DRAFT

EUROPEAN TELECOMMUNICATION STANDARD

pr **ETS 300 392-7**

May 1999

Second Edition

Source: TETRA

Reference: RE/TETRA-06001-7

ICS: 33.020

Key words: TETRA, V+D, security

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

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
Internet: secretariat@etsi.fr - http://www.etsi.org

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

Contents

Foreword....7

1 Scope....9

2 References....9

3 Definitions and abbreviations....10
3.1 Definitions....10
3.2 Abbreviations....12

4 Air Interface authentication and key management mechanisms....13
4.1 Air interface authentication mechanisms....13
4.1.1 Overview....13
4.1.2 Authentication of a user....13
4.1.3 Authentication of the infrastructure....14
4.1.4 Mutual authentication of user and infrastructure....15
4.1.5 The authentication key....17
4.1.5.1 Making K available in an MS....18
4.1.6 Equipment authentication....18
4.2 Air Interface key management mechanisms....18
4.2.1 The DCK....19
4.2.2 The GCK....19
4.2.3 The CCK....20
4.2.4 The SCK....21
4.2.5 Encrypted Short Identity (ESI) mechanism....22
4.2.6 Summary of AI key management mechanisms....23
4.3 Service description and primitives....24
4.3.1 Authentication primitives....24
4.3.2 SCK transfer primitives....24
4.3.3 GCK transfer primitives....25
4.4 Authentication protocol....26
4.4.1 Authentication state transitions....26
4.4.1.1 Description of authentication states....28
4.4.2 Authentication protocol sequences and operations....29
4.4.2.1 Case 1: SwMI authenticates MS....30
4.4.2.2 Case 2: MS authenticates SwMI....32
4.4.2.3 Case 3: Authentication initiated by SwMI and made mutual by the MS....34
4.4.2.4 Case 4: Authentication initiated by MS and made mutual by the SwMI....36
4.4.2.5 Case 5: SwMI authenticates MS during registration....38
4.4.2.6 Case 6: MS authenticates SwMI during registration....42
4.4.2.7 Case 7: Authentication initiated by MS during registration and made mutual by the SwMI....45
4.4.2.8 Case 8: Authentication initiated by SwMI during registration and made mutual by the MS....48
4.4.2.9 Case 9: SwMI rejects authentication demand from MS....52
4.4.2.10 Case 10: MS rejects authentication demand from SwMI....53
4.4.3 CCK delivery - protocol functions....53
4.4.3.1 SwMI-initiated CCK provision....54
4.4.3.2 MS-initiated CCK provision with U-OTAR CCK Demand....55
4.4.3.3 MS-initiated CCK provision with announced cell reselection....56
4.4.3.4 MS initiated CCK provision within registration (without authentication)....56
4.4.4 OTAR protocol functions - SCK....58
4.4.4.1 MS requests provision of SCK(s)....58

4.4.4.2 SwMI provides SCK(s) to MS ... 59
4.4.5 OTAR protocol functions - GCK ... 60
4.4.5.1 MS requests provision of GCK ... 60
4.4.5.2 SwMI provides GCK to MS ... 61
4.4.6 Notification of key change over the air ... 62
4.4.6.1 Security class 3 ... 62
4.4.6.1.1 Change of DCK ... 62
4.4.6.1.2 Change of CCK ... 62
4.4.6.1.3 Change of GCK ... 63
4.4.6.2 Security class 2 ... 63
4.4.7 PDU descriptions ... 63
4.4.7.1 D-AUTHENTICATION DEMAND ... 64
4.4.7.2 D-AUTHENTICATION REJECT ... 64
4.4.7.3 D-AUTHENTICATION RESPONSE ... 64
4.4.7.4 D-AUTHENTICATION RESULT ... 65
4.4.7.5 D-CK CHANGE DEMAND ... 65
4.4.7.6 D-OTAR CCK Provide ... 66
4.4.7.7 D-OTAR GCK Provide ... 66
4.4.7.8 D-OTAR SCK Provide ... 66
4.4.7.9 U-AUTHENTICATION DEMAND ... 67
4.4.7.10 U-AUTHENTICATION REJECT ... 67
4.4.7.11 U-AUTHENTICATION RESPONSE ... 67
4.4.7.12 U-AUTHENTICATION RESULT ... 68
4.4.7.13 U-CK CHANGE RESULT ... 68
4.4.7.14 U-OTAR CCK Demand ... 68
4.4.7.15 U-OTAR CCK Result ... 69
4.4.7.16 U-OTAR GCK Demand ... 69
4.4.7.17 U-OTAR GCK Result ... 69
4.4.7.18 U-OTAR SCK Demand ... 70
4.4.7.19 U-OTAR SCK Result ... 70
4.4.7.20 U-TEI PROVIDE ... 71
4.4.8 MM PDU type 3 information elements coding ... 71
4.4.8.1 Authentication downlink ... 71
4.4.8.2 Authentication uplink ... 71
4.4.9 PDU Information elements coding ... 72
4.4.9.1 Address extension ... 72
4.4.9.2 Authentication reject reason ... 72
4.4.9.3 Authentication result ... 72
4.4.9.4 CCK identifier ... 72
4.4.9.5 CCK information ... 73
4.4.9.6 CCK provision flag ... 73
4.4.9.7 CCK request flag ... 73
4.4.9.8 GCK key and identifier ... 73
4.4.9.9 GCK version number ... 73
4.4.9.10 GSSI ... 74
4.4.9.11 Location area ... 74
4.4.9.12 Location area bit mask ... 74
4.4.9.13 Location area information ... 74
4.4.9.14 Location area list ... 75
4.4.9.15 Location area range ... 75
4.4.9.16 Mobile country code ... 75
4.4.9.17 Mobile network code ... 75
4.4.9.18 Mutual authentication flag ... 75
4.4.9.19 Number of location areas ... 76
4.4.9.20 Number of SCKs provided ... 76
4.4.9.21 Number of SCKs requested ... 76
4.4.9.22 OTAR sub-type ... 76
4.4.9.23 PDU type ... 77
4.4.9.24 Proprietary ... 77
4.4.9.25 Provision result ... 77
4.4.9.26 Random challenge ... 77
4.4.9.27 Random seed ... 77
4.4.9.28 Reject cause ... 78

4.4.9.29 Response value 78
4.4.9.30 SCK key and identifier 78
4.4.9.31 SCK number 78
4.4.9.32 SCK number and result 79
4.4.9.33 SCK version number 79
4.4.9.34 Sealed Key (Sealed CCK, Sealed SCK, Sealed GCK) 79
4.4.9.35 SSI 79
4.4.9.36 TEI 79
4.4.9.37 TEI request flag 79
4.4.9.38 Type 3 element identifier 80
4.5 Boundary conditions for the cryptographic algorithms and procedures 80
4.6 Dimensioning of the cryptographic parameters 84
4.7 Summary of the cryptographic processes 85

5 Enable and disable mechanism 85
5.1 General relationships 85
5.2 Enable/disable state transitions 86
5.3 Mechanisms 87
5.3.1 Disable of MS equipment 88
5.3.2 Disable of MS subscription 88
5.3.3 Disable an MS subscription and equipment 88
5.3.4 Enable an MS equipment 88
5.3.5 Enable an MS subscription 88
5.3.6 Enable an MS equipment and subscription 88
5.4 Enable/disable protocol 89
5.4.1 General case 89
5.4.2 Status of cipher key material 89
5.4.3 Specific protocol exchanges 89
5.4.3.1 Disabling an MS with authentication 90
5.4.3.2 Enabling an MS with authentication 91
5.4.4 Enabling an MS without authentication 92
5.4.5 Disabling an MS without authentication 93
5.4.6 Rejection of disable command 94
5.4.7 MM service primitives 94
5.4.7.1 TNMM-DISABLING primitive 94
5.4.7.2 TNMM-ENABLING primitive 95
5.4.8 MM PDUs structures and contents 95
5.4.8.1 D-DISABLE 95
5.4.8.2 D-ENABLE 95
5.4.8.3 U-DISABLE STATUS 96
5.4.9 MM Information elements coding 96
5.4.9.1 Address extension 96
5.4.9.2 Authentication challenge 96
5.4.9.3 Disabling type 97
5.4.9.4 Enable/Disable result 97
5.4.9.5 Equipment disable 97
5.4.9.6 Equipment enable 97
5.4.9.7 Equipment status 98
5.4.9.8 Intent/confirm 98
5.4.9.9 PDU Type 98
5.4.9.10 Proprietary 98
5.4.9.11 Subscription disable 99
5.4.9.12 Subscription enable 99
5.4.9.13 Subscription status 99
5.4.9.14 TETRA equipment identity 99

6 Air Interface (AI) encryption 99
6.1 General principles 99
6.1.1 Security class 100
6.1.1.1 Constraints on LA and Registration Area arising from cell class 102
6.2 Key Stream Generator (KSG) 102
6.2.1 KSG numbering and selection 102

6.2.2 Interface parameters 102
6.2.2.1 Initial Value (IV) 102
6.2.2.2 Cipher Key 103
6.3 Encryption mechanism 103
6.3.1 Synchronization of data calls where data is multi-slot interleaved 105
6.3.2 Recovery of stolen frames from interleaved data 106
6.4 Use of cipher keys 107
6.4.1 Identification of encryption state of downlink MAC PDUs 108
6.4.1.1 Class 1 cells 108
6.4.1.2 Class 2 cells 108
6.4.1.3 Class 3 cells 108
6.4.2 Identification of encryption state of uplink MAC PDUs 108
6.5 Mobility procedures 109
6.5.1 General requirements 109
6.5.1.1 Negotiation of cipher parameters 109
6.5.1.1.1 Class 1 cells 110
6.5.1.1.2 Class 2 cells 110
6.5.1.1.3 Class 3 cells 110
6.5.1.2 Initial and undeclared cell re-selection 110
6.5.1.3 Unannounced cell re-selection 110
6.5.1.4 Announced cell re-selection type-3 111
6.5.1.5 Announced cell re-selection type-2 111
6.5.1.6 Announced cell re-selection type-1 111
6.6 Positioning of encryption process 111
6.7 Encryption control 112
6.7.1 Data to be encrypted 112
6.7.1.1 Downlink control channel requirements 112
6.7.1.2 Encryption of MAC header elements 113
6.7.1.3 Traffic channel encryption control 113
6.7.2 Service description and primitives 113
6.7.2.1 Mobility Management (MM) 113
6.7.2.2 Mobile Link Entity (MLE) 114
6.7.2.3 Layer 2 116
6.7.3 Protocol functions 116
6.7.3.1 MM 116
6.7.3.2 MLE 116
6.7.3.3 LLC 116
6.7.3.4 MAC 116
6.7.4 PDUs for cipher negotiation 116

7 End-to-end encryption 117
7.1 Introduction 117
7.2 Voice encryption and decryption mechanism 117
7.2.1 Protection against replay 118
7.3 Data encryption mechanism 119
7.4 Exchange of information between encryption units 119
7.4.1 Synchronization of encryption units 119
7.4.2 Encrypted information between encryption units 120
7.4.3 Transmission 121
7.4.4 Reception 123
7.4.5 Stolen frame format 123
7.5 Location of security components in the functional architecture 124
7.6 End-to-end Key Management 126

Annex A (informative): Bibliography 127

History 128

Foreword

This draft European Telecommunication Standard (ETS) has been produced by the Terrestrial Trunked Radio (TETRA) Project of the European Telecommunications Standards Institute (ETSI), and is now submitted for the Public Enquiry phase of the ETSI standards approval procedure.

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

Part 1: "General network design";

Part 2: "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";

NOTE: This second edition of part 7 is not compatible with the first edition of part 7.

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".

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

Blank page

1 Scope

This ETS 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.

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

Clause 4 describes the authentication and key management mechanisms for the TETRA air interface. The following two authentication services have been specified for the air-interface in ETR 086-3 [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 for end-to-end confidentiality described.

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

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

2 References

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

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

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

[3] ETS 300 392-7 (Ed.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

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

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

3 Definitions and abbreviations

3.1 Definitions

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

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

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 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])

Common Cipher Key (CCK): cipher key that is generated by the infrastructure to protect group addressed signalling and traffic

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 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

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): long lifetime 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 to give a Modified Group Cipher Key (MGCK)

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

Personal Identification Number (PIN): entered by the user into the MS and used to authenticate the user to the MS. It may also be used to generate the authentication Key (K) together with the User Authentication Key (UAK)

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

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

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

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

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

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

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

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

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

synchronous stream cipher: encryption method in which a cipher text symbol completely represents the corresponding plain text symbol. 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 this ETS, the following abbreviations apply:

AC	Authentication Code
AI	Air Interface
AS	Alias Stream
AESI	Alias Encrypted Short Identity
ASSI	Alias Short Subscriber Identity
BS	Base Station
CCK	Common Cipher Key
CCK-id	CCK identifier
CK	Cipher Key
C-PLANE	Control-PLANE
CT	Cipher Text
DCK	Derived Cipher Key
DCK1	Part 1 of the DCK
DCK2	Part 2 of the DCK
DK	Derived Key
EKSG	End-to-end Key Stream Generator
EKSS	End-to-end Key Stream Segment
ESI	Encrypted Short Identity
F	Function
FEC	Forward Error Correction
GCK	Group Cipher Key
GCK-VN	GCK-Version Number
GESI	Group Encrypted Short Identity
GSSI	Group Short Subscriber Identity
GTSI	Group TETRA Subscriber Identity
HSC	Half-Slot Condition
HSI	Half-Slot Importance
HSN	Half-Slot Number
HSS	Half-Slot Stolen
HSSE	Half-Slot Stolen by Encryption unit
IESI	Individual Encrypted Short Identity
ISSI	Individual Short Subscriber Identity
ITSI	Individual TETRA Subscriber Identity
IV	Initialization Value
K	authentication Key
KS, KS'	Session authentication Key
KSG	Key Stream Generator
KSO	Session Key OTAR
KSS	Key Stream Segment
LA	Location Area
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	Air Re-keying
PDU	Protocol Data Unit
PIN	Personal Identification Number
PT	Plain Text
RAND1	RANDom challenge 1
RAND2	RANDom challenge 2
RES1	RESponse 1
RES2	RESponse 2
RS	Random Seed

RSO	Random Seed for OTAR
SAP	Service Access Point
SCCK	Sealed Common Cipher Key
SCK	Static Cipher Key
SCK-VN	SCK Version Number
SCKN	Static Cipher Key Number
SDU	Service Data Unit
SF	Synchronization Frame
SGCK	Sealed GCK
SHSI	Stolen Half-Slot Identifier
SS	Synchronization Status
SSCK	Sealed SCK
SSI	Short Subscriber Identity
STCH	STolen CHannel
SV	Synchronization Value
SwMI	Switching and Management Infrastructure
TA	TETRA Algorithm
TCH	Traffic Channel type
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). At the air interface the Base Station (BS) is assumed to be trusted by the SwMI and the authentication exchange proves knowledge given to the BS by the authentication centre. This knowledge shall be the session authentication key.

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

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

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

4.1.2 Authentication of a user

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

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

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

The process is summarized in figure 1.

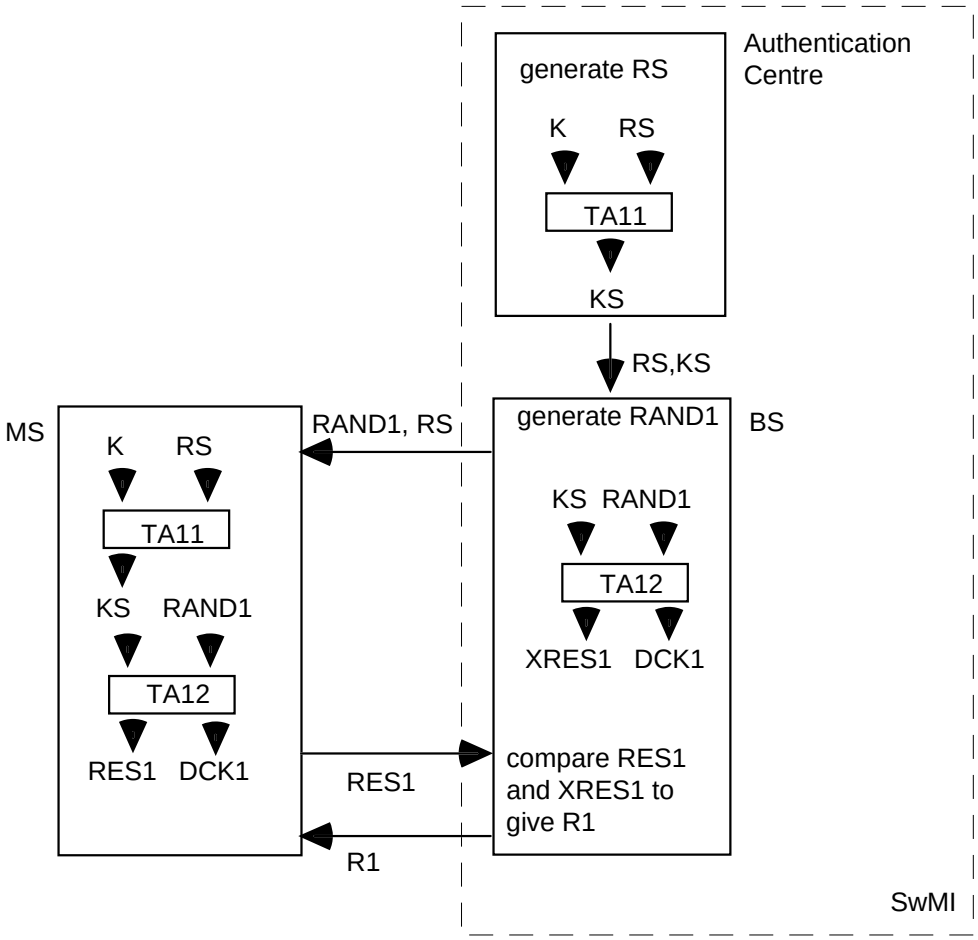


Figure 1: Authentication of a user by the infrastructure

4.1.3 Authentication of the infrastructure

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

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

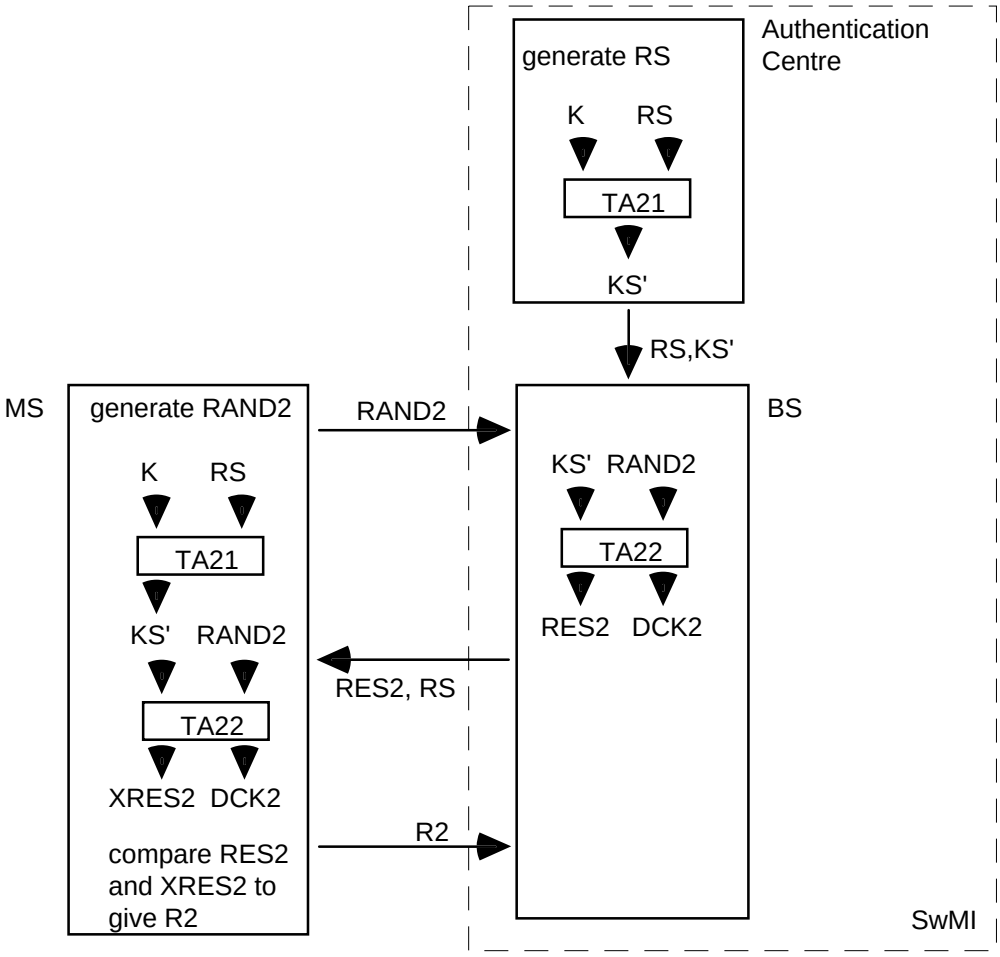


Figure 2: Authentication of the infrastructure by a user

4.1.4 Mutual authentication of user and infrastructure

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

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

If the authentication was initiated by the SwMI, it shall use K and one random seed RS with algorithms TA11 and 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 subclause 4.2.1.

The process is shown in figure 3.

