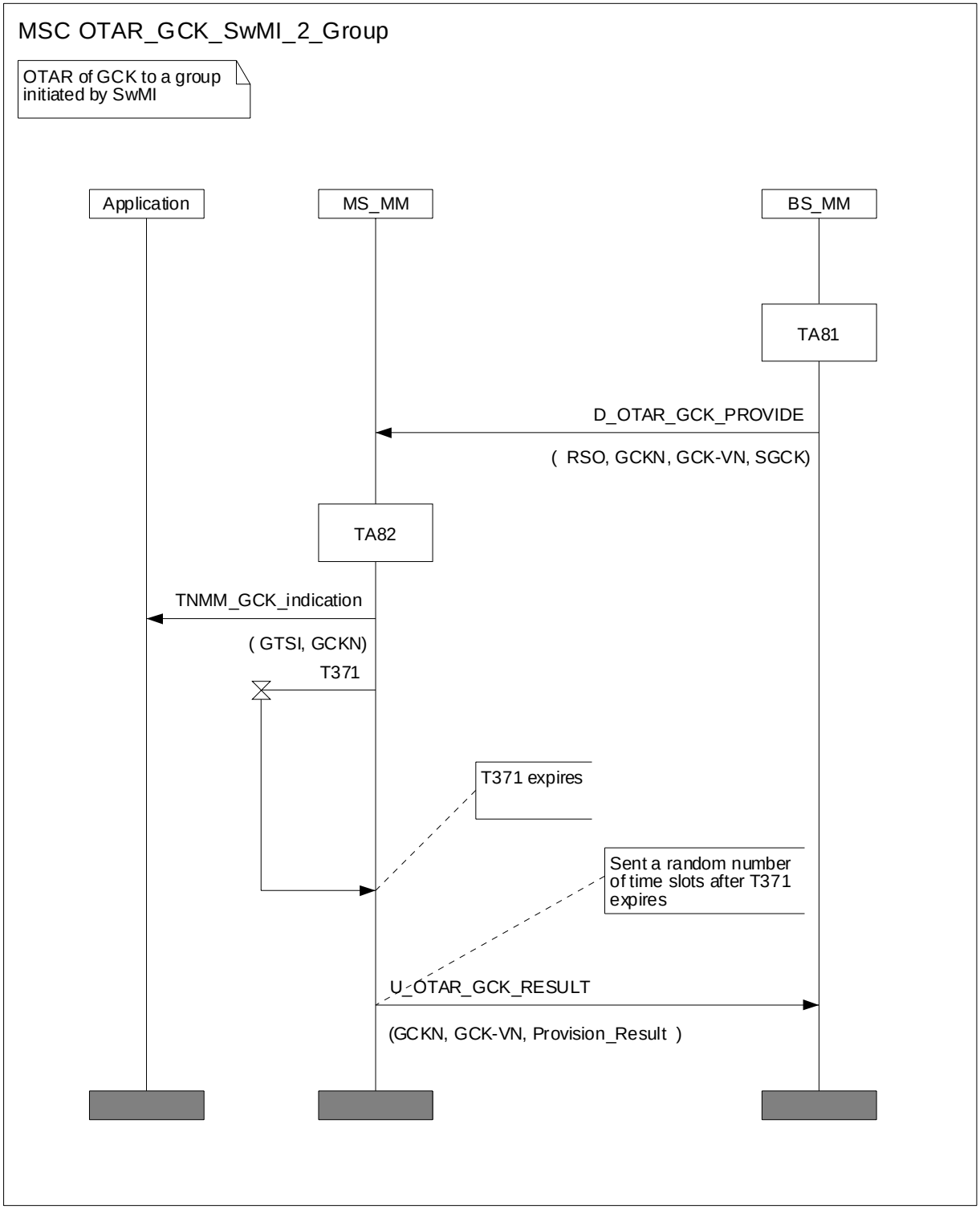


Figure 34: GCK delivery to a group initiated by SwMI

4.5.4 Cipher key association to group address

4.5.4.1 SCK association for DMO

The OTAR KEY ASSOCIATE protocol exchange allows the SwMI to make links between keys and addresses.

The SwMI may request that the MS associates a particular SCK (identified by SCKN) with up to 31 groups (identified by the 'Number of groups' element of the PDU) for which the GSSI of each is listed. In this case the key-type element of the D-OTAR KEY ASSOCIATE DEMAND shall be set to SCK.

The SwMI may also demand that groups may be associated to SCKs by groups of MSs. In this case, the D-OTAR KEY ASSOCIATE DEMAND PDU is addressed to the group of MSs. If the Acknowledgement Flag element is set to indicate acknowledgement required, the MS shall start random timer T371 on reception of D-OTAR KEY ASSOCIATE DEMAND and send the U-OTAR KEY ASSOCIATE STATUS on expiry of T371. T371 is described in clause 4.5.2.3.

The normal message sequence in this case shall be according to figure 35.

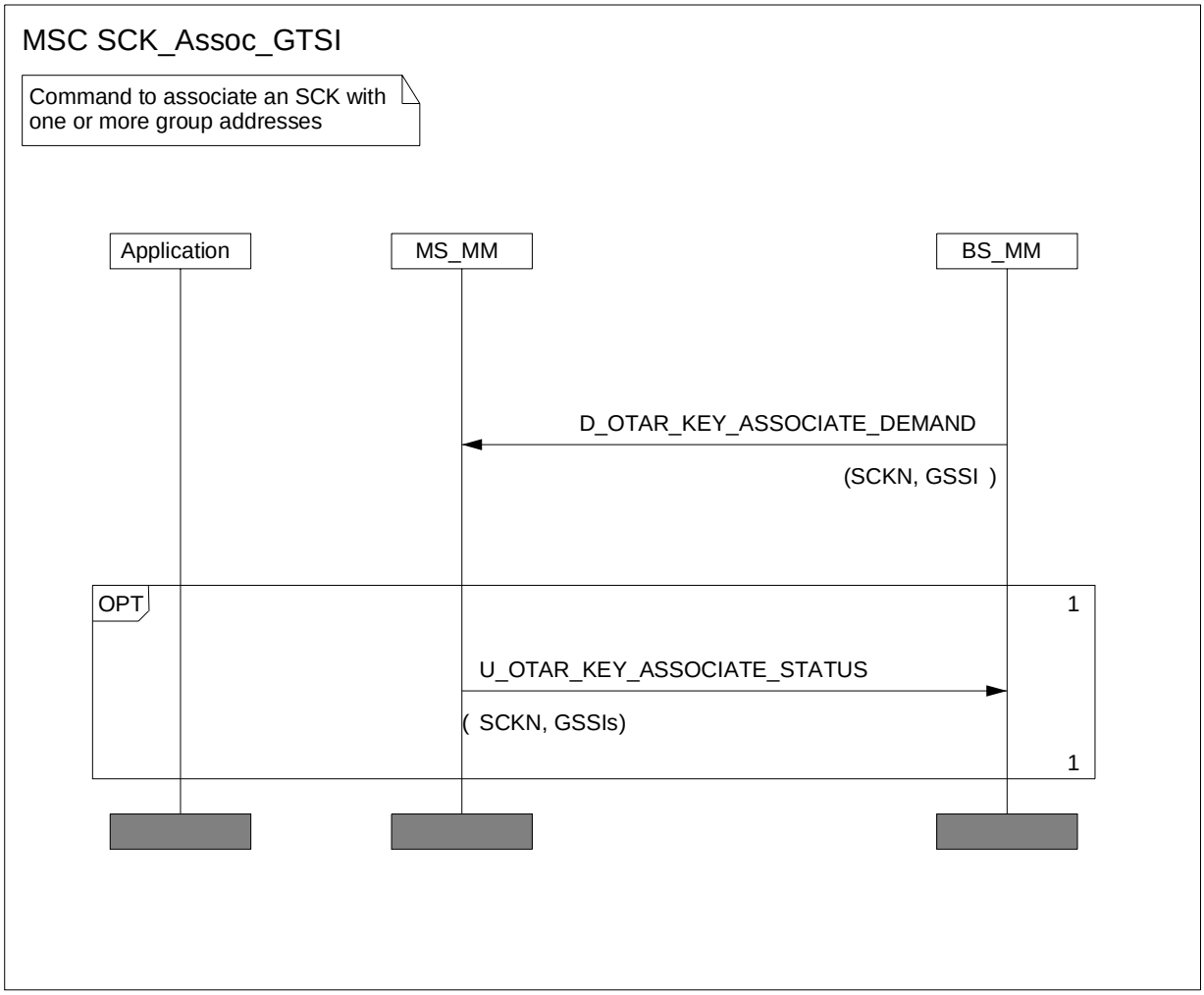


Figure 35: SCK association by SwMI

The SwMI may demand that the SCKs currently associated with the groups are disassociated forcing the groups to revert to clear operation. This is done by setting the "SCK select number" element to the value for "No SCKN selected".

The normal message sequence in this case shall be according to figure 36.

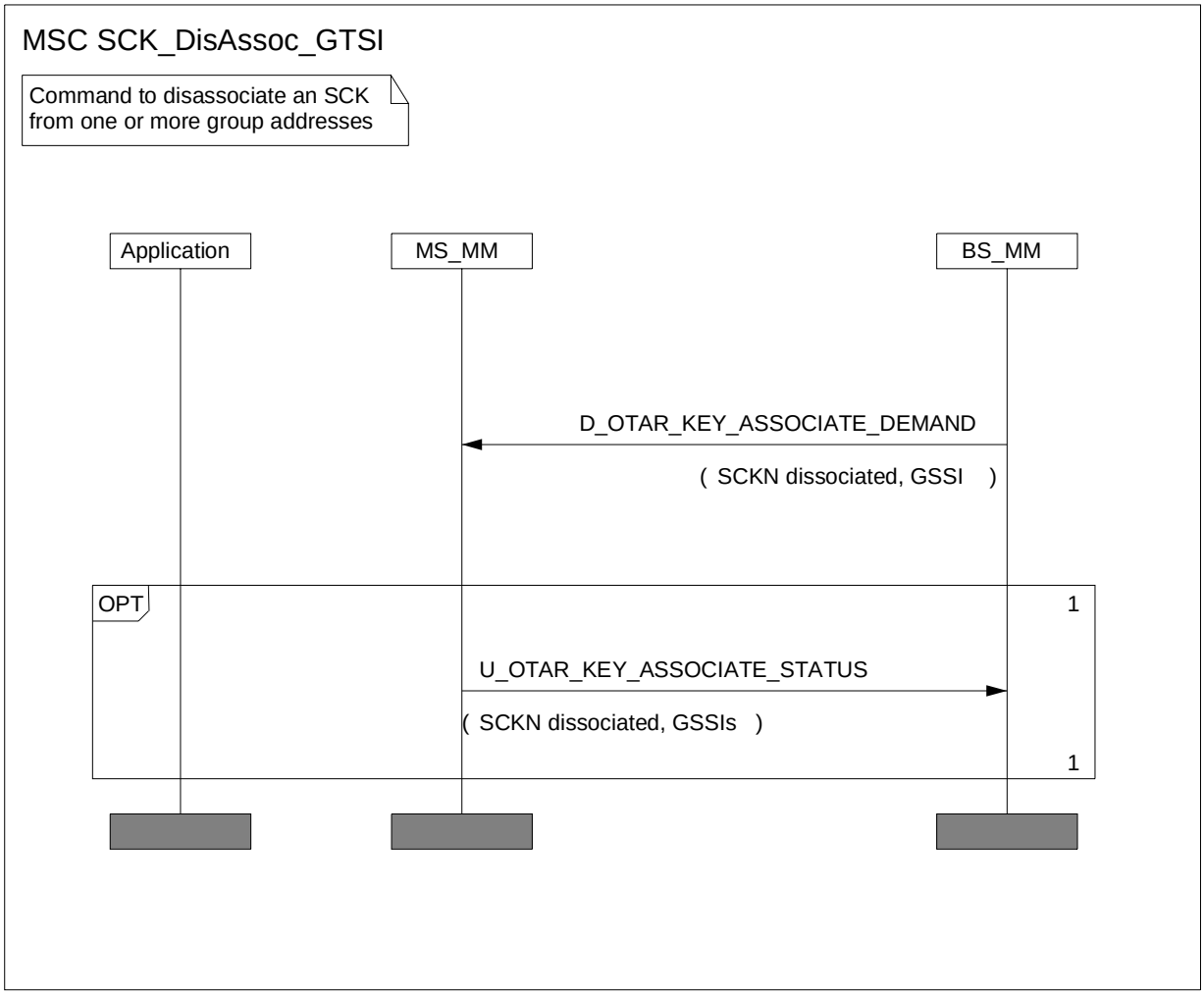


Figure 36: SCK disassociation by SwMI

4.5.4.2 GCK association

This scenario shows the case where the SwMI requests the MS to associate a GCK (which the MS already has) with between 1 and 31 groups.

The SwMI may also demand that groups may be associated to GCKs by groups of MSs. In this case, the D-OTAR KEY ASSOCIATE DEMAND PDU is addressed to the group of MSs. If the Acknowledgement Flag element is set to indicate acknowledgement required, the MS shall start random timer T371 on reception of D-OTAR KEY ASSOCIATE DEMAND and send the U-OTAR KEY ASSOCIATE STATUS on expiry of T371. T371 is described in clause 4.5.2.3.

The normal message sequence in this case shall be according to figure 37.

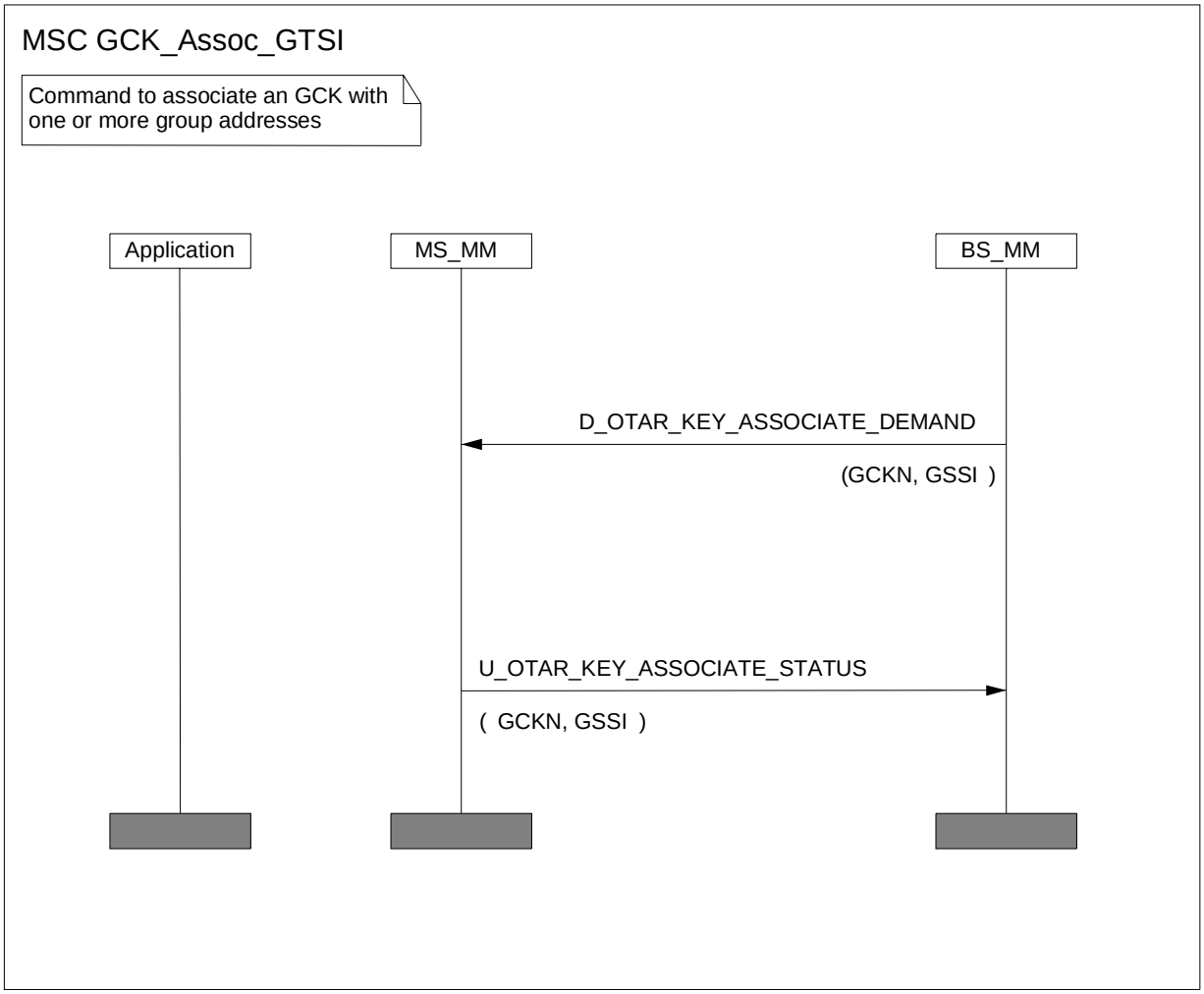


Figure 37: GCK association by SwMI

4.5.5 Notification of key change over the air

The MM security function of the BS/SwMI shall use the exchange shown in figure 38 to inform registered MSs of a future key change. In each case the SwMI should have previously distributed the new cipher key using the key management mechanisms described in clauses 4.4.2 through 4.4.5.

The D-CK CHANGE DEMAND/U-CK CHANGE RESULT shall be used to explicitly inform the MS of the time when a key shall be considered valid. The time may be described as either a value of IV (the composite of slot number, frame number, multiframe number and hyper frame number), or a time based upon UTC as described in EN 300 392-2 [2]. The key-id shall be one of CCK-id, SCKN, GCKN.

On receipt of D-CK CHANGE DEMAND by MS-MM the indicated key and associated parameters shall be notified to the MAC using the MLE-ENCRYPTION request primitive. When the key is applied the MAC shall inform MS-MM of the change using the MLE-ENCRYPTION confirm primitive. If requested the MS-MM shall acknowledge the D-CK CHANGE DEMAND using the U-CK CHANGE RESULT PDU.

Acknowledgement of D-CK CHANGE DEMAND shall be made for ITSI based key delivery using the U-CK CHANGE RESULT PDU by setting the "acknowledgement flag" element on the downlink PDU to TRUE.

The D-CK CHANGE DEMAND may also be transmitted addressed to a group of MSs. In this case acknowledgement is optional, either acknowledgement shall not be requested by setting the "acknowledgement flag" element to FALSE, or if acknowledgement is requested the MS shall start timer T371 with a randomly selected value on receipt of the D-CK CHANGE DEMAND. The procedure for randomly selecting the signalling slot shall follow the procedure for "Choosing from a new access frame" as defined in EN 300 392-2 [2] clause 23.5.1.4.6. On expiry of T371, the MS responds with a U-CK CHANGE RESULT PDU. The value of T371 shall be such that the acknowledgement is received by the SwMI before the time that the key becomes valid.

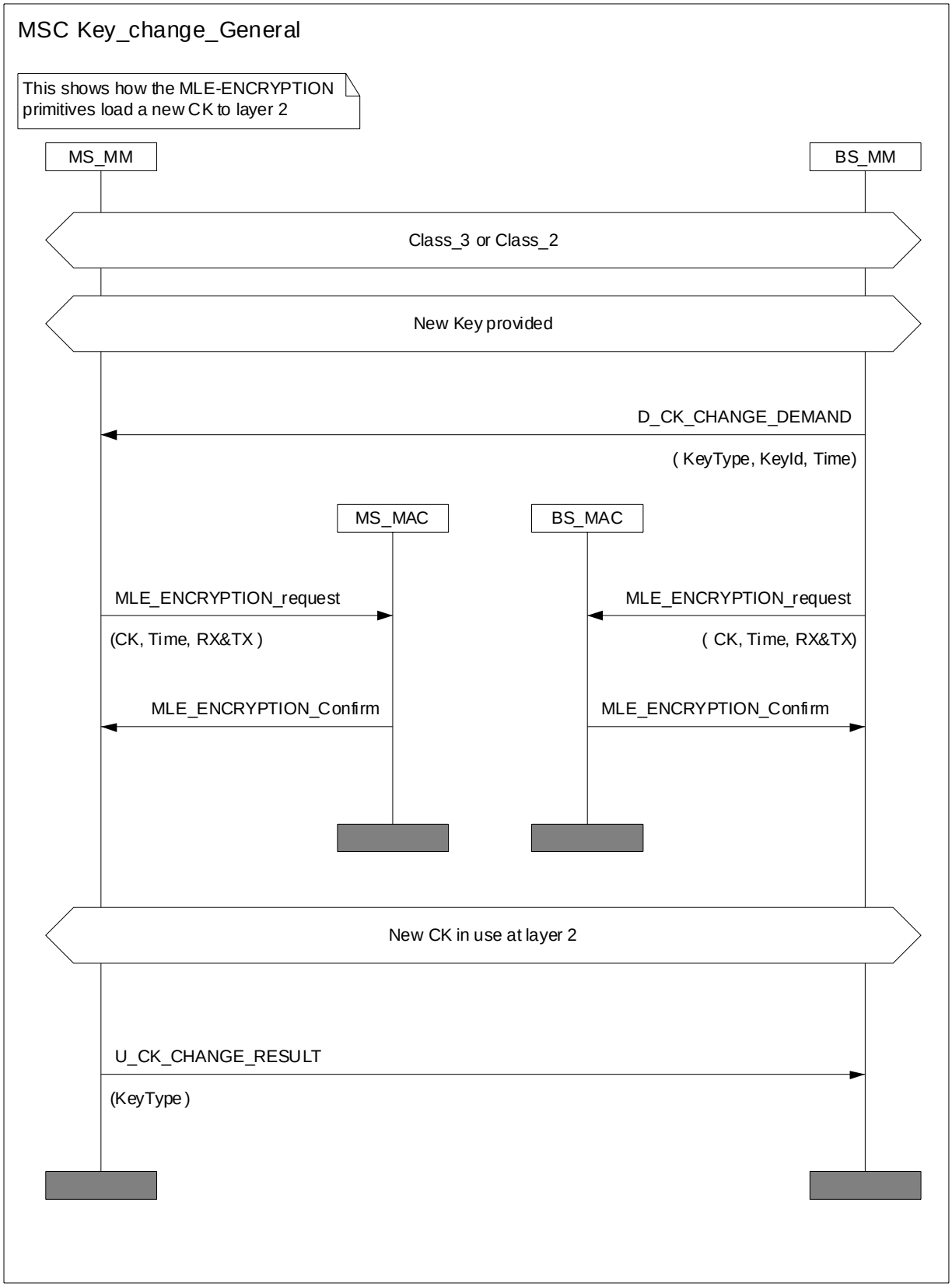


Figure 38: Key change protocol

4.5.5.1 Change of DCK

In cells of security class 3 DCK shall be changed explicitly using the authentication protocols described in clause 4.