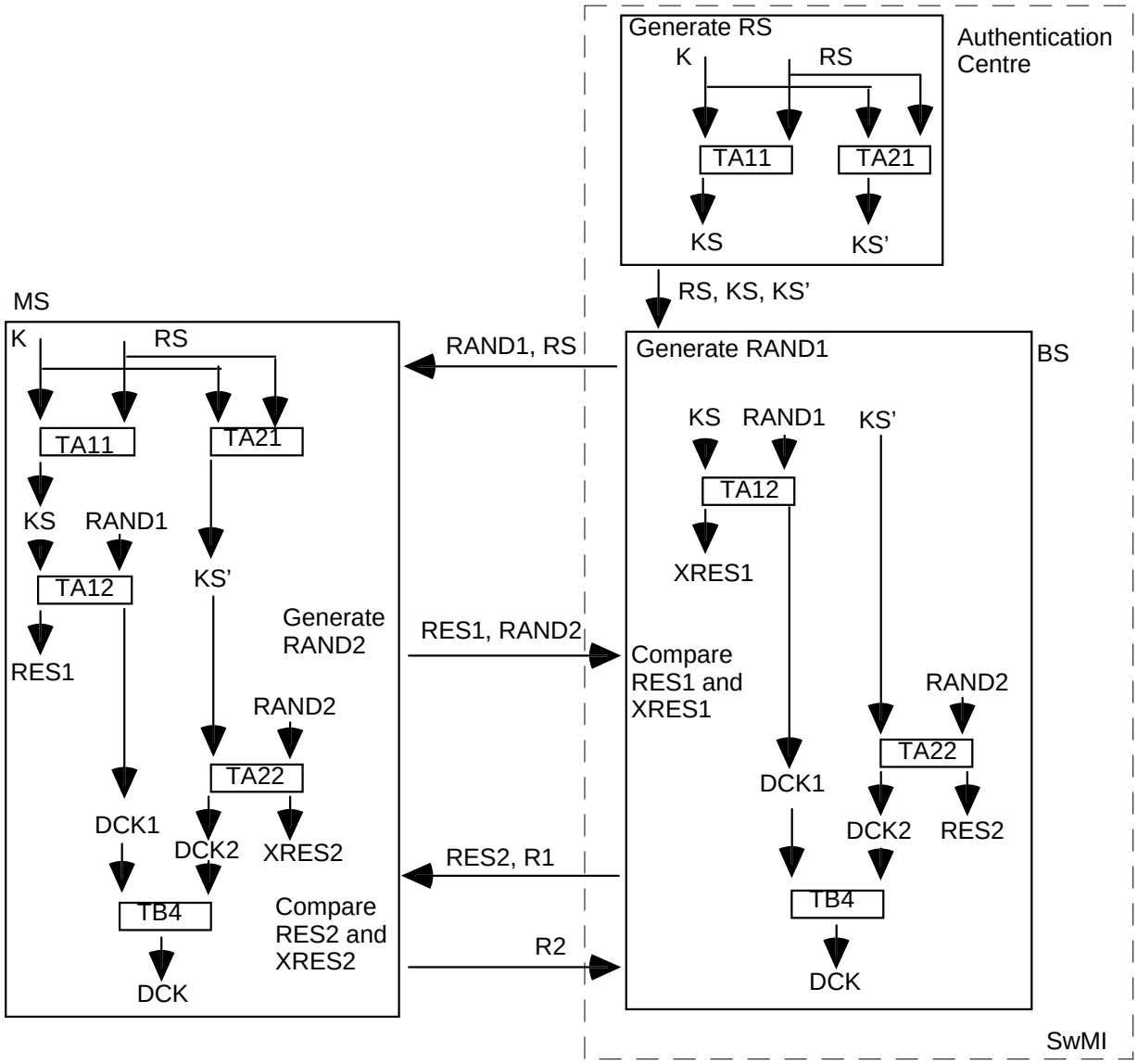


Figure 3: Mutual authentication initiated by SwMI

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

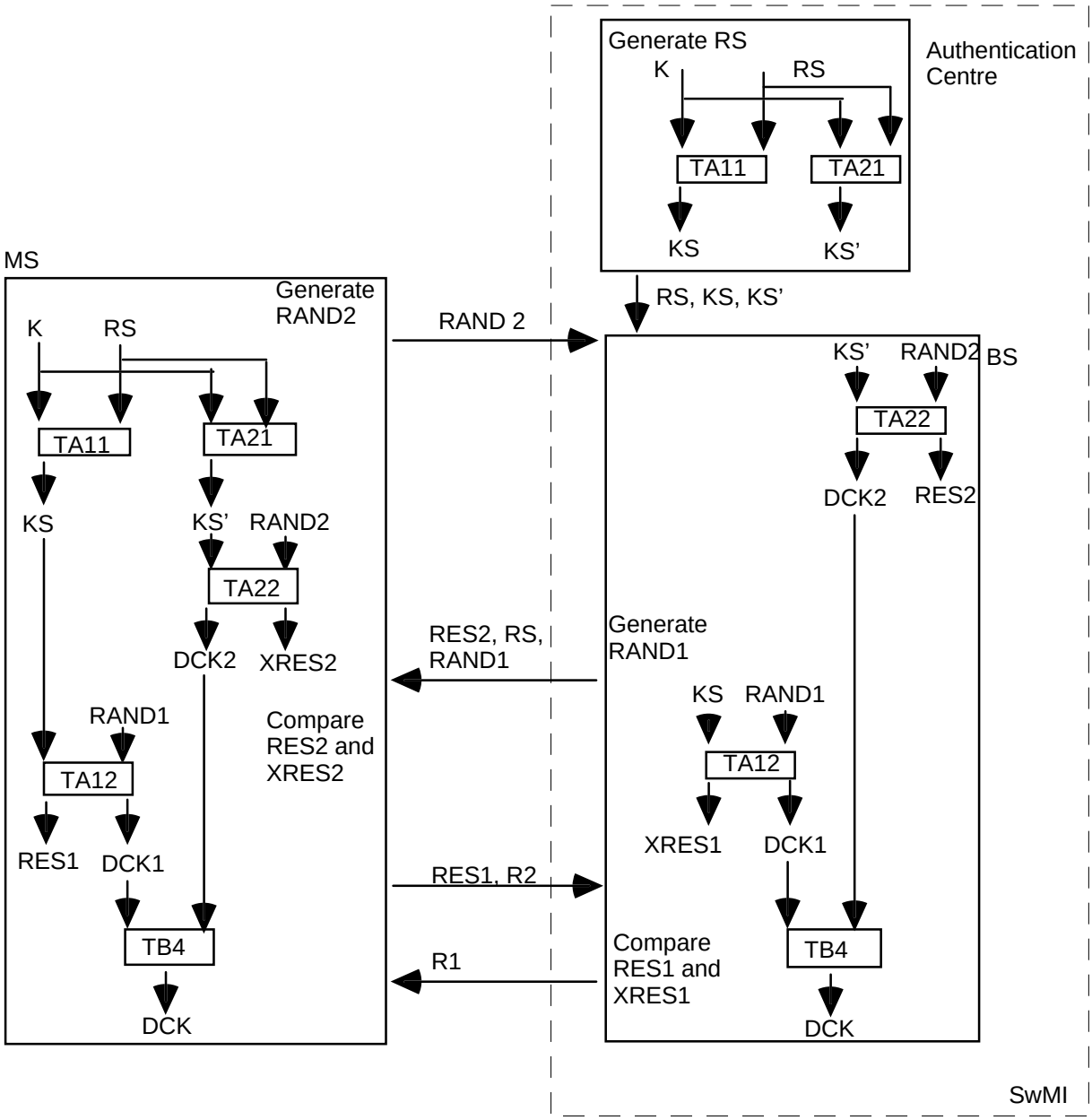


Figure 4: Mutual authentication initiated by MS

4.1.5 The authentication key

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

4.1.5.1 Making K available in an MS

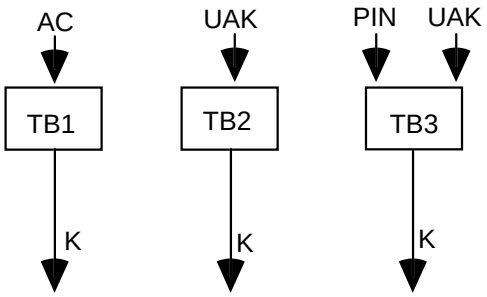


Figure 5: Making authentication key K available in an MS by user input

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

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

A user shall not be able to change the input to the algorithm and retain access to K, and thence to successful authentication without harmonizing the change of input with the authentication centre in the SwMI. This ETS 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 this ETS. However the protocol described in subclause 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

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

Four types of key are managed over the air interface:

- the Derived Cipher Key (DCK);
- the Common Cipher Key (CCK);
- the Group Cipher Key (GCK);
- the Static Cipher Key (SCK).

4.2.1 The DCK

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.

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

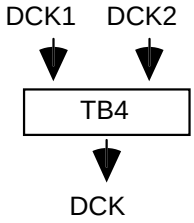


Figure 6: Derivation of the DCK from its two parts

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

In class 3 cells 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

GCK applies only to class 3 cells.

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. Within each LA the GCK shall be modified by CCK (see subclause 4.2.3) using algorithm TA71 to provide a Modified GCK (MGCK) for use on the air interface. The process is shown in figure 7.

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

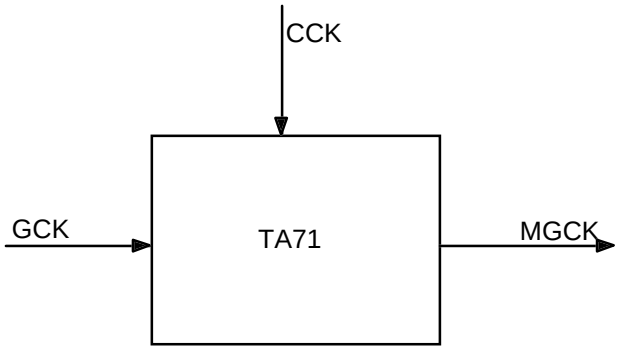


Figure 7: Generation of MGCK from GCK and CCK

GCK may be provided by an Over The Air Re-keying (OTAR) mechanism similar to that for CCK and SCK.

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

The process is summarized in figure 8.

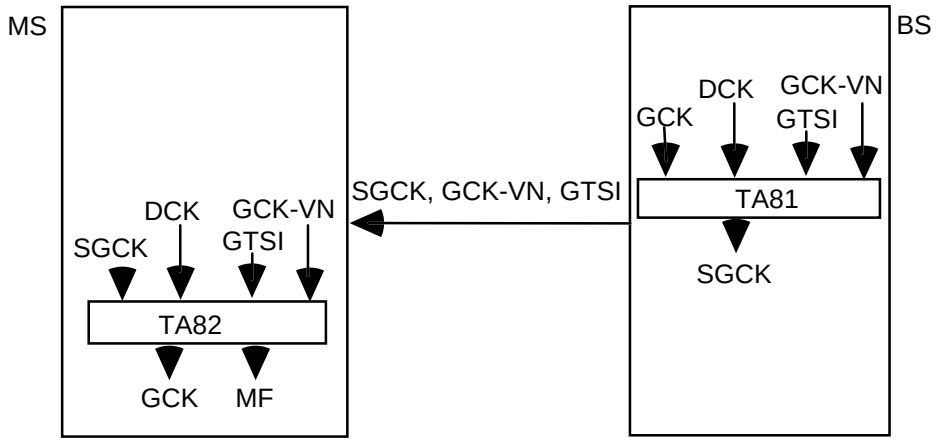


Figure 8: Distribution of a group cipher key

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

4.2.3 The CCK

CCK applies only to class 3 cells.

When DCK is used for air interface encryption CCK shall be used to give protection of the downlink on all group addressed signalling and traffic either as a key modifier of GCK (see subclause 4.2.2) or as a standalone key. In addition CCK shall be used to generate ESI as described in subclause 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. By checking that CCK-id of a newly distributed CCK has been increased, the MS may protect itself against replay of old keys.

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.

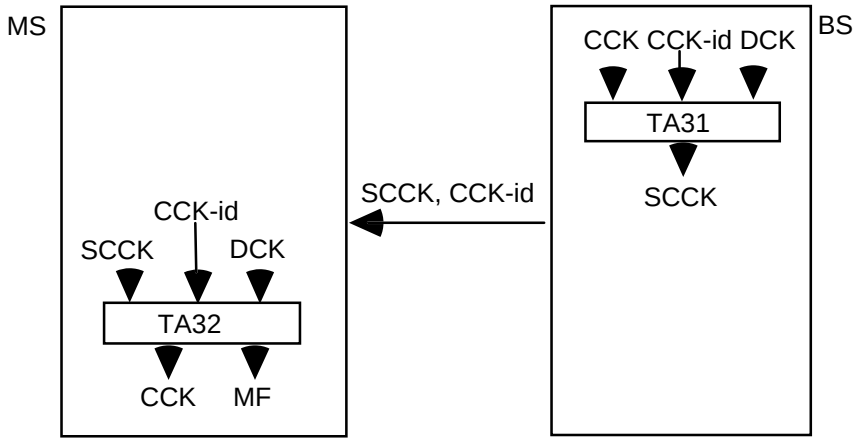


Figure 9: Distribution of a common cipher key

In class 3 cells CCK shall be used (optionally in partnership with the GCK (see 4.2.2)) to protect voice, data, and signalling sequences between the infrastructure and an MS when using group addresses. In addition CCK shall be used to provide address encryption using the ESI mechanism described in 4.2.5).

4.2.4 The SCK

SCK applies only to class 2 cells.

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

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

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

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

When distributing SCK by an OTAR mechanism (algorithms TA51 and TA52) a session key for OTAR (KSO) shall be used to protect the SCK as no DCK exists. KSO shall be individual to each user and shall be derived from a user's authentication key (K) and a random seed RSO with algorithm TA41.

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

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

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

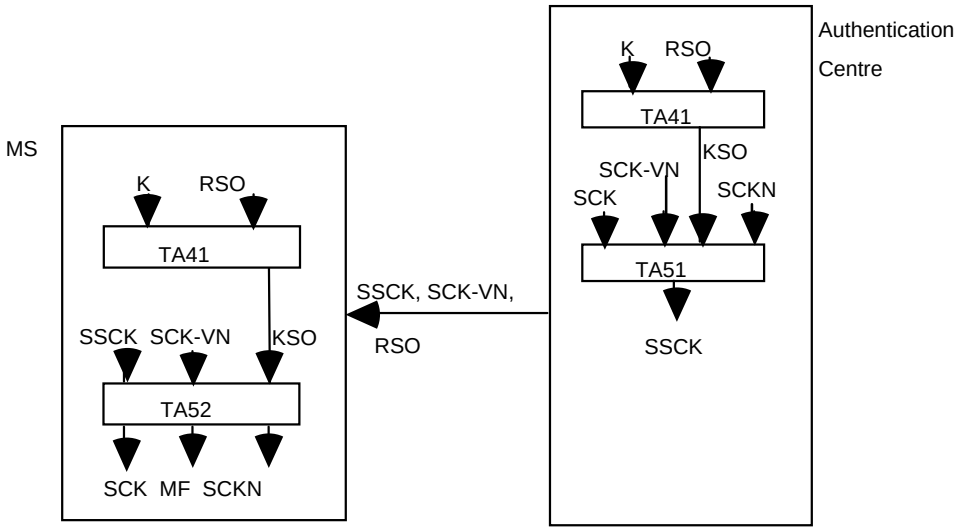


Figure 10: Distribution of SCK by an authentication centre

SCK shall be used to protect voice, data, and signalling sequences between the infrastructure and an individual MS in a class 2 cell.

4.2.5 Encrypted Short Identity (ESI) mechanism

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

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

This subclause describes a mechanism that allows an MS to encrypt addresses used by layer 2. 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 11.

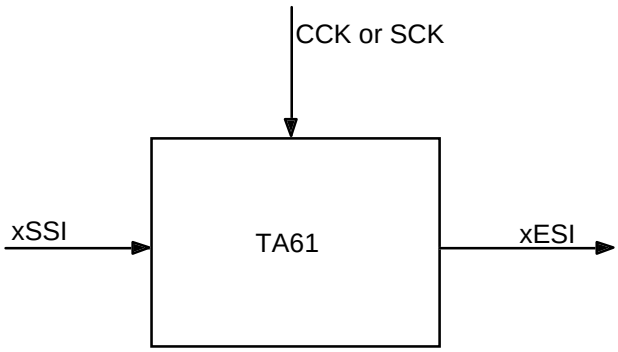


Figure 11: Generation of ESI from SSI and a cipher key

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.

NOTE: The layer 2 addresses that may be encrypted are either an SSI, an SSI + event label, event label, SSI + usage marker, or SMI.

The bits incorporated in the MAC header to indicate encryption control shall also indicate application of ESI. Thus, if the bits are set to "0", encryption off, ESI shall not be used in that PDU, and the true SSI shall be transmitted. This enables a clear registration to be carried out with the MS's true identity visible. The use of signalling for AI encryption management is more fully described in subclause 6.4.

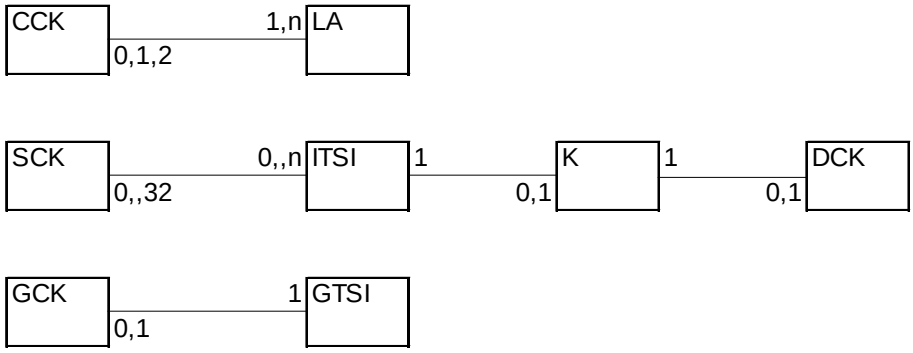
4.2.6 Summary of AI key management mechanisms

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

Table 1: Cipher Key pre-conditions and lifetime

Key	Pre-condition	Lifetime
K	none	ITSI (note 1)
DCK	authentication	Authentication period (note 2)
CCK	authentication	Not defined (note 3)
SCK	none	Not defined (note 1)
GCK	authentication	Not defined
NOTE 1: If OTAR is used for SCK, K is required as the key is sealed with a function of K.		
NOTE 2: In an MS DCK may be deleted on power down.		
NOTE 3: CCK should be deleted from the MS on power down.		

Figure 12 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 (uniqueness criteria).

NOTE 7: Before committal there may be temporary store of 2 DCK, this is not shown.

Figure 12: 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 2: 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 =
  - never mutually authenticate;
  - always mutually authenticate;
  - never authenticate at registration;
  - always authenticate at registration;
  - authenticate only in ITIS-Attach registration.

4.3.2 SCK transfer primitives

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

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

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

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

Table 3: TNMM SCK service primitives

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

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

- result =

  SCK received successfully;
  SCK failed to decrypt;

- SCKN =

  1;
  2;
  3;
  …;
  32;

- SCK-VN =

  0;
  ….
  2^{16}-1.

4.3.3 GCK transfer primitives

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

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

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

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

Table 4: TNMM GCK service primitives

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

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

- result =

  GCK received successfully;
  GCK failed to decrypt;

- GTSI =

  0;
  1;
  2;
  ….
  2^{48}-1;

- GCK-VN =

  0;
  ….
  2^{16}-1.

4.4 Authentication protocol

4.4.1 Authentication state transitions

Figures 13 and 14 give an overview of the received PDUs that result in a change of authentication state.

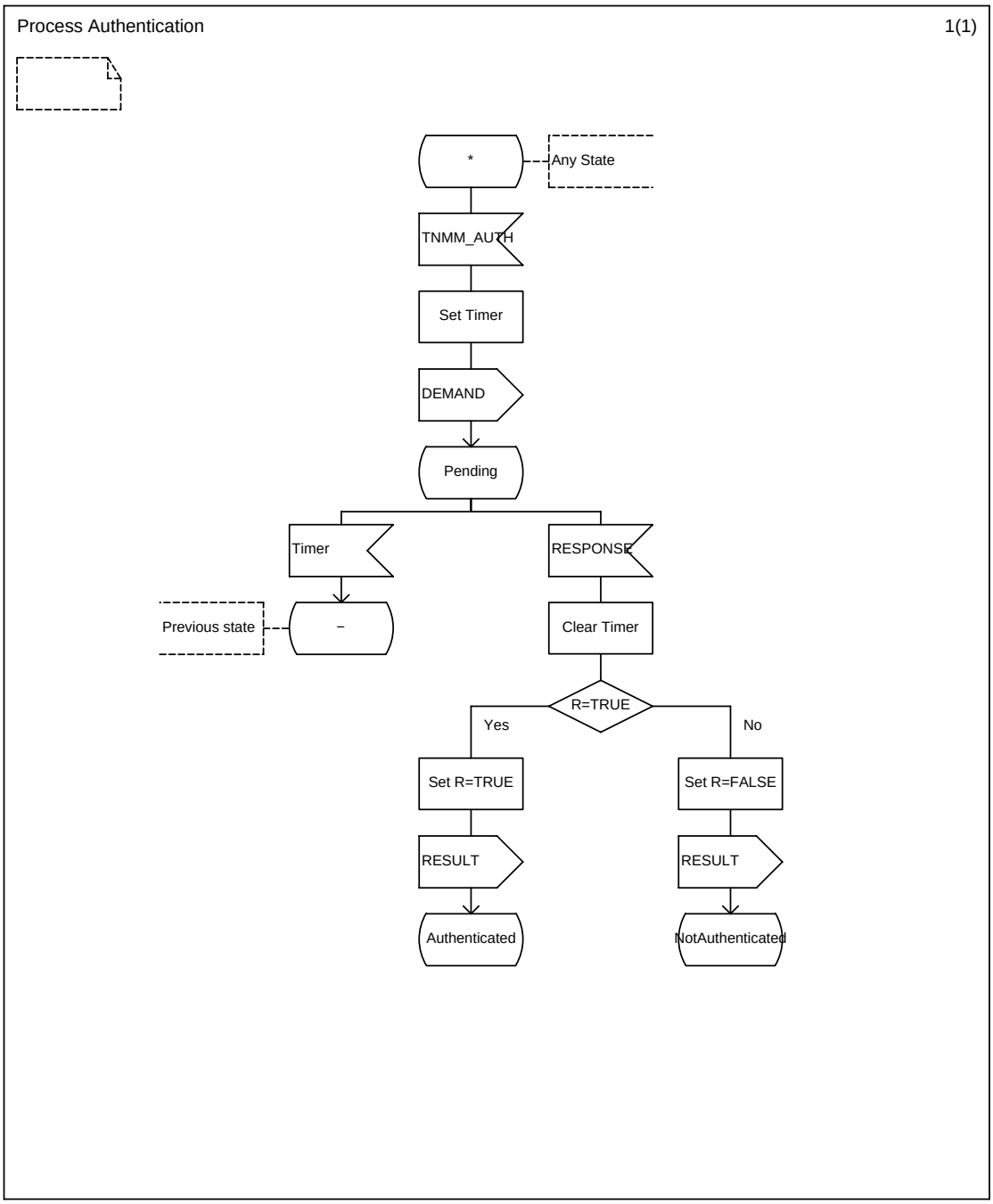


Figure 13: State transitions for outgoing authentication

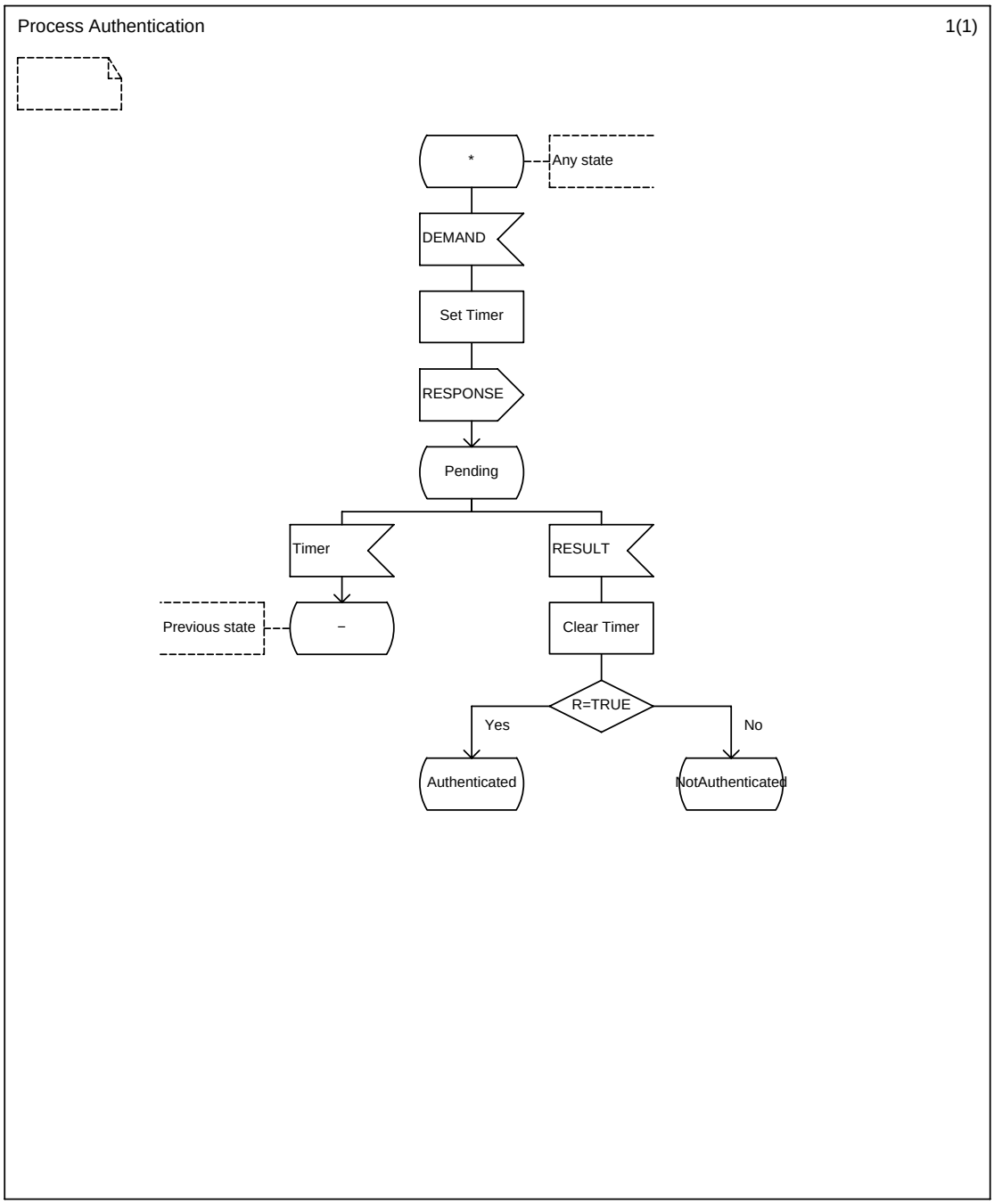


Figure 14: State transitions for incoming authentication

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 or has failed an authentication attempt. 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 MM services;

- **Pending:** an authentication sequence has begun and not yet completed. In this state no other signalling is allowed.

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 ETS 300 392-2 [2], clause 14).

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

- if a terminal supports authentication it shall support all authentication modes;

  NOTE: An authentication mode is one of invoke, respond, combine with registration, combine with other layer 3 service.

- if the authentication procedure fails to complete within time τ_A 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 not take place until after completion of the U-plane transmission;

- forward registration type 1 shall allow cell change to be carried out without a change in encryption state of the roaming or migrating mobile (see also clause 6);

- 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).

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

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

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.

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

The following MSCs are grouped into 3:

- authentication protocols (cases 1-4);

- registration combined with authentication and key management (cases 5-8);

- failure scenarios (cases 9-10).

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

The authentication timer τ_A shall always be less than or equal in value to the registration timer T351 (see ETS 300 392-2 [2], subclause 16.11.1.1). When τ_A is running only authentication signalling as defined in cases 1 through 10 in subclauses 4.4.2.1 to 4.4.2.10 shall be accepted by MS-MM and BS-MM.

All MM security services shall use the acknowledged layer 2 service of the TETRA protocol stack (TL-DATA request and TL-DATA confirm). The data transmission and its acknowledgement shall use the same cipher parameters. In class 3 cells where successful authentication produces a new DCK this DCK shall not be invoked until after receipt of the acknowledgement to the PDU containing the RESULT of the authentication.

4.4.2.1 Case 1: SwMI authenticates MS

Pre-requisite: MS is registered to SwMI.

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

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

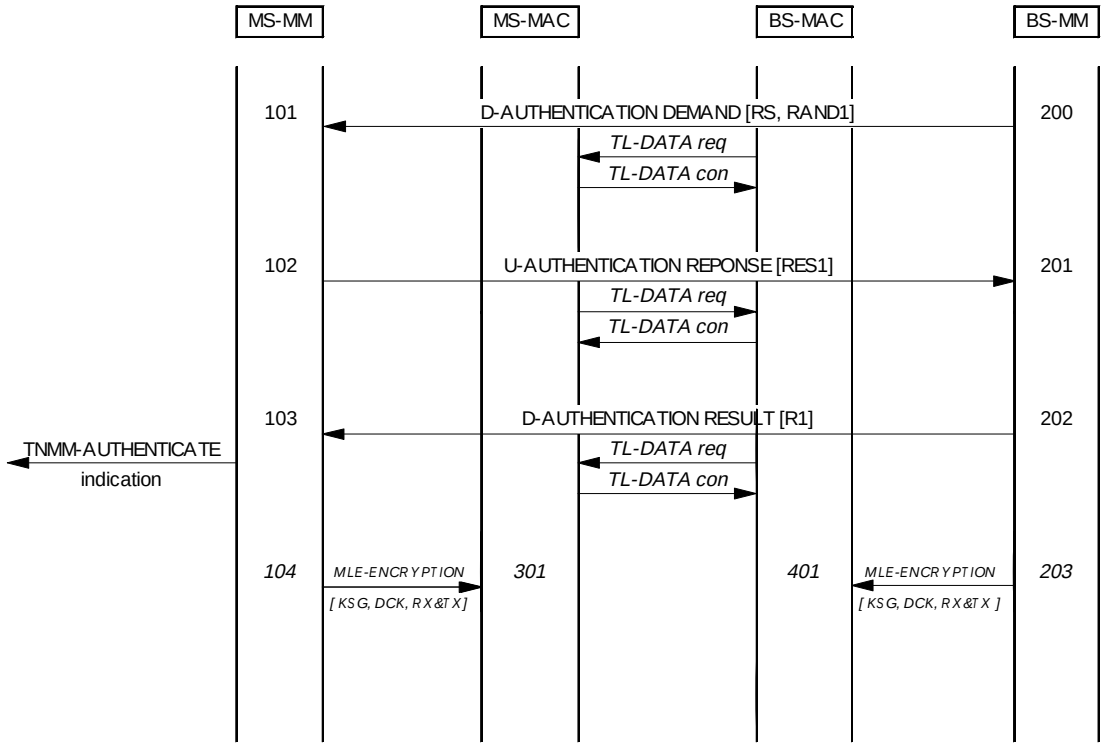


Figure 15: Authentication of MS by SwMI

200 D-AUTHENTICATION DEMAND at BS-MM:

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

101 D-AUTHENTICATION DEMAND at MS-MM:

- MS-MM shall retrieve RS and RAND1 from the authentication challenge. The MS shall start timer τ_A, and shall run algorithms TA11 and TA12 to generate RES1 and DCK1;
- in a class 3 cell and since in this scenario the MS is configured for unilateral authentication, the MS-MM shall run algorithm TB4 with DCK1 and DCK2 = 0 to generate DCK;
- if the MS is configured to respond to authentication challenges from BS-MM with a mutual authentication, MS-MM should not calculate DCK since MS-MM does not yet have DCK2. This scenario is described in case 3, subclause 4.4.2.3.

102 U-AUTHENTICATION RESPONSE at MS-MM:

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

201 U-AUTHENTICATION RESPONSE at BS-MM:

- upon receipt of U-AUTHENTICATION RESPONSE the BS shall stop timer τ_A. BS-MM shall retrieve RES1 and compare it with the previously calculated XRES1 (as described in 200) to decide whether or not authentication was successful;
- in a class 3 cell, if the MS authentication was successful BS-MM shall run algorithm TB4 with DCK1 and DCK2 = 0 as inputs to generate DCK;
- if authentication of the MS was not successful, BS-MM shall not calculate DCK.

202 D-AUTHENTICATION RESULT at BS-MM:

- if authentication was successful, BS-MM shall set authentication result to TRUE and shall send D-AUTHENTICATION RESULT to MS-MM;
- since mutual authentication has not been requested BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESULT to be false and RES2 shall not be included in this PDU;
- if authentication of the MS was not successful, BS-MM shall set authentication result (R1) to FALSE and shall send D-AUTHENTICATION RESULT. The "Mutual authentication flag" in D-AUTHENTICATION RESULT shall be set to false and RES2 shall not be included in this PDU.

103 D-AUTHENTICATION RESULT at MS-MM:

- MS-MM shall retrieve R1 to check whether authentication was successful. The MS shall stop timer τ_A.

104 MLE-ENCRYPTION request at MS-MM (in class 3 cells only):

- if authentication was successful MS-MM shall configure MS-MAC to receive and transmit with the newly calculated DCK;
- if authentication was not successful the MS shall continue to receive and transmit with the same ciphering parameters the MS was using before this authentication procedure was started. In this case the MS-MM shall not reconfigure MS-MAC.

301 MLE-ENCRYPTION request at MS-MAC:

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

203 MLE-ENCRYPTION request at BS-MM (in class 3 cells only):

- if the authentication was successful BS-MM shall configure BS-MAC to receive and transmit with the newly calculated DCK;
- if the authentication was not successful the SwMI shall continue to receive and transmit using the ciphering parameters in use before this authentication procedure was initiated. In this case BS-MM shall not reconfigure BS-MAC.

401 MLE-ENCRYPTION request at BS-MAC:

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

4.4.2.2 Case 2: MS authenticates SwMI

Pre-requisite: MS is registered to SwMI.

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

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

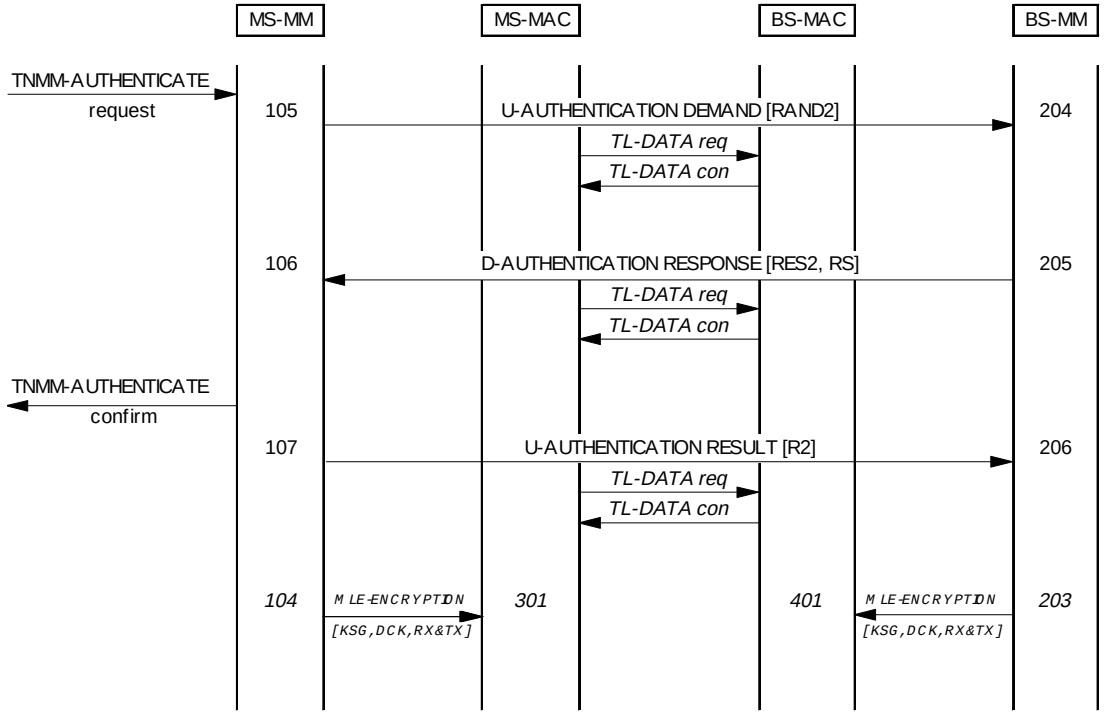


Figure 16: Authentication of the SwMI by the MS

105 U-AUTHENTICATION DEMAND at MS-MM:

- MS-MM shall challenge BS-MM to authenticate by sending the challenge, RAND2. The MS shall start timer τ_A.

204 U-AUTHENTICATION DEMAND at BS-MM:

- BS-MM shall retrieve RAND2 and run algorithms TA21 and TA22 to generate RES2, and DCK2. The BS shall start timer τ_A;

- in a class 3 cell since in this scenario the SwMI is configured for unilateral authentication, BS-MM shall run TB4 with DCK2 and DCK1 = 0 to generate DCK;

- if the SwMI is configured to respond to authentication challenges from MS-MM with a mutual authentication, BS-MM should not calculate DCK since BS-MM does not yet have DCK1. This scenario is described in case 4, subclause 4.4.2.4.

205 D-AUTHENTICATION RESPONSE at BS-MM:

- BS-MM shall respond to the authentication challenge by sending RES2 and RS to MS-MM;

- since the SwMI is not configured to mutually authenticate the MS, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESPONSE to be false and RAND1 shall not be included in this PDU.

106 D-AUTHENTICATION RESPONSE at MS-MM:

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

- in a class 3 cell if authentication was successful, and since the SwMI has not requested mutual authentication, MS-MM shall run algorithm TB4 with DCK2 and DCK1 = 0 to generate DCK;

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

107 U-AUTHENTICATION RESULT at MS-MM:

- the MS shall stop timer τ_A;

- if authentication was successful, MS-MM shall send the result R2 to BS-MM in the U-AUTHENTICATION RESULT PDU;

- since there is no mutual authentication, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be false and RES1 shall not be included in this PDU;

- if authentication was not successful, MS-MM shall send the result R2 = FALSE in the U-AUTHENTICATION RESULT PDU. MS-MM shall set the "Mutual authentication flag" to FALSE and RES1 shall not be included in this PDU.

206 U-AUTHENTICATION RESULT at BS-MM:

- the BS shall stop timer τ_A. BS-MM shall retrieve R2 to check whether authentication was successful.

104 MLE-ENCRYPTION request at MS-MM (in class 3 cells only):

- if authentication was successful MS-MM shall configure MS-MAC to receive and transmit with the newly calculated DCK;

  if authentication was not successful the MS shall continue to receive and transmit with the same ciphering parameters the MS was using before this authentication procedure was started. In this case the MS-MM shall not reconfigure MS-MAC.

301 MLE-ENCRYPTION request at MS-MAC:

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

203 MLE-ENCRYPTION request at BS-MM (in class 3 cells only):

- if the authentication was successful BS-MM shall configure BS-MAC to receive and transmit with the newly calculated DCK;

- if the authentication was not successful the SwMI shall continue to receive and transmit using the ciphering parameters in use before this authentication procedure was initiated. In this case BS-MM shall not reconfigure BS-MAC.

401 MLE-ENCRYPTION request at BS-MAC:

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

4.4.2.3 Case 3: Authentication initiated by SwMI and made mutual by the MS

Pre-requisite: MS is registered to SwMI.

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

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

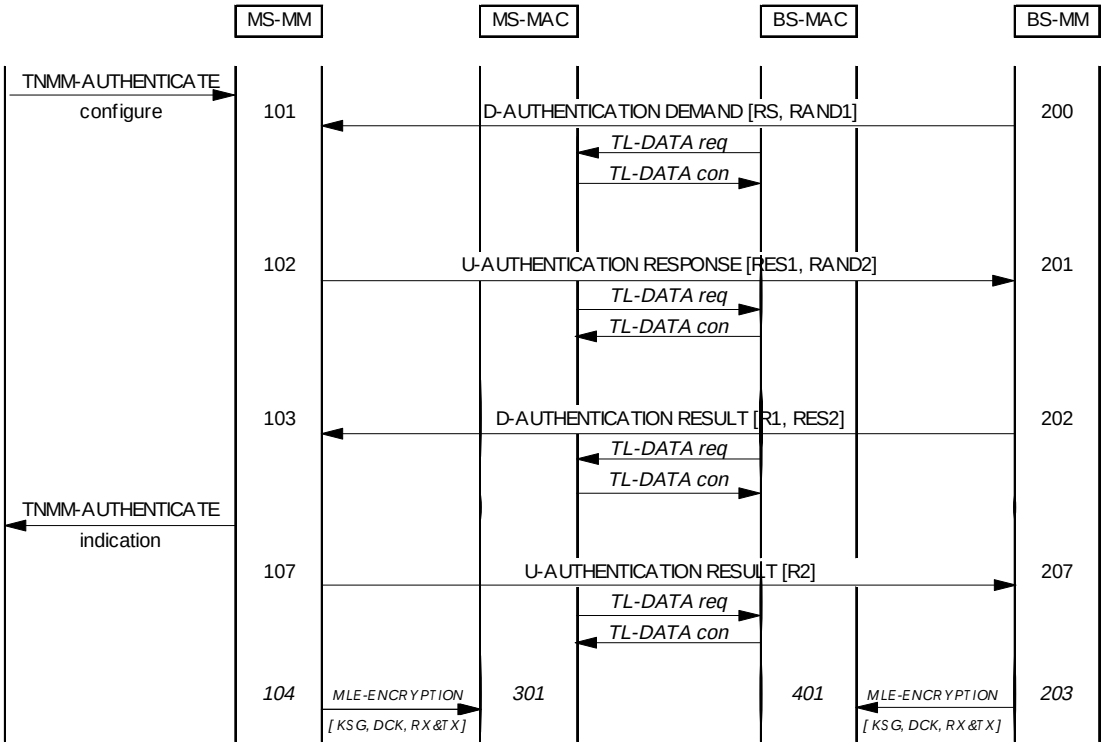


Figure 17: Authentication initiated by SwMI and made mutual by the MS

200 D-AUTHENTICATION DEMAND at BS-MM:

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

101 D-AUTHENTICATION DEMAND at MS-MM:

- MS-MM shall retrieve RS and RAND1 from the authentication challenge. The MS shall start timer τ_A, and shall run algorithms TA11 and TA12 to generate RES1 and DCK1;
- since the MS is configured to respond to authentication challenges from BS-MM with a mutual authentication, MS-MM shall not calculate DCK since MS-MM does not yet have DCK2.

102 U-AUTHENTICATION RESPONSE at MS-MM:

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

201 U-AUTHENTICATION RESPONSE at BS-MM:

- upon receipt of U-AUTHENTICATION RESPONSE BS-MM shall retrieve RES1 and compare it with the previously calculated XRES1 (as described in 200) to decide whether or not authentication was successful;

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

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

202 D-AUTHENTICATION RESULT at BS-MM:

- if authentication was successful, BS-MM shall set authentication result to TRUE and shall send D-AUTHENTICATION RESULT to MS-MM. Since mutual authentication has been requested BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESULT to be true and the response, RES2, shall be included in this PDU;

- if authentication of the MS was not successful, BS-MM shall set authentication result (R1) to FALSE and shall send D-AUTHENTICATION RESULT. The "Mutual authentication flag" in D-AUTHENTICATION RESULT shall be set to false and RES2 shall not be included in this PDU.

103 D-AUTHENTICATION RESULT at MS-MM:

- MS-MM shall retrieve R1 to check whether the authentication of MS was successful;

- since mutual authentication is required and if R1 indicates successful authentication, MS-MM shall retrieve RES2 and the MS shall run algorithms TA21 and TA22 to generate DCK2 and XRES2. MS-MM shall then compare XRES2 and RES2 to decide whether or not authentication of the SwMI was successful. If authentication of the SwMI and MS were both successful, the MS shall run algorithm TB4 with DCK1 and DCK2 as inputs to give DCK;

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

107 U-AUTHENTICATION RESULT at MS-MM:

- the MS shall stop timer τ_A;

- if authentication was successful for both instances, MS-MM shall send the result R2 to BS–MM in the U-AUTHENTICATION RESULT PDU. MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be false and RES1 shall not be included in this PDU;

- if authentication of the SwMI was not successful MS-MM shall send the result R2 = FALSE to MS-MM in the U-AUTHENTICATION RESULT PDU. MS-MM shall set the "Mutual authentication flag" to be false and RES1 shall not be included in this PDU;

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

207 U-AUTHENTICATION RESULT at BS-MM:

- the BS shall stop timer τ_A. BS-MM shall retrieve R2 to check whether the authentication of SwMI was successful.

104 MLE-ENCRYPTION request at MS-MM (in class 3 cells only):

- if authentication was successful MS-MM shall configure MS-MAC to receive and transmit with the newly calculated DCK;
- if authentication was not successful the MS shall continue to receive and transmit with the same ciphering parameters the MS was using before this authentication procedure was started. In this case the MS-MM shall not reconfigure MS-MAC.

301 MLE-ENCRYPTION request at MS-MAC:

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

203 MLE-ENCRYPTION request at BS-MM (in class 3 cells only):

- if the authentication was successful BS-MM shall configure BS-MAC to receive and transmit with the newly calculated DCK;
- if the authentication was not successful the SwMI shall continue to receive and transmit using the ciphering parameters in use before this authentication procedure was initiated. In this case BS-MM shall not reconfigure BS-MAC.

401 MLE-ENCRYPTION request at BS-MAC:

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

4.4.2.4 Case 4: Authentication initiated by MS and made mutual by the SwMI

Pre-requisite: MS is registered to SwMI.

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

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

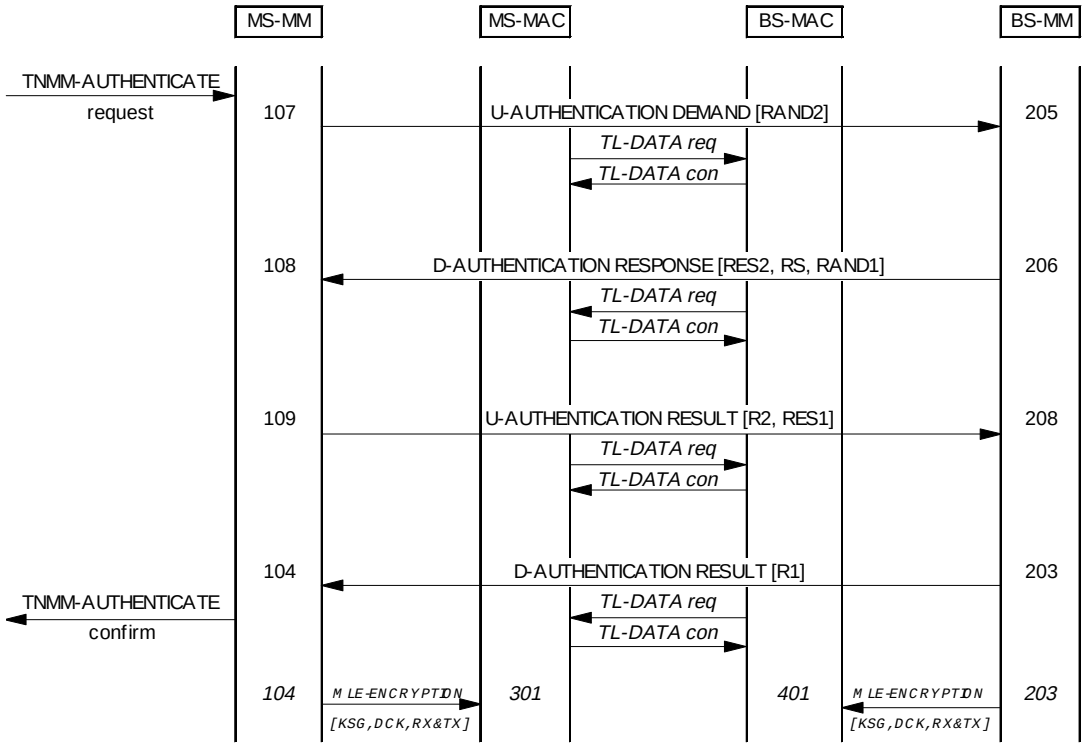


Figure 18: Authentication initiated by MS and made mutual by the MS

107 U-AUTHENTICATION DEMAND at MS-MM:

- MS-MM shall challenge BS-MM to authenticate by sending the challenge, RAND2. The MS shall start timer τ_A.

205 U-AUTHENTICATION DEMAND at BS-MM:

- BS-MM shall retrieve RAND2 and run algorithms TA21 and TA22 to generate RES2, and DCK2. The BS shall start timer τ_A;

- since the SwMI is configured to respond to authentication challenges from MS-MM with a mutual authentication, BS-MM shall not calculate DCK since BS-MM does not yet have DCK1.

206 D-AUTHENTICATION RESPONSE at BS-MM:

- BS-MM shall respond to the authentication challenge by sending RES2 and RS to MS-MM;

- since the SwMI is configured for mutual authentication, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESPONSE to be true and RAND1 shall be included in this PDU.

108 D-AUTHENTICATION RESPONSE at MS-MM:

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

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

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

109 U-AUTHENTICATION RESULT at MS-MM:

- if authentication was not successful, MS-MM shall send the result R2 = FALSE to BS-MM in the U-AUTHENTICATION RESULT PDU.MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be false and RES1 shall not be included in this PDU;

- since mutual authentication is in progress and if authentication of the SwMI was successful as indicated by R2, MS-MM shall send both the authentication result, R2, and the authentication response RES1 to BS-MM in U-AUTHENTICATION RESULT. MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be true.

208 U-AUTHENTICATION RESULT at BS-MM:

- BS-MM shall retrieve R2 to check whether the authentication of SwMI was successful;

- since mutual authentication has been attempted and if R2 indicates successful authentication, BS-MM shall retrieve RES1 and the SwMI shall run algorithms TA11 and TA12 to generate DCK1 and XRES1. BS-MM shall then compare XRES1 and RES1 to decide whether or not authentication of the MS was successful (R1). If both R1 and R2 indicate successful authentication, the SwMI shall run algorithm TB4 with DCK1 and DCK2 as inputs to generate DCK.

203 D-AUTHENTICATION RESULT at BS-MM:

- the BS shall stop timer τ_A;

- if authentication for both instances was successful, BS-MM shall set authentication result to TRUE and shall send D-AUTHENTICATION RESULT to MS-MM. BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESULT to be false and RES2 shall not be included in this PDU;

- if authentication of the MS was not successful, BS-MM shall set authentication result (R1) to FALSE and shall send D-AUTHENTICATION RESULT. The "Mutual authentication flag" in D-AUTHENTICATION RESULT shall be set to false and RES2 shall not be included in this PDU.