The DCK in use shall change at the following times:

- on successful authentication;
- if a DCK has been previously established and is in use it shall be retained throughout the authentication protocol and only discarded after confirmation of the success of the authentication (R1 and/or R2 = TRUE).

The new DCK shall be considered valid after the last repeat of the PDU containing the result R1 or R2 (as authentication PDUs are transmitted using layer 2 acknowledgement the receipt of the acknowledgement of the RESULT PDU shall be the trigger to invoke the new DCK). The MS and SwMI shall be synchronized at this time.

4.5.5.2 Change of CCK

The SwMI may administer the change of CCK using the D-CK-CHANGE-DEMAND PDU. Each cell in an LA shall update the CCK in use at the same time as indicated in the D-CK-CHANGE-DEMAND PDU. If the CCK is valid for several LAs the CCK change shall be done at the same time in all cells belonging to these LAs.

NOTE: It is at the discretion of the SwMI how much warning of CCK change is given.

The SwMI MM shall request a CCK change using the MLE-ENCRYPTION request primitive by setting key download type to CCK, CCK-id pair and providing the CCK and CCK-id to layer 2. Upon receipt of the CCK, CCK-id pair the MAC layer of the SwMI shall discard the old CCK, recalculate the ESI address table, and notify all MSs in the cell of the new CCK-id in the SYSINFO broadcast and in the header of the MAC–RESOURCE PDU described in clause 6.4.1.

For change of CCK the D-CK-CHANGE-DEMAND may be addressed to group and broadcast addresses.

4.5.5.3 Change of GCK

The SwMI may administer the change of GCK using the D-CK CHANGE DEMAND PDU. Where the procedure is used the D-CK CHANGE DEMAND PDU may be addressed to group and broadcast addresses.

For key change type "All GCK" the GCK-VN value in the D-CK CHANGE DEMAND PDU shall apply to all GCKN.

4.5.5.4 Change of SCK for TMO

If over the air cipher key selection is provided the SwMI may administer the change of SCK using the D-CK CHANGE DEMAND PDU. This shall be performed across the entire network.

For change of SCK the D-CK CHANGE DEMAND may be addressed to group and broadcast addresses.

4.5.5.5 Change of SCK for DMO

The "SCK use" element in the OTAR SCK PDU shall indicate whether the SCK is to be used for DMO or TMO operation. The SwMI may use the D-CK CHANGE DEMAND PDU to inform the MS which SCK(s) are in use for Direct Mode Operation (DMO). The use of SCK in DMO shall be indicated in the "SCK use" element. The change of SCK may be immediate or instead occur on a specific IV/network time.

4.5.5.6 Synchronization of Cipher Key Change

When the D-CK CHANGE DEMAND PDU is used to indicate a change of cipher key or security class of the LA, the "Time Type" element shall be used to indicate the exact moment of change.

- Absolute IV - The SwMI shall activate the new cipher key on the indicated IV. In this case the uplink/downlink element of IV shall be ignored.
- Network time - The SwMI shall activate the new cipher key on the Network time. If the Network time falls between slot boundaries, the SwMI shall round-up to the next slot number of the downlink.

- Immediate - The SwMI shall activate the new cipher key on the first slot of the first frame of the next downlink multiframe.

When D-CK CHANGE DEMAND is used to indicate a change of cipher key and/or security class, the security parameters transmitted in MAC-SYSINFO shall also be synchronized with the change of cipher key or security class.

4.5.6 Security class change

4.5.6.1 Change of security class to security class 1

The SwMI may use the D-CK CHANGE DEMAND PDU to inform the MS that the security class of the LA will change to security class 1. In this instance, the SwMI shall identify no cipher key as being active. The change of security class may be immediate or instead occur on a specific IV/network time.

The SwMI shall set the class change element of D-CK CHANGE DEMAND to true, and set the key change type element to "No cipher key ".

When the security class of the cell changes from 3 or 2 to 1, the following criteria shall apply to MS registered on the cell:

- all MS shall remain registered and shall revert to clear connection (no AI encryption). However if the MS supports DCK or SCK encryption, it may invoke cell re-selection procedures to find a cell supporting class 3 or class 2 to preserve a higher security level.

4.5.6.2 Change of security class to security class 2

The SwMI may use the D-CK CHANGE DEMAND PDU to inform the MS that the security class of the LA will change to security class 2. In this instance, the SwMI shall identify the active SCKN and SCK-VN. The change of security class may be immediate or instead occur on a specific IV/network time.

When the security class of the cell changes from 3 to 2, the following criteria shall apply to MS registered on the cell:

- MS that do not support SCK AI encryption shall invoke cell re-selection procedures if the cell does not support security class 1 MS.

- MS that do not support SCK AI encryption shall **remain registered** and shall revert to clear connection (no AI encryption) if the cell supports security class 1 MS. However if the MS supports DCK encryption, it may invoke cell re-selection procedures to find a cell supporting class 3 to preserve the same security level.

- MS that support SCK AI encryption but have not successfully registered with ciphering on shall send U-LOCATION UPDATE DEMAND PDU proposing SCK encryption.

- MS that support SCK AI encryption and have already registered with ciphering on but do not possess the SCK currently in use by the SwMI shall send U-LOCATION UPDATE DEMAND PDU proposing SCK encryption.

- MS that support SCK AI encryption and have already registered with ciphering on and possess the SCK currently in use by the SwMI shall **remain registered** and shall revert to SCK encryption.

When the security class of the cell changes from 1 to 2, the following criteria shall apply to MS registered on the cell:

- MS that do not support SCK AI encryption shall invoke cell re-selection procedures if the cell does not support security class 1 MS.

- MS that do not support SCK AI encryption shall **remain registered** if the cell supports security class 1 MS.

- MS that support SCK AI encryption shall send U-LOCATION UPDATE DEMAND PDU proposing SCK encryption.

- MS that support SCK AI encryption and have previously registered proposing SCK encryption with the SCK now in use shall remain registered and revert to SCK encryption.

4.5.6.3 Change of security class to security class 3

The MS may use the D-CK CHANGE DEMAND PDU to inform the MS that the security class of the LA will change to security class 3. In this instance, the SwMI shall identify the active CCK-id. The change of security class may be immediate or instead occur on a specific IV/network time.

When the security class of the cell changes from 1 to 3, the following criteria shall apply to MS registered on the cell:

- MS that do not support DCK AI encryption shall invoke cell re-selection procedures if the cell does not support security class 1 MS;
- MS that do not support DCK AI encryption shall **remain registered** if the cell supports security class 1 MS;
- MS that support DCK AI encryption but have not successfully registered with ciphering on shall send U-LOCATION UPDATE DEMAND PDU proposing DCK encryption; and,
- MS that support DCK AI encryption and have previously registered with ciphering on and possess valid CCK and DCK shall **remain registered** and shall revert to DCK encrpytion.

When the security class of the cell changes from 2 to 3, the following criteria shall apply to MS registered on the cell:

- MS that do not support DCK AI encryption shall invoke cell re-selection procedures if the cell does not support security class 1 MS;
- MS that do not support DCK AI encryption shall **remain registered** and shall revert to clear connection (no AI encryption) if the cell supports security class 1 MS. However if the MS supports SCK encryption, it may invoke cell re-selection procedures to find a cell supporting class 2 to preserve the same security level;
- MS that support DCK AI encryption but have not successfully registered with ciphering on shall send U-LOCATION UPDATE DEMAND PDU proposing DCK encryption;
- MS that support DCK AI encryption and have already registered with ciphering on but do not possess a valid CCK and/or DCK (see note) shall send U-LOCATION UPDATE DEMAND PDU proposing DCK encryption (the PDU shall contain CCK request if the MS does not possess a valid CCK); and,
- MS that support DCK AI encryption and have already successfully registered with ciphering on and possess a valid CCK and DCK (see note) shall **remain registered** and shall revert to DCK encryption.

NOTE: If the 'DCK retrieval during initial cell selection' is not supported by the SwMI, the MS may consider the previously established DCK to be valid only if the DCK has been generated after the last ITSI-Attach or migration location updating in this SwMI. If the SwMI does not support the 'DCK retrieval during cell re-selection', the MS may consider the previously established DCK to be valid only if the DCK has been last used within this LA and after the last ITSI-Attach or migration location updating.

5 Enable and disable mechanism

NOTE: Without authentication capability in the MS it is possible that a SwMI (real or spoofed) can temporarily deny service to the MS. The use of authentication embedded into the enable/disable mechanism as described in this clause minimizes this risk.

An MS moving from DMO to TMO, or from TMO to DMO, shall retain its disabled state. Thus if an MS is disabled in TMO it shall remain disabled even if the user attempts to switch to DMO.

5.1 General relationships

All TETRA MSs shall support enable and disable as described in this clause.

Figure 39 shows the relationship of user subscription, identified by ITSI, and the hardware of the MS, identified by TEI. 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, for example, field programming equipment.

If a SIM is used to store the ITSI the procedures described in ETS 300 812 [7], clause 11.4.4 shall be enforced in addition to the protocols described in this clause.

ITSI and TEI are described in ETS 300 392-1 [1], clause 7.

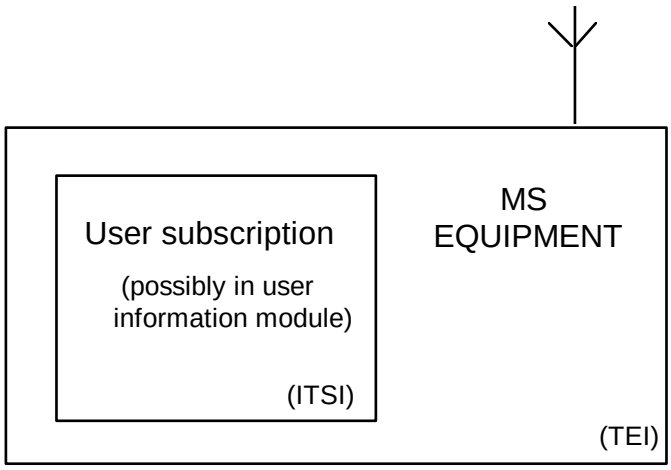
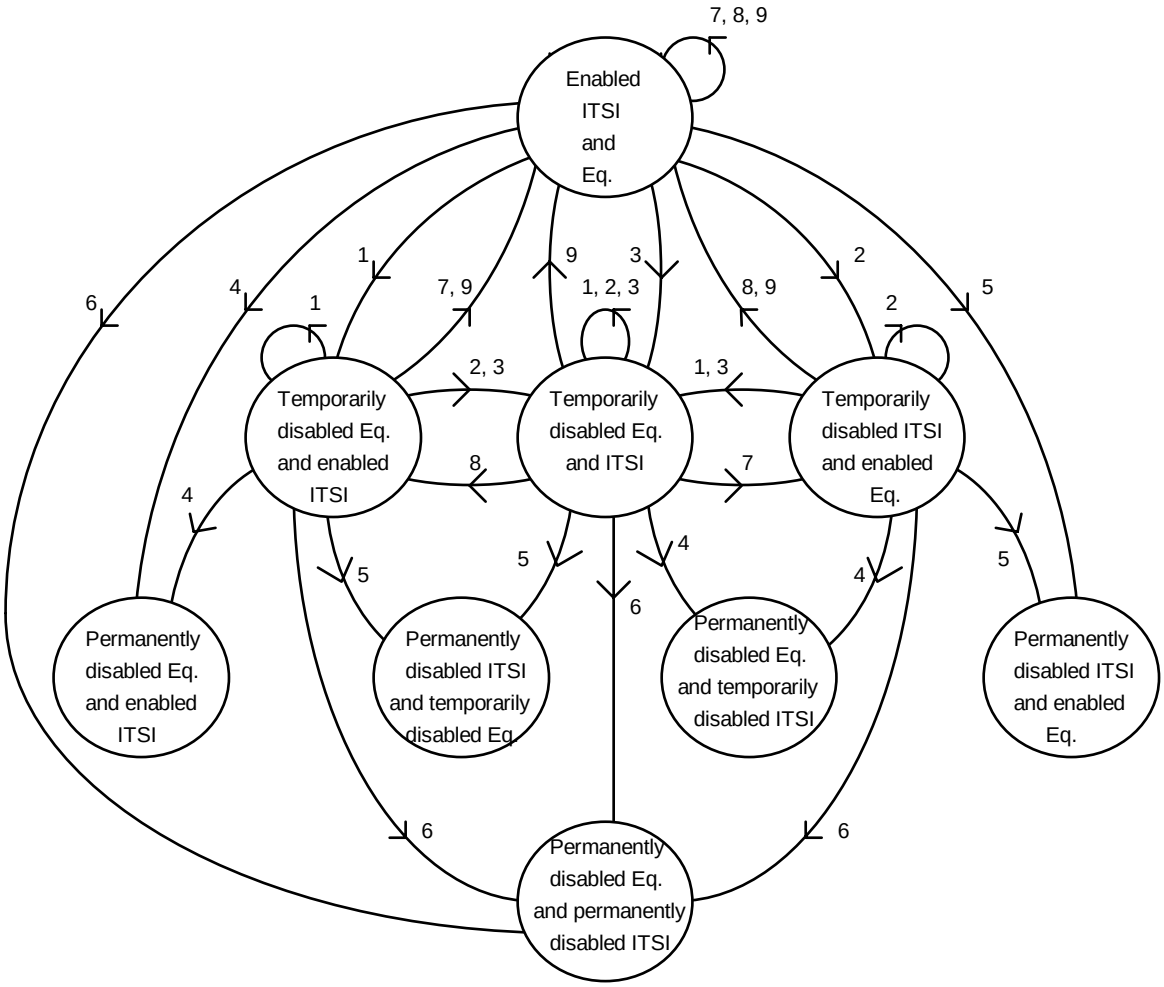


Figure 39: Relationship of TEI and ITSI in MS

5.2 Enable/disable state transitions

Figure 40 shows all possible enabled and disabled states of one pair of MS equipment and ITSI and the transitions between the states. This diagram does not show state transitions due to separation of ITSI from, or fitting of ITSI into, an MS equipment.



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 40: State transitions of enable/disable mechanism

5.3 Mechanisms

An MS and SwMI operating in security class 3 or security class 2 shall perform enabling and disabling with encryption applied. An MS and SwMI operating in security class 1 shall perform enabling and disabling in clear. If authentication is required by the SwMI it shall be applied for enable and disable operations by the inclusion of an authentication challenge in the D-DISABLE or D-ENABLE PDU.

An MS may reject an ENABLE or a temporary DISABLE command generated by a network without security (class 1 without authentication). In cases where authentication has been initiated by the SwMI it should be made mutual by the MS. In this edition of the present document detailed sequences are shown only for the mutual authentication case but this does not preclude later editions of the present document describing in addition unilateral authentication cases. If the SwMI proposes permanent disable without authentication the MS shall reject it with cause "Authentication required".

There are nine 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 clauses 5.3.1 to 5.3.6 in which the temporary and permanent distinctions are amalgamated.

There may be other mechanisms that withdraw service or disable the equipment that are outside the scope of the present document.

Equipment or subscriptions that have been temporarily disabled may be enabled by the enable mechanisms described in clauses 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 shall be capable of receiving enable commands addressed invidually with a valid L2 address for the MS, i.e. ISSI/ASSI in the home network and ITSI/(V)ASSI in a foreign network (during migration). The PDU shall include the TEI of the MS equipment. 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 shall be capable of receiving enable commands addressed individully with a valid L2 address for the MS, i.e. ISSI/ASSI in the home network and ITSI/(V)ASSI in a foreign network (during migration). The PDU shall include the TEI of the MS equipment. Only MS subscription that has been temporarily disabled may be enabled by this method: 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.

5.3.6 Enable an MS equipment and subscription

The MS equipment and subscription shall be enabled using commands addressed to a valid L2 individual address for the MS, i.e. ISSI/ASSI in the home network and ITSI/(V)ASSI in a foreign network (during migration), 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. The PDU shall include the TEI of the MS equipment.

Where the ITSI is not separable, an MS may be disabled by utilizing any of the mechanisms described in clauses 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 clause 5.3.1 shall only be enabled using the mechanisms described in clause 5.3.4 or clause 5.3.6; an MS disabled by the mechanism described in clause 5.3.2 shall only be enabled by the mechanisms described in clause 5.3.5 or clause 5.3.6; and an MS disabled by the mechanism described in clause 5.3.3 shall only be enabled by the mechanism described in clause 5.3.6.

5.4 Enable/disable protocol

5.4.1 General case

All signalling should be directed to an MS using L3 commands transported in valid individually addressed L2 PDUs, i.e. ISSI/ASSI in the home network and ITSI/(V)ASSI in a foreign network (during migration): The SwMI needs to know the ITSI/TEI binding where necessary, for example by obtaining ITSI-TEI mapping at registration. Confirmation of the target for disabling and enabling is then provided by including the ITSI and/or TEI of the MS in the PDUs. 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 cell of class 2 or 3 as described in clause 6. In class 1 cells the TEI shall be transferred in the air interface in clear form, it is recommended that this is avoided.

The enabling and disabling is enacted by the primitives MLE-CLOSE, MLE-DEACTIVATE and MLE–OPEN. The MLE-CLOSE primitive is used to indicate that access to the communication resources has been closed to the other higher layer entities; SNDCPand CMCE. MM shall then issue an MLE-DEACTIVATE request primitive. If the disabling is temporary the MS shall remain disabled in the sense that access to the communication resources shall remain closed for the CMCE and SNDCP entities. MM should remain active so that any roaming functions when requested by the SwMI, can be carried out in order that the MS can receive an enable instruction later. Should the MS be powered down the MS shall retain the information that it is temporarily disabled.

In the temporarily disabled state whilst the MS shall not be able to invoke any function of the CMCE and SNDCP entities it may be possible, for the sole purpose of supporting the Supplementary Service Ambience Listening, for the SwMI to invoke the relevant CMCE entities.

In a permanent disable the disablement of all radio functions shall be carried out using the MLE–DEACTIVATE request. This shall be used by the MM entity to request the de-activation of all MLE procedures and to return to the NULL state. No communication resources are available for use after this primitive has been issued. It shall not be possible to reverse the permanent disable state by user intervention or by a TETRA protocol.

5.4.2 Status of cipher key material

In the event of permanent disable of an ITSI all key material should be destroyed (i.e. K, SCK, GCK and all dynamic keys (CCK, DCK, MGCK)).

In the event of permanent disable of an equipment (TEI) all key material maintained on the equipment should be destroyed.

It is advised that where possible as a result of permanent disable algorithms should be destroyed.

In the event of temporary disable of an ITSI all shared long lifetime key material (GCK, DM-SCK) should be destroyed. The fallback SCK for TMO, and K should not be deleted.

5.4.3 Specific protocol exchanges

The normal message exchanges for the various cases shall be according to clauses 5.4.3.1 through 5.4.3.3.

The MS shall send U-DISABLE STATUS even if there is no resulting change in state of the MS arising from the ENABLE or DISABLE request. Even when no change in state occurs, the complete protocol, including authentication where required, shall be followed..

5.4.3.1 Disabling an MS with authentication

This shall apply for MS and SwMI in all class 3 cells and in class 2 and class 1 cells that enforce authentication. The authentication mechanisms and PDUs are described in clause 4 of this document. The MSC shows as optional the key change procedure described in clause 4.5.5 which shall be considered mandatory for class 3 cells. The use of MLE-DEACTIVATE is shown as optional and shall apply when the disabling type is permanent.

Figure 41 shows the (mandatory) normal message sequence in this case.

The optional change of DCK shall be as described in clause 4.5.5.1.

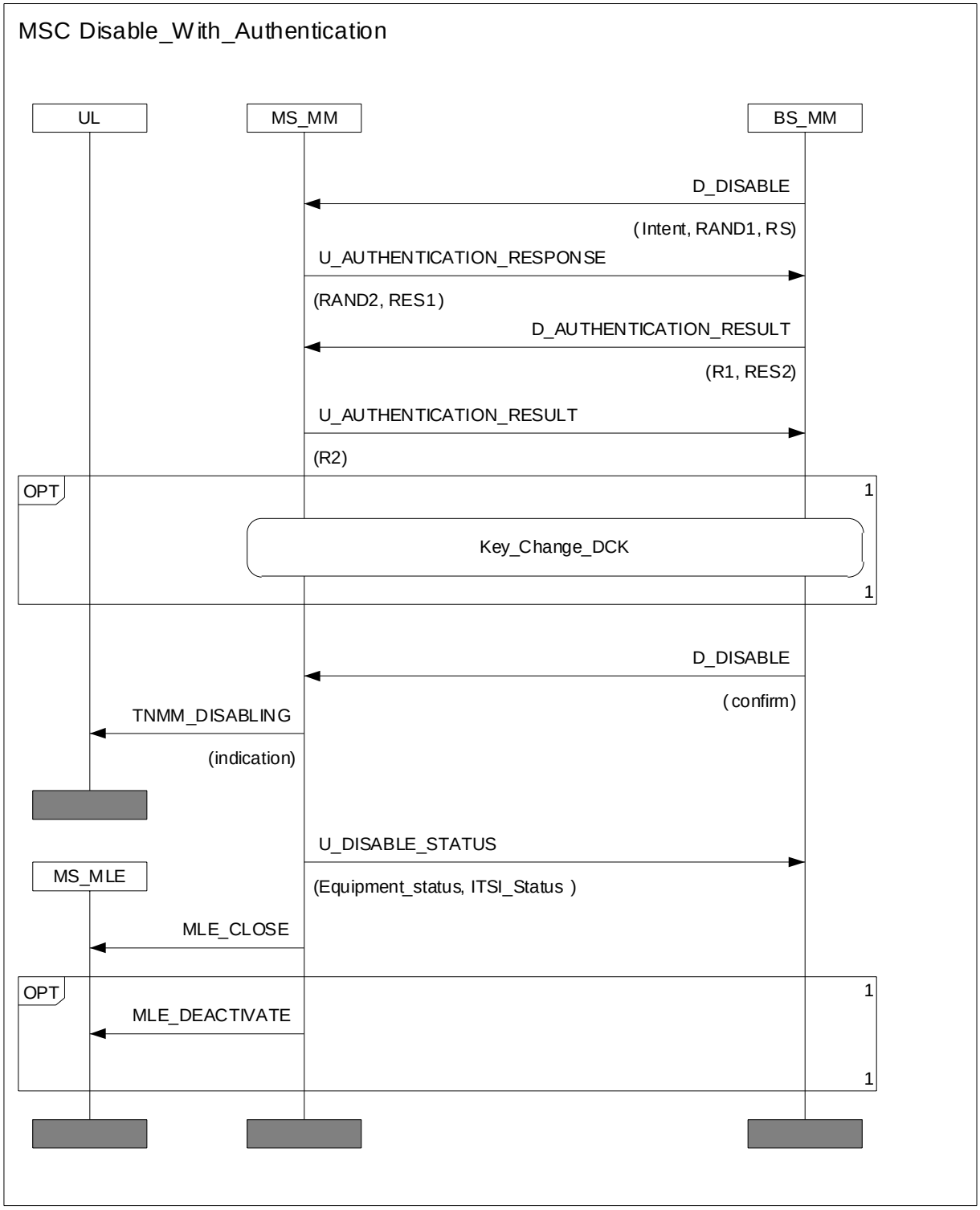


Figure 41: Disabling an MS with authentication

5.4.3.2 Enabling an MS with authentication

This shall apply for MS and SwMI in all class 3 cells and in class 2 and class 1 cells that enforce authentication. The authentication mechanisms and PDUs are described in clause 4 of this document. The MSC shows as optional the key change procedure described in clause 4.5.5 which shall be considered mandatory for class 3 cells.

Figure 42 shows the (mandatory) normal message sequence in this case.

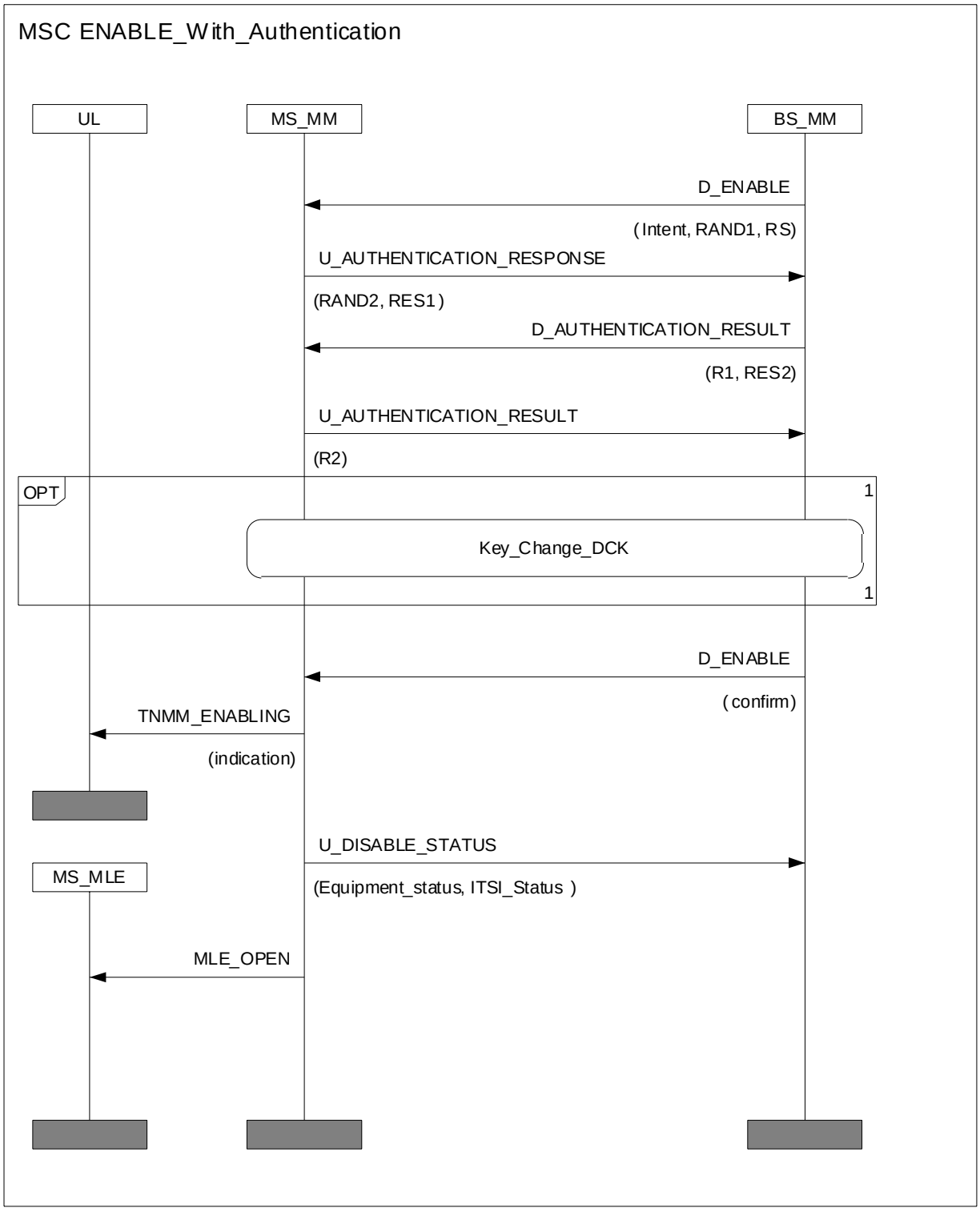


Figure 42: Enabling an MS with authentication

5.4.4 Enabling an MS without authentication

This shall only apply for MS and SwMI in class 2 and class 1 cells that do not enforce authentication.

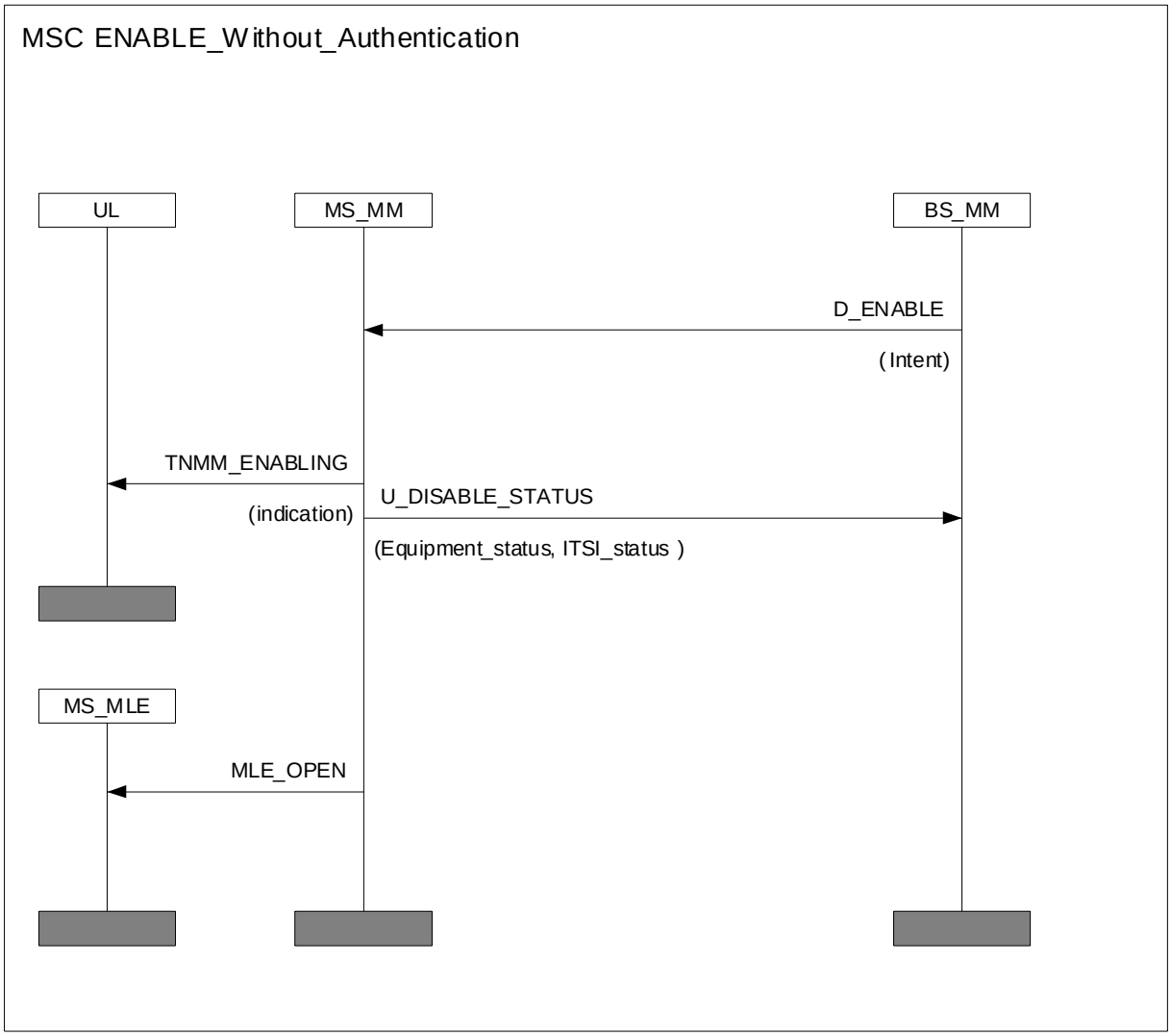


Figure 43: Enabling an MS without authentication

5.4.5 Disabling an MS without authentication

This shall only apply for MS and SwMI in class 2 and class 1 cells that do not enforce authentication.

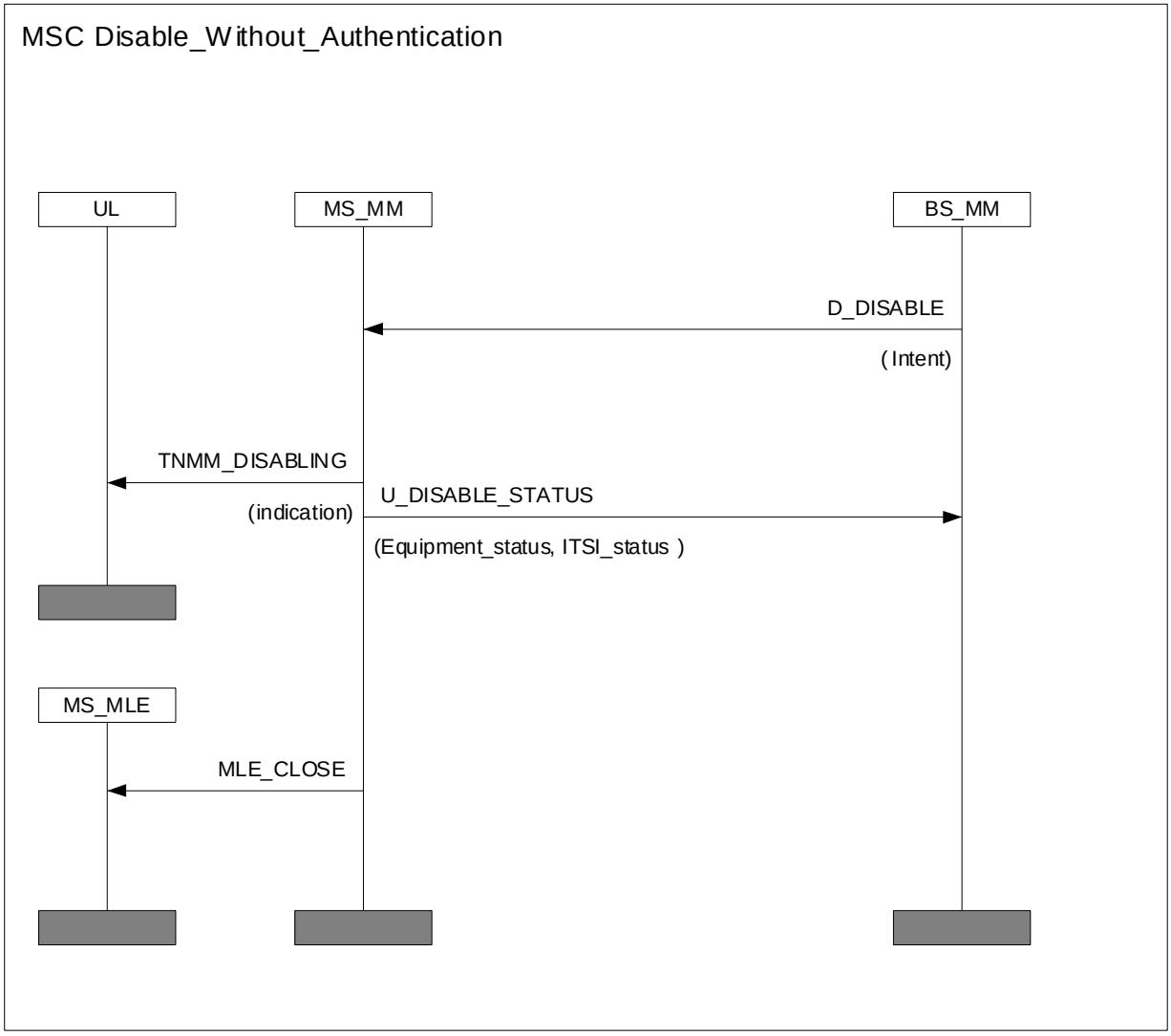


Figure 44: Disabling an MS without authentication

5.4.6 Rejection of enable or disable command

The rejection of an enable or disable command shall be determined by the system class.

System class	MS Behaviour
1	Should accept enable/disable command.
2	Should accept enable/disable command.
3	Shall accept enable/disable command.

An MS that does not support authentication (class 1 or class 2) shall be able to reject a permanent disabling command with the reason "Authentication is required" returned to the SwMI in the U-DISABLE STATUS PDU.

If the MS receives a command requesting action against TEI where the TEI does not match that of the current terminal the command shall be rejected with reason "TEI mismatch".

An MS that supports authentication may be able to reject a temporary disable request command received from an unauthenticated source.

An MS shall not reject a temporary disabling or enabling command unless it is configured to normally operate in class 2 or class 3 systems and receives the command while operating in a class 1 cell.

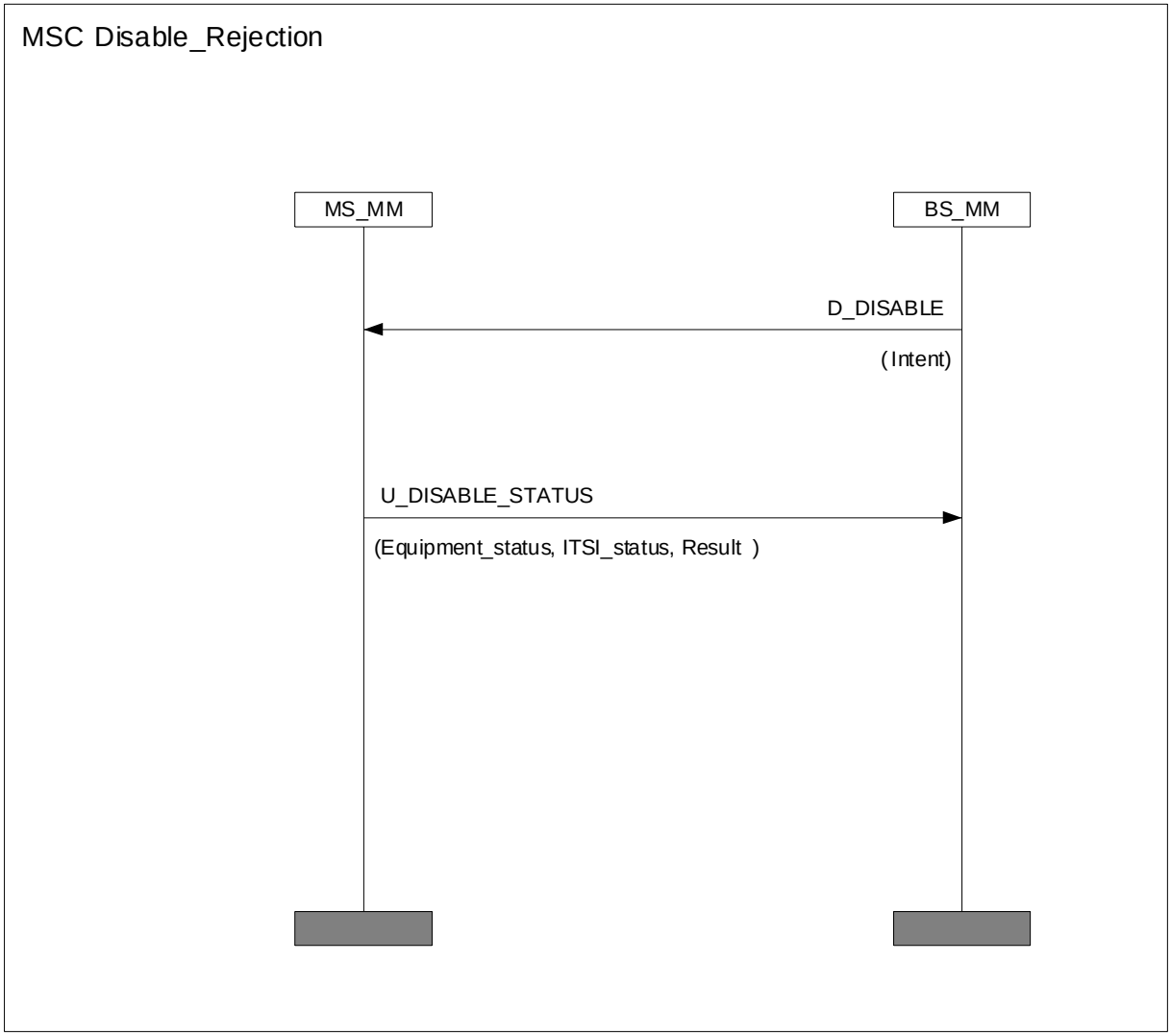


Figure 45: Rejection of permanent disabling by an MS without authentication

5.4.7 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 clauses.

5.4.7.1 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.

Table 7 defines the parameters for TNMM-DISABLING indication.

Table 7: Parameters for the primitive TNMM-DISABLING indication

Parameter	Indication
Enable/disable status	M

5.4.7.2 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.

Table 8 defines the parameters for TNMM-ENABLING indication.

Table 8: 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	Equipment enabled
	Subscription enabled
	Equipment temporary disabled
	Equipment permanently disabled
	Subscription temporary disabled
	Subscription permanently disabled

6 Air Interface (AI) encryption

6.1 General principles

AI encryption shall provide confidentiality on the radio link between MS and BS and be resident in the upper part of the MAC layer of the TETRA protocol stack, 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, enables receiving parties to determine the applicability of a message received over air for them, and enables application of the correct key for the decryption process. Figure 46 illustrates this placement.

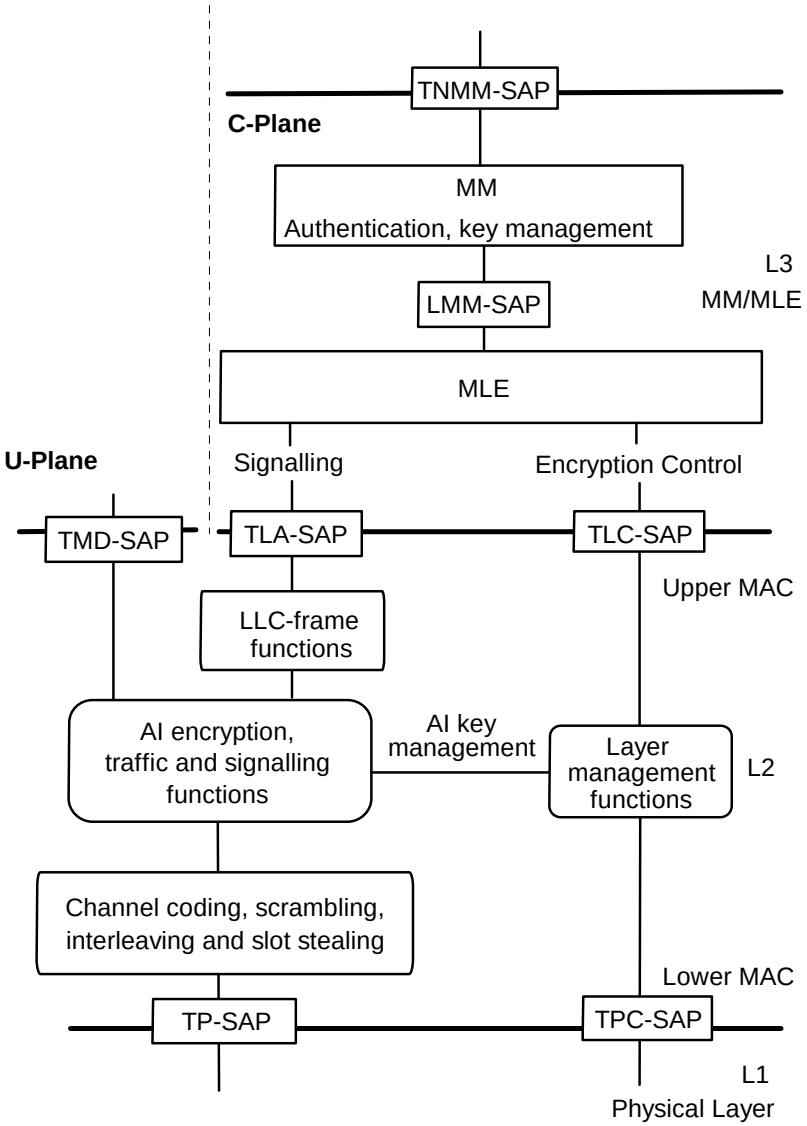


Figure 46: Relationship of security functions to layers functions in MS

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 present document.

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 clause 8 of ETS 300 392-1 [1], 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.

6.2 Security class

Two encryption modes are described, each of which shall use the same encryption process:

SCK mode: for AI encryption without enforced authentication. This mode shall use SCK for address encryption;

DCK mode: for AI encryption where authentication is mandatory. This mode shall use CCK for address encryption, and shall also use CCK to encrypt group addressed signalling and traffic alone or in combination with GCK.

Table 9 summarizes the encryption modes into a set of three security (equipment) classes. These classes apply to cells within a SwMI and may be used to classify terminal capability.

Table 9: Security classes

Class 1:	Shall not use encryption
	May use authentication
Class 2: SCK Mode	Shall use SCK encryption
	Shall use ESI with SCK
	May use MGCK encryption
	May use authentication
Class 3: DCK Mode	Shall use authentication
	Shall use DCK, CCK and/or MGCK encryption
	Shall use ESI with CCK

The present document describes a system in which all signalling and traffic within that system comply with the same security class. However signalling permits more than one security class to be supported concurrently within a SwMI, and movements between these classes are described in the present document. The SwMI shall control the state of AI encryption.

An MS may support one, several, or all security classes. Each cell may support at any one time one of the following options:

class 1 only;

class 2 only;

class 2 and class 1;

class 3 only; or

class 3 and class 1.