104 D-AUTHENTICATION RESULT at MS-MM:

- MS-MM shall retrieve R1 to check whether the authentication of MS was successful. The MS shall stop timer τ_A.

104 MLE-ENCRYPTION request at MS-MM (in class 3 cells only):

- if authentication was successful MS-MM shall configure MS-MAC to receive and transmit with the newly calculated DCK;

- if authentication was not successful the MS shall continue to receive and transmit with the same ciphering parameters the MS was using before this authentication procedure was started. In this case the MS-MM shall not reconfigure MS-MAC.

301 MLE-ENCRYPTION request at MS-MAC:

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

203 MLE-ENCRYPTION request at BS-MM (in class 3 cells only):

- if the authentication was successful BS-MM shall configure BS-MAC to receive and transmit with the newly calculated DCK;

- if the authentication was not successful the SwMI shall continue to receive and transmit using the ciphering parameters in use before this authentication procedure was initiated. In this case BS-MM shall not reconfigure BS-MAC.

401 MLE-ENCRYPTION request at BS-MAC:

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

4.4.2.5 Case 5: SwMI authenticates MS during registration

Pre-requisite: MS is camped on a cell.

Pre-requisite: MS is camped on a cell of the SwMI.

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

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

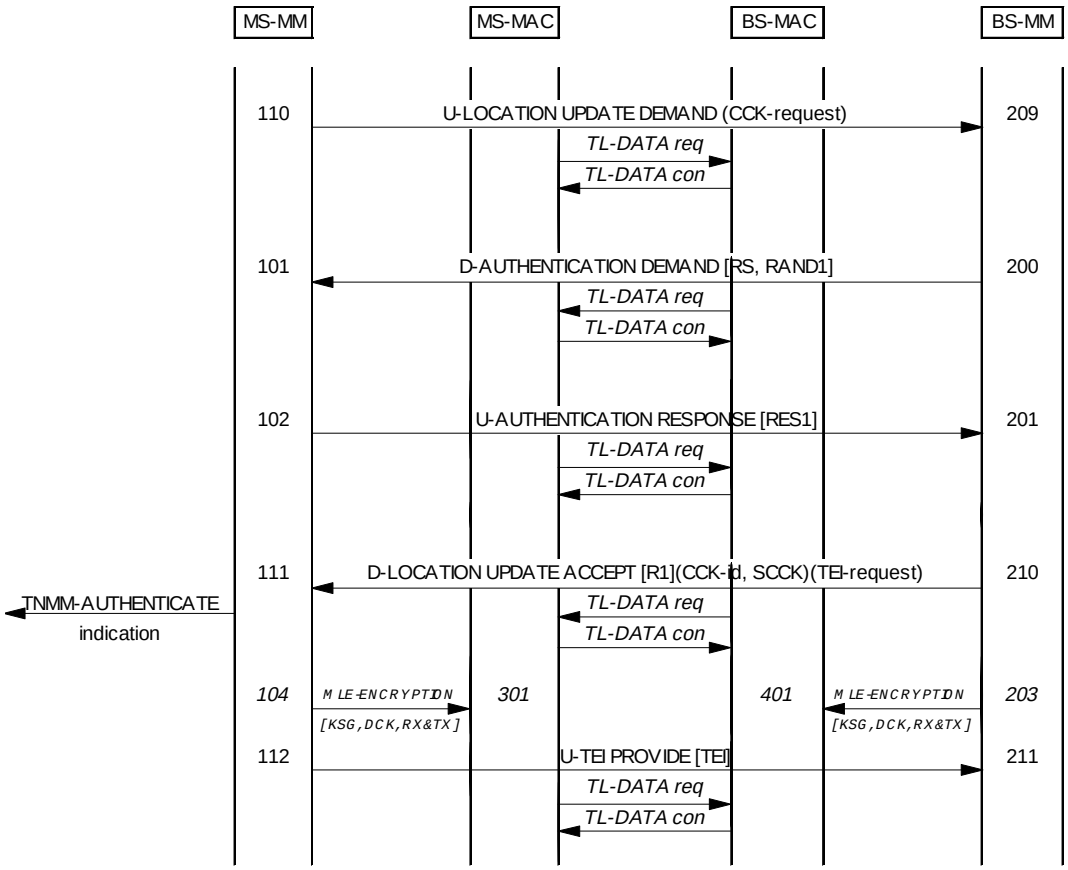


Figure 19: SwMI authentication of MS during registration procedure

110 U-LOCATION UPDATE DEMAND at MS-MM:

- MS-MM may include the type 3 element "Authentication uplink" in U-LOCATION UPDATE DEMAND. This allows an MS to request:
  - that the SwMI supplies the CCK for the location area with which the MS is attempting to register;
  - authentication of the SwMI;
  - both authentication and CCK provision.
- since in this scenario MS-MM is not configured to authenticate the SwMI at registration, MS-MM shall not include the RAND2 element in the type 3 element "Authentication uplink". If MS-MM requests CCK for the LA the type 3 element "Authentication uplink" shall be included with CCK request flag set to true;
- in class 3 cells where the MS requests the CCK of the current cell in the U-LOCATION UPDATE DEMAND PDU, the PDU exchange shall be in clear until MS has received D–LOCATION UPDATE ACCEPT containing the CCK as MS cannot form an ESI without knowledge of CCK.

209 U-LOCATION UPDATE DEMAND at BS-MM:

- a SwMI may be configured to authenticate an MS at registration, if this is the case the SwMI shall initiate authentication of the MS as described in subclause 4.4.2.8.

200 D-AUTHENTICATION DEMAND at BS-MM:

- BS-MM shall challenge MS-MM to authenticate by sending RS and RAND1. If the MS has requested CCK information the D-AUTHENTICATION DEMAND PDU is sent in clear. The SwMI shall also calculate XRES1 and DCK1 using algorithms TA11 and TA12 using RS and RAND1 as inputs;

- the BS shall start timer τ_A.

101 D-AUTHENTICATION DEMAND at MS-MM:

- MS-MM shall retrieve RS and RAND1 from the authentication challenge. The MS shall start timer τ_A, and shall run algorithms TA11 and TA12 to generate RES1 and DCK1;

- in class 3 cells since in this scenario the MS is configured for unilateral authentication, MS-MM shall run algorithm TB4 with DCK1 and DCK2 = 0 to generate DCK;

- if the MS is configured to respond to authentication challenges from BS-MM with a mutual authentication, MS-MM should not calculate DCK since MS-MM does not yet have DCK2. This scenario is described in case 8, subclause 4.4.2.8.

102 U-AUTHENTICATION RESPONSE at MS-MM:

- MS-MM shall respond to the authentication challenge by sending RES1 to BS-MM;

- since the MS is not configured to mutually authenticate the SwMI, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESPONSE to be false and RAND2 shall not be included in this PDU.

201 U-AUTHENTICATION RESPONSE at BS-MM:

- upon receipt of U-AUTHENTICATION RESPONSE the BS-MM shall retrieve RES1 and compare it with the previously calculated XRES1 (as described in 200) to decide whether or not authentication was successful;

- in class 3 cells since authentication is not mutual and if the MS authentication was successful BS-MM shall run algorithm TB4 with DCK1 and DCK2 = 0 as inputs to generate DCK;

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

210 D-LOCATION UPDATE ACCEPT at BS-MM:

- if authentication of the MS was successful and registration is to be accepted by the SwMI, BS-MM shall include the "Authentication downlink" type 3 element in D-LOCATION UPDATE ACCEPT to convey R1. BS-MM may request MS-MM to supply the MS TEI by setting the "TEI request flag" in the "Authentication downlink" element. If the MS requested the CCK information in U-LOCATION UPDATE DEMAND, BS-MM shall seal the CCK which is valid for the LA with which the MS is trying to register using algorithm TA41. CCK shall be sealed with the newly calculated DCK. BS-MM shall include the "CCK information for current LA" in the "Authentication downlink" element;

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

- if authentication of the MS was not successful, BS-MM shall send D-LOCATION UPDATE REJECT to MS-MM. D-LOCATION UPDATE REJECT shall contain a reject reason which shall indicate that authentication has failed and shall always be sent in clear in class 3 cells.

111 D-LOCATION UPDATE ACCEPT at MS-MM:

- the MS shall stop timer τ_A;

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

- if authentication was successful and the MS requested CCK information in U-LOCATION UPDATE DEMAND, MS-MM shall retrieve the "CCK information for current LA" from the "Authentication downlink" element in D-LOCATION UPDATE ACCEPT.

104 MLE-ENCRYPTION request at MS-MM (in class 3 cells only):

- if authentication was successful MS-MM shall configure MS-MAC to receive and transmit with the newly calculated DCK;

- if authentication was not successful the MS shall continue to receive and transmit with the same ciphering parameters the MS was using before this authentication procedure was started. In this case the MS-MM shall not reconfigure MS-MAC.

301 MLE-ENCRYPTION request at MS-MAC:

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

203 MLE-ENCRYPTION request at BS-MM (in class 3 cells only):

- if the authentication was successful BS-MM shall configure BS-MAC to receive and transmit with the newly calculated DCK;

- if the authentication was not successful the SwMI shall continue to receive and transmit using the ciphering parameters in use before this authentication procedure was initiated. In this case BS-MM shall not reconfigure BS-MAC.

401 MLE-ENCRYPTION request at BS-MAC:

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

112 U-TEI PROVIDE at MS-MM:

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

NOTE 2: The BS should not ask the MS to supply its TEI unless encryption is on. The MS should not provide its TEI over the air interface in clear in class 2 and class 3 cells.

- if the SwMI did not request the MS TEI in D-LOCATION UPDATE ACCEPT, U-TEI PROVIDE shall not be sent.

211 U-TEI PROVIDE at BS-MM:

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

4.4.2.6 Case 6: MS authenticates SwMI during registration

Pre-requisite: MS is camped on a cell of the SwMI.

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

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

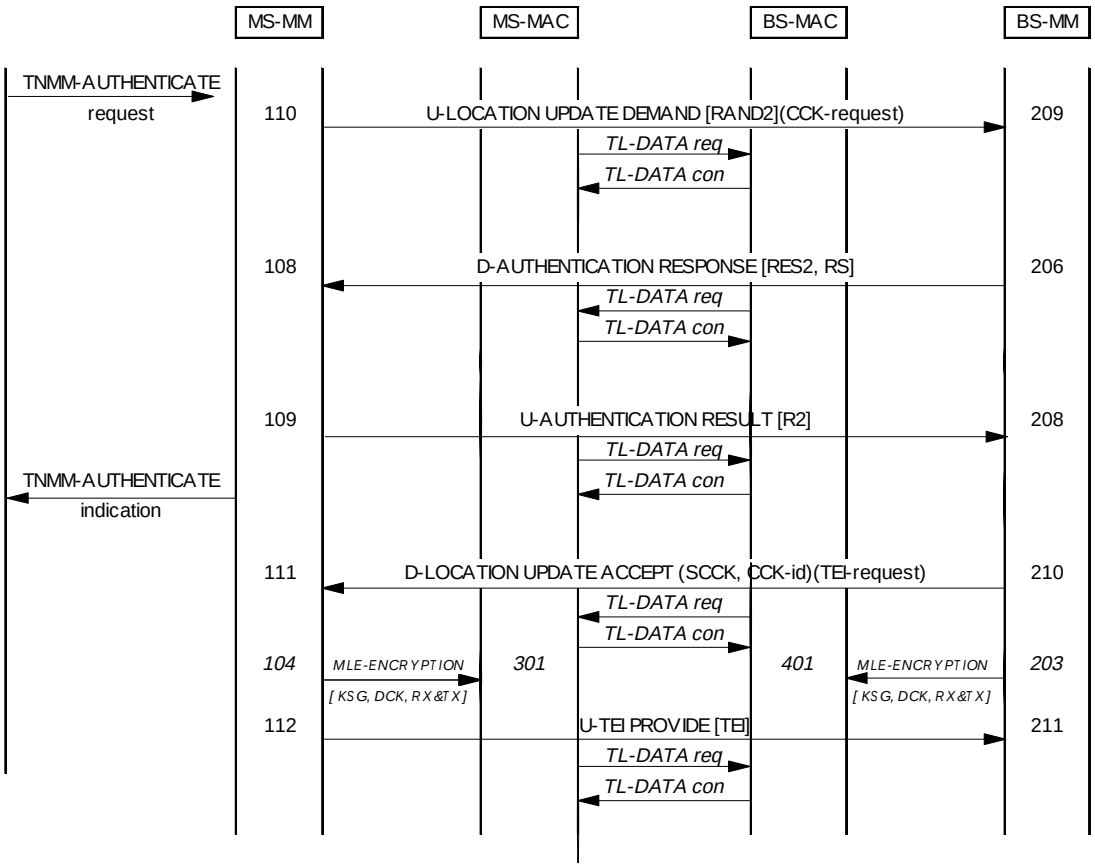


Figure 20: MS authentication of SwMI by the MS during registration

110 U-LOCATION UPDATE DEMAND at MS-MM:

- MS-MM may include the type 3 element "Authentication uplink" in U-LOCATION UPDATE DEMAND. This allows an MS to request:
  - that the SwMI supplies the CCK for the location area with which the MS is attempting to register;
  - authentication of the SwMI;
  - both authentication and CCK provision;
- since in this scenario MS-MM is configured to authenticate the SwMI at registration, MS-MM shall include the type 3 element "Authentication uplink" with the random challenge, RAND2, in this element. The MS shall start timer τ_A;
- in class 3 cells where the MS requests the CCK of the current cell in the U-LOCATION UPDATE DEMAND PDU, the PDU exchange shall be in clear until MS has received D-LOCATION UPDATE ACCEPT containing the CCK as MS cannot form an ESI without knowledge of CCK.

209 U-LOCATION UPDATE DEMAND at BS-MM:

- if the type-3 element "Authentication uplink" has been received with the random challenge BS-MM shall retrieve RAND2 and run algorithms TA21 and TA22 to generate RES2 and DCK2. The BS shall start timer τ_A;

- since in this scenario the SwMI is not configured for mutual authentication, BS-MM shall run TB4 with DCK2 and DCK1 = 0 to generate DCK;

- if the SwMI is configured for mutual authentication, BS-MM respond to the authentication request from the MS as described in 4.4.2.7.

206 D-AUTHENTICATION RESPONSE at BS-MM:

- BS-MM shall respond to the authentication challenge by sending RES2 and RS to MS-MM;

- since the SwMI is not configured to mutually authenticate the MS, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESPONSE to be false and RAND1 shall not be included in this PDU.

108 D-AUTHENTICATION RESPONSE at MS-MM:

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

- in class 3 cells if authentication was successful, and since the SwMI has not requested mutual authentication, MS-MM shall run algorithm TB4 with DCK2 and DCK1 = 0 to generate DCK. If authentication of the SwMI was not successful, MS-MM shall not calculate DCK.

109 U-AUTHENTICATION RESULT at MS-MM:

- the MS shall stop timer τ_A;

- if authentication was successful, MS-MM shall send the result R2 to BS-MM in the U-AUTHENTICATION RESULT PDU;

- since there is no mutual authentication, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be false and RES1 shall not be included in this PDU;

- if authentication was not successful MS-MM shall send the result R2 = FALSE to BS-MM in the U-AUTHENTICATION RESULT PDU. MS-MM shall set the "Mutual authentication flag" to be false and RES1 shall not be included in this PDU.

208 U-AUTHENTICATION RESULT at BS-MM:

- the BS shall stop timer τ_A;

- BS-MM shall retrieve R2 to check whether the authentication of the SwMI was successful.

210 D-LOCATION UPDATE ACCEPT at BS-MM:

- if authentication of the SwMI was successful BS-MM shall send the D-LOCATION UPDATE ACCEPT to MS-MM. BS-MM may request MS-MM to supply the MS TEI by setting the "TEI request flag" in the "Authentication downlink" element. If the MS requested the CCK information in U-LOCATION UPDATE DEMAND, BS-MM shall seal the CCK which is valid for the LA with which the MS is trying to register using algorithm TA41. CCK shall be sealed with the newly calculated DCK. BS-MM shall include the "CCK information for current LA" in the "Authentication downlink" element;

NOTE 1: The SwMI should not ask the MS to supply its TEI unless the TEI can be sent using an encrypted PDU. The MS should not provide its TEI over the air interface in clear in class 2 and class 3 cells.

- if authentication of the SwMI was not successful, BS-MM shall send D-LOCATION UPDATE REJECT to MS-MM. D-LOCATION UPDATE REJECT shall contain a reject reason which shall indicate that authentication has failed and shall always be sent in clear.

111 D-LOCATION UPDATE ACCEPT at MS-MM:

- if MS-MM receives D-LOCATION UPDATE ACCEPT and if the MS requested CCK information in U-LOCATION UPDATE DEMAND, MS-MM shall retrieve the "CCK information for current LA" from the "Authentication downlink" element in D-LOCATION UPDATE ACCEPT.

104 MLE-ENCRYPTION request at MS-MM (in class 3 cells only):

- if authentication was successful MS-MM shall configure MS-MAC to receive and transmit with the newly calculated DCK;

- if authentication was not successful the MS shall continue to receive and transmit with the same ciphering parameters the MS was using before this authentication procedure was started. In this case the MS-MM shall not reconfigure MS-MAC.

301 MLE-ENCRYPTION request at MS-MAC:

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

203 MLE-ENCRYPTION request at BS-MM (in class 3 cells only):

- if the authentication was successful BS-MM shall configure BS-MAC to receive and transmit with the newly calculated DCK;

- if the authentication was not successful the SwMI shall continue to receive and transmit using the ciphering parameters in use before this authentication procedure was initiated. In this case BS-MM shall not reconfigure BS-MAC.

401 MLE-ENCRYPTION request at BS-MAC:

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

112 U-TEI PROVIDE at MS-MM:

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

NOTE 2: The BS should not ask the MS to supply its TEI unless encryption is on. The MS should not provide its TEI over the air interface in clear in class 3 and class 2 cells.

- if the SwMI did not request the MS TEI in D-LOCATION UPDATE ACCEPT, U-TEI PROVIDE shall not be sent.

211 U-TEI PROVIDE at BS-MM:

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

4.4.2.7 Case 7: Authentication initiated by MS during registration and made mutual by the SwMI

Pre-requisite: MS is camped on a cell of the SwMI.

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

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

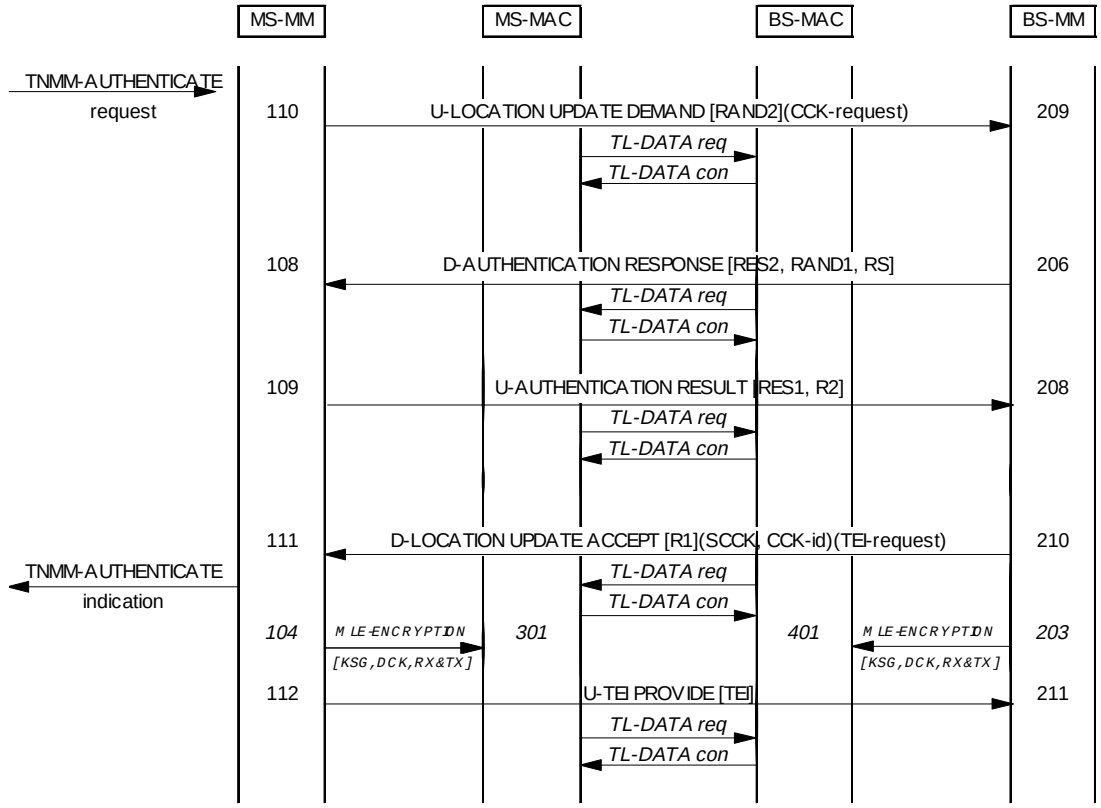


Figure 21: Authentication initiated by the MS during registration and made mutual by the SwMI

110 U-LOCATION UPDATE DEMAND at MS-MM:

- MS-MM may include the type 3 element "Authentication uplink" in U-LOCATION UPDATE DEMAND. This allows an MS to request:
  - that the SwMI supplies the CCK for the location area with which the MS is attempting to register;
  - authentication of the SwMI;
  - both authentication and CCK provision.
- since in this scenario MS-MM is configured to authenticate the SwMI at registration, MS-MM shall include the type 3 element "Authentication uplink" with the random challenge, RAND2, in this element. The MS shall start timer τ_A;
- in class 3 cells where the MS requests the CCK of the current cell in the U-LOCATION UPDATE DEMAND PDU, the PDU exchange shall be in clear until MS has received D–LOCATION UPDATE ACCEPT containing the CCK as MS cannot form an ESI without knowledge of CCK.

209 U-LOCATION UPDATE DEMAND at BS-MM:

- if the type-3 element "Authentication uplink" has been received with the random challenge BS-MM shall retrieve RAND2 and run algorithms TA21 and TA22 to generate RES2 and DCK2. The BS shall start timer τ_A.

206 D-AUTHENTICATION RESPONSE at BS-MM:

- BS-MM shall respond to the authentication challenge by sending RES2 and RS to MS-MM;

- since the SwMI is configured for mutual authentication, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESPONSE to be true and RAND1 shall be included in this PDU.

108 D-AUTHENTICATION RESPONSE at MS-MM:

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

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

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

109 U-AUTHENTICATION RESULT at MS-MM:

- if authentication of SwMI was not successful as indicated by R2, MS-MM shall send the result R2 = FALSE to BS-MM in the U-AUTHENTICATION RESULT PDU. MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be false and RES1 shall not be included in this PDU;

- since mutual authentication is in progress and if authentication of the SwMI was successful as indicated by R2, MS-MM shall send both the authentication result, R2, and the authentication response RES1 to BS-MM in U-AUTHENTICATION RESULT. MS-MM shall set the "Mutual authentication flag" to be true.

208 U-AUTHENTICATION RESULT at BS-MM:

- BS-MM shall retrieve R2 to check whether the authentication of the SwMI was successful;

- since mutual authentication has been attempted and if R2 indicates successful authentication, BS-MM shall retrieve RES1 and the SwMI shall run algorithms TA11 and TA12 to generate DCK1 and XRES1. BS-MM shall then compare XRES1 and RES1 to decide whether or not authentication of the MS was successful (R1). If both R1 and R2 indicate successful authentication, the SwMI shall run algorithm TB4 with DCK1 and DCK2 as inputs to generate DCK.

210 D-LOCATION UPDATE ACCEPT at BS-MM:

- if authentication of the MS and SwMI were successful and registration is to be accepted by the SwMI, BS-MM shall include the "Authentication downlink" type 3 element in D-LOCATION UPDATE ACCEPT to convey R1. BS-MM may request MS-MM to supply the MS TEI by setting the "TEI request flag" in the "Authentication downlink" element. If the MS requested the CCK information in U-LOCATION UPDATE DEMAND, BS-MM shall seal the CCK which is valid for the LA with which it is trying to register using algorithm TA41. CCK shall be sealed using the newly calculated DCK. BS-MM shall include the "CCK information for current LA" in the "Authentication downlink" element;

- the BS shall stop timer τ_A;

NOTE 1: The SwMI should not ask the MS to supply its TEI unless the TEI can be sent using an encrypted PDU. The MS should not provide its TEI over the air interface in clear in class 2 and class 3 cells.

- if authentication of either MS or SwMI was not successful, BS-MM shall send D-LOCATION UPDATE REJECT to MS-MM. D-LOCATION UPDATE REJECT shall contain a reject reason which shall indicate that authentication has failed and shall always be transmitted in clear.

111 D-LOCATION UPDATE ACCEPT at MS-MM:

- if MS-MM receives D-LOCATION UPDATE ACCEPT, MS-MM shall retrieve R1 which should indicate successful authentication. If authentication has failed, the MS should receive D-LOCATION UPDATE REJECT. The MS shall stop timer τ_A;

- if authentication was successful and if the MS requested CCK information in U-LOCATION UPDATE DEMAND, MS-MM shall retrieve the "CCK information for current LA" from the "Authentication downlink" element in D-LOCATION UPDATE ACCEPT.

104 MLE-ENCRYPTION request at MS-MM (in class 3 cells only):

- if authentication was successful MS-MM shall configure MS-MAC to receive and transmit with the newly calculated DCK;

- if authentication was not successful the MS shall continue to receive and transmit with the same ciphering parameters the MS was using before this authentication procedure was started. In this case the MS-MM shall not reconfigure MS-MAC.

301 MLE-ENCRYPTION request at MS-MAC:

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

203 MLE-ENCRYPTION request at BS-MM (in class 3 cells only):

- if the authentication was successful BS-MM shall configure BS-MAC to receive and transmit with the newly calculated DCK;

- if the authentication was not successful the SwMI shall continue to receive and transmit using the ciphering parameters in use before this authentication procedure was initiated. In this case BS-MM shall not reconfigure BS-MAC.

401 MLE-ENCRYPTION request at BS-MAC:

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

112 U-TEI PROVIDE at MS-MM:

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

NOTE 2: The BS should not ask the MS to supply its TEI unless encryption is on. The MS should not provide its TEI over the air interface in clear in class 2 and class 3 cells.

- if the SwMI did not request the MS TEI in D-LOCATION UPDATE ACCEPT, U-TEI PROVIDE shall not be sent.

211 U-TEI PROVIDE at BS-MM:

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

4.4.2.8 Case 8: Authentication initiated by SwMI during registration and made mutual by the MS

Pre-requisite: MS is camped on a cell of the SwMI.

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

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

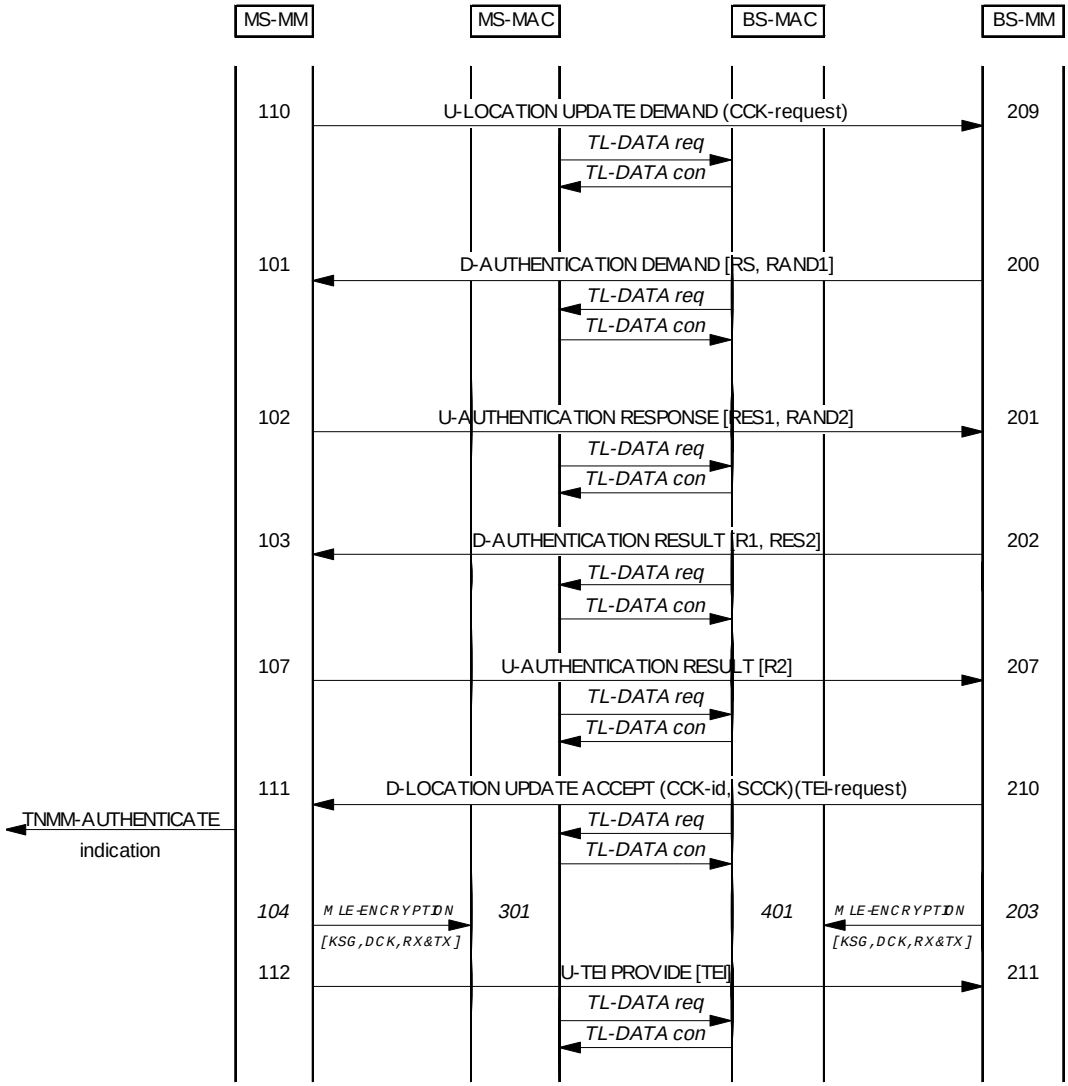


Figure 22: Authentication initiated by SwMI during registration and made mutual by the MS

110 U-LOCATION UPDATE DEMAND at MS-MM:

- MS-MM may include the type 3 element "Authentication uplink" in U-LOCATION UPDATE DEMAND. This allows an MS to request:
  - that the SwMI supplies the CCK for the location area with which the MS is attempting to register;
  - authentication of the SwMI;

- both authentication and CCK provision.

- since in this scenario MS-MM is not configured to authenticate the SwMI at registration, MS-MM shall not include the RAND2 element in the type 3 element "Authentication uplink". If MS-MM requests CCK for the LA the type 3 element "Authentication uplink" shall be included with CCK request flag set to true;

  in class 3 cells where the MS requests the CCK of the current cell in the U-LOCATION UPDATE DEMAND PDU, the PDU exchange shall be in clear until MS has received D–LOCATION UPDATE ACCEPT containing the CCK as MS cannot form an ESI without knowledge of CCK.

209 U-LOCATION UPDATE DEMAND at BS-MM:

- a SwMI may be configured to authenticate an MS at registration, if this is the case the SwMI shall initiate authentication of the MS as described in subclause 4.4.2.1.

200 D-AUTHENTICATION DEMAND at BS-MM:

- BS-MM shall challenge MS-MM to authenticate by sending RS and RAND1. If the MS has requested CCK information the D-AUTHENTICATION DEMAND PDU is sent in clear. The SwMI shall also calculate XRES1 and DCK1 using algorithms TA11 and TA12 using RS and RAND1 as inputs;

- the BS shall start timer τ_A.

101 D-AUTHENTICATION DEMAND at MS-MM:

- MS-MM shall retrieve RS and RAND1 from the authentication challenge. The MS shall start timer τ_A, and shall run algorithms TA11 and TA12 to generate RES1 and DCK1;

- if the MS is configured to respond to authentication challenges from BS-MM with a mutual authentication, MS-MM should not calculate DCK since MS-MM does not yet have DCK2.

102 U-AUTHENTICATION RESPONSE at MS-MM:

- MS-MM shall respond to the authentication challenge by sending RES1 to BS-MM;

- since the MS is configured for mutual authentication, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESPONSE to be true and RAND2 shall be included in this PDU.

201 U-AUTHENTICATION RESPONSE at BS-MM:

- upon receipt of U-AUTHENTICATION RESPONSE, BS-MM shall retrieve RES1 and compare it with the previously calculated XRES1 (as described in 200) to decide whether or not authentication was successful;

- since authentication is mutual and if the MS authentication was successful BS-MM shall retrieve RAND2 from U-AUTHENTICATION RESPONSE and the SwMI shall generate DCK2 and RES2 using algorithm TA21 and TA22. BS-MM shall then run algorithm TB4 with DCK1 and DCK2 as input to generate DCK;

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

202 D-AUTHENTICATION RESULT at BS-MM:

- if authentication was successful, BS-MM shall set authentication result to TRUE and shall send D-AUTHENTICATION RESULT to MS-MM. Since mutual authentication has been requested BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESULT to be true and the response, RES2, shall be included in this PDU;

- if authentication of the MS was not successful, BS-MM shall set authentication result (R1) to FALSE and shall send D-AUTHENTICATION RESULT. The "Mutual authentication flag" in D-AUTHENTICATION RESULT shall be set to false and RES2 shall not be included in this PDU.

103 D-AUTHENTICATION RESULT at MS-MM:

- MS-MM shall retrieve R1 to check whether the authentication of MS was successful;

- since mutual authentication is required and if R1 indicates successful authentication, MS-MM shall retrieve RES2 and the MS shall run algorithms TA21 and TA22 to generate DCK2 and XRES2. MS-MM shall then compare XRES2 and RES2 to decide whether or not authentication of the SwMI was successful. If authentication of the SwMI and MS were both successful, the MS shall run algorithm TB4 with DCK1 and DCK2 as inputs to give DCK;

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

107 U-AUTHENTICATION RESULT at MS-MM:

- if authentication was successful for both instances, MS-MM shall send the result R2 to BS–MM in the U-AUTHENTICATION RESULT PDU. MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be false and RES1 shall not be included in this PDU;

- if authentication of the SwMI was not successful MS-MM shall send the result R2 = FALSE to MS-MM in the U-AUTHENTICATION RESULT PDU. MS-MM shall set the "Mutual authentication flag to be false and RES1 shall not be included in this PDU;

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

207 U-AUTHENTICATION RESULT at BS-MM:

- the BS shall stop timer τ_A. BS-MM shall retrieve R2 to check whether the authentication of SwMI was successful.

104 MLE-ENCRYPTION request at MS-MM (in class 3 cells only):

- if authentication was successful MS-MM shall configure MS-MAC to receive and transmit with the newly calculated DCK;

- if authentication was not successful the MS shall continue to receive and transmit with the same ciphering parameters the MS was using before this authentication procedure was started. In this case the MS-MM shall not reconfigure MS-MAC.

210 D-LOCATION UPDATE ACCEPT at BS-MM:

- if authentication was successful, BS-MM shall send the D-LOCATION UPDATE ACCEPT. BS-MM may request MS-MM to supply the MS TEI by setting the "TEI request flag" in the "Authentication downlink" element. If the MS requested the CCK information in U-LOCATION UPDATE DEMAND, BS-MM shall seal the CCK which is valid for the LA with which the MS is trying to register using algorithm TA41. CCK shall be sealed with the newly calculated DCK. BS-MM shall include the "CCK information for current LA" in the "Authentication downlink" element;

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

- if authentication of the MS or SwMI was not successful, BS-MM shall send D-LOCATION UPDATE REJECT to MS-MM. D-LOCATION UPDATE REJECT shall contain a reject reason which shall indicate that authentication has failed and shall always be sent in clear in class 3 cells.

111 D-LOCATION UPDATE ACCEPT at MS-MM:

- the MS shall stop timer τ_A;

- if authentication is successful, MS-MM receives D-LOCATION UPDATE ACCEPT and if the MS requested CCK information in U-LOCATION UPDATE DEMAND, MS-MM shall retrieve the "CCK information for current LA" from the "Authentication downlink" element in D-LOCATION UPDATE ACCEPT;

- if authentication has failed, the MS should receive D-LOCATION UPDATE REJECT.

104 MLE-ENCRYPTION request at MS-MM (in class 3 cells only):

- if authentication was successful MS-MM shall configure MS-MAC to receive and transmit with the newly calculated DCK;

- if authentication was not successful the MS shall continue to receive and transmit with the same ciphering parameters the MS was using before this authentication procedure was started. In this case the MS-MM shall not reconfigure MS-MAC.

301 MLE-ENCRYPTION request at MS-MAC:

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

203 MLE-ENCRYPTION request at BS-MM (in class 3 cells only):

- if the authentication was successful BS-MM shall configure BS-MAC to receive and transmit with the newly calculated DCK;

- if the authentication was not successful the SwMI shall continue to receive and transmit using the ciphering parameters in use before this authentication procedure was initiated. In this case BS-MM shall not reconfigure BS-MAC.

401 MLE-ENCRYPTION request at BS-MAC:

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

112 U-TEI PROVIDE at MS-MM:

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

NOTE 2: The BS should not ask the MS to supply its TEI unless encryption is on. The MS should not provide its TEI over the air interface in clear in class 2 and class 3 cells.

- if the SwMI did not request the MS TEI in D-LOCATION UPDATE ACCEPT, U-TEI PROVIDE shall not be sent.

211 U-TEI PROVIDE at BS-MM:

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

4.4.2.9 Case 9: SwMI rejects authentication demand from MS

Pre-requisite: MS is registered to SwMI.

- U-AUTHENTICATION DEMAND shall contain RAND2;
- D-AUTHENTICATION REJECT shall contain the authentication reject reason.

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

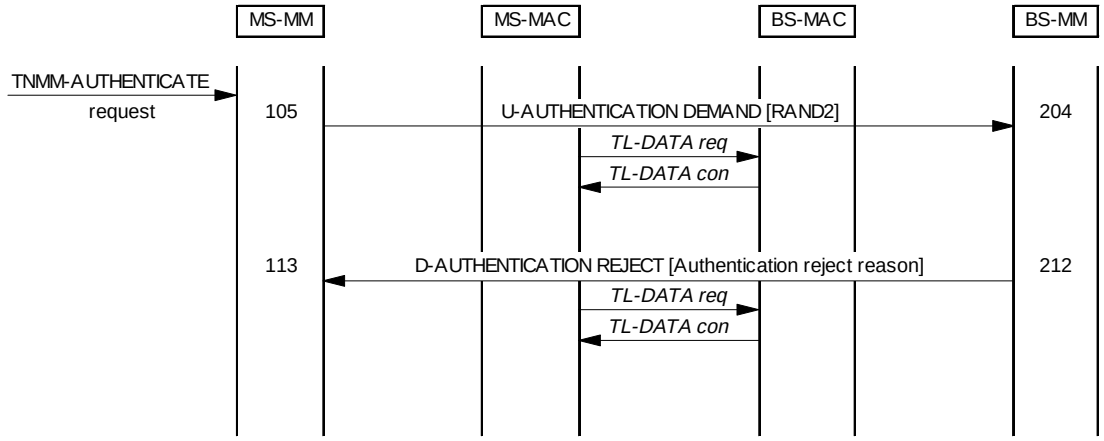


Figure 23: Authentication of the SwMI by the MS

105 U-AUTHENTICATION DEMAND at MS-MM:

- MS-MM shall challenge BS-MM to authenticate by sending the challenge, RAND2. The MS attemps to authenticate the SwMI could also be sent in the "Authentication uplink" type 3 element in U-LOCATION UPDATE DEMAND;

- the MS shall start timer τ_A.

204 U-AUTHENTICATION DEMAND at BS-MM:

BS-MM receives MS-MM authentication challenge.

212 D-AUTHENTICATION REJECT at BS-MM:

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

- if the MS has sent an authentication challenge as part of a registration request (U-LOCATION UPDATE DEMAND) and the MS has selected invalid ciphering parameters in U-LOCATION UPDATE DEMAND, BS-MM shall reject the request by sending D-LOCATION UPDATE REJECT instead of D-AUTHENTICATION REJECT, with reject cause indicating cipher parameter mismatch. The MS may then attempt to register again with the correct ciphering parameters and authentication request.

113 D-AUTHENTICATION REJECT at MS-MM:

- MS-MM shall reset timer τ_A;

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

4.4.2.10 Case 10: MS rejects authentication demand from SwMI

Pre-requisite: MS is registered to SwMI.

- D-AUTHENTICATION DEMAND shall contain RAND1 + RS;
- U-AUTHENTICATION REJECT shall contain the authentication reject reason.

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

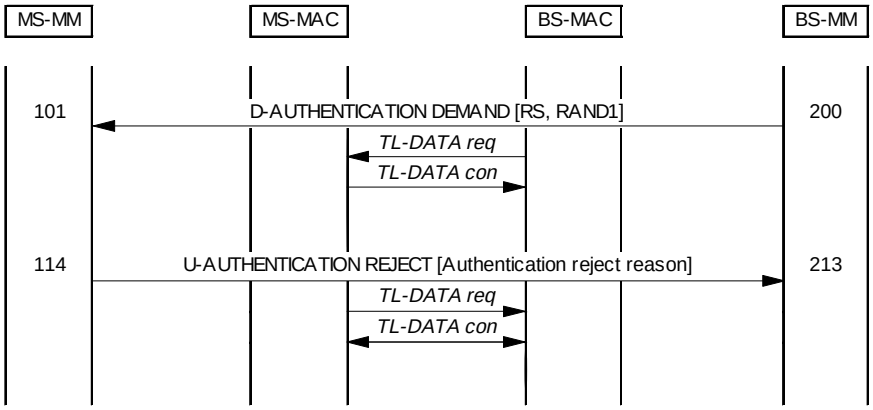


Figure 24: Authentication of MS by SwMI

200 D-AUTHENTICATION DEMAND at BS-MM:

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

- the BS shall start timer τ_A.

101 D-AUTHENTICATION DEMAND at MS-MM:

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

114 U-AUTHENTICATION REJECT at MS-MM:

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

213 U-AUTHENTICATION REJECT at BS-MM:

- BS-MM shall stop and reset timer τ_A;

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

4.4.3 CCK delivery - protocol functions

The CCK delivery functions described in this subclause 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 subclause describes the key management protocols used to support the algorithms and mechanisms described in subclause 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 subclause 4.2.5).

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

When scanning a cell prior to registration an MS shall receive the CCK-id of the CCK in use on that cell in the D-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 this ETS.

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 current LA identity.

The CCK may be provided explicitly by the SwMI using the "D-OTAR CCK Provide" 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–PREPARE PDU", or in a registration demand may be requested during the registration procedure using the MM type 3 element "Authentication uplink".

4.4.3.1 SwMI-initiated CCK provision

This scenario shows how the SwMI can distribute new CCK information. The SwMI can initiate CCK provision as 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 24.

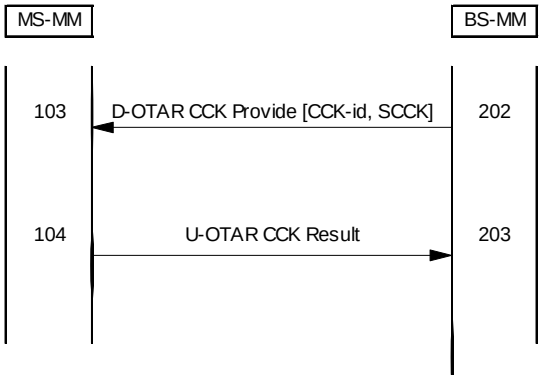


Figure 25: SwMI-initiated CCK provision

202 The SwMI shall distribute CCK information to an MS by sending D-OTAR CCK Provide to that MS. D-OTAR Provide shall contain a "CCK provision flag" set to TRUE and "CCK Information" element which shall contain information about the scope of usage of the CCK in this PDU. The CCK information element shall indicate if the CCK is for the current LA, for other LAs or for the entire system (i.e. all location areas for this SwMI). The "CCK provision flag" shall not be set to FALSE for SwMI-initiated CCK OTAR.

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

The SwMI shall include information relating to the location area scope of the CCK in the location area information subelement of the CCK information element.

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

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

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

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

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

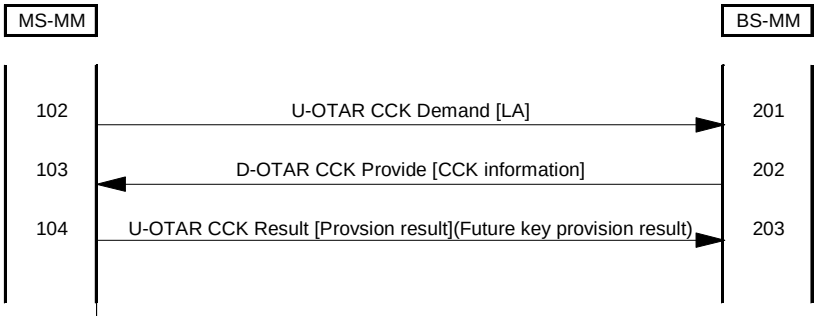


Figure 26: MS-initiated CCK provision

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

NOTE: The MS may send U-OTAR CCK Demand at any time to obtain CCK information for an LA.

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

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

If the SwMI is unable to deliver the requested CCK it shall send the D-OTAR CCK Provide PDU with no CCK information element.

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

If D-OTAR CCK Provide PDU contains no CCK information element the MS shall assume that the SwMI was unable to deliver the requested CCK. In this case the MS may request the CCK once camped on the nominated cell.

104 The MS shall send U-OTAR CCK Result to the SwMI.

4.4.3.3 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 cell type 1, 2 and 3 cell re-selection mechanisms (see also 6.5.1). In order to support roaming between 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 registering:

   the CCK request shall be sent in the U-LOCATION DEMAND PDU carried by the U–PREPARE PDU;

2) MS not registering:

   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 PDU may be sent in the U-PREPARE PDU.

The SwMI may supply the CCK of the requested LA using the D-OTAR Provide PDU, which may be contained in the D-NEW CELL PDU.

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 CCK request (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.

For roaming between cells of class 3 only using announced type 3 or 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 SwMI shall ensure that the new serving cell, and the LA to which it belongs, has DCK of the roaming ITSI (in effect this extends the registered area to include the new cell). The acceptance of the cell reselection shall be contained in D-NEW-CELL containing the CCK information of the new cell (using D-OTAR CCK Provide).

If the MS selects a new cell which is of a different security class than the current cell the MS shall be forced to register.

See also subclause 6.8.3.1 for change of class on moving cells.

4.4.3.4 MS initiated CCK provision within registration (without authentication)

Pre-requisite: MS is camped on a cell.

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

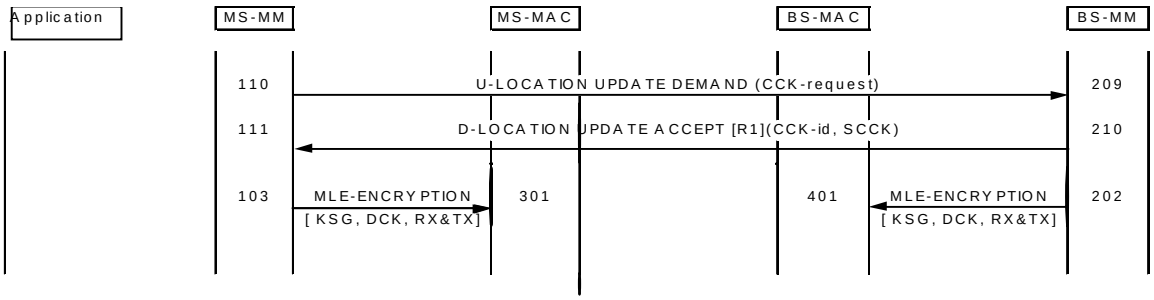


Figure 27: MS initiated CCK provision within registration (without authentication)

110 U-LOCATION UPDATE DEMAND at MS-MM:

- MS-MM may include the type 3 element "Authentication uplink" in U-LOCATION UPDATE DEMAND. This allows an MS to request:
  - that the SwMI supplies the CCK for the location area with which the MS is attempting to register;
  - authentication of the SwMI;
  - both authentication and CCK provision;
- MS-MM shall request the CCK of the current cell by setting value "CCK requested" to "CCK request" element of "Authentication uplink" element;
- since in this scenario MS-MM is not configured to authenticate the SwMI at registration, MS-MM shall not include the random challenge, RAND2. Scenarios where MS-MM is configured to authenticate the SwMI at registration are described in subclauses 4.4.2.6 and 4.4.2.7.