Class 2 and class 3 are not permitted to be supported at the same time in any cell because of address conflicts that could arise from using short identity encryption with two different keys.

The security class and other parameters shall be broadcast by each cell in the SYSINFO element contained in the Broadcast Network CHannel (BNCH) (see EN 300 392-2 [2], clause 21). The broadcast shall use the Extended Service Broadcast information element defined in EN 300 392-2 [2] edition 2 [2] table 334A and signalled by setting the "Optional Field flag" element of SYSINFO to 11_2. If the "timeshare cell and AI encryption information" elements are not present in the D-NWRK-BROADCAST PDU, then the MS should assume that the neighbour cells have the same security class and keys as the current LA, i.e. that the network is homogenous.

The CCK-id in cells of class 3, or SCK-VN in cells of class 2, shall be broadcast with the Hyper–Frame number as described in clause 6.3.2.1.

The security class of cells shall also be distributed using the D-NWRK-BROADCAST PDU defined in ETS 300 392–2 [2], clause 18. The element "Timeshare cell and AI encryption information" shall be encoded for security purposes as shown in table 10.

Table 10: Timeshare cell and AI encryption information element

Information element	Type	Length	Value	Remark
Discontinuous mode/AI encryption information	M	2	00	AI encryption information
			Others	Defined in EN 300 392-2 [2], table 255
Authentication flag (note 2)	M	1	0	Authentication not required on this cell
			1	Authentication required on this cell
Class 1	M	1	0	MS of security class 1 not supported on this cell
			1	MS of security class 1 supported on this cell
Security class 2 or 3 (note 1, note 3)	M	1	0	MS of security class 2 supported on this cell
			1	MS of security class 3 supported on this cell
NOTE 1: Security class 2 and security class 3 are mutually exclusive. NOTE 2: If the "Air interface encryption service" element in the BS service details element contained in the D-MLE SYSINFO PDU contains value 0, "Service is not available on this cell", then the value of this element has no meaning. NOTE 3: This field is ignored if BS Service Details indicate no support of AI encryption				

An MS shall register to the SwMI at the highest security class mutually available to the MS and SwMI (i.e. if BS supports class 3 and class 1 mobiles, and the mobile also supports class 3 and class 1, the MS shall register at class 3). The MS shall use the following information elements in the class of MS element to indicate at registration the capabilities of the MS for security.

Table 11: Air Interface encryption service element (normative source: EN 300 392-2 [2], Table 167)

Information element	Length	Value	Remark
Authentication	1	0	Authentication not supported
		1	Authentication supported
DCK encryption	1	0	DCK encryption not supported
		1	DCK encryption supported
SCK encryption	1	0	SCK encryption not supported
		1	SCK encryption supported

The TETRA Air Interface standard version number given in EN 300 392-2 [2], table 167, applies for value 000_2 to EN 300 392-2 edition 1 [2] only. Value 001_2 shall apply to EN 300 392-2 edition 1 [2], plus ETS 300 392-7 edition 2 [3]. Value 010_2 shall apply to EN 300 392-2 edition 2 [2] plus ETS 300 392-7 edition 2 [3]. There shall be no signalling to indicate that an MS complies to ETS 300 392-7 [3] edition 1 [3], implying that ETS 300 392-7 edition 1 [3] is not accepted as a valid implementation.

6.2.1 Constraints on LA arising from cell class

In a fully operational LA all cells should be of the same security class (see also 6.5.1).

6.3 Key Stream Generator (KSG)

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

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

The KSG shall have two inputs, an Initial Value (IV) and a cipher key. These parameters shall be as specified in clause 6.3.2. 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.

6.3.1 KSG numbering and selection

TETRA supports both standard and proprietary algorithms. Location update signalling shall identify which algorithm is in use. Migration should only be possible if there is agreement between operators on the algorithm used.

The SwMI should only have one encryption algorithm. An MS may have more than one algorithm but shall use the algorithm indicated by the SwMI.

Table 12 shows that the values 0000_2 to 0111_2 of KSG number used in signalling shall be reserved for the TETRA standard algorithms (see also EN 300 392-2 [2], clause 16.10.29).

Table 12: KSG Number element contents

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

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

Where a SwMI supports more than one encryption algorithm in class 3 systems the CCK has to be common in order for commonality of ESI. Groups of users should be differentiated by GCK. Terminals shall support only one active encryption algorithm. There shall be no dynamic change of registered algorithm for users in a session. If PDUs explicitly broadcast addressed are encrypted, then the CCK (class 3) or SCK (class 2) keys shall be used to encrypt the broadcast identity and the message contents. If there is more than one KSG in use in the SwMI, then broadcast messages should not be encrypted.

6.3.2 Interface parameters

6.3.2.1 Initial Value (IV)

The composition of the slot and frame numbering input to 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 (EN 300 392-2 [2], clause 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 (EN 300 392-2 [2], clause 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 (EN 300 392-2 [2], clause 9.3.7);

- the next 15 bits IV(13) to IV(27) shall correspond to the 15 least significant bits of an extension that numbers the hyper-frames. These can take all values from 0 to 32767. IV(13) shall correspond to the least significant bit of the hyper-frame numbering extension (EN 300 392-2 [2], clause 9.3.8); and,

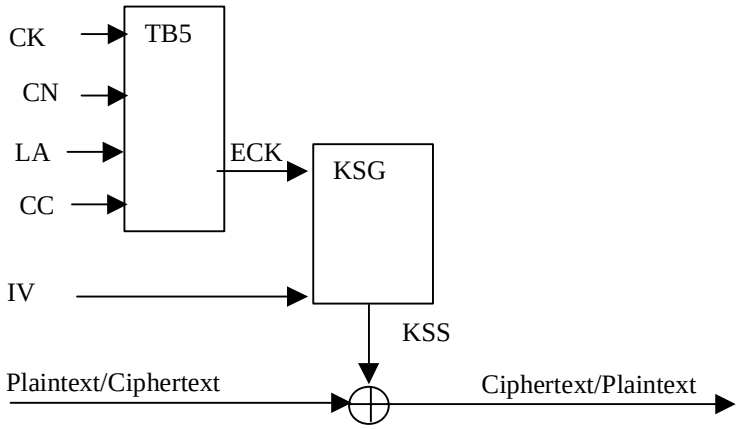
- the final bit, IV(28), shall be given the value 0 for downlink transmissions, and shall be given the value 1 for uplink transmissions.

The value of IV shall be maintained by the SwMI and broadcast on the SYNC and SYSINFO PDUs (layer 2). The value of hyper-frame (IV(13) to IV(27)) shall be broadcast to a schedule determined by the SwMI with the value of CCK-id on cells of security class 3, and with the value of SCK-VN in cells of security class 2, in the SYSINFO broadcast.

6.3.2.2 Cipher Key

The CK shall not be used directly at the air interface for encryption but shall be modified by the Colour Code (CC), LA-id and Carrier Number (CN) using algorithm TB5 (see figure 47). This shall randomize the input to the encryption algorithm amongst the carriers of a single cell and between cells in a location area.

The ciphering process shall be as shown in figure 47. 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 ECK(0) … ECK(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 clause 6.5.



NOTE: CN of the main carrier, CC, LA-id, and initialising values of IV are received at the MS from the BS broadcast signalling messages. After initialization IV is locally generated at the MS. When camped on a cell CN values are received at the MS from downlink MAC-RESOURCE and MAC-END PDUs. IV is locally generated at the BS.

Figure 47: Speech and control information encryption

6.4 Encryption mechanism

The KSS 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 clause 6.7.1.2.

6.4.1 Allocation of KSS to logical channels

KSS shall be allocated to TETRA logical channels as shown in table 13 and the unused bits (also indicated) shall be discarded.

Table 13: KSS allocation to logical channels

Locical channel	Bits in channel	KSS assignment
TCH/2.4	144	KSS(124..267)
TCH/4.8	288	KSS(124..411)
TCH/7.2 (note 1)	432	KSS(0..431)
STCH+TCH/2.4	124+144	KSS(0..123)+KSS(124..267)
STCH+TCH/4.8	124+288	KSS(0..123)+KSS(124..411)
STCH+TCH/7.2	124+432	KSS(0..123)+KSS(0..431) (note)
TCH/S (full)	274	KSS(0..273)
STCH+TCH/S	124+137	KSS(0..123)+KSS(216..352)
SCH/F	268	KSS(0..267)
SCH/HU (note 2)	92	KSS(0..91)
SCH/HU+SCH/HU	92+92	KSS(0..91)+KSS(216..307)
SCH/HD+SCH/HD	124+124	KSS(0..123)+KSS(216..339)
STCH+STCH	124+124	KSS(0..123)+KSS(216..339)
NOTE 1: Where TCH/7.2 is stolen the first 216 encrypted bits of TCH/7.2 are not transmitted. NOTE 2: SCH/HU KSS allocation applies whether the first or second half slot is selected for transmission.		

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

6.4.2 Allocation of KSS to logical channels with PDU association

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 and may use different cipher keys. The MAC headers themselves may be of varying lengths. To allow for this, the KSS shall be restarted at the commencement of each SDU.

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

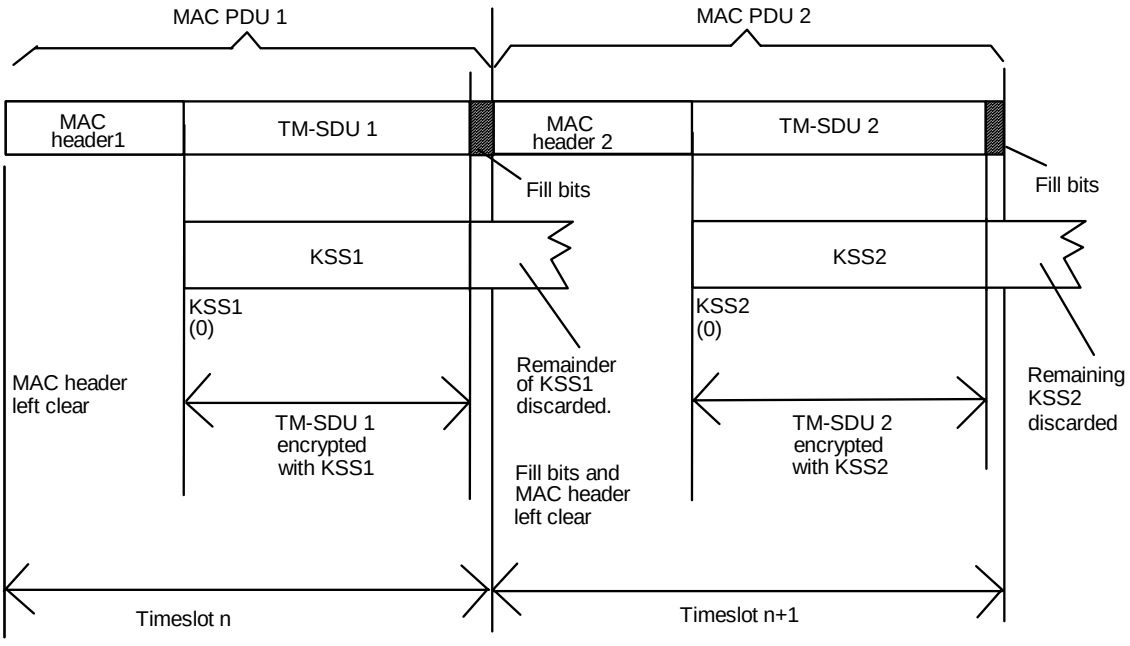
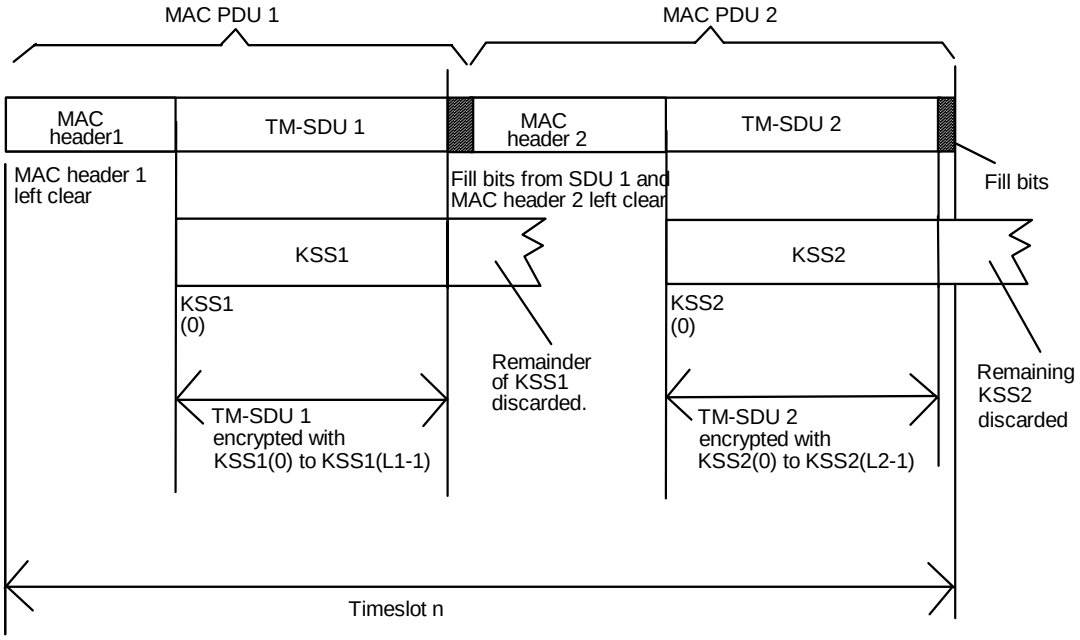
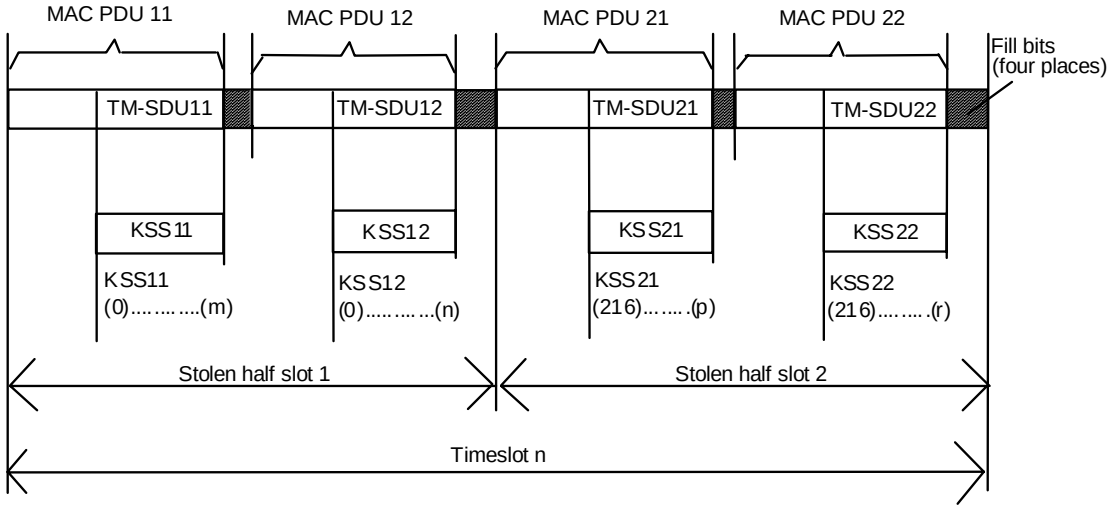


Figure 48: Allocation of KSS to encrypt MAC PDUs



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

Figure 49: Allocation of KSS to encrypt MAC PDUs with PDU Association for full slot logical channels



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 50: Allocation of KSS to encrypt MAC PDUs with PDU Association for half slot logical channels

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

- sending more than one SDU encrypted with the same encryption key within one logical channel.

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

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

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

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

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

NOTE 1: IV_{Start} is the value of IV used in the synchronization bursts.
NOTE 2: Actual IV value is to be used for decryption of non-traffic bursts.

Figure 51: Value of IV to be used for TCH/4.8 or TCH/2.4 with interleaving depth of 4

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

Transmission across frame 18 shall be treated as shown in figure 52.

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

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

Figure 52: Treatment of IV for TCH/4.8 or TCH/2.4 with interleaving depth of 4 at frame 18

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

6.4.4 Recovery of stolen frames from interleaved data

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

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

6.5 Use of cipher keys

The cipher keys and their allocation are described in clauses 4.2.1 to 4.2.5.

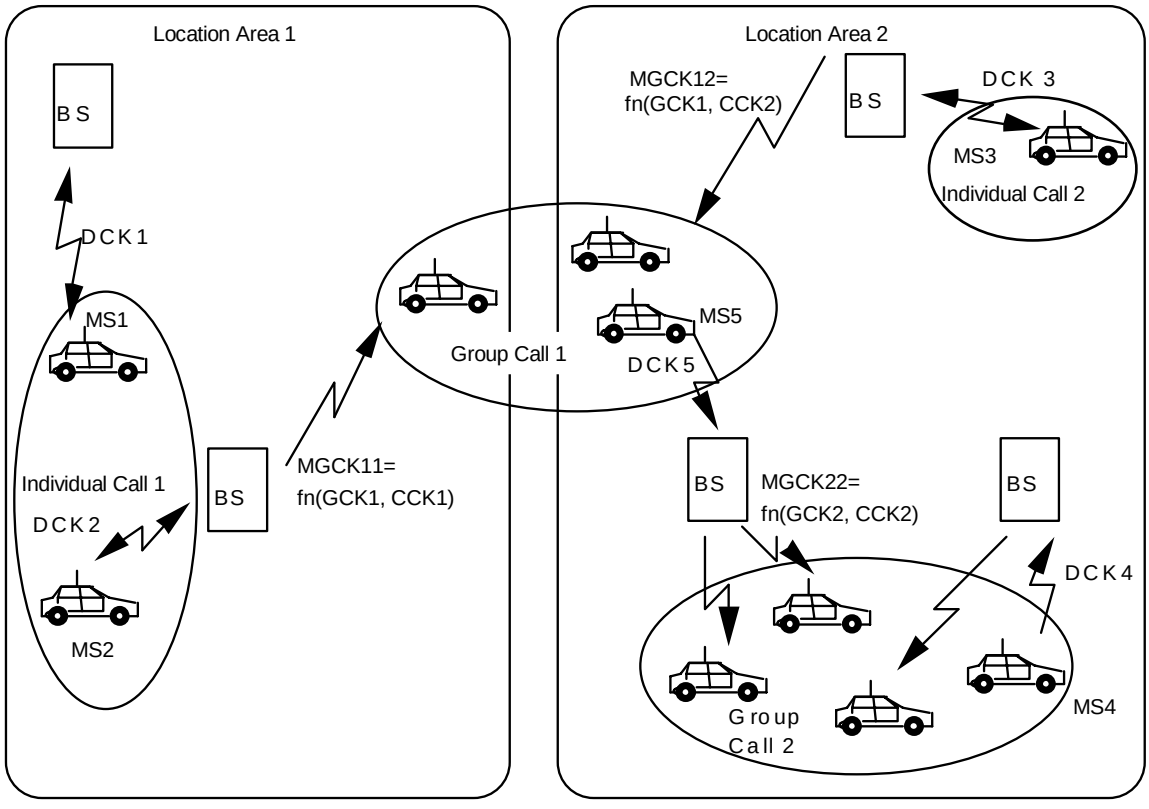
The header of MAC PDUs transmitted over the air interface shall contain indication whether the MAC PDU and some elements of the MAC Header (SSI address and channel allocation elements) are encrypted or not. In addition the header of MAC downlink PDUs shall indicate which version of CCK or SCK is used. This indication is used as a safeguard to the MS to detect if the CCK or SCK has been changed if the D-CK CHANGE DEMAND PDU has been missed.

In cells of security class 2 the SCK shall be used to encrypt individual addressed signalling and traffic. In cells that supportgroup call, a GCK may be associated with a single or multiple group addresses at any time. The SCK shall be used as a key modifier to produce the MGCK which shall be used to encrypt group addressed signalling and traffic (see 4.2.2). If no GCK is assigned to a group then SCK shall be used to encrypt all group addressed signalling and traffic. SCK shall also be used with the identity encryption mechanism to conceal identities in use at the air interface within a SwMI. Only one SCK shall be in use within a SwMI at any one time except during key change period.

In cells of security class 3 the DCK shall 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.

In cells of security class 3 that support group calls a GCK may be associated with a single or multiple group addresses 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 (see 4.2.2). If no GCK is assigned to a group then CCK shall be used to encrypt all group addressed signalling and traffic. CCK shall also be used in conjunction with the identity encryption mechanism to protect all SSIs used with encryption within an LA. An MS may store the CCKs in use in more than one LA to ease cell re-selection.

The use of cipher keys for security class 3 is illustrated in figure 53.



BS = Base Station
MS = Mobile Station

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

Figure 53: Illustration of cipher key use in class 3 system

6.5.1 Identification of encryption state of downlink MAC PDUs

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 the encryption state of each TM-SDU for each cell security class as shown in clauses 6.5.1.1 through 6.5.1.3. These bits also indicate the use of the ESI mechanism.

6.5.1.1 Class 1 cells

In a cell supporting only class 1 the following values and interpretations shall apply:

Table 14: Encryption mode element in class 1 cell contents

Information Element	Length	Value	Remark
Encryption mode element	2	00_2	PDU not encrypted
		Others	Reserved

6.5.1.2 Class 2 cells

In a class 2 cell the following values and interpretations shall apply:

Table 15: Encryption mode element in class 2 cell contents

Information Element	Length	Value	Remark
Encryption mode element	2	00_2	PDU not encrypted
		01_2	Reserved
		10_2	PDU encrypted, SCK-VN is even
		11_2	PDU encrypted, SCK-VN is odd

To prevent attacking by replaying a previous key, the SCK shall be identified by a longer SCK-VN which shall be sent to an MS together with the SCK.

6.5.1.3 Class 3 cells

In a class 3 cell the following values and interpretations shall apply:

Table 16: Encryption mode element in class 3 cell contents

Information Element	Length	Value	Remark
Encryption mode element	2	00_2	PDU not encrypted
		01_2	Reserved
		10_2	PDU encrypted, CCK-id is even
		11_2	PDU encrypted, CCK-id is odd

In class 3 cells every cell in an LA shall use the same CCK and the CCK shall be identified by common CCK-id in all the cells of the LA. SwMI may also provide CCK informing that it is applicable for several LAs, then the CCK shall be identified by common CCK-id in all these applicable LAs. CCK change shall therefore be synchronized across all cells in an LA, and across all LAs in which SwMI tells that the same CCK is applicable.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.

When CCK-id rolls over from 2^{16}-1 to 0 the value of 0 shall be considered higher than 2^{16}-1 for the purposes above.

6.5.2 Identification of encryption state of uplink MAC PDUs

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 shall be achieved by the 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 use of the encrypted short identity mechanism described in clause 4.2.6 for cells of class 2 and class 3.

6.6 Mobility procedures

6.6.1 General requirements

The cell selection procedures are defined in EN 300 392-2 [2], clause 18.3.4 and shall always apply with the additional security criteria defined below:

1) if the MS does not support the security class of the cell it shall not select the cell;

2) if the MS does not support authentication as required by the cell it shall not select the cell;

3) if moving to a new cell of different class from the current serving cell the MS may have to perform the location update procedure at the new cell.

In moving from a cell of security class 3 or security class 2 to a cell of security class 1 the SwMI shall determine if the call can be restored. The SwMI may wish to deny call restoration in this case because the air interface security has been changed.

6.6.1.1 Additional requirements for class 3 systems

Where scanning of adjacent cells is performed by the moving MS the MS shall gain knowledge of the CCK-id of the CCK in use on the adjacent cell by receiving the SYSINFO broadcast, and of the value of IV on that cell by receiving the SYNC and SYSINFO broadcasts. The broadcast parameters shall be made available to the MM sub-layer by MLE using the MLE-INFOindication primitive.

Within an LA of security class 3 all cells shall have knowledge of the DCK in use for each ITSI operating in that LA. If the SwMI offers a registered area to the MS it shall ensure that all LAs have knowledge of the DCK for that MS operating in that registered area.

6.6.2 Protocol description

If the SwMI supports GCK operation the SwMI shall indicate this using the "GCK Supported" field in the extended service broadcast described in EN 300 392-2 [2]. This field shall be used to indicate to the MS when GCKs are in use or not in use by the system. If in use, all cells in the SwMI should advertise "GCKs are supported". If not in use, all cells in the SwMI should advertise "GCKs are not supported". When GCKs are not supported, the SwMI and MS shall revert to using the SCK in class 2 cells, and CCK in class 3 cells, for all group addressed signalling and traffic.

6.6.2.1 Negotiation of cipher parameters

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.

Every registration shall include cipher parameter negotiation to allow the MS to establish the security parameters advised in the cell broadcast.

EN 300 392-2 [2] defines the presence of cipher parameters in the D-LOCATION UPDATE COMMAND, D-LOCATION UPDATE REJECT and U-LOCATION UPDATE DEMAND PDUs. The use of these parameters is described in this part of the EN.

The ciphering parameters shall be used to negotiate SCKN and KSG in class 2 cells, and KSG in class 3 cells using the cipher parameters element defined in table 17.

Table 17: Cipher parameters element contents

Information sub-element	Length	Type	C/O/M	Remark
KSG number	4	1	M	
Security class	1	1	M	Value = 0 = Class 2 Value = 1 = Class 3
SCK number	5	1	C	If class 2
Reserved	5	1	C	If class 3, default value 0

If a cell supports class 2 and class 1, or class 3 and class 1, negotiation of cipher parameters by the MS shall be at the highest security class possible for the MS.

6.6.2.1.1 Class 1 cells

Cipher control shall always be set to false and the ciphering parameters shall not be provided.

6.6.2.1.2 Class 2 cells

Cipher control shall always be set to true.

On registration the MS shall declare its preferred KSG and SCKN (broadcast by the cell) to the SwMI. If these parameters are accepted by the SwMI the registration shall continue as described in EN 300 392-2 [2], clause 16. If the parameters are unacceptable the SwMI shall reject the registration and shall indicate the preferred parameters in the D-LOCATION UPDATE REJECT PDU.

6.6.2.1.3 Class 3 cells

Cipher control shall always be set to true.

On registration the MS shall declare its preferred KSG to the SwMI. If these parameters are accepted by the SwMI the registration shall continue as described in EN 300 392-2 [2], clause 16. If the parameters are unacceptable the SwMI shall reject the registration and shall indicate the preferred parameters in the D-LOCATION UPDATE REJECT PDU.

6.6.2.2 Initial and undeclared cell re-selection

See also EN 300 392-2 [2], clause 18.3.4.7.2.

In cells of security class 3 the MS may register and authenticate to the new cell and in so doing receive new values of DCK and CCK. If when camped on the cell the MS confirms that it holds a valid CCK for the cell (from capturing the CCK-id in SYSINFO) it may not refresh the CCK during registration.

NOTE: The broadcast parameters are available to MM from the MLE-INFO indication primitive.

In cells of security class 2 the MS may, if required, register and authenticate to the new cell.

If the MS knows the preferred neighbour cell it may indicate the LA of the new cell using the U-OTAR PREPARE PDU and shall start timer T372. On receipt of U-OTAR PREPARE the SwMI shall forward the DCK belonging to the MS to the cells belonging to the LA (DCK forwarding) if possible. The MS shall reset timer T372 on receipt of D-OTAR NEWCELL. Following this, the MS may apply AI encryption to location update signalling on the new cell if the DCK forwarding was successful and it possesses a valid CCK for the LA of the new cell. This procedure is shown in figure 54 where the LA-id of the new cell is known to the MS.

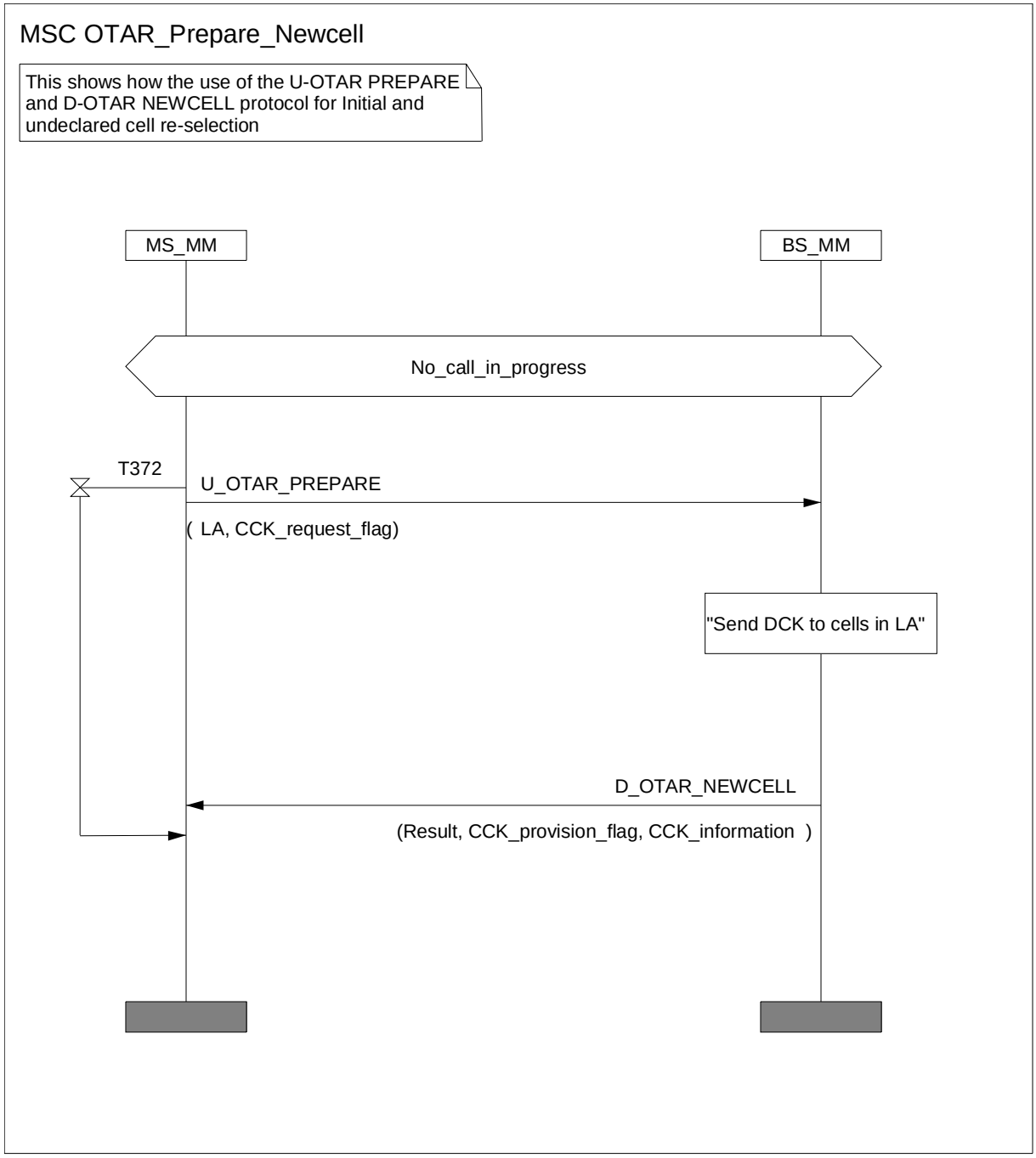


Figure 54: Use of U-OTAR PREPARE and D-OTAR NEWCELL protocol

If the MS does not know a preferred neighbour cell it cannot indicate the preferred neighbour cell to the SwMI and therefore the SwMI can not forward the DCK to the new cell. On successful completion of cell re-selection, the MS may only apply AI encryption if the SwMI indicates it supports "DCK retrieval during cell re-selection" (DCK retrieval), shown in table 18, and the MS possesses a valid CCK for the LA of the new cell.

For initial cell selection (power on) in the home network, the MS may only apply AI encryption if the SwMI indicates it supports "DCK retrieval during initial cell selection" (DCK retrieval), shown in table 18, and the MS possesses a valid DCK and a valid CCK for the LA of the cell. A valid DCK is defined as the DCK that was last derived between the MS and the home SwMI.

For initial cell selection (power on) in a foreign network, the MS shall assume that the DCK generated in the previous network is no longer valid. Therefore, the MS shall not apply AI encryption independent of the indication by the SwMI to support "DCK retrieval during initial cell selection" (DCK retrieval), shown in table 18.

When the MS has successfully invoked initial cell selection with the SwMI but suffers momentary radio link failure, the MS may use 'roaming location updating' when the radio link is re-established, in which case the MS may only apply AI encryption if the SwMI indicates it supports "DCK retrieval during cell re-selection" (DCK retrieval), shown in table 18, and the MS possesses a valid DCK and a valid CCK for the LA of the cell. A valid DCK is defined as the DCK that was last derived between the MS and the SwMI.

6.6.2.3 Unannounced cell re-selection

See also EN 300 392-2 [2], clause 18.3.4.7.3.

In cells of security class 3 the MS may register and authenticate to the new cell and in so doing receive new values of DCK and CCK.

In cells of security class 2 the MS may register and if required authenticate to the new cell.

After successful registration and restoration of security parameters any calls in progress may be restored.

If the MS knows the preferred neighbour cell it may indicate the LA of the new cell using the U-OTAR PREPARE PDU and shall start timer T372. When the SwMI receives this signalling it shall forward the DCK belonging to the MS to the cells belonging to the LA (DCK forwarding) if possible. The MS shall reset timer T372 on receipt of D-OTAR NEWCELL. Following this, the MS may apply AI encryption to location update signalling on the new cell if the DCK forwarding was successful and it possesses a valid CCK for the LA of the new cell.

If the MS does not know a preferred neighbour cell it cannot indicate the preferred neighbour cell to the SwMI and therefore the SwMI can not forward the DCK to the new cell. On successful completion of cell re-selection, the MS may only apply AI encryption if the SwMI indicates it supports "DCK retrieval during cell re-selection" (DCK retrieval), shown in table 18, and the MS possesses a valid CCK for the LA of the new cell.

6.6.2.4 Announced cell re-selection type-3

See also EN 300 392-2 [2], clause 18.3.4.7.4.

On successful completion of cell re-selection, the MS may only apply AI encryption if the SwMI indicates it supports "DCK retrieval during cell re-selection" (DCK retrieval), see table 18, and the MS possesses a valid CCK for the location area of the new cell.

If the MS knows the preferred neighbour cell it may indicate the LA of the new cell using the U-OTAR PREPARE PDU and shall start timer T372. When the SwMI receives this signalling it shall forward the DCK belonging to the MS to the cells belonging to the LA (DCK forwarding) if possible. The MS shall reset timer T372 on receipt of D-OTAR NEWCELL. Following this, the MS may apply AI encryption to location update signalling on the new cell if the DCK forwarding was successful and it possesses a valid CCK for the LA of the new cell.

6.6.2.5 Announced cell re-selection type-2

See also EN 300 392-2 [2], clause 18.3.4.7.5.

The SwMI shall use the cell identifier in the U-PREPARE to forward the DCK to the new cell (DCK forwarding). On successful completion of cell re-selection, the MS may apply AI encryption on the new cell if it possesses a valid CCK for the location area of the new cell.

6.6.2.6 Announced cell re-selection type-1

See also EN 300 392-2 [2], clause 18.3.4.7.6.

The SwMI shall use the cell identifier in the U-PREPARE to forward the DCK to the new cell (DCK forwarding). On successful completion of cell re-selection, the MS may apply AI encryption on the new cell if it possesses a valid CCK for the location area of the new cell.

6.6.2.7 Key forwarding

The U-OTAR PREPARE / D-OTAR NEWCELL signalling is used for DCK forwarding to the new LA and CCK retreival from the new LA. No other mobility management nor call restoration functionality shall be assumed by the SwMI nor the MS.

Timer T372, Key Forwarding Timer, shall have a value of 5 seconds.

T372 shall indicate the maximum time the MM shall wait for a response to U-OTAR PREPARE. If timer T372 expires, or radio link failure occurs, the MS shall abandon signalling and initiate the cell change procedure immediately (see figure 55).

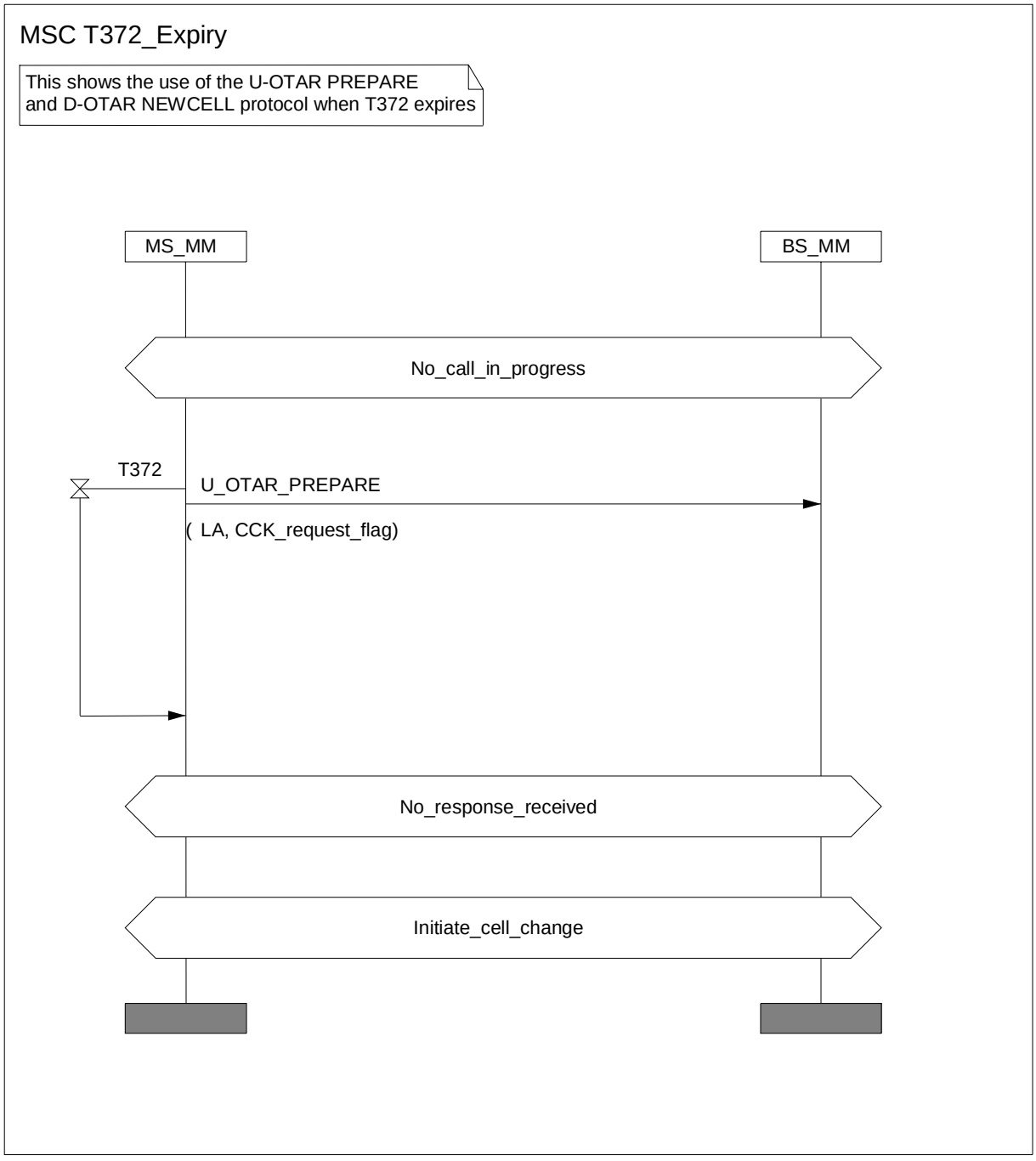


Figure 55: Use of U-OTAR PREPARE and D-OTAR NEWCELL protocol with T372 expiry

6.7 Encryption control

The following clauses apply for class 2 and class 3 cells.

6.7.1 Data to be encrypted

6.7.1.1 Downlink control channel requirements

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

- cell synchronization messages sent to the MAC via the TMB-SAP (SYNC, SYSINFO).

The ACCESS DEFINE PDU is not encrypted as it has no associated TM-SDU.

6.7.1.2 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 EN 300 392-2 [2], clause 21.4.3.1) all information following the channel allocation flag shall be encrypted. The channel allocation flag shall not be included in the data to be encrypted;

- in the downlink MAC-END PDU (see EN 300 392-2 [2], clause 21.4.3.3) all information following the channel allocation flag shall be encrypted. The channel allocation flag shall not 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.

The KSG shall be initialized as described in clause 6.3.2.1.

6.7.1.3 Traffic channel encryption control

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

Traffic slots do not incorporate a separate MAC header in the same way as control (signalling) slots. Instead, the entire slot is used for traffic data. Therefore on a traffic slot, the SDU that is encrypted is the entire content of the transmitted slot.

The initial use of encryption on the U-plane shall maintain the use of encryption of the C-plane signalling message which causes the switch to the U-plane (see EN 300 392-2 [2], clauses 14.5.1.4 and 14.5.2.4).

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

In the case that U-Plane mode is 'encrypted' the MS shall send all signalling encrypted (sent with one of stealing, Fast Associated Control Channel (FACCH), Slow Associated Control Channel (SACCH)). In the case where U-Plane mode is 'clear' the MS shall send all call related signalling in clear (sent with one of stealing, FACCH, SACCH) and all call unrelated signalling may be encrypted.

6.7.2 Service description and primitives

Each layer in the protocol stack provides a set of services to the layer above. This clause describes the services that are added to those provided by each layer due to the incorporation of encryption, in addition to those specified in EN 300 392-2 [2]. The primitives that are passed between the layers are also described.

The primitives required to control encryption are summarized in figure 56.

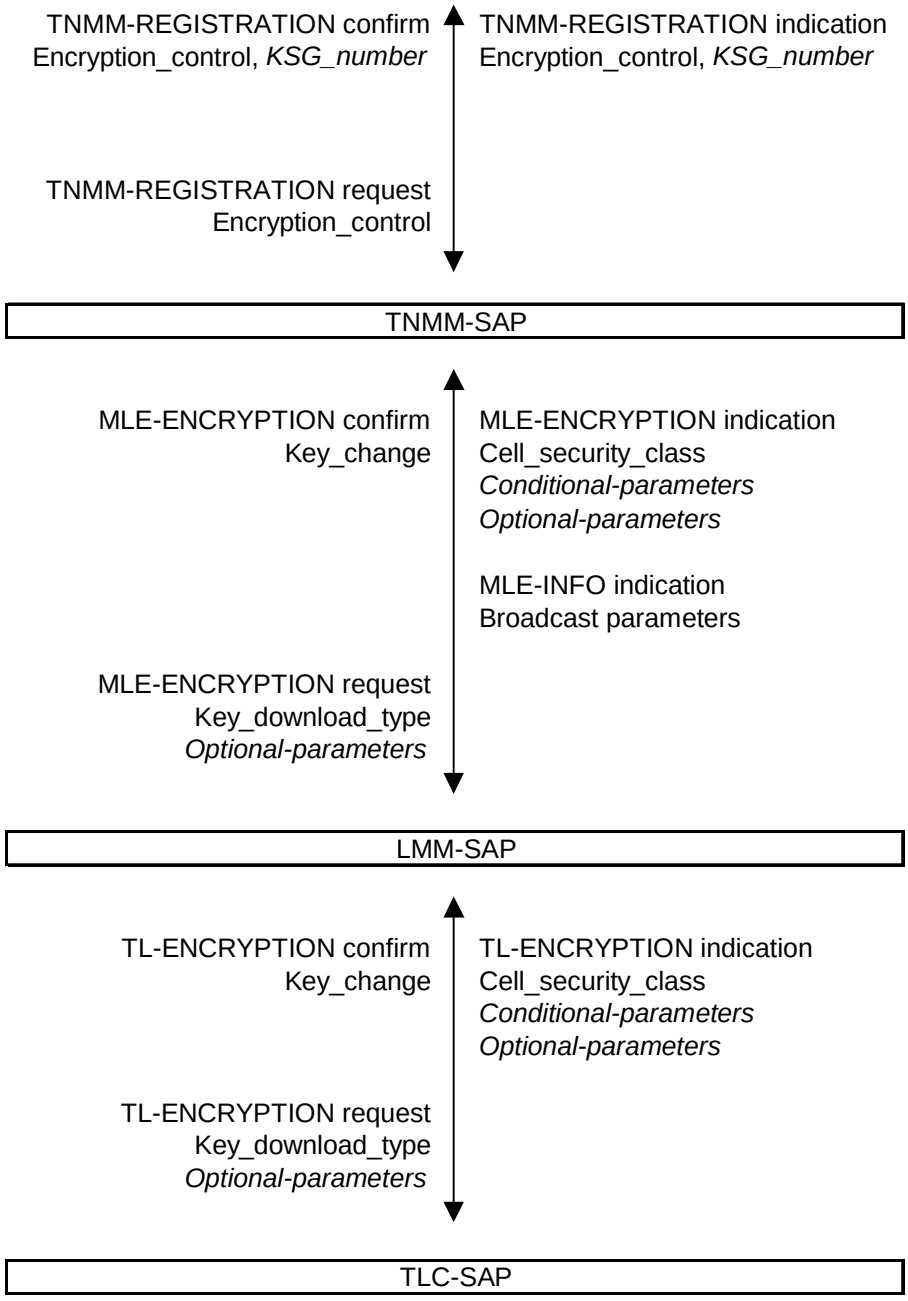


Figure 56: Protocol stack and primitives for encryption control

6.7.2.1 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 18: TNMM-REGISTRATION parameters (c.f. EN 300 392-2 [2], clause 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.			