NOTE: In this case MS requests for CCK of the current cell in the U-LOCATION UPDATE DEMAND PDU and the PDU exchange shall be in clear until MS has received D–LOCATION UPDATE ACCEPT containing the CCK (MS can not form ESI address without knowing CCK).

209 U-LOCATION UPDATE DEMAND at BS-MM:

- a SwMI may be configured to authenticate an MS at registration; this case is described in subclause 4.4.2.5.

210 D-LOCATION UPDATE ACCEPT at BS-MM:

- if registration is to be accepted by the SwMI, BS-MM shall include the "Authentication downlink" element in D-LOCATION UPDATE ACCEPT to provide the CCK of the current cell. BS-MM shall seal the CCK which is valid for the LA using algorithm TA41 and DCK of the MS. BS-MM shall set the "CCK provision flag" true and include the "CCK information" element in the "Authentication downlink" element;
- if registration was not accepted, BS-MM shall send D-LOCATION UPDATE REJECT to MS-MM. D-LOCATION UPDATE REJECT shall contain a valid reject reason.

111 D-LOCATION UPDATE ACCEPT at MS-MM:

- if MS-MM receives D-LOCATION UPDATE ACCEPT, MS-MM shall retrieve the "CCK information" from the "Authentication downlink" element in D-LOCATION UPDATE ACCEPT;
- if MS-MM receives D-LOCATION UPDATE REJECT, MS-MM shall inspect the reject reason and react as specified for the reason.

202 MLE-ENCRYPTION request at BS-MM:

- if registration was accepted, BS-MM shall configure MS-MAC to receive and transmit with new DCK.

401 MLE-ENCRYPTION request at BS-MAC:

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

103 MLE-ENCRYPTION request at MS-MM:

- if registration was accepted, MS-MM shall configure MS-MAC to receive and transmit with DCK.

301 MLE-ENCRYPTION request at MS-MAC:

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

4.4.4 OTAR protocol functions - SCK

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

4.4.4.1 MS requests provision of SCK(s)

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

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

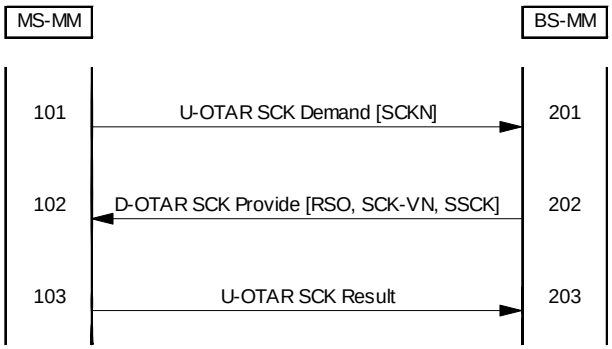


Figure 28: SCK delivery initiated by MS

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

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

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

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

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

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

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

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

4.4.4.2 SwMI provides SCK(s) to MS

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

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

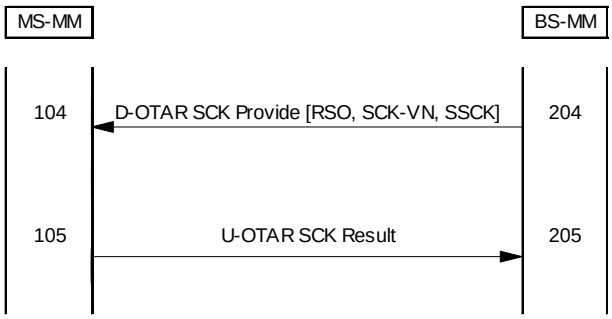


Figure 29: SCK delivery initiated by SwMI

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

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

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

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

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

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

4.4.5 OTAR protocol functions - GCK

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

4.4.5.1 MS requests provision of GCK

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

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

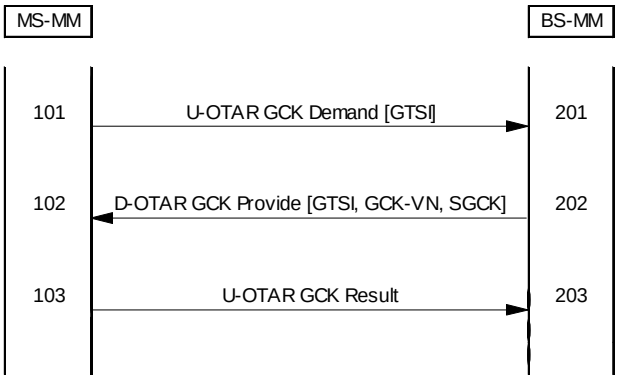


Figure 30: GCK delivery initiated by MS

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

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

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

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

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

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

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

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

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

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

4.4.5.2 SwMI provides GCK to MS

This scenario shows the case where the SwMI provides a GCK to an MS without the MS first requesting GCK provision. The SwMI may initiate this procedure at any time. The 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 29.

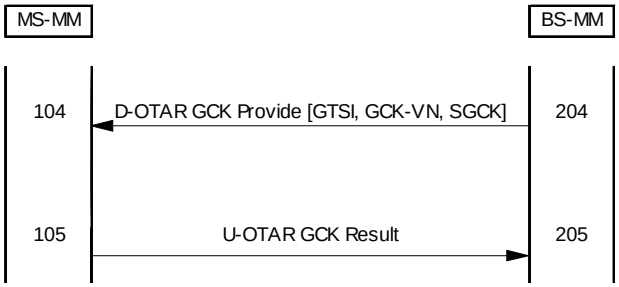


Figure 31: GCK delivery initiated by SwMI

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

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

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

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

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

4.4.6 Notification of key change over the air

The MM security function of the BS/SwMI shall use the exchange shown in figure 31 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 4.4.3 through 4.4.5.

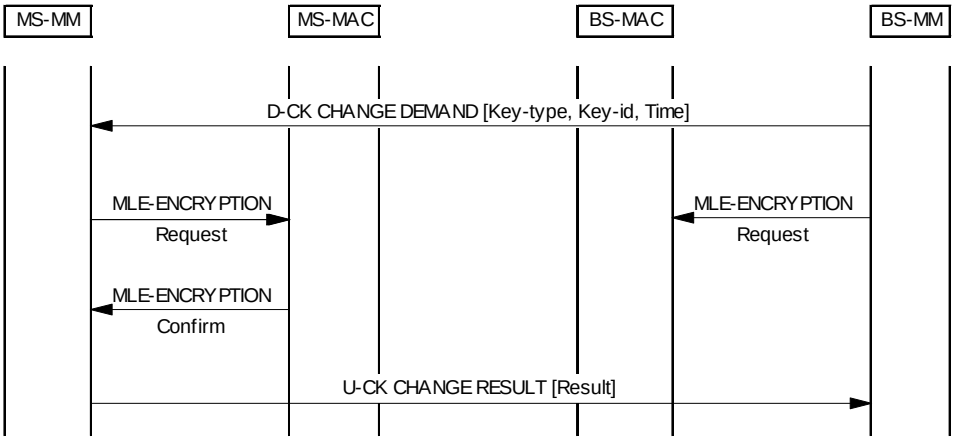


Figure 32: Key change protocol

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.

4.4.6.1 Security class 3

4.4.6.1.1 Change of DCK

In cells of security class 3 DCK shall be changed explicitly using the authentication protocols described in clause 4. Similarly in cells of security class 3 CCK shall be delivered to the security component of MM using the 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).

4.4.6.1.2 Change of CCK

The SwMI shall 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-ENCRPYTION 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 subclause 6.4.1.

4.4.6.1.3 Change of GCK

The SwMI shall administer the change of GCK using the D-CK-CHANGE-DEMAND PDU. The D-CK CHANGE DEMAND PDU shall be sent to the group address holding the new GCK.

4.4.6.2 Security class 2

If over the air cipher key selection is provided the SwMI shall administer the change of SCK using the D–CK-CHANGE-DEMAND PDU.

4.4.7 PDU descriptions

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

The general format of the PDU is defined for all MM PDUs in ETS 300 392-2 [2], subclause 14.7.

There shall be 7 PDUs defined at the air interface some of which shall have subtypes as shown in table 5.

Table 5: AIR INTERFACE PDUs and related sub-types

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

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

4.4.7.1 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 6: D-AUTHENTICATION DEMAND PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0001_2
Authentication sub-type	2	1	M	00_2
Random challenge [RAND1]	80	1	M	
Random seed [RS]	80	1	M	
Proprietary element		3	O	

4.4.7.2 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 7: D-AUTHENTICATION REJECT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0001_2
Authentication sub-type	2	1	M	11_2
Authentication reject reason	3	1	M	

4.4.7.3 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 8: D-AUTHENTICATION RESPONSE PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0001_2
Authentication sub-type	2	1	M	01_2
Random seed [RS]	80	1	M	
Response value [RES2]	32	1	M	
Mutual authentication flag	1	1	M	
Random challenge [RAND1]	80	1	C	Note
Proprietary element		3	O	
NOTE: RAND1 is conditional on the Mutual authentication flag element. RAND1 shall be present if Mutual authentication flag = 1. Otherwise, RAND1 shall not be present in the PDU.				

4.4.7.4 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 9: D-AUTHENTICATION RESULT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0001_2
Authentication sub-type	2	1	M	10_2
Authentication result [R1]	1	1	M	
Mutual authentication flag	1	1	M	
Response Value [RES2]	32	1	C	Note
Proprietary element		3	O	
NOTE: RES2 is conditional on the Mutual authentication flag element. RES2 shall be present if Mutual authentication flag = 1. Otherwise, RES2 shall not be present in the PDU.				

4.4.7.5 D-CK CHANGE DEMAND

Shall be used by SwMI to indicate a future cipher key change.

Direction: SwMI to MS;
Service used: MM;
Response to: none;
Response expected: U-CK CHANGE RESULT or none.

Table 10: D-CK CHANGE DEMAND contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0010_2
Acknowledgement flag	1	1	M	If true acknowledgement is required
Key type	2	1	M	SCK (00), CCK (01), GCK (10) value 11 reserved
SCK Number	5	1	C	Provided if key type = SCK
SCK Version number	16	1	C	Provided if key type = SCK
CCK-id	16	1	C	Provided if key type = CCK
GCK Version number	16	1	C	Provided if key type = GCK
Time type	1	1	M	Absolute IV (0) or system time (1)
IV	29	1	C	Provided if time type = Absolute IV
System time	40	1	C	Provided if time type = system time

4.4.7.6 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 11: D-OTAR CCK Provide PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0000_2
OTAR sub-type	3	1	M	CCK Provide
CCK provision flag	1	1	M	
CCK information	varies	1	C	If CCK provision flag is true
Proprietary element		3	O	

4.4.7.7 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 12: D-OTAR GCK Provide PDU contents

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

4.4.7.8 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 13: D-OTAR SCK Provide PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0000_2
OTAR sub-type	3	1	M	SCK Provide
Random seed	80	1	M	
Number of SCKs provided	3	1	M	
SCK key and identifier	141	1	C	Note
Proprietary element		3	O	
NOTE: The SCK and identifier element is conditional on the Number of SCKs element. There shall be as many SCK and identifier elements in the PDU as indicated by the Number of SCKs element. If "Number of SCKs" = 0, there shall be no "SCK key and identifier" elements in the PDU.				

4.4.7.9 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 14: U-AUTHENTICATION DEMAND PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0000_2
Authentication sub-type	2	1	M	00_2
Random challenge [RAND2]	80	1	M	
Proprietary element		3	O	

4.4.7.10 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 15: U-AUTHENTICATION REJECT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0000_2
Authentication sub-type	2	1	M	11_2
Authentication reject reason	3	1	M	

4.4.7.11 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 16: U-AUTHENTICATION RESPONSE PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0000_2
Authentication sub-type	2	1	M	01_2
Response Value [RES1]	32	1	M	
Mutual authentication flag	1	1	M	
Random challenge [RAND2]	80	1	C	Note
Proprietary element		3	O	
NOTE: RAND2 is conditional on the Mutual authentication flag element. RAND2 shall be present if Mutual authentication flag = 1. Otherwise, RAND2 shall not be present in the PDU.				

4.4.7.12 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 17: U-AUTHENTICATION RESULT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0000_2
Authentication sub-type	2	1	M	10_2
Authentication result [R2]	1	1	M	
Mutual authentication flag	1	1	M	
Response Value [RES1]	32	1	C	Note
Proprietary element		3	O	
NOTE: RES1 is conditional on the Mutual authentication flag element. RES1 shall be present if Mutual authentication flag = 1. Otherwise, RES1 shall not be present in the PDU.				

4.4.7.13 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 18: U-CK CHANGE RESULT contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0100_2
Result	1	1	M	

4.4.7.14 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 19: U-OTAR CCK Demand PDU contents

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

4.4.7.15 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 20: U-OTAR CCK Result PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0101_2
OTAR sub-type	3	1	M	CCK Result
Provision result	3	1	M	Provision result for CCK
Future key flag	1	1	M	
Future key provision result	3	1	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.				

4.4.7.16 U-OTAR GCK Demand

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

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

Table 21: U-OTAR GCK Demand PDU contents

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

4.4.7.17 U-OTAR GCK Result

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

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

Table 22: U-OTAR GCK Result PDU contents

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

4.4.7.18 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 23: U-OTAR SCK Demand PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0101_2
OTAR sub-type	3	1	M	SCK Demand
Number of SCKs requested	2	1	M	
SCK number (SCKN)	5	1	C	Note
Proprietary element		3	O	
NOTE: The SCK number element is conditional on the Number of SCKs element. There shall be as many SCK number elements in the PDU as indicated by the Number of SCKs element.				

4.4.7.19 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 24: U-OTAR SCK Result PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0101_2
OTAR sub-type	3	1	M	SCK Result
Number of SCKs requested	2	1	M	
SCK number and result	8	1	C	Note
Proprietary element		3	O	
NOTE: The SCK number and result element is conditional on the Number of SCKs requested element. There shall be as many SCK number and result elements in the PDU as indicated by the Number of SCKs requested element. Note that this PDU reports the result of a number of SCKs which were provided which may not be the same as the number of SCKs actually requested in the first place.				

4.4.7.20 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 25: U-TEI PROVIDE PDU contents

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

4.4.8 MM PDU type 3 information elements coding

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

4.4.8.1 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 26: Authentication downlink element contents

Information Element	Length	Type	C/O/M	Remark
Authentication result [R1]	1	1	M	
TEI request flag	1	1	M	
CCK provision flag	1	1	M	If true then CCK information is provided
CCK information	varies	1	C	

4.4.8.2 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 27: Authentication uplink element contents

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

4.4.9 PDU Information elements coding

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

4.4.9.1 Address extension

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

Table 28: Address extension element contents

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

4.4.9.2 Authentication reject reason

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

Table 29: Authentication reject reason element contents

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

4.4.9.3 Authentication result

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

Table 30: Authentication result element contents

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

4.4.9.4 CCK identifier

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

Table 31: CCK Identifier element contents

Information element	Length	Value	Remark
CCK Identifier	16	Any	

4.4.9.5 CCK information

The CCK information element is defined as below:

Table 32: 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	
Location area information	2-214	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

4.4.9.6 CCK provision flag

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

Table 33: CCK request flag element contents

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

4.4.9.7 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 34: CCK request flag element contents

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

4.4.9.8 GCK key and identifier

The CCK key and identifier element is defined as below:

Table 35: GCK key and identifier element contents

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

4.4.9.9 GCK version number

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

Table 36: GCK version number element contents

Information element	Length	Value	Remark
GCK-VN	16	any	

4.4.9.10 GSSI

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

Table 37: GSSI element contents

Information element	Length	Value	Remark
GSSI	24	any	

4.4.9.11 Location area

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

Table 38: Location area element contents

Information element	Length	Value	Remark
Location area	14	any	

4.4.9.12 Location area bit mask

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

Table 39: Location area bit mask element contents

Information element	Length	Value	Remark
Location area bit mask	14	any	The location area bit mask shall act as a subnet mask. The mask is logically ANDed with the LA-id. IF LA-id after the AND operation is intact (unchanged) then the LA is valid for the CCK. If LA-id is modified after the AND operation then the LA-id is not valid for the CCK.

4.4.9.13 Location area information

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

Table 40: 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 range	28	1	C	If Type = 11
NOTE: The location area bit mask shall act as a subnet mask. The mask is logically ANDed with the LA-id. IF LA-id after the AND operation is intact (unchanged) then the LA is valid for the CCK. If LA-id is modified after the AND operation then the LA-id is not valid for the CCK.				

4.4.9.14 Location area list

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

Table 41: Location area list element contents

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

4.4.9.15 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 42: 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.			

4.4.9.16 Mobile country code

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

Table 43: Mobile country code element contents

Information element	Length	Value	Remark
Mobile country code	10	any	

4.4.9.17 Mobile network code

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

Table 44: Mobile network code element contents

Information element	Length	Value	Remark
Mobile network code	14	any	

4.4.9.18 Mutual authentication flag

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

Table 45: Mutual authentication flag element contents

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

4.4.9.19 Number of location areas

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

Table 46: Number of location areas element contents

Information element	Length	Value	Remark
Number of location areas	4	0000_2	Reserved
		0001_2 to 1111_2	1 to 15 location areas

4.4.9.20 Number of SCKs provided

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

Table 47: Number of SCKs provided element contents

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

4.4.9.21 Number of SCKs requested

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

Table 48: Number of SCKs requested element contents

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

4.4.9.22 OTAR sub-type

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

Table 49: OTAR sub-type element contents

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

4.4.9.23 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 ETS 300 392-2 [2], clause 16.

Table 50: PDU type element contents

Information element	Length	Value	Downlink Assignment	Uplink Assignment
PDU Type	4	0000_2	D-OTAR	U-AUTHENTICATION
		0001_2	D-AUTHENTICATION	
		0010_2	D-CK CHANGE DEMAND	
		0011_2	D-DISABLE	
		0100_2	D-ENABLE	U-CK CHANGE RESULT
		0101_2		U-OTAR
		1001_2		U-TEI PROVIDE
		1011_2		U-DISABLE STATUS

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

4.4.9.24 Proprietary

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

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

4.4.9.25 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 51: Provision result element contents

Information element	Length	Value	Remark
Provision result	3	000_2	Sealed key accepted
		001_2	Sealed key failed to decrypt
		010_2	Incorrect KN
		011_2 to 111_2	Reserved

4.4.9.26 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 52: Random challenge element contents

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

4.4.9.27 Random seed

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

Table 53: Random seed element contents

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

4.4.9.28 Reject cause

The reject cause element is defined in clause 16 of ETS 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 54: Reject cause element contents

Information element	Length	Value	Remark
Reject cause	5	01101_2	No cipher KSG
		01110_2	Identified cipher KSG not supported
		01111_2	Requested cipher key not available
		10000_2	Identified cipher key not available
		10010_2	Ciphering required
		10011_2	Authentication failure

4.4.9.29 Response value

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

Table 55: Response value element contents

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

4.4.9.30 SCK key and identifier

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

Table 56: SCK key and number element contents

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

4.4.9.31 SCK number

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

Table 57: SCK number element contents

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

4.4.9.32 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 58: SCK number and result element contents

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

4.4.9.33 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 59: SCK version number element contents

Information element	Length	Value	Remark
SCK version number	16	Any	

4.4.9.34 Sealed Key (Sealed CCK, Sealed SCK, Sealed GCK)

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

Table 60: Sealed Key element contents

Information element	Length	Value	Remark
Sealed Key	120	Any	

4.4.9.35 SSI

This is the short subscriber identity of the MS. For a full definition see ETS 300 392-1 [1], clause 7.

Table 61: TEI contents

Information element	Length	Value	Remark
SSI	24	Any	

4.4.9.36 TEI

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

Table 62: TEI contents

Information element	Length	Value	Remark
Terminal equipment identifier	60	Any	

4.4.9.37 TEI request flag

This bit indicates whether the MS should supply the TEI.

Table 63: TEI request flag contents

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

4.4.9.38 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 this part of the ETS only and are taken from the reserved values of type 3 element identifier defined in the MM protocol. For more details, see ETS 300 392-2 [2], clause 16.

Table 64: Type 3 element identifier element contents

Information element	Length	Value	Remarks
Type 3 element identifier	4	1001_2	Authentication uplink
		1010_2	Authentication downlink

4.5 Boundary conditions for the cryptographic algorithms and procedures

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

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

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

Output: Bit string of length |KS|.

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

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

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

Output: Bit string of length |KS'|.

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

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

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

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

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

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

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

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

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

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

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

Output: Bit string of length |SCCK|.

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

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

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

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

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

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

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

Output 1: Bit string of length |KSO|.

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

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

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

Output: Bit string of length |SSCK|.

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

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

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

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

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

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

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

Output 1: Bit string of length |ESI|.

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

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

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

Output 1: Bit string of length |MGCK|.

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

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

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

Output: Bit string of length |SGCK|.

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

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

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

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

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

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

Input: Bit string of length |AC|;

Output: Bit string of length |K|.

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

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

Input: Bit string of length |UAK|;

Output: Bit string of length |K|.

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

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

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

Output: Bit string of length |K|.

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

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

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

Output: Bit string of length |DCK|.

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

4.6 Dimensioning of the cryptographic parameters

Table 62 shows the lengths of the cryptographic parameters given in subclause 4.5.

Table 65: Dimensioning of cryptographic parameters

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

4.7 Summary of the cryptographic processes

A summary of the authentication mechanisms explained in the previous subclauses is given in figure 30. Only the paths where keys are generated by an algorithm are shown and only the CCK option for generating MGCK from GCK is shown.

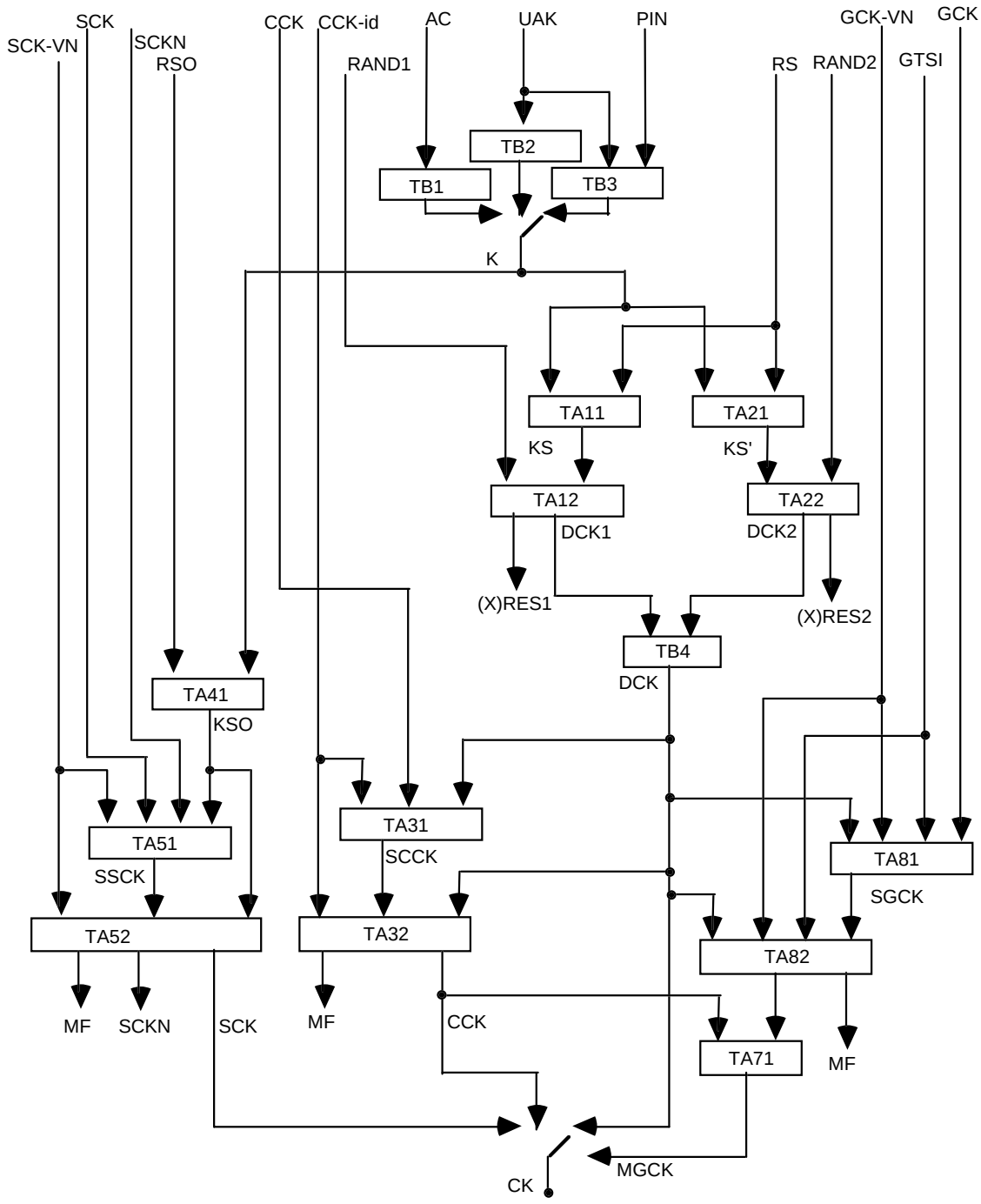


Figure 33: Overview of air interface authentication and key management

5 Enable and disable mechanism

5.1 General relationships

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

Figure 34 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], subclause 11.4.4 shall be enforced in addition to the protocols described in this subclause.

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

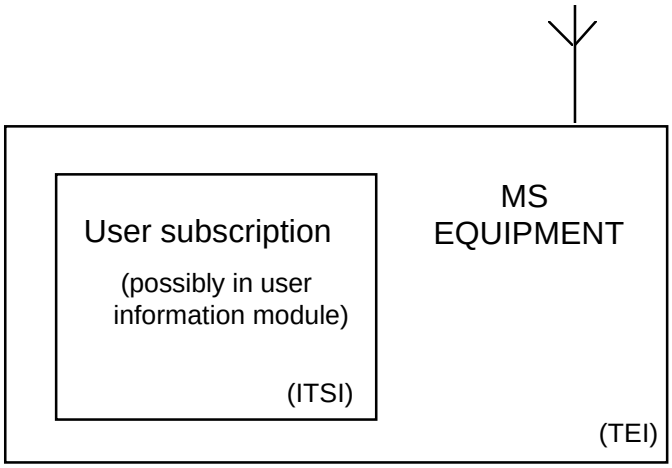
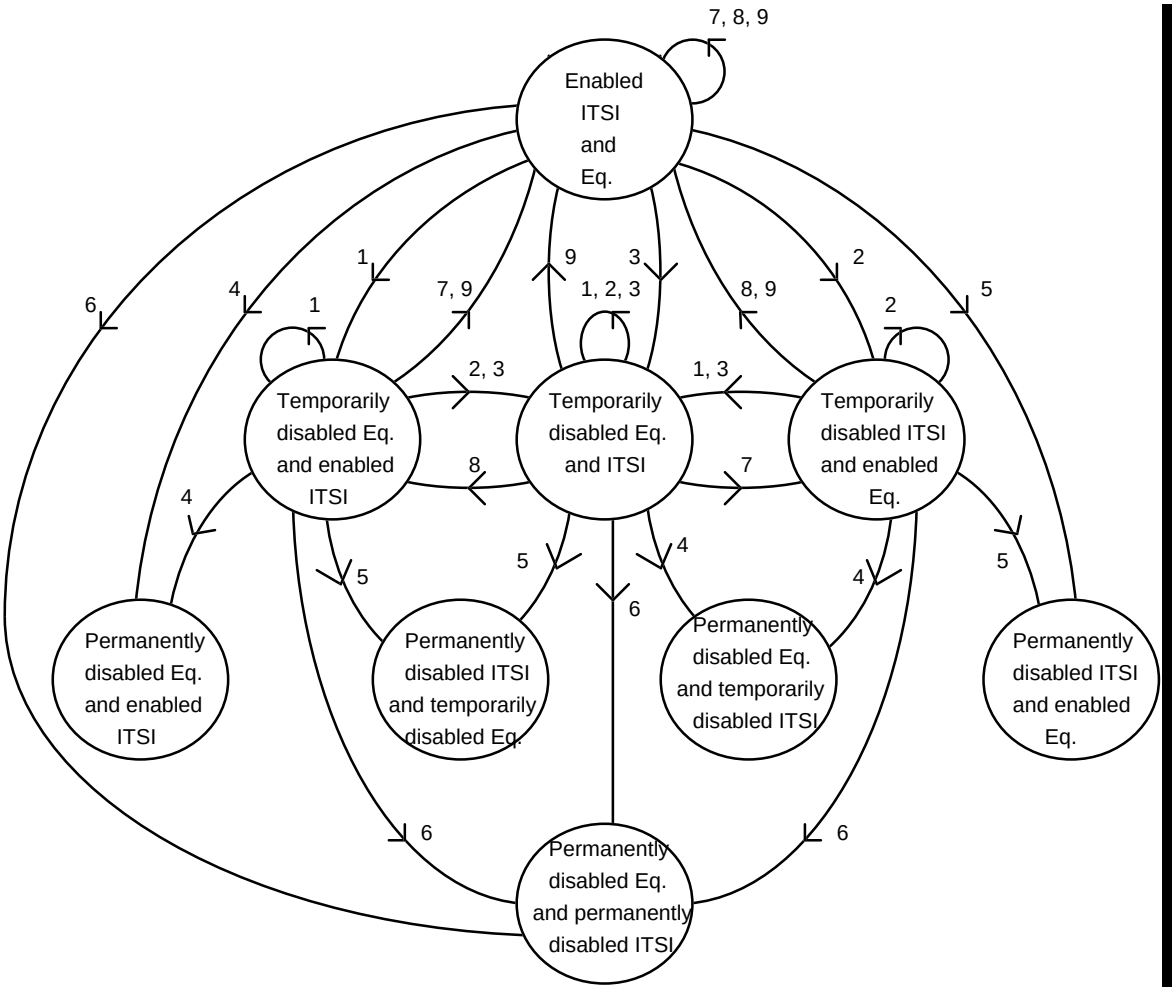


Figure 34: Relationship of TEI and ITSI in MS

5.2 Enable/disable state transitions

Figure 35 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 35: State transitions of enable/disable mechanism

5.3 Mechanisms

An MS and SwMI operating in security class 3 shall perform disabling with authentication and encryption applied. After temporary disable in a class 3 equipment and whilst still registered by the system enable shall be performed with authentication and encryption applied.

An MS and SwMI operating in security class 2 shall perform enabling and disabling with encryption applied. If authentication is required by the SwMI it shall be applied for enable and disable operations.

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.

All MS (irrespective of security class) shall support temporary disabling and enabling of both ITSI and TEI. For all MS that support authentication (mandatory in class 3, optional in class 1 and 2) they shall additionally support permanent disabling of both ITSI and TEI. In all cases authentication shall be initiated by the SwMI and made mutual by the MS. If the SwMI proposes permanent disable without authentication the MS may reject it with cause "Authentication required".

There are six possible transactions necessary for the enable/disable procedure which allow disable and enable of the MS equipment, the users' subscription, or both. These are detailed in subclauses 5.3.1 to 5.3.6.

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

Equipment or subscriptions that have been temporarily disabled may be enabled by the enable mechanisms described in subclauses 5.3.4 to 5.3.6. Equipment or subscriptions that have been permanently disabled shall not be enabled by these mechanisms.

5.3.1 Disable of MS equipment

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

5.3.2 Disable of MS subscription

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

5.3.3 Disable an MS subscription and equipment

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

5.3.4 Enable an MS equipment

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

5.3.5 Enable an MS subscription

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

5.3.6 Enable an MS equipment and subscription

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

Where the ITSI is not separable, an MS may be disabled by utilizing any of the mechanisms described in subclauses 5.3.1, 5.3.2 and 5.3.3. However, to re-enable an MS the SwMI shall use the corresponding mechanism or a mechanism including it. Therefore, an MS temporarily disabled using the mechanism described in subclause 5.3.1 shall only be enabled using the mechanisms described in subclause 5.3.4 or subclause 5.3.6; an MS disabled by the mechanism described in subclause 5.3.2 shall only be enabled by the mechanisms described in subclause 5.3.5 or subclause 5.3.6; and an MS disabled by the mechanism described in subclause 5.3.3 shall only be enabled by the mechanism described in subclause 5.3.6.

5.4 Enable/disable protocol

5.4.1 General case

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

The TEI when included in PDUs is not protected by any specific cryptographic sealing mechanism. It should therefore only be provided when encryption parameters have been established, and air interface encryption is operating on a 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, therefore it is recommended where possible that the MS authenticates the SwMI when instructed by the SwMI to disable by TEI in class 1 cells.

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; CONP, SCLNP and 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, CONP and SCLNP entities. MM should remain active so that any roaming functions 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 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.

5.4.3 Specific protocol exchanges

The normal message exchanges for the various cases shall be according to subclauses 5.4.2.1 through 5.4.2.3.

All MM security services shall use the acknowledged layer 2 service of the TETRA protocol stack (TL–DATA request and TL-DATA confirm). The data transmission and its acknowledgement shall use the same cipher parameters. In class 3 cells where successful authentication produces a new DCK this DCK shall not be invoked until after receipt of the acknowledgement to the PDU containing the RESULT of the authentication.

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.

Figure 36 shows the (mandatory) normal message sequence in this case.

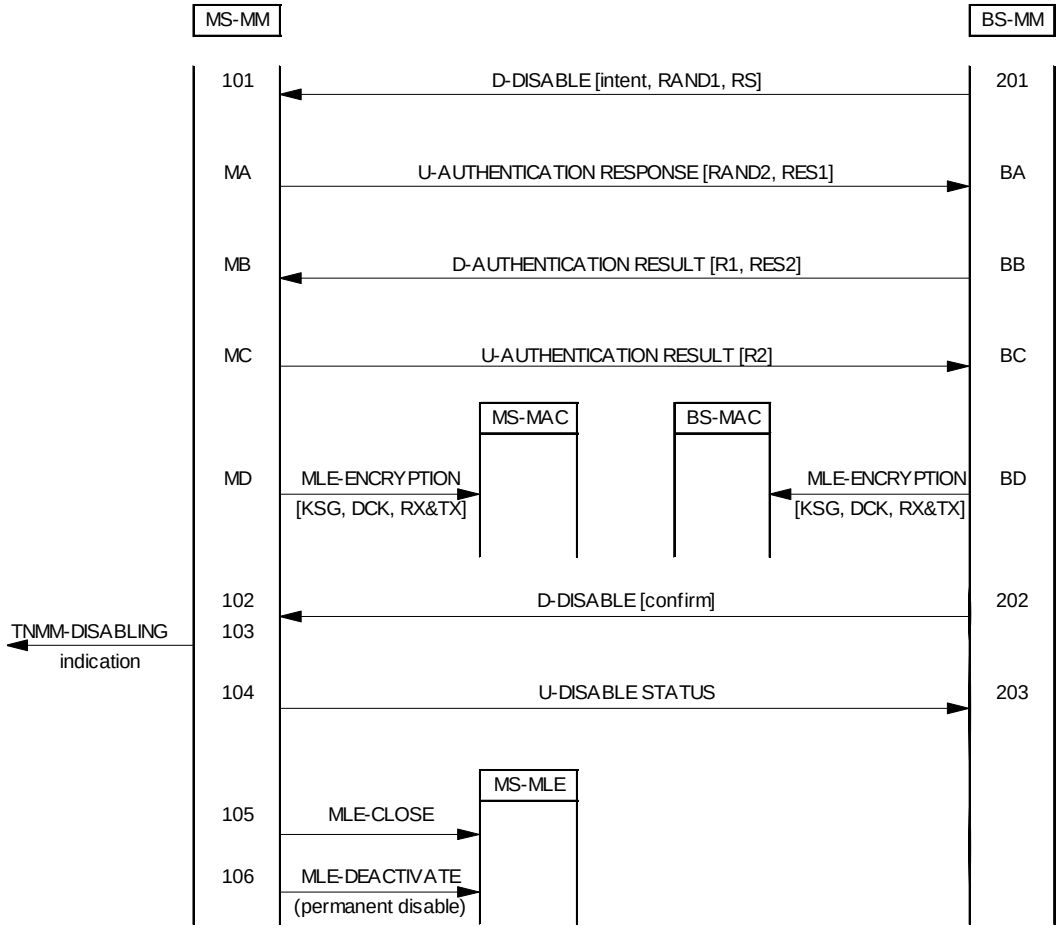


Figure 36: Disabling an MS with authentication

201 BS-MM shall send to MS-MM the D-DISABLE PDU with element Intent/Confirm set to Intent.

In class 3 cells, and in class 1 and class 2 cells requiring authentication, the authentication challenge element shall be included and the timer τ_A shall be set.

The "Equipment disable" and "Subscription disable" elements shall indicate whether the equipment or subscription or both are to be disabled. If the subscription is to be disabled, the "SSI" and "Address extension" elements shall be present; and if the equipment is to be disabled, the "TEI" element shall be present. The D-DISABLE intent shall indicate whether the disabling is temporary or permanent by setting the "Disabling type" element appropriately.

101 If the TEI and/or ITSI included in D-DISABLE intent match those of the MS it shall prepare to obey the command.

If the received D-DISABLE intent includes an authentication challenge the MS shall follow the procedure for mutual authentication described in 4.4.2.3.

The actions of the MS and BS shown in figure 35 as MA, MB, MC, MD and BA, BB, BC, BD shall be as defined in 4.4.2.3 for authentication initiated by the SwMI and made mutual by the MS.

202 Where authentication was a success the BS/SwMI shall confirm the original command using the D-DISABLE confirm PDU.

103 Since the D-DISABLE intent contained an authentication challenge and the ensuing authentication was a success the MS shall check that the D-DISABLE confirm PDU contains the same command as the exchange started with.

MS-MM shall inform the application of the disabling procedure about to be invoked using the TNMM-DISABLING indication primitive.

105 The MS shall comply with the request, and disable itself, sending an MLE-CLOSE req primitive from MM to MLE to prevent the MS from taking part in calls.

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

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

For more details on the authentication protocols used as part of the disable procedure, see subclause 4.4.2.3 which shows SwMI authentication of the MS made mutual by the MS.

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.

Figure 37 shows the (mandatory) normal message sequence in this case.

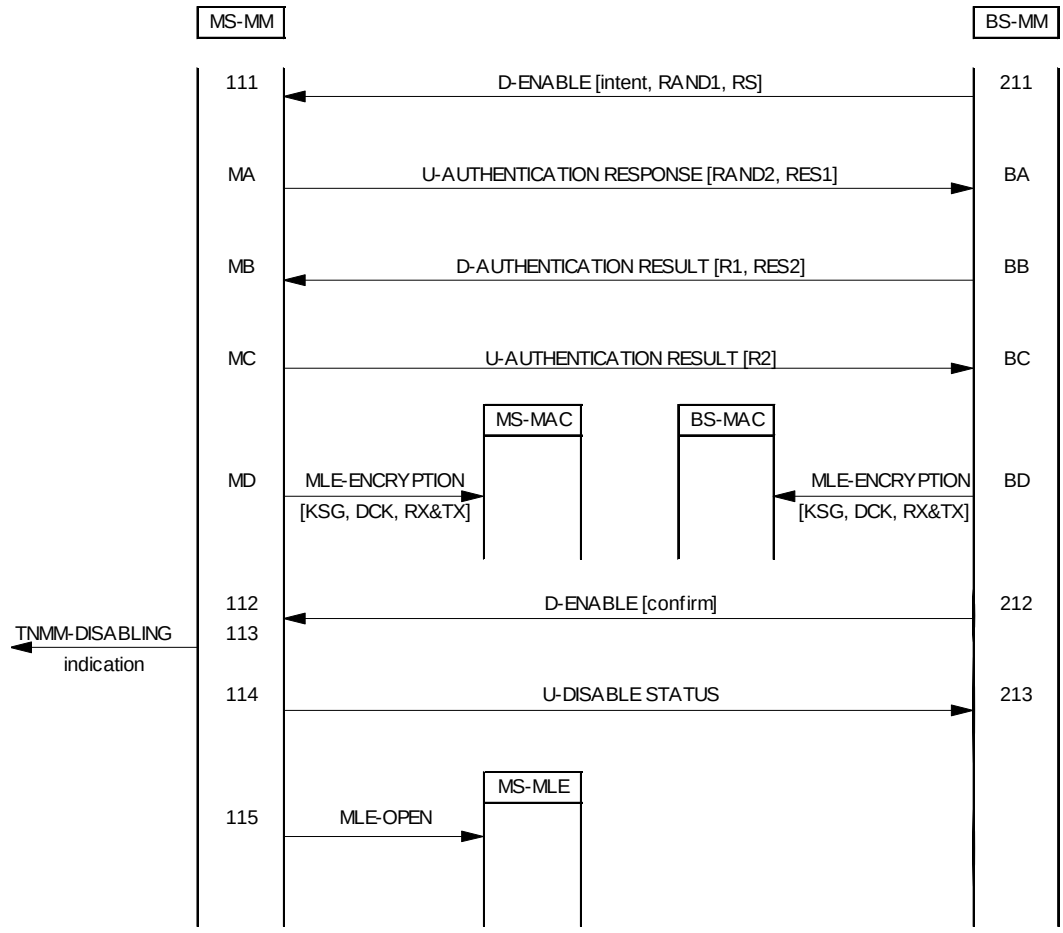


Figure 37: Enabling an MS with authentication

211 BS-MM shall send to MS-MM the D-ENABLE PDU with element Intent/Confirm set to Intent. Since in this case the authentication challenge element is included the timer τ_A shall be set and the authentication procedure described in 4.4.2.3 shall be followed. The "Equipment enable" and "Subscription enable" elements shall indicate whether the equipment or subscription or both are to be enabled. If the subscription is to be disabled, the "SSI" and "Address extension" elements shall be present; and if the equipment is to be disabled, the "TEI" element shall be present.

111 If the TEI and/or ITSI included in D-ENABLE intent match those of the MS it shall prepare to obey the command. Since in this case the received D-ENABLE intent included an authentication challenge the MS shall follow the procedure for mutual authentication described in 4.4.2.3.

212 If authentication was a success the BS/SwMI shall confirm the original command using the D-ENABLE confirm PDU.

112 If the authentication was a success the MS shall confirm that the D-ENABLE confirm PDU contains the same command as the exchange started with.

113 MS-MM shall inform the application of the enabling procedure about to be invoked using the TNMM-ENABLING indication primitive.

115 The MS shall comply with the request, and enable itself, sending an MLE-OPEN req primitive from MM to MLE to allow the MS to take part in calls.

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.

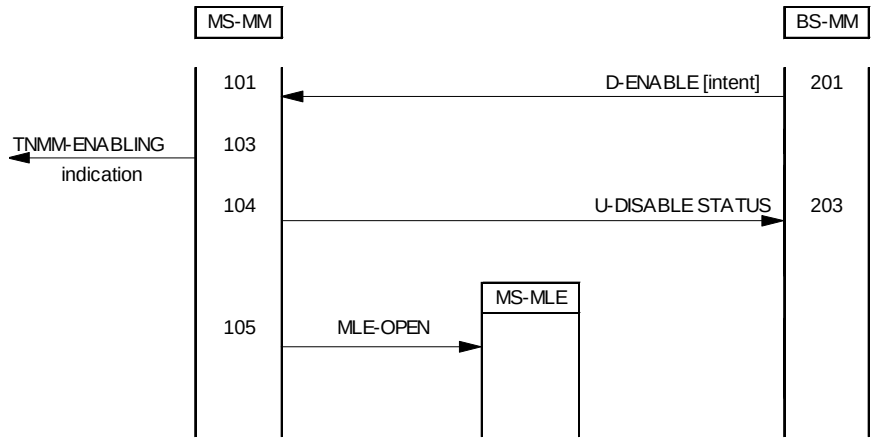


Figure 38: Enabling an MS without authentication

201 BS-MM shall send to MS-MM the D-ENABLE PDU with element Intent/Confirm set to Intent. The "Equipment enable" and "Subscription enable" elements shall indicate whether the equipment or subscription or both are to be enabled. If the subscription is to be enabled, the "SSI" and "Address extension" elements shall be present; and if the equipment is to be enabled, the "TEI" element shall be present.

101 If the TEI and/or ITSI included in D-ENABLE intent match those of the MS it shall prepare to obey the command.

103 MS-MM shall inform the application of the enabling procedure about to be invoked using the TNMM-ENABLING indication primitive.

104 MS-MM shall send confirmation that the enabling command is to be carried out using the U–DISABLE STATUS PDU.

105 The MS shall comply with the request, and enable itself, sending an MLE-OPEN req primitive from MM to MLE to allow the MS to take part in calls.

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.

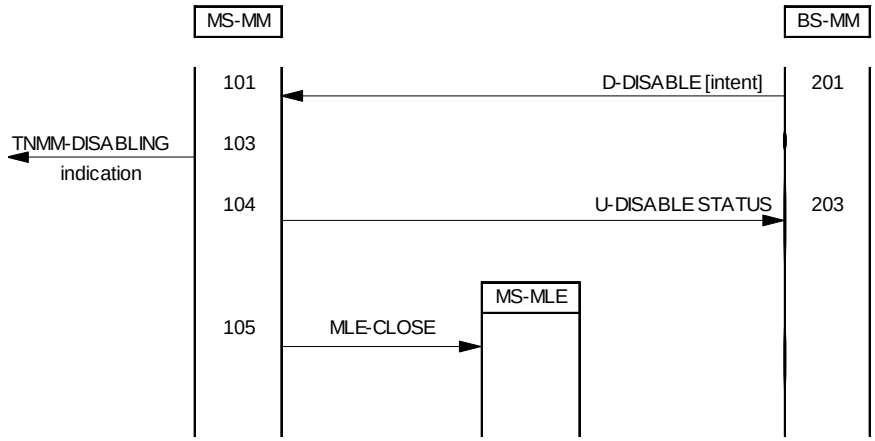


Figure 39: Disabling an MS without authentication

201 BS-MM shall send to MS-MM the D-DISABLE PDU with element Intent/Confirm set to Intent. The "Equipment disable" and "Subscription disable" elements shall indicate whether the equipment or subscription or both are to be disabled. If the subscription is to be disabled, the "SSI" and "Address extension" elements shall be present; and if the equipment is to be disabled, the "TEI" element shall be present.

102 If the TEI and/or ITSI included in D-DISABLE intent match those of the MS it shall prepare to obey the command.

103 MS-MM shall inform the application of the disabling procedure about to be invoked using the TNMM-DISABLING indication primitive.

104 MS-MM shall send confirmation that the disabling command is to be carried out using the U–DISABLE STATUS PDU.

105 The MS shall comply with the request, and disable itself, sending an MLE-CLOSE req primitive from MM to MLE to prevent the MS from taking part in calls.

5.4.6 Rejection of disable command

An MS that does not support authentication 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.

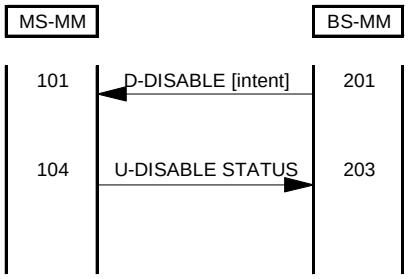


Figure 40: Rejection of permanent disabling by an MS without authentication

201 BS-MM shall send to MS-MM the D-DISABLE PDU with element Intent/Confirm set to Intent. The "Equipment disable" and "Subscription disable" elements shall indicate whether the equipment or subscription or both are to be disabled. If the subscription is to be disabled, the "SSI" and "Address extension" elements shall be present; and if the equipment is to be disabled, the "TEI" element shall be present. In this instance the disabling type element shall be set to "Permanent".

101 If the TEI and/or ITSI included in D-DISABLE intent match those of the MS it shall prepare to obey the command. In this instance the SwMI is attempting permanent disable without authentication. This shall be rejected by the MS.