6.7.2.2 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 SYSINFO PDU.

The MAC shall indicate to MM if the short CCK-id or short SCK-VN (in the MAC RESOURCE PDU) does not correspond to the CCK identifier or SCK-VN of the CCK or SCK that MLE is currently using. In addition the MAC shall indicate to MM if the encryption information received in SYSINFO has changed.

Table 19: MLE-ENCRYPTION parameters

Parameter	Request	Confirm	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		C
SCK-VN	C		C
SCKN	C		C
MGCK (note 2)	C		-
GTSI (note 3)	C		-
xSSI (note 5)	C		-
GSKO	C		
Cipher usage (note 1)	O		-
Time (note 6)	O		
Key change (note 6)	-	M	-
Cell security class			M
Cell parameters changed			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. NOTE 6: If invoked from KEY CHANGE DEMAND.			

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, SCKN, SCK-VN;

DCK, xSSI pair;

CCK, CCK-id, LA-id;

MGCK, GTSI

GSKO

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.

6.7.2.3 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 EN 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.

6.7.3 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 clauses.

6.7.3.1 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 may have to perform a re-registration if the SwMI requires a change in the encryption parameters including on-off control of encryption.

6.7.3.2 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.

6.7.3.3 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.

6.7.3.4 MAC

The MAC shall indicate to MM a change in the CCK-id broadcast in MAC SYSINFO using the MLE-INFO primitive.

The MAC shall indicate to MM a change of security class broadcast in MAC SYSINFO using the MLE-INFO primitive.

6.7.4 PDUs for cipher negotiation

Ciphering elements shall be contained in the U-LOCATION UPDATE DEMAND, D-LOCATION UPDATE COMMAND, and the D-_LOCATION UPDATE REJECT PDUs to permit negotiation of encryption parameters. These PDUs are described in EN 300 392-2 [2], clause 16.9.

The definition of reject cause is given in EN 300 392-2 [2], clause 16.10.42

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 type 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 clause 4.4.7.

7 End-to-end encryption

7.1 Introduction

End-to-end encryption algorithms and key management are outside the scope of the present document. This clause describes a standard mechanism for synchronization of the encryption system that may be employed when using a synchronous stream cipher. The mechanism also permits transmission of encryption related and other signalling information. The mechanism shall apply only to U-plane traffic and U-plane signalling. The method described shall use the Stealing Channel, STCH, for synchronization during transmission (see EN 300 392-2 [2], clause 23.8.4).

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

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

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

7.2 Voice encryption and decryption mechanism

Figure 57 shows a functional diagram of the voice encryption and decryption mechanism based on the synchronous stream cipher principle. This demonstrates the symmetry of transmitter and receiver with each side having common encryption units.

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

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

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

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

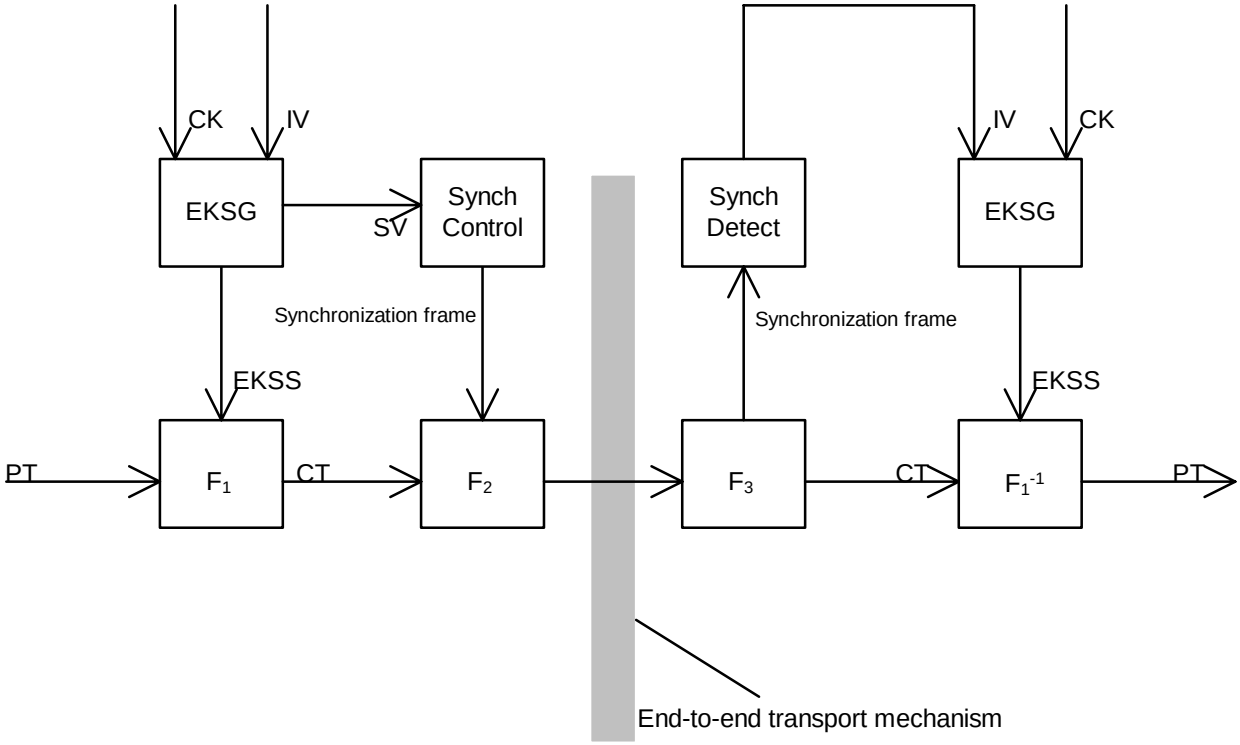


Figure 57: Functional diagram of voice encryption and decryption mechanisms

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 or a similarly time variant cipher key.

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

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

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 clause 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 the present document.

7.4.1 Synchronization of encryption units

Figure 57 shows the processing blocks "synchronization control" and "synchronization detect" and their associated functions F_2 and F_3 that shall provide the means of synchronizing the EKSG.

There shall be two synchronization cases to consider:

- initial synchronization; and
- re-synchronization.

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

Both cases shall use frame stealing as a means of inserting synchronization data in the traffic path (see EN 300 392-2 [2], clause 23.8.4).

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

Table 20 shows the TMD-UNITDATA primitive that shall be used by the frame stealing mechanism to address the MAC (request) and to inform the U-plane (indication).

Table 20: 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

Table 21 shows the parameters of the TMD-REPORT primitive that shall be used for any further communication from MAC to the U-plane.

Table 21: Parameters used in the TMD-REPORT primitive

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

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

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

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

7.4.2 Encrypted information between encryption units

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

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

Table 20 shows the TMD-UNITDATA primitive that shall be used by the frame stealing mechanism to address the MAC (request) and to inform the U-plane (indication).

Table 21 shows the parameters of the TMD-REPORT primitive that shall be used for any further communication from MAC to the U-plane.

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

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

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

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

Table 22: Maximum average frequency of stealing

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

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

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

If the encryption unit steals a frame it shall update the header of the stolen frame 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 AI to allow the receiving MS to recognize a stolen frame.

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

Figure 58 gives an example for determining the points of time of transmitting a new SV by the "sync-control" process. Transmission of a new SV may be forced after a period of 1 s after the last transmission of an SV. More SV's may be transmitted to improve reliability of synchronization and to allow for late entry.

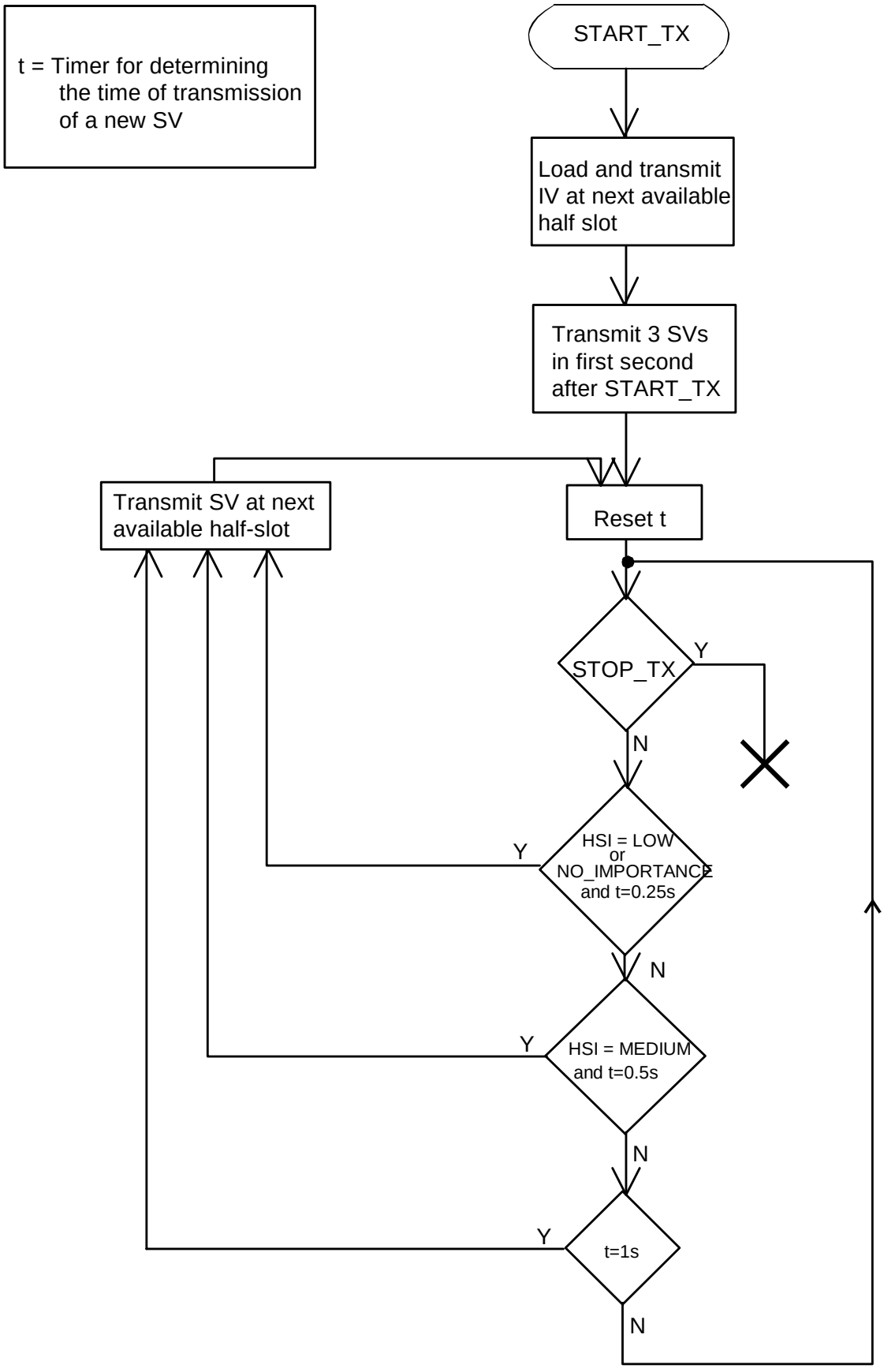


Figure 58: Flow chart of an example transmitter "sync-control" process

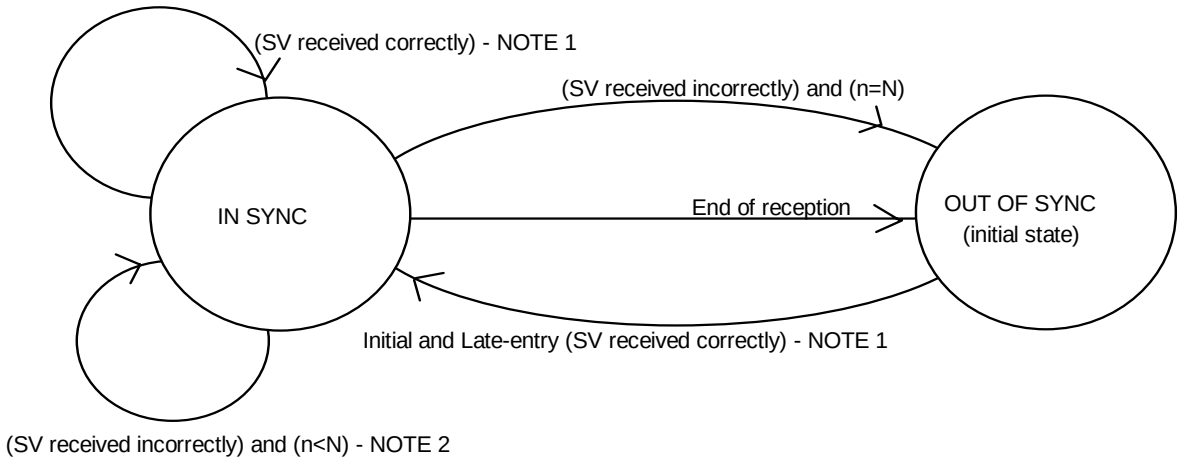
7.4.4 Reception

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

If HSC≠GOOD, the half slot content should be discarded and a flywheel mechanism in the synchronization detect unit should be used to maintain synchronization until a valid synchronization frame is received.

Figure 59 shows a state diagram of an example sync detect process.



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

In the flywheel mechanism the receiver should use locally generated Synchronization Values (SVs) if an SV is not received correctly. Incrementing, or generation of, SV should be pre-determined by the encryption units.

7.4.5 Stolen frame format

Table 23 defines the format of a stolen frame (half-slot).

Table 23: Stolen frame format (half-slot)

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

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

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

- algorithm number;

- key number;
- SV.

Where a codec is the U-plane traffic source/sink it should not make any interpretation of data in a stolen frame if that data has been stolen by the encryption unit. The matrix below (see table 24) indicates the terminating devices for stolen frames based upon the values of HSSE and SHSI where a codec is present:

Table 24: 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 clause describes the location of the encryption unit in the U-plane.

Figure 60 shows that 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 [6]), or any circuit mode data unit.

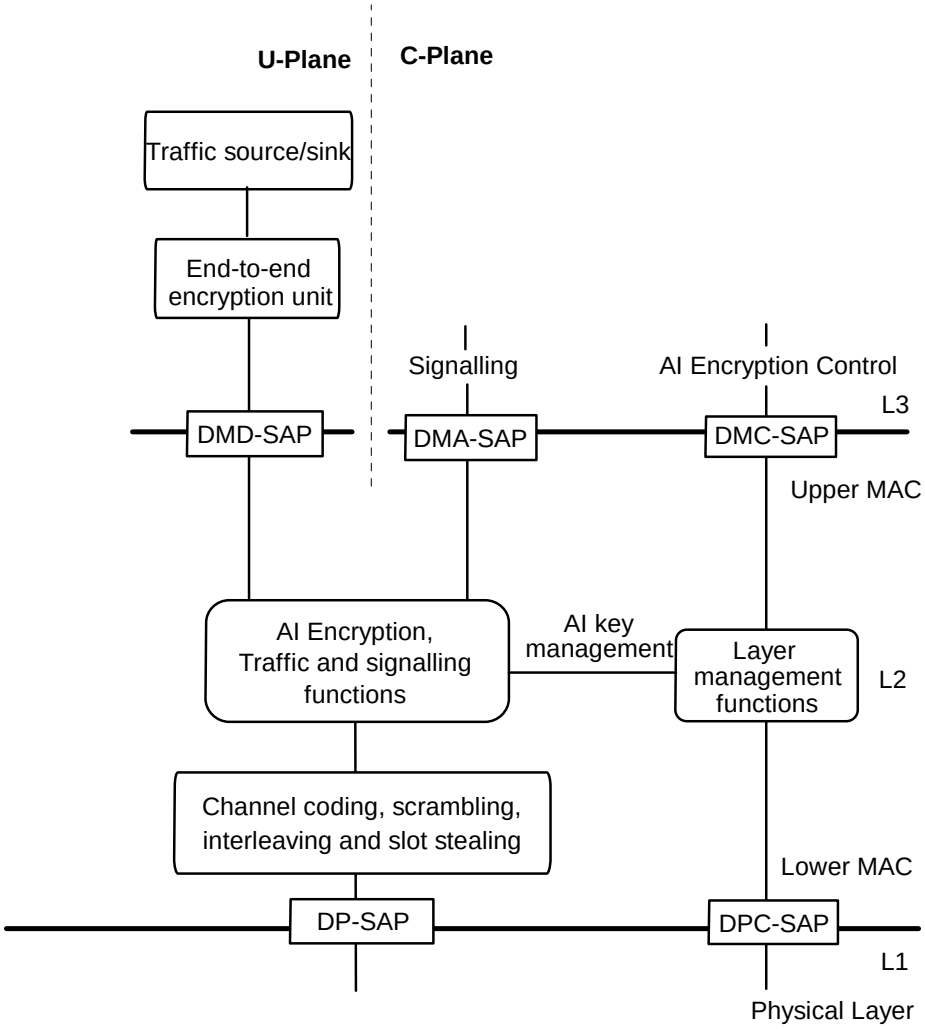


Figure 60: Position of end-to-end encryption unit in MS

The services offered on the U-Plane side, as shown in figure 60, may be further expanded as shown in figure 61.

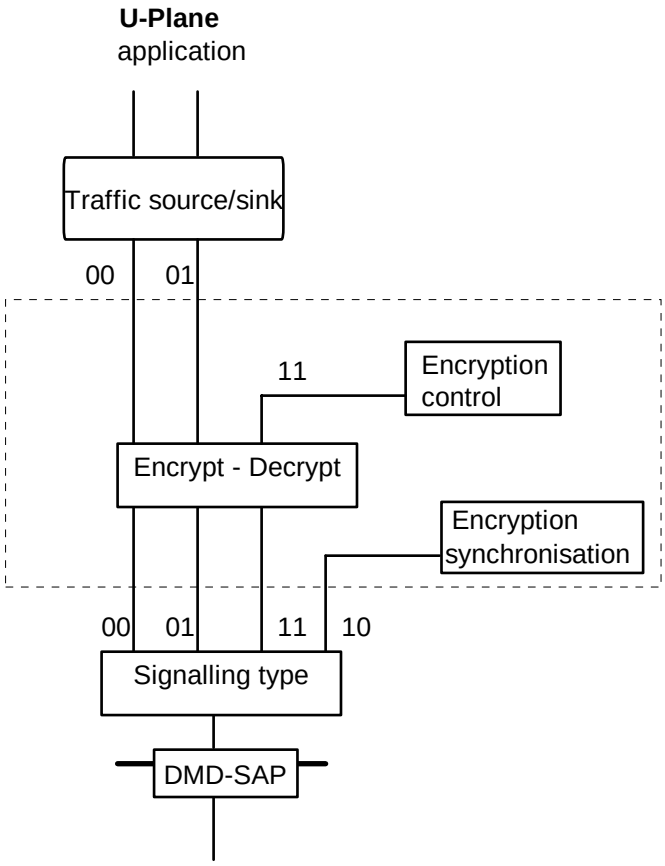


Figure 61: Functional model of the encryption unit

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

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

The short data service type 4 shall incorporate a header in the first byte of the user defined content as given by EN 300 392-2 [2], clause 29.3.5.8

Annex A (normative): PDU and element definitions

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

The general format and encoding rules are defined for all MM PDUs in EN 300 392-2 [2], clause 14.7.

A.1 Authentication PDUs

A.1.1 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 A.1: D-AUTHENTICATION DEMAND PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-AUTHENTICATION
Authentication sub-type	2	1	M	DEMAND
Random challenge [RAND1]	80	1	M	
Random seed [RS]	80	1	M	
Proprietary element		3	O	

A.1.2 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 A.2: D-AUTHENTICATION REJECT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-AUTHENTICATION
Authentication sub-type	2	1	M	REJECT
Authentication reject reason	3	1	M	

A.1.3 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 A.3: D-AUTHENTICATION RESPONSE PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-AUTHENTICATION
Authentication sub-type	2	1	M	RESPONSE
Random seed [RS]	80	1	M	
Response value [RES2]	32	1	M	
Mutual authentication flag	1	1	M	
Random challenge [RAND1]	80		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.				

A.1.4 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 A.4: D-AUTHENTICATION RESULT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-AUTHENTICATION
Authentication sub-type	2	1	M	RESULT
Authentication result [R1]	1	1	M	
Mutual authentication flag	1	1	M	
Response Value [RES2]	32		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.				

A.1.5 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 A.5: U-AUTHENTICATION DEMAND PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-AUTHENTICATION
Authentication sub-type	2	1	M	DEMAND
Random challenge [RAND2]	80	1	M	
Proprietary element		3	O	

A.1.6 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 A.6: U-AUTHENTICATION REJECT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-AUTHENTICATION
Authentication sub-type	2	1	M	REJECT
Authentication reject reason	3	1	M	

A.1.7 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 A.7: U-AUTHENTICATION RESPONSE PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-AUTHENTICATION
Authentication sub-type	2	1	M	RESPONSE
Response Value [RES1]	32	1	M	
Mutual authentication flag	1	1	M	
Random challenge [RAND2]	80		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.				

A.1.8 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 A.8: U-AUTHENTICATION RESULT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-AUTHENTICATION
Authentication sub-type	2	1	M	RESULT
Authentication result [R2]	1	1	M	
Mutual authentication flag	1	1	M	
Response Value [RES1]	32		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.				

A.2 OTAR PDUs

A.2.1 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 A.9: D-OTAR CCK Provide PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	CCK Provide
CCK provision flag	1	1	M	
CCK information	Varies		C	If CCK provision flag is true
Proprietary element		3	O	

A.2.2 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 A.10: U-OTAR CCK Demand PDU contents

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

A.2.3 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 A.11: U-OTAR CCK Result PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	CCK Result
Provision result	3	1	M	Provision result for CCK
Future key flag	1	1	M	
Provision result (Future key)	3		C	If future key flag is true (note)
Proprietary element		3	O	
NOTE: If D-OTAR Provide gives both current and future CCK then this flag is set true and this PDU shall contain two provision result fields. If D-OTAR Provide PDU provides only a future CCK then this flag shall be false.				

A.2.4 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 A.12: D-OTAR GCK Provide PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	GCK Provide
Session key	1	1	M	Identifies if provided for group or individual
RSO	80		C	Provided if session key for individual
GCK key and identifier	152	1	M	Contains SGCK, GCKN and GCK-VN
KSG number	4	1	M	Allows GCK/GTSI to be associated with a particular encryption algorithm
Group association	1	1	M	
GSSI	24		C	If Group association = GSSI
Address extension	24	2	O	Note
Proprietary element		3	O	
NOTE: The address extension element is only present if the network code for which the provided GSSIs relate is different to the serving network.				

A.2.5 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 A.13: U-OTAR GCK Demand PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	GCK Demand
KSG number	4	1	M	Allows GCK to be associated with a particular encryption algorithm
Group association	1	1	M	
GCKN	16		C	If Group association = GCKN
GSSI	24		C	If Group association = GSSI
Address Extension	24	2	O	Note
Proprietary element		3	O	
NOTE: The address extension element is only present if the network code for which the provided GSSIs relate is different to the serving network.				

A.2.6 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 A.14: U-OTAR GCK Result PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	GCK Result
GCKN	16	1	M	
GCK Version Number	16	1	M	
Provision result (GCK)	3	1	M	
Current GCK Version number	16		C	Defined as GCK-VN and sent when provision result has value incorrect key-VN.
Group association	1	1	M	
GSSI	24		C	If Group association = GSSI
Address Extension	24	2	O	Note
Proprietary element		3	O	
NOTE: The address extension element is only present if the network code for which the provided GSSIs relate is different to the serving network.				

A.2.7 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 A.15: D-OTAR SCK Provide PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	SCK Provide
Session key	1	1	M	Identifies if provided for group or individual
Random seed for OTAR	80		C	Provided if session key for individual
Number of SCKs provided	3	1	M	Note 2,3
SCK key and identifier	141		C	Note 1
KSG number	4	1	M	Allows SCK to be associated with a particular encryption algorithm
Proprietary element		3	O	
NOTE 1: 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. NOTE 2: The number of SCKs provided may not be the same as the number of SCKs demanded in the first place. NOTE 3: The maximum number of SCKs provided is 4.				

A.2.8 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 A.16: U-OTAR SCK Demand PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	SCK Demand
KSG number	4	1	M	Allows SCK to be associated with a particular encryption algorithm
Number of SCKs requested	3	1	M	
SCK number (SCKN)	5		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.				

A.2.9 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 A.17: U-OTAR SCK Result PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	SCK Result
Number of SCKs provided	3	1	M	
SCK number and result	8/24		C	Note
Proprietary element		3	O	
NOTE: The SCK number and result element is conditional on the Number of SCKs provided element. There shall be as many SCK number and result elements in the PDU as indicated by the Number of SCKs provided element.				

A.2.10 D-OTAR GSKO Provide

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

Direction: SwMI to MS;

Service used: MM;

Response to: U-OTAR GSKO Demand or none;

Response expected: U-OTAR GSKO Result.

Table A.18: D-OTAR GSKO Provide PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	GSKO Provide
Random seed for OTAR	80	1	M	
GSKO-VN	16	1	M	
SGSKO	120	1	M	
KSG number	4	2	O	Allows GSKO to be associated with a particular encryption algorithm
Proprietary element		3	O	

A.2.11 U-OTAR GSKO Demand

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

Direction: MS to SwMI;

Service used: MM;

Response to: none;

Response expected: D-OTAR GSKO Provide.

Table A.19: U-OTAR GSKO Demand PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	GSKO Demand
Proprietary element		3	O	

A.2.12 U-OTAR GSKO Result

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

Direction: MS to SwMI;

Service used: MM;

Response to: D-OTAR GSKO Provide;

Response expected: none.

Table A.20: U-OTAR GSKO Result PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	GSKO Result
GSKO-VN	16	1	M	
Provision result	3	1	M	
Proprietary element		3	O	

A.3 PDUs for key association to GTSI

A.3.1 D-OTAR KEY ASSOCIATE DEMAND

Shall be used by SwMI to associate or disassociate a cipher key with one or more groups.

Direction: SwMI to MS;

Service used: MM;

Response to: none;

Response expected: U-OTAR KEY ASSOCIATE STATUS or none.

Table A.21: D-OTAR KEY ASSOCIATE DEMAND contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub type	4	1	M	Key associate demand
Acknowledgement flag	1	1	M	If true acknowledgement is required
Key association type	1	1	M	SCK (0), GCK (1)
SCK select number	6		C	Provided if key type = SCK
GCK select number	17		C	Provided if key type = GCK
Number of groups	5	1	M	(0) reserved, (1-31) number of groups.
GSSI (note 1)	24		C	Repeated element
Address extension (note 2)	24	2	O	
NOTE 1: The GSSI element is repeated; total number GSSI elements = value of 'Number groups' element. GSSI can only be provided for a single network within the same PDU.				
NOTE 2: The address extension element is only present if the network code for which the provided GSSIs relate is different to the serving network.				

A.3.2 U-OTAR KEY ASSOCIATE STATUS

Shall be used by MS to indicate successful association or disassociation of a cipher key with one or more groups.

Direction: MS to SwMI;

Service used: MM;

Response to: D-OTAR KEY ASSOCIATE DEMAND

Response expected: None.

Table A.22: U-OTAR KEY ASSOCIATE STATUS contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub type	4	1	M	Key associate status
Key association status	3	1	M	
Number of groups	5		C	Sent if result indicates unknown address and contains the number of unknown address, hence the number of GSSI fields that follow
GSSI	24		C	Repeated element sent if result indicates unknown address and contains the unknown address
Address extension (note)	24	2	O	
NOTE: The address extension element is only present if the network code for which the provided GSSIs relate is different to the serving network.				

A.4 PDUs to synchronise key or security class change

A.4.1 D-CK CHANGE DEMAND

Shall be used by SwMI to indicate a cipher key change either in the future or immediately.

Direction: SwMI to MS;

Service used: MM;

Response to: none;

Response expected: U-CK CHANGE RESULT or none.

Table A.23: D-CK CHANGE DEMAND contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-CK CHANGE DEMAND
Acknowledgement flag	1	1	M	
Change of Security Class	2	1	M	
Key change type	3	1	M	
SCK use	1		C	Provided if key change type = SCK
Number of SCKs changed	4		C	Provided if key change type = SCK; Reserved (0000_2).
SCK data (note 1)	21		C	Provided if key change type = SCK; repeated element.
CCK-id	16		C	Provided if key change type = CCK.
Number of GCKs changed	4		C	Provided if key change type = GCK; Reserved (0000_2).
GCK data (note 1)	32		C	Provided if key change type = GCK; repeated element.
GCK-VN	16		C	Provided if key change type = All GCK.
Time type	2	1	M	
Slot number	2		C	Provided if time type = Absolute IV
Frame number	5		C	Provided if time type = Absolute IV
Multiframe number	6		C	Provided if time type = Absolute IV
Hyperframe number	16		C	Provided if time type = Absolute IV
Network time (note 2)	48		C	Provided if time type = network time
NOTE 1: The SCK data or GCK data elements are repeated; total number of SCK data or GCK data elements = value of 'Number of SCKs changed' element. NOTE 2: As specified in EN 300 392-2 [2], clause 18.5.24.				

A.4.2 U-CK CHANGE RESULT

Shall be used by MS-MM to inform the SwMI that it has registered the required cipher key change.

Direction: MS to SwMI;

Service used: MM;

Response to: D-CK CHANGE DEMAND;

Response expected: none.

Table A.24: U-CK CHANGE RESULT contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-CK CHANGE RESULT
Change of Security Class	2	1	M	
Key change type	3	1	M	
SCK use	1		C	Provided if key change type = SCK
Number of SCKs changed	4		C	Provided if key change type = SCK; Reserved (0000_2).
SCK data (note)	21		C	Provided if key change type = SCK; repeated element.
CCK-id	16		C	Provided if key change type = CCK or no CK.
Number of GCKs changed	4		C	Provided if key change type = GCK; Reserved (0000_2).
GCK data (note)	32		C	Provided if key change type = GCK; repeated element.
GCK-VN	16		C	Provided if key change type = All GCK.
NOTE: The SCK Number or GCK Number elements are repeated to inform the SwMI of all keys that have been successfully selected. This may not be the same number as demanded by the SwMI.				

A.5 Other security domain PDUs

A.5.1 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 A.25: U-TEI PROVIDE PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-TEI PROVIDE
TEI	60	1	M	
SSI	24	1	M	
Address extension	24	2	O	
Proprietary element		3	O	

A.5.2 U-OTAR PREPARE

Shall be used by MS-MM to inform the SwMI that it intends to change to a new cell.

Direction: MS to SwMI;

Service used: MM;

Response to: none;

Response expected: D-OTAR NEWCELL.

Table A.26: U-OTAR PREPARE

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	OTAR PREPARE
Location Area	14	1	M	The Location Area of the preferred neighbour cell.
CCK request flag	1	1	M	
Proprietary element		3	O	

A.5.3 D-OTAR NEWCELL

Shall be used by SwMI to inform the MS of the result of the U-OTAR PREPARE exchange.

Direction: SwMI to MS;

Service used: MM;

Response to: U-OTAR PREPARE;

Response expected: none.

Table A.27: D-OTAR NEWCELL

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	OTAR NEWCELL
DCK Forwarding Result	1	1	M	
CCK provision flag	1	1	M	
CCK information	Varies		C	
Proprietary element		3	O	

A.6 PDUs for Enable and Disable

A.6.1 D-DISABLE

This message is sent by the Infrastructure to indicate that the mobile station shall be disabled (permanently or temporarily).

Direction: SwMI to MS;

Service used: MM;

Response to: -;

Response expected: U-DISABLE STATUS or U-AUTHENTICATION RESPONSE;

Table A.28: D-DISABLE contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-DISABLE
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		C	Present if equipment disable = 1
Subscription disable	1	1	M	Disable subscription
Address Extension	24		C	Present if Subscription disable = 1
SSI	24		C	Present if Subscription disable = 1
Authentication challenge	160	2	O	
Proprietary		3	O	

A.6.2 D-ENABLE

This message is sent by the Infrastructure to indicate that the mobile station shall be enabled after a disable.

Direction: SwMI to MS;

Service used: MM;

Response to: -;

Response expected: U-DISABLE STATUS or U-AUTHENTICATION RESPONSE;

Table A.29: D-ENABLE contents

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

A.6.3 U-DISABLE STATUS

This message is sent by the mobile station to inform the infrastructure of its response to an enable or disable request and its resulting status.

Direction: MS to SwMI;

Service used: MM;

Response to: D-DISABLE or D-ENABLE;

Response expected: None.

Table A.30: U-DISABLE STATUS contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-DISABLE STATUS
Equipment status	2	1	M	Indicates disabled state of equipment
Subscription status	2	1	M	Indicates disabled state of subscription
Enable/Disable result	3	1	M	
Address Extension	24	2	O	Present only if in response to enable/disable of susbscription
SSI	24	2	O	Present only if in response to enable/disable of susbscription
TETRA Equipment Identity	60	2	O	Present only if in response to enable/disable of equipment
Proprietary		3	O	

A.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 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 clause.

A.7.1 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 cell to which it is registering.

Direction: SwMI to MS;

MM PDU: D-LOCATION UPDATE ACCEPT;

Response to: U-AUTHENTICATION RESPONSE;

Response expected: none.

Table A.31: Authentication downlink element contents

Information Element	Length	Type	C/O/M	Remark
Authentication result [R1]	1	1	M	Only valid for authentication exchanges
TEI request flag	1	1	M	
CK provision flag	1	1	M	
CK provision information	varies	1	C	Provided if CK provision flag=TRUE

A.7.2 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 cell to which it is registering.

Direction: MS to SwMI;

MM PDU: U-LOCATION UPDATE DEMAND;

Response to: D-LOCATION UPDATE COMMAND or none;

Response expected: D-AUTHENTICATION RESPONSE.

Table A.32: Authentication uplink element contents

Information Element	Length	Type	C/O/M	Remark
CK request flag	1	1	M	If this is TRUE then the CK requested shall be implied by the security class field in ciphering parameters
Random challenge [RAND2]	80	2	O	

A.8 PDU Information elements coding

The encoding of the elements for the PDUs described in clause 4.4.7 is given in the following clauses. The most significant bit of the values shown in the tables is transmitted first.

A.8.1 Acknowledgement flag

The acknowledgement flag element shall be used to indicate whether or not U-OTAR KEY ASSOCIATE RESULT is expected after sending D-OTAR KEY ASSOCIATE DEMAND.

Table A.33: Acknowledgement flag element contents

Information element	Length	Value	Remark
Acknowledgement flag	1	0	No acknowledgement required
		1	Acknowledgement required

A.8.2 Address extension

The Address Extension Element is defined in ETS 300 392-1 [1] .

A.8.3 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 A.34: Authentication challenge element contents

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

A.8.4 Authentication reject reason

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

Table A.35: Authentication reject reason element contents

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

A.8.5 Authentication result

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

Table A.36: 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

A.8.6 Authentication sub-type

Authentication subtype identifies the specific PDUwhen PDU-type is 0000 (uplink) or 0001 (downlink).

Table A.37: Authentication sub-type element contents

Information element	Length	Value	Remark
Authentication sub-type (uplink)	2	00	U-AUTHENTICATION DEMAND
		01	U-AUTHENTICATION RESPONSE
		10	U-AUTHENTICATION RESULT
		11	U-AUTHENTICATION REJECT
Authentication sub-type (downlink)	2	00	D-AUTHENTICATION DEMAND
		01	D-AUTHENTICATION RESPONSE
		10	D-AUTHENTICATION RESULT
		11	D-AUTHENTICATION REJECT

A.8.7 CCK identifier

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

Table A.38: CCK Identifier element contents

Information element	Length	Value	Remark
CCK Identifier	16	Any	

A.8.8 CCK information

The CCK information element is defined as below.

Table A.39: CCK information element contents

Information Element	Length	Type	C/O/M	Remark
CCK identifier (CCK-id)	16	1	M	
Key type flag	1	1	M	0 = Current, 1 = Future
Sealed CCK (SCCK)	120	1	M	
CCK location area information	2-216	1	M	
Future key flag	1	1	M	Always false if key type flag = future
Sealed CCK (SCCK)	120	1	C	If future key flag = true

A.8.9 CCK Location area information

The CCK location area information element indicates how location area data is to be provided for any CCK.

Table A.40: CCK Location area information element contents

Information Element	Length	Type	C/O/M	Remark
Type	2	1	M	00 = All location areas
				01 = List is provided
				10 = LA-id mask is provided
				11 = Range of LA-ids is provided
Location area list	18-214	1	C	If Type = 01
Location area bit mask	14	1	C	If Type = 10
Location area selector	14	1	C	If Type = 10
Location area range	28	1	C	If Type = 11
NOTE: The mask is logically ANDed with the LA-id. If the result is equal to the selector, then LA-id is valid for the CCK.				

A.8.10 CCK request flag

The CCK request flag is used to ask the SwMI to send the CCK in use in the location area to which the MS is attempting to register.

Table A.41: CCK request flag element contents

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

A.8.11 Change of security class

The change of security class information element indicates to the MS that the current key change is, or is not, associated with a change in security class of the cell.

Table A.42: Change of security class element contents

Information element	Length	Value	Remark
Change of Security Class	2	00	No change of security class
		01	Transition to Security Class 1
		10	Transition to Security Class 2
		11	Transition to Security Class 3

A.8.12 Cipher parameters

The cipher parameters element is used to negotiate SCKN and KSG in class 2 cells, and KSG in class 3 cells.

Table A.43: Cipher parameters element contents

Information sub-element	Length	Type	C/O/M	Remark
KSG number	4	1	M	
Security class	1	1	M	Value = 0 = Class 2 Value = 1 = Class 3
SCK number	5	1	C	If class 2
Reserved	5	1	C	If class 3, default value 0

A.8.13 CK provision flag

The CK provision flag is used to indicate that CK information is present in the PDU.

Table A.44: CK provision flag element contents

Information element	Length	Value	Remark
CK provision flag	1	0	No CK information provided (FALSE)
		1	CK information provided (TRUE)

A.8.14 CK provisioning information

The CK provisioning information element is used to indicate that either SCK information, CCK information or both are present in the PDU.

Table A.45: CK provisioning information flag element contents

Information sub-element	Length	Type	C/O/M	Remark
SCK provision flag	1	1	M	
SCK information	Varies	1	C	If SCK provision flag=TRUE
CCK provision flag	1	1	M	
CCK information	Varies	1	C	If CCK provision flag=TRUE

A.8.15 CK request flag

The CK request flag is used to ask the SwMI to send the CCK or SCK in use in the location area to which the MS is attempting to register. The type of key requested by the MS shall be inferred by the security class field in the ciphering parameters information element, contained within the same PDU as the CK request flag.

Table A.46: CK request flag element contents

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

A.8.16 Class Change flag

The Class Change flag is used to indicate that the class to the SwMI is to change.

Table A.47: Class Change flag element contents

Information element	Length	Value	Remark
Class Change flag	1	0	No Class change
		1	Class change

A.8.17 DCK forwarding result

The purpose of the DCK forwarding result element is to indicate if the SwMI was able to forward DCK to the requested new cell.

Table A.48: DCK forwarding result element contents

Information element	Length	Value	Remark
DCK Forwarding Result	1	0	DCK forwarding failure
		1	DCK forwarding successful

A.8.18 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 A.49: Disabling Type element contents

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

A.8.19 Enable/Disable result

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

Table A.50: Enable/Disable result element contents

Information element	Length	Value	Remark
Enable/Disable result	3	000	Enable/disable successful
		001	Enable/disable failure, address mismatch
		010	Enable/disable failure, TEI mismatch
		011	Enable/disable failure, TEI and address mismatch
		100	Enable/disable failure, authentication is required
		101	Enable/disable failure, encryption is required
		110	Enable/disable failure, encryption and authentication are required
		others	Reserved for future expansion

A.8.20 Encryption mode

A.8.20.1 Class 1 cells

In a cell supporting only class 1 the following values and interpretations shall apply:

Table A.51: Encryption mode element in class 1 cell contents

Information Element	Length	Value	Remark
Encryption mode element	2	00_2	PDU not encrypted
		Others	Reserved

A.8.20.2 Class 2 cells

In a class 2 cell the following values and interpretations shall apply:

Table A.52: Encryption mode element in class 2 cell contents

Information Element	Length	Value	Remark
Encryption mode element	2	00_2	PDU not encrypted
		01_2	Reserved
		10_2	PDU encrypted, SCK-VN is even
		11_2	PDU encrypted, SCK-VN is odd

A.8.20.3 Class 3 cells

In a class 3 cell the following values and interpretations shall apply:

Table A.53: Encryption mode element in class 3 cell contents

Information Element	Length	Value	Remark
Encryption mode element	2	00_2	PDU not encrypted
		01_2	Reserved
		10_2	PDU encrypted, CCK-id is even
		11_2	PDU encrypted, CCK-id is odd

A.8.21 Equipment disable

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

Table A.54: Equipment disable element contents

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

A.8.22 Equipment enable

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

Table A.55: Equipment enable element contents

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

A.8.23 Equipment status

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

Table A.56: Equipment status element contents

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

A.8.24 Frame number

Refer to EN 300 392-2 [2], clause x.x.

A.8.25 Future key flag

The future key flag information element is defined in table A.57.

Table A.57: Future key flag information element contents

Information Element	Length	Value	Remark
Future key flag	1	0	Indicates that no future key data is provided
		1	Indicates that future key data is provided

A.8.26 GCK data

The GCK data information element is defined in table A.58.

Table A.58: GCK data information element contents

Information Element	Length	Type	C/O/M	Remark
GCK Number	16	1	M	
GCK Version number	16	1	M	

A.8.27 GCK key and identifier

The GCK key and identifier element is defined as below:

Table A.59: GCK key and identifier element contents

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

A.8.28 GCK Number (GCKN)

The GCKN is the identifier for a GCK used to associate it to one or more groups.

Table A.60: GCKN element contents

Information element	Length	Value	Remark
GCKN	16	any	

A.8.29 GCK select number

The GCKN contained in OTAR key associate messages to indicate either which key should be associated with the signalled group(s); or whether no key should be associated and existing key disassociated.

Table A.61: GCK select number element contents

Information element	Length	Value	Remark
GCK select number	17	$0\text{-}2^{16}\text{-}1$	GCK number (GCKN) selected
		2^{16}	No GCKN selected
		$2^{16}+1\text{-}2^{17}\text{-}1$	Reserved

A.8.30 GCK Version Number (GCK-VN)

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

Table A.62: GCK-VN element contents

Information element	Length	Value	Remark
GCK-VN	16	any	

A.8.31 Group association

The group association element determines whether the provided GCK is for association with one specific group, or for association with all groups linked to a specific GCKN.

Table A.63: Group association element contents

Information element	Length	Value	Remark
Group association	1	0	Associated with GCKN.
		1	Associated with specific GSSI.

A.8.32 GSKO Version Number (GSKO-VN)

The GSKO-VN shall be used in the group addressed OTAR mechanism to uniquely identify a key version number.

Table A.64: GSKO Version Number (GSKO-VN) element contents

Information element	Length	Value	Remark
GSKO-VN	16	any	

A.8.33 GSSI

See ETS 300 392-1 [1], clause 7.

A.8.34 Hyperframe number

Refer to EN 300 392-2 [2].

A.8.35 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 A.65: Intent/confirm element contents

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

A.8.36 IV

The initialisation value (composite of frame number, slot number, multiframe number and hyper frame number) which is used as input to the Key Stream Generator (KSG) for production of the Key Stream Segment (KSS).

Table A.66: IV element contents

Information element	Length	Value	Remark
Slot number	2	00	Slot 1
		01	Slot 2
		10	Slot 3
		11	Slot 4
Frame number	5	00000	Not used
		00001 to 10010	Frame 1 to 18
		Others	Not used
Multiframe number	6	000001 to 111100	
		Others	Not used
Truncated Hyperframe number	15	Any	The 15 least significant bits of the transmitted hyperframe number
Uplink/downlink flag	1	0	Downlink transmission
		1	Uplink transmission

A.8.37 Key association status

The key association status is sent by the MS to the SwMI to indicate the result of the key association Protocol exchange.

Table A.67: Key association result element contents

Information element	Length	Value	Remark
Key association status	3	000	Association carried out as requested
		001	Key not valid
		010	Address not valid
		Others	Reserved

A.8.38 Key association type

Key association type identifies the type of key to be associated to a group.

Table A.68: Key association type information element contents

Information Element	Length	Value	Remark
Key association type	1	0	SCK
		1	GCK

A.8.39 Key change type

Key change type identifies the type of key to be changed using the CK CHANGE protocol.