104 MS-MM shall send rejection of the disabling command with reason "Authentication is required" using the U-DISABLE STATUS PDU.

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 subclauses.

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 66 defines the parameters for TNMM-DISABLING indication:

Table 66: 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 67 defines the parameters for TNMM-ENABLING indication:

Table 67: Parameters for the primitive TNMM-ENABLING indication

Parameter	Indication
Enable/disable status	M

The parameters in the primitives may take the following values:

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

5.4.8 MM PDUs structures and contents

5.4.8.1 D-DISABLE

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

Table 68: D-DISABLE contents

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

5.4.8.2 D-ENABLE

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

Table 69: D-ENABLE contents

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

5.4.8.3 U-DISABLE STATUS

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

Table 70: U-DISABLE STATUS contents

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

5.4.9 MM Information elements coding

5.4.9.1 Address extension

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

Table 71: Address Extension element contents

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

5.4.9.2 Authentication challenge

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

Table 72: Authentication challenge element contents

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

5.4.9.3 Disabling type

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

Table 73: Disabling Type element contents

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

5.4.9.4 Enable/Disable result

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

Table 74: Enable/Disable result element contents

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

5.4.9.5 Equipment disable

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

Table 75: Equipment disable element contents

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

5.4.9.6 Equipment enable

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

Table 76: Equipment enable element contents

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

5.4.9.7 Equipment status

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

Table 77: Equipment status element contents

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

5.4.9.8 Intent/confirm

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

Table 78: Intent/confirm element contents

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

5.4.9.9 PDU Type

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

Table 79: PDU Type element contents

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

NOTE: Values not shown on both uplink and downlink are assigned to other PDU types, which are given in ETS 300 392-2 [2], subclause 16.10.39, and as given in subclause 4.4.9.21 of this part of the ETS.

5.4.9.10 Proprietary

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

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

5.4.9.11 Subscription disable

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

Table 80: Subscription disable element contents

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

5.4.9.12 Subscription enable

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

Table 81: Subscription enable element contents

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

5.4.9.13 Subscription status

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

Table 82: Subscription status element contents

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

5.4.9.14 TETRA equipment identity

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

Table 83: TETRA Equipment Identity element contents

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

6 Air Interface (AI) encryption

6.1 General principles

AI encryption shall provide confidentiality on the radio link between MS and BS and be resident in layer 2 of the TETRA protocol stack.

The intention of this ETS is to describe a system in which all signalling and traffic within that system comply to 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 this ETS. The SwMI shall control the state of AI encryption. The security class is defined at a cell level and rules for clustering cells into location areas (LAs) and registration areas (RAs) are given.

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

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.

6.1.1 Security class

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

- 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 84 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 84: Security classes

Class 1:	Shall not use encryption
	May use authentication
Class 2:	Shall use SCK encryption
	Shall use ESI with SCK
	May use authentication
	May support class 1 terminals
Class 3:	Shall use authentication
	Shall use DCK encryption
	Shall use ESI with CCK
	May support class 1 terminals

An MS may support one, several, or all security classes. Each cell may support at one time either class 1 only, class 2 only, class 2 and class 1, class 3 only, class 3 and class 1. Class 2 and class 3 are not permitted to be supported at the same time in any cell.

The security class and other parameters shall be broadcast by each cell in the SYSINFO element contained in the BNCH (Broadcast Normal CHannel) (see ETS 300 392-2 [2], clause 21). The broadcast shall use the AI Encryption information element defined in table 82 and signalled by setting the "Optional Field flag" element of SYSINFO to 11_2. This element shall be sent at least once every multiframe.

The CCK-id in cells of class 3, or SCK-VN in cells of class 2, shall be alternately broadcast with the Hyper–Frame number as described in subclause 6.2.2.1.

Table 85: AI encryption information element

Information element	Type	Length	Value	Remark
Authentication	M	1	0	Authentication not required on this cell
			1	Authentication required on this cell
Security 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 (note 1)	M	1	0	MS of security class 2 not supported on this cell
			1	MS of security class 2 supported on this cell
Security class 3 (note 1, note 2)	M	1	0	MS of security class 3 not supported on this cell
			1	MS of security class 3 supported on this cell
SCKN	C	5		If security class 2 on this cell
Reserved	C	11		If security class 2 on this cell
Reserved	C	16		If security class 1 or security class 3 on this cell
NOTE 1: Security class 2 and security class 3 are mutually exclusive. NOTE 2: If TRUE then Authentication shall be TRUE.				

The security class of cells shall also be distributed using the D-NWRK-BROADCAST PDU defined in ETS 300 392–2 [2], clause 16. The element "Timeshare cell and AI encryption information" shall be encoded for security purposes as shown in table 83.

Table 86: 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 ETS 300 392-2 [2], table 255
Authentication flag	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 2)	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 class 3 then Authentication shall be TRUE.				

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 87: Class of MS element (c.f. Table 167 from ETS 300 392-2 [2])

Information element	Length	Value	Remark
Authentication (note)	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
NOTE: Renamed "Air Interface encryption service" element.			

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

6.1.1.1 Constraints on LA and Registration Area arising from cell class

In an LA all cells shall be of the same security class (see also 6.6.1).

In a registration area all LAs shall be of the same security class (see also 6.6.1).

6.2 Key Stream Generator (KSG)

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

The KSG shall form an integral part of 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 subclause 6.2.2. 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.

6.2.1 KSG numbering and selection

There shall be at least three TETRA standard algorithms. Air interface signalling shall identify which algorithm is in use (see table 85). Migration should only be possible if there is agreement between operators on the algorithm used.

Table 88 shows that the values 0000_2 to 0111_2 of KSG-id used in signalling shall be reserved for the TETRA standard algorithms (see also ETS 300 392-2 [2], subclause 16.10.29).

Table 88: 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 to 0111_2	Reserved for future expansion
		$1xxx_2$	Proprietary TETRA Algorithms

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

6.2.2 Interface parameters

6.2.2.1 Initial Value (IV)

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

The composition of the IV shall be as follows:

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

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

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

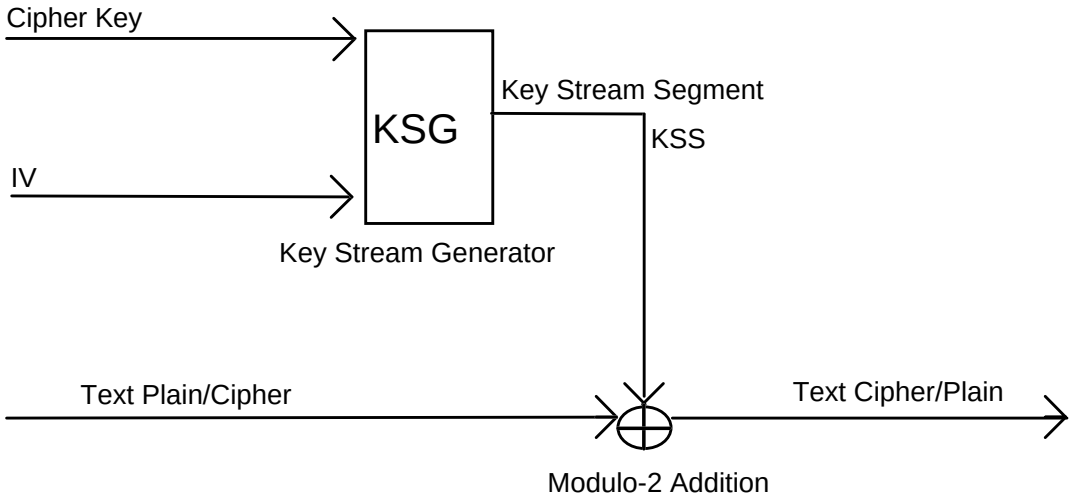
- the next 15 bits IV(13) to IV(27) shall correspond to the 15 least significant bits of an extension that numbers the hyper-frames. These can take all values from 0 to 32767. IV(13) shall correspond to the least significant bit of the hyper-frame numbering extension (ETS 300 392-2 [2], subclause 9.3.8);

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

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 alternated 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.

6.2.2.2 Cipher Key

The ciphering process shall be as shown in figure 36. A cipher key shall be used in conjunction with a KSG to generate a key stream for encryption and decryption of information at the MAC layer. It can be considered a binary vector of 80 bits, labelled CK(0) … CK(79). The cipher key used for encryption and decryption of the uplink may be different from the cipher key used for encryption and decryption of the downlink, as described in subclause 6.4.



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

Figure 41: Speech and control information encryption

6.3 Encryption mechanism

The key stream bits shall be modulo 2 added (XORed) with plain text bits in data, speech and control channels to obtain encrypted cipher text bits, with the exception of the MAC header bits and fill bits. KSS(0) shall be XORed with the first transmitted bit of the first TM-SDU, and so on. There shall be one exception to this procedure which occurs when the MAC header includes channel allocation element data. This is described in subclause 6.5.2.

If the information in a slot has fewer bits than the length of KSS produced, the last unused bits of KSS shall be discarded. For example, if there are M information bits, KSS(0) to KSS(M-1) shall be utilized, KSS(M) to KSS(n-1) shall be discarded.

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

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

Figure 42 illustrates the process where each PDU occupies one complete timeslot. Figure 43 illustrates the process with PDU association within one timeslot.

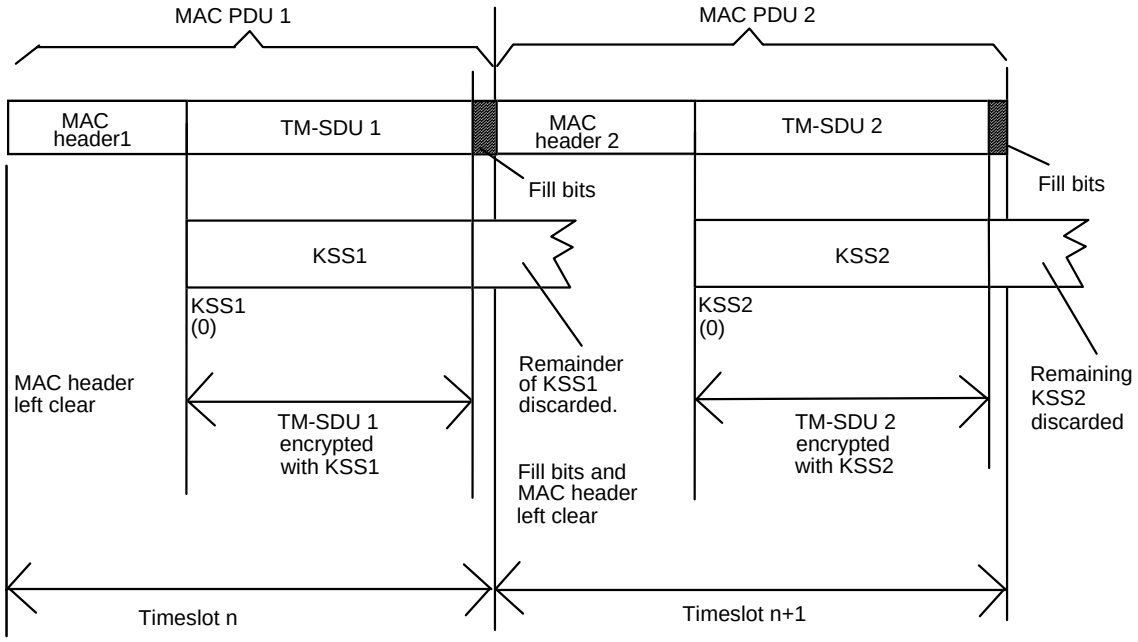
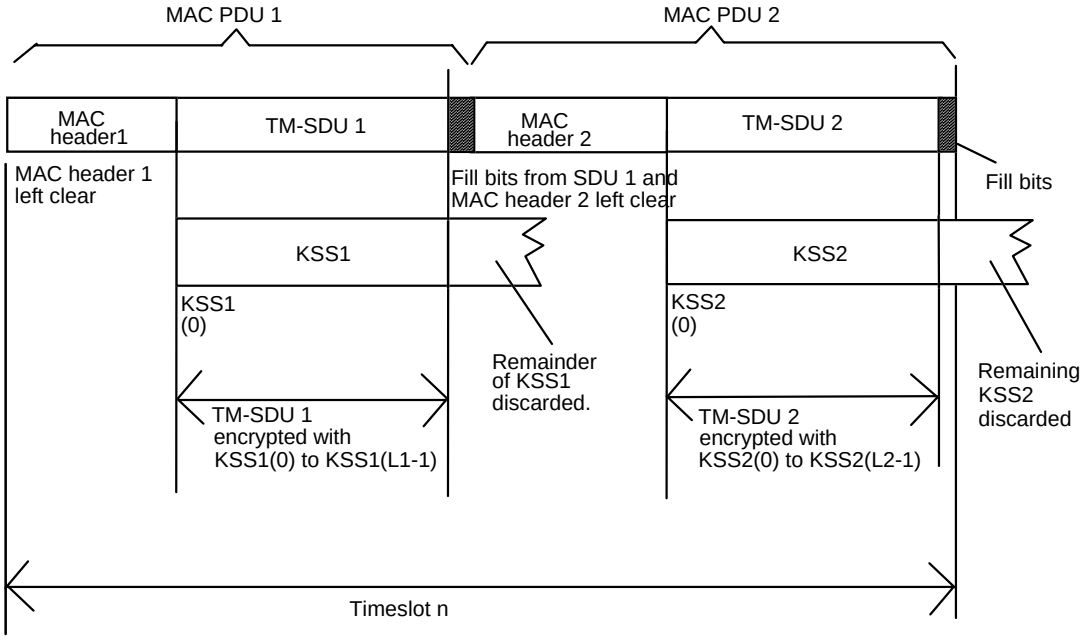


Figure 42: Allocation of KSS to encrypt MAC PDUs



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

Figure 43: Allocation of KSS to encrypt MAC PDUs with PDU Association

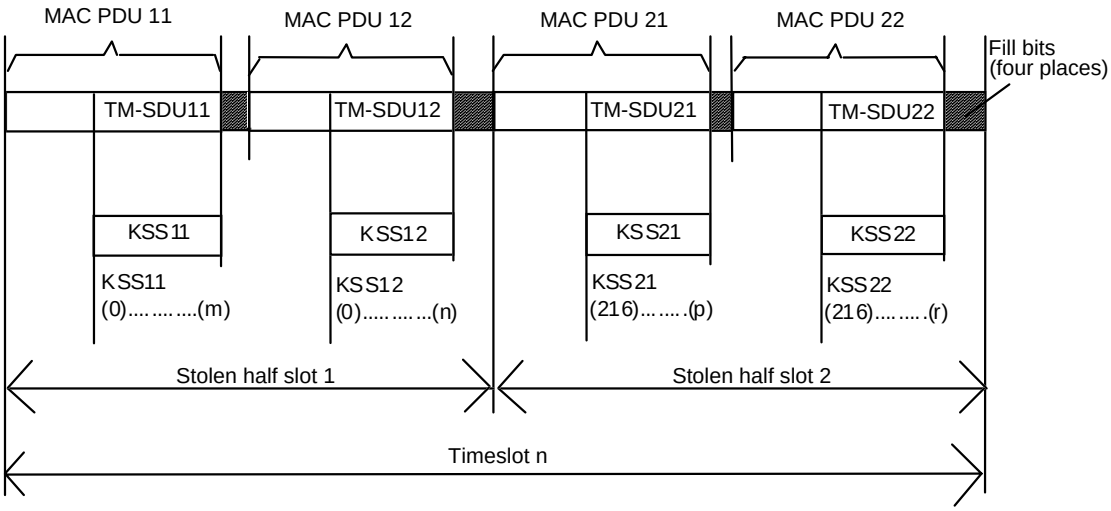
In the case of traffic channels, where one half or both halves of a timeslot are stolen for either C-Plane or U-plane signalling, the mechanism shall be as described below. This mechanism shall apply on both uplink and downlink. The keystream used to encrypt information in each half slot shall be generated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

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

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

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

This process is illustrated in figure 44.



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

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

- control channel: sending more than one SDU addressed to the same identity within one slot;
- traffic channel: sending more than one SDU addressed to the same identity within one stolen half slot.

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

6.3.1 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	IVS+1	IVS+5	IVS+9	IVS+13	IVS+17	IVS+21	IVS+25	IVS+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	IVS+1	IVS+5	IVS+9	IVS+13	IVS+17
Actual IV value	IVS+13	IVS+17	IVS+21	IVS+25	IVS+29

NOTE 1: IV_S 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 45: 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 46:

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 46: 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.

6.3.2 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.

6.4 Use of cipher keys

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

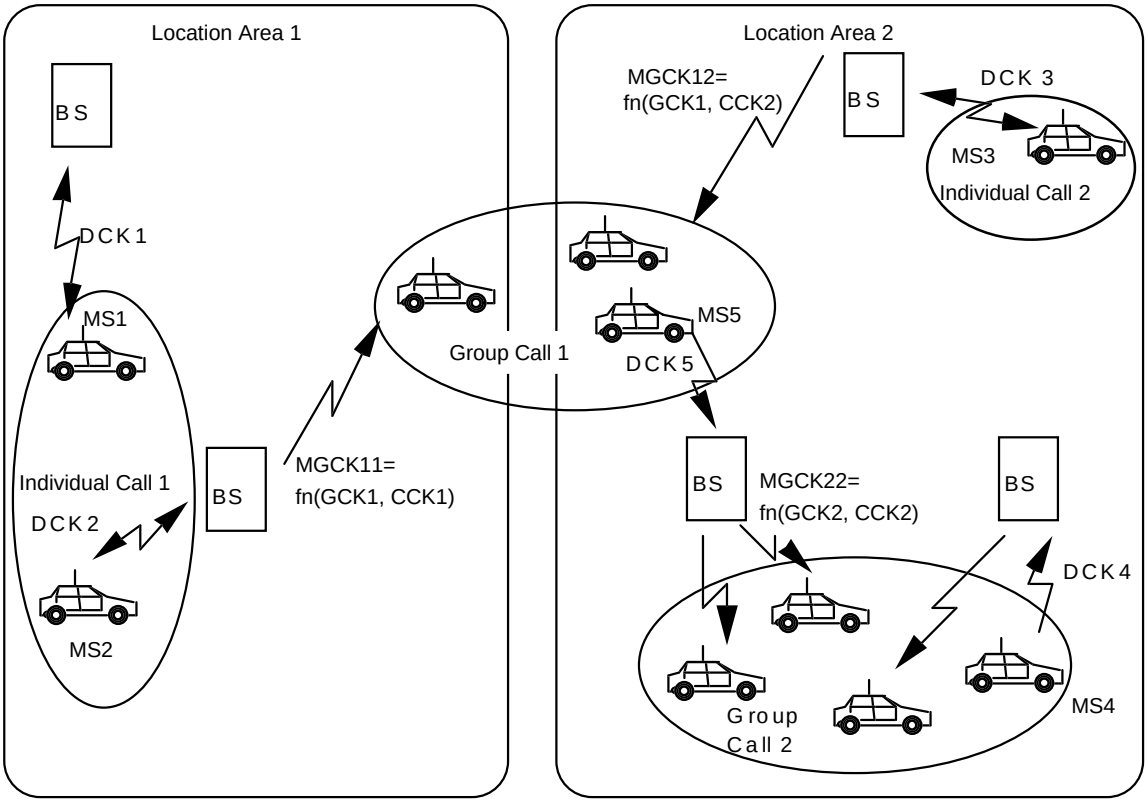
The header of MAC PDUs transmitted over the air interface shall contain indication whether the MAC PDU and some elements of the MAC Header (SSI address and channel allocation elements) are encrypted or not. In addition the header of MAC downlink PDUs shall indicate which version of CCK or SCK is used. 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 and group addressed signalling. SCK shall also be used with the identity encryption system to conceal identities in use at the air interface within a SwMI. Only one SCK may be in use within a SwMI at any one time.

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

The use of cipher keys for security class 3 is illustrated in figure 47.



BS = Base Station
MS = Mobile Station

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

Figure 47: Illustration of cipher key use

6.4.1 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 PDU for each cell security class as shown in subclauses 6.4.1.1 through 6.4.1.3.

6.4.1.1 Class 1 cells

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

Table 89: Encryption mode element in class 1 cell contents

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

6.4.1.2 Class 2 cells

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

Table 90: Encryption mode element in class 2 cell contents

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

6.4.1.3 Class 3 cells

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

Table 91: Encryption mode element in class 3 cell contents

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

In class 3 cells every cell in an LA shall use the same CCK and this shall be identified by common CCK-id. CCK change shall therefore be synchronized across all cells in an LA, and across all LAs in which the CCK is used.

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

6.4.2 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 should 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 subclause 4.2.5 for cells of class 2 and class 3.

In class 2 and class 3 cells the default value shall be "encryption on". In class 1 cells the default value shall be "encryption off".

6.5 Mobility procedures

6.5.1 General requirements

The cell selection procedures are defined in ETS 300 392-2 [2], subclause 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 shall register to the new cell.

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.

Within an LA of security class 3 all cells shall have knowledge of the DCK in use for each ITSI operating in that LA. Within a registration area all LAs shall have knowledge of the DCK for each ITSI operating in that registration area.

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.

The transfer of security information should be made entirely within the TETRA network and should not involve any unprotected transmission on the air interface, this is especially true when transferring the cipher key. If this protected transfer is impossible then a new cipher key shall be established, requiring re-authentication. If the new cell belongs to another SwMI (migration being invoked) then the ISI security procedures should be invoked prior to the migration being confirmed.

6.5.1.1 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.

ETS 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 ETS.

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 92.

Table 92: 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 support 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 supported by the MS.

6.5.1.1.1 Class 1 cells

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

6.5.1.1.2 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 ETS 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.

6.5.1.1.3 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 ETS 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.

6.5.1.2 Initial and undeclared cell re-selection

See also ETS 300 392-2 [2], subclause 18.3.4.7.2.

In this case no circuit mode call or CONP transfer is in progress for the roaming or migrating MS.

In cells of security class 3 the MS shall 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.

In cells of security class 2 the MS shall register and if required authenticate to the new cell prior to establishing encryption with the SCK valid for the cell.

6.5.1.3 Unannounced cell re-selection

See also ETS 300 392-2 [2], subclause 18.3.4.7.3.

In this case a circuit mode call or CONP transfer is in progress for the roaming or migrating MS. The MS has suffered radio link failure or is a listening party in a group call.

The higher layers of the call control protocols are broken (i.e. data transfer or speech calls are interrupted for later restoration).

In cells of security class 3 the MS shall 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 shall register and if required authenticate to the new cell prior to establishing encryption with the SCK valid for the cell.

After successful registration and restoration of security parameters the previous call in progress may be restored.

6.5.1.4 Announced cell re-selection type-3

See also ETS 300 392-2 [2], subclause 18.3.4.7.4.

In this case a circuit mode call or CONP transfer is in progress for the roaming or migrating MS. The MS is in transmission mode for a group call or is involved in a current individual call but has not scanned the neighbour cell.

The MS shall inform the serving cell using the U-PREPARE PDU with no cell id (i.e. cell to move to is not known) that cell re-selection is to take place. If advised by the SwMI to change channel the MS shall camp on the new cell and register as for unannounced cell re-selection.

6.5.1.5 Announced cell re-selection type-2

See also ETS 300 392-2 [2], subclause 18.3.4.7.5.

In this case a circuit mode call or CONP transfer is in progress for the roaming or migrating MS. The MS is in transmission mode for a group call or is involved in a current individual call and has scanned the neighbour cell to select it.

The MS shall inform the serving cell using the U-PREPARE PDU with the chosen cell-id of the new serving cell.

Once agreed by the SwMI the MS shall register to the new cell as per unannounced cell re-selection.

6.5.1.6 Announced cell re-selection type-1

See also ETS 300 392-2 [2], subclause 18.3.4.7.6.

In this case a circuit mode call or CONP transfer is in progress for the roaming or migrating MS. The MS is in transmission mode for a group call or is involved in a current individual call and has scanned the neighbour cell to select it.

The MS shall inform the serving cell using the U-PREPARE PDU with the chosen cell-id of the new serving cell and shall include the registration request for the new cell. The current serving cell shall act as an agent for the registration to the new cell. On successful registration the MS shall receive service from the new cell.

6.6 Positioning of encryption