Table A.69: Key change type information element contents

Information Element	Length	Value	Remark
Key change type	3	000	SCK
		001	CCK
		010	GCK
		011	Fallback SCK
		100	All GCKs
		101	No cipher key
		Others	Reserved for future use

A.8.40 Key type flag

Table A.70: Key type flag information element contents

Information Element	Length	Value	Remark
Key type flag	1	0	Current
		1	Future

A.8.41 KSG-number

KSG number identifies the encryption algorithm in use.

Table A.71: KSG Number element contents

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

A.8.42 Location area

See EN 300 392-2 [2], clause 16.

A.8.43 Location area bit mask

The location area bit mask element provides an indication of location areas.

Table A.72: Location area bit mask element contents

Information element	Length	Value	Remark
Location area bit mask	14	any	Mask to be logically ANDed with LA-id for CCK distribution

A.8.44 Location area selector

The location area selector is used in conjunction with the location area bit mask element to provide an indication of location areas.

Table A.73: Location area selector element contents

Information element	Length	Value	Remark
Location area selector	14	any	Bit pattern for comparison with local LA-id

A.8.45 Location area list

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

Table A.74: 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.				

A.8.46 Location area range

The location area range element provides a list of location areas that runs from Low Location Area value to High Location Area value.

Table A.75: Location area range element contents

Information element	Length	Value	Remark
Low Location Area value (LLAV)	14	1 to 2^{14}-1	Lowest value of LA-id for which CCK is valid
High Location Area value (HLAV)	14	1 to 2^{14}-1	Highest value of LA-id for which CCK is valid
NOTE: HLAV shall always be greater that LLAV.			

A.8.47 Mobile country code

See ETS 300 392-1 [1], clause 7.

A.8.48 Mobile network code

See ETS 300 392-1 [1], clause 7.

A.8.49 Multiframe number

See EN 300 392-2 [2].

A.8.50 Mutual authentication flag

The Mutual Authentication Identifier is used to indicate whether or not mutual authentication elements are included in the PDU.

Table A.76: Mutual authentication flag element contents

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

A.8.51 Network time

See EN 300 392-2 [2], clause 18.5.24 [2].

A.8.52 Number of GCKs changed

The Number of GCKs changed element indicates how many group cipher keys were changed in the OTAR protocol.

Table A.77: Number of GCKs changed element contents

Information element	Length	Value	Remark
Number of GCKs changed	4	0000	No GCKs changed
		0001	1 GCK changed
		0010	2 GCKs changed
		0011	3 GCKs changed
		0100	4 GCKs changed
		Others	Etc. up to 15 GCKs changed

A.8.53 Number of groups

The Number of groups element indicates how many GSSI elements there are to follow in the PDU.

Table A.78: Number of groups element contents

Information element	Length	Value	Remark
Number of groups	5	Any	Value of 0 reserved.

A.8.54 Number of location areas

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

Table A.79: Number of location areas element contents

Information element	Length	Value	Remark
Number of location areas	4	0000	Reserved
		0001 to 1111	1 to 15 location areas

A.8.55 Number of SCKs changed

The Number of SCKs changed element indicates how many static cipher keys were changed in the OTAR protocol.

Table A.80: Number of SCKs changed element contents

Information element	Length	Value	Remark
Number of SCKs changed	4	0000	No SCKs changed
		0001	1 SCK changed
		0010	2 SCKs changed
		0011	3 SCKs changed
		0100	4 SCKs changed
		Others	Etc. up to 15 SCKs

A.8.56 Number of SCKs provided

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

Table A.81: Number of SCKs provided element contents

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

A.8.57 Number of SCKs requested

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

Table A.82: Number of SCKs requested element contents

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

A.8.58 OTAR sub-type

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

Table A.83: OTAR sub-type element contents

Information element	Length	Value	Remark
OTAR sub-type	4	0000	CCK Demand (uplink) or CCK Provide (downlink)
		0001	CCK Result
		0010	SCK Demand (uplink) or SCK Provide (downlink)
		0011	SCK Result
		0100	GCK Demand (uplink) or GCK Provide (downlink)
		0101	GCK Result
		0110	Key associate Demand (downlink) or Key associate Status (uplink)
		0111	OTAR Prepare (Uplink) or OTAR NEWCELL (downlink)
		1000	GSKO Demand (uplink) or GSKO Provide (downlink)
		1001	GSKO Result
		1000 to 1111	Reserved

A.8.59 PDU type

The PDU type indicates the MM PDU type for all the security PDUs including 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 EN 300 392-2 [2], clause 16.

Table A.84: PDU type element contents

Information element	Length	Value	Downlink Assignment	Uplink Assignment
PDU Type	4	0000	D-OTAR	U-AUTHENTICATION
		0001	D-AUTHENTICATION	
		0010	D-CK CHANGE DEMAND	
		0011	D-DISABLE	
		0100	D-ENABLE	U-CK CHANGE RESULT
		0101		U-OTAR
		1001		U-TEI PROVIDE
		1011		U-DISABLE STATUS

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

A.8.60 Proprietary

See EN 300 392-2 [2] table 120a.

A.8.61 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 A.85: Provision result element contents

Information element	Length	Value	Remark
Provision result	3	000	Sealed key accepted
		001	Sealed key failed to decrypt
		010	Incorrect key number (e.g. SCKN, GCKN)
		011	OTAR rejected
		100	Incorrect Key version number (e.g. SCK-VN, GCK-VN)
		Others	Reserved

A.8.62 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 A.86: Random challenge element contents

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

A.8.63 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 processes.

Table A.87: Random seed element contents

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

A.8.64 Random seed for OTAR

The random seed for OTAR (RSO) is an 80 bit number used as the input to the session key for OTAR generation algorithm when sealing GCK, GSKO and SCK. 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 A.88: Random seed element contents

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

A.8.65 Reject cause

The reject cause element is defined in clause 16 of EN 300 392-2 [2] for the MM PDU, D-LOCATION UPDATE REJECT. The following table those reject causes which are defined by the security protocols.

Table A.89: Reject cause element contents

Information element	Length	Value	Remark
Reject cause	5	01101	No cipher KSG
		01110	Identified cipher KSG not supported
		01111	Requested cipher key type not available
		10000	Identified cipher key not available
		10010	Ciphering required
		10011	Authentication failure
		Others	See EN 300 392-2 [2] clause 16

A.8.66 Response value

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

Table A.90: Response value element contents

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

A.8.67 SCK data

The SCK data information element is defined in table A.91.

Table A.91: SCK data information element contents

Information Element	Length	Type	C/O/M	Remark
SCK Number	5	1	M	
SCK Version number	16	1	M	

A.8.68 SCK information

The SCK information element is defined in table A.92.

Table A.92: SCK information element contents

Information Element	Length	Type	C/O/M	Remark
SCK number (SCKN)	5	1	M	
SCK version number (SCK-VN)	16	1	M	
Key type flag	1	1	M	0 = Current, 1 = Future
Sealed SCK (SSCK)	120	1	M	
Future key flag	1	1	M	Always false if key type flag = future
Sealed SCK (SSCK)	120	1	C	If future key flag = true

A.8.69 SCK key and identifier

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

Table A.93: SCK key and identifier element contents

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

A.8.70 SCK number (SCKN)

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 A.94: SCK number element contents

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

A.8.71 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 A.95: 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	
Current SCK Version number	16	1	C	Defined as SCK-VN and sent when provision result has value incorrect key-VN.

A.8.72 SCK provision flag

The SCK provision flag is used to indicate that SCK information is present in the PDU.

Table A.96: SCK provision flag element contents

Information element	Length	Value	Remark
SCK provision flag	1	0	No SCK information provided (FALSE)
		1	SCK information provided (TRUE)

A.8.73 SCK select number

The SCK select number is contained in OTAR key associate messages to indicate either which key should be associated with the signalled group(s); or whether no key should be associated and any existing key disassociated. It is also used to indicate which keys have been selected in result PDUs.

Table A.97: SCK select number element contents

Information element	Length	Value	Remark
SCK select	6	000000 to 011111	SCK number (SCKN) selected
		100000	No SCKN selected
		100001	SCKN dissociated
		100010 to 111111	Reserved

A.8.74 SCK use

The SCK use information element indicates if the SCK being provided is intended for use in Trunked Mode Operation or for use in Direct Mode Operation.

Table A.98: SCK version number element contents

Information element	Length	Value	Remark
SCK use	1	0	Trunked Mode Operation
		1	Direct Mode Operation

A.8.75 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 A.99: SCK version number element contents

Information element	Length	Value	Remark
SCK version number	16	Any	

A.8.76 Sealed Key (Sealed CCK, Sealed SCK, Sealed GCK, Sealed GSKO)

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

Table A.100: Sealed Key element contents

Information element	Length	Value	Remark
Sealed Key	120	Any	

A.8.77 Security information element

The Security information element is found in the SYSINFO broadcast message and indicates to the MS the current security capabilities of the cell.

Table A.101: Security information element in SYSINFO

Information element	C/O/M	Length	Value	Remark
Authentication (note 4)	M	1	0	Authentication not required on this cell
			1	Authentication required on this cell
Security Class 1 (note 1)	M	1	0	Security Class 1 MS not supported on this cell
			1	Security Class 1 MS supported on this cell
Security Class 2 or 3 (note 1)	M	1	0	Security Class 2 MS supported on this cell
			1	Security Class 3 MS supported on this cell
SCKN (notes 1 and 2)	C	5		If Security Class 2 MS supported on this cell
DCK retrieval during initial Cell selection (notes 1 and 3)	C	1	0	Service not supported.
			1	Service supported.
DCK retrieval during cell Re-selection (notes 1 and 3)	C	1	0	Service not supported.
			1	Service supported.
Reserved (see note 3)	C	3	0	Reserved
NOTE 1: If the "Air interface encryption service" element in the BS service details element contained in the D-MLE SYSINFO PDU contains value 0, "Service is not available on this cell", then the value of this element has no meaning. NOTE 2: If Security Class 2 MS supported on this cell. NOTE 3: If Security Class 2 MS not supported on this cell. NOTE 4: An MS that does not support authentication should not select a cell that broadcasts "authentication required"				

A.8.78 Session key

The Session key element indicates whether a key has been sealed using a Group Session Key for OTAR known to members of a group, or sealed with a Session Key for OTAR (KSO) which is individually generated by an MS.

Table A.102: Session key element contents

Information element	Length	Value	Remark
Session key	1	0	Sealed key has been generated using individually generated session key KSO for MS
		1	Sealed key has been generated using Group Session Key for OTAR known to group of MSs.

A.8.79 Slot Number

See EN 300 392-2 [2], clause 7.

A.8.80 SSI

See ETS 300 392-1 [1], clause 7.

A.8.81 Subscription disable

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

Table A.103: Subscription disable element contents

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

A.8.82 Subscription enable

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

Table A.104: Subscription enable element contents

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

A.8.83 Subscription status

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

Table A.105: Subscription status element contents

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

A.8.84 TEI

This is the terminal equipment identifier of the MS. For a full definition see ETS 300 392-1 [1], clause 7. The definition given here expands that given in ETS 300 392-1 [1], clause 7 for encoding of TEI for transmission over the radio interface.

Table A.106: TEI contents

Information element	Length	Value	Remark
Terminal equipment identifier digit #1	4		BCD encoded digit
Terminal equipment identifier digit #2	4		BCD encoded digit
Terminal equipment identifier digit #3	4		BCD encoded digit
Terminal equipment identifier digit #4	4		BCD encoded digit
Terminal equipment identifier digit #5	4		BCD encoded digit
Terminal equipment identifier digit #6	4		BCD encoded digit
Terminal equipment identifier digit #7	4		BCD encoded digit
Terminal equipment identifier digit #8	4		BCD encoded digit
Terminal equipment identifier digit #9	4		BCD encoded digit
Terminal equipment identifier digit #10	4		BCD encoded digit
Terminal equipment identifier digit #11	4		BCD encoded digit
Terminal equipment identifier digit #12	4		BCD encoded digit
Terminal equipment identifier digit #13	4		BCD encoded digit
Terminal equipment identifier digit #14	4		BCD encoded digit
Terminal equipment identifier digit #15	4		BCD encoded digit

A.8.85 TEI request flag

This bit indicates whether the MS should supply the TEI.

Table A.107: TEI request flag contents

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

A.8.86 Time type

The time type element indicates what form time is expressed in the PDU.

Table A.108: Time type information element contents

Information element	Length	Value	Remark
Time type	2	00	Absolute IV
		01	Network time
		10	Immediate, first slot of first frame of next multiframe
		11	Reserved for future use

A.8.87 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 identified in the present document only and are taken from the reserved values of type 3 element identifier defined in the MM protocol. For more details, see EN 300 392-2 [2], clause 16.

Table A.109: Type 3 element identifier element contents

Information element	Length	Value	Remarks
Type 3 element identifier	4	1001	Authentication uplink
		1010	Authentication downlink

Annex B (normative): 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, or from GCK and SCK. The algorithm shall have the following properties:

Input 1: Bit string of length |GCK|;

Input 2: Bit string of length |CCK| (or bit string of length |SCK|);

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, GCKN**,** GCK-VN and KSO. 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 |KSO|;

Input 4: Bit string of length |GCKN|;

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 and GCKN from SGCK, GCK-VN, and KSO. The algorithm shall have the following properties:

Input 1: Bit string of length |SGCK|;

Input 2: Bit string of length |KSO|;

Input 3: Bit string of length |GCK-VN|;

Output 1: Bit string of length |GCK|;

Output 2: Boolean.

Output 3: Bit string of length |GCKN|;

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 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).

TA91: shall be used to compute SGSKO from GSKO, GSKO-VN and KSO. The algorithm shall have the following properties:

Input 1: Bit string of length |GSKO|;

Input 2: Bit string of length |GSKO-VN|;

Input 3: Bit string of length |KSO|;

Output: Bit string of length |SGSKO|.

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).

TA92: shall be used to compute GSKO from SGSKO, GSKO-VN, and KSO. The algorithm shall have the following properties:

Input 1: Bit string of length |SGSKO|;

Input 2: Bit string of length |KSO|;

Input 3: Bit string of length |GSKO-VN|;

Output 1: Bit string of length |GSKO|;

Output 2: Boolean.

The algorithm should be designed such that it is difficult to find for a fixed Input 1 values for Input 3 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 AC. The algorithm shall have the following properties:

Input 1: Bit string of length |AC|;

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.

TB5: shall be used to compute ECK from CK, CC, CN (see ref [2] clause 21.5) and LA. The algorithm shall have the following properties:

Input 1: Bit string of length |CK|;

Input 2: Bit string of length |LA|;

Input 3: Bit string of length |CN|;

Input 4: Bit string of length |CC|;

Output: Bit string of length |ECK|.

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

TB6: Reserved for DMO Security (ETS 300 396-6 [8]).

TB7: shall be used to compute EGSKO from GSKO. The algorithm shall have the following properties:

Input: Bit string of length |GSKO|;

Output: Bit string of length |EGSKO|.

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

B.1 Dimensioning of the cryptographic parameters

Table B.1 shows the lengths of the cryptographic parameters given in annex B.

Table B.1: Dimensioning of cryptographic parameters

Abbreviation	No. of Bits
AC	16 - 32
CC	6
CCK	80
CCK-id	16
CK	80
CN	12
DCK	80
DCK1	80
DCK2	80
ECK	80
EGSKO	128
ESI	24
GCK	80
GCKN	16
GCK-VN	16
GSKO	96
GSKO-VN	16
K	128
KS	128
KS'	128
KSO	128
LA	14
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
SGSKO	120
SSCK	120
SSI	24
UAK	128
XRES1	32
XRES2	32

B.2 Summary of the cryptographic processes

A summary of the authentication mechanisms explained in the previous clauses is given in figures B.1 and B.2. Only the paths where keys are generated by an algorithm are shown.

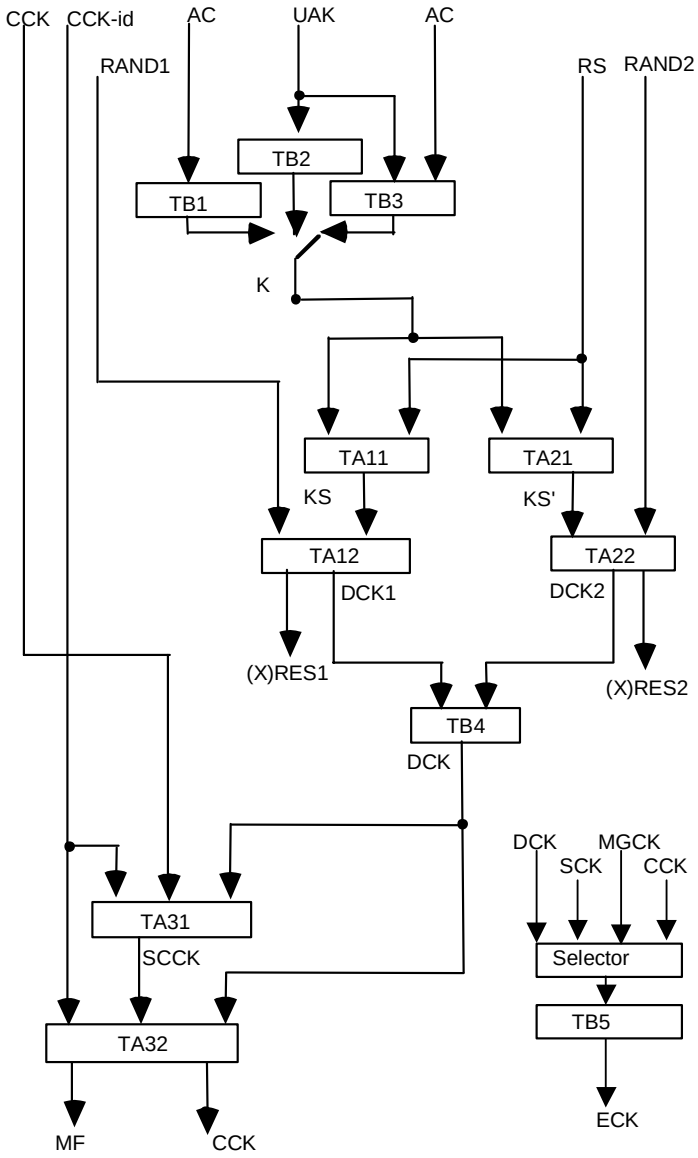


Figure B.1: Overview of air interface authentication and key management (sheet 1 of 2)

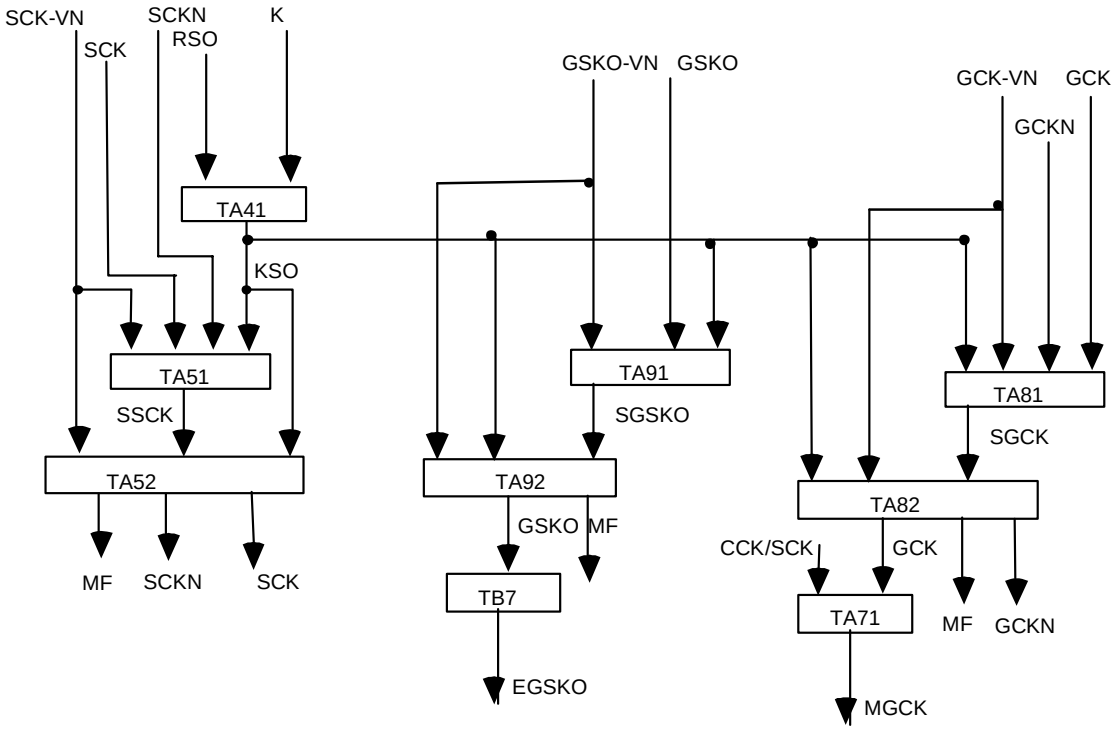


Figure B.2: Overview of air interface authentication and key management (sheet 2 of 2)

Annex C (normative): Timers

C.1 T354, authorisation protocol timer

The value of T354 shall be 30 seconds.

C.2 T371, Delay timer for group addressed delivery of SCK and GCK

T371 is a timer with a value randomized to fall within the range 1s and 65535s (18,2 hours).

T371 is started on reception of the D-OTAR SCK PROVIDE or D-OTAR GCK PROVIDE. On expiry of T371 shall send U-OTAR SCK RESULT or U-OTAR GCK RESULT as appropriate.

T371 is started on reception of the D-CK CHANGE DEMAND PDU when addressed to a group of MSs with the "acknowledgement flag" element set to TRUE. On expiry of T371, the MS shall respond with a U-CK CHANGE RESULT PDU. The value of T371 shall be such that the acknowledgement is received by the SwMI before the time that the key becomes valid.

C.3 T372, Key forwarding timer

The value of T372 shall be 5 seconds.

T372 shall be started on sending of U-OTAR PREPARE and stopped on receipt of D-OTAR NEWCELL.

If T372 expires the MS shall abandon signalling and initiate the cell change procedure immediately.

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

- ETS 300 395-3: "Terrestrial Trunked Radio (TETRA); Speech codec for full-rate traffic channel; Part 3: Specific operating features".

History

Document history		
Edition 1	December 1996	Publication as ETS 300 392-7
Edition 2	May 1999	Public Enquiry PE 9940: 1999-05-05 to 1999-10-01
		Converted into an EN between Public Enquiry and Vote
V2.1.1	December 2000	Vote V20010209: 2000-12-11 to 2001-02-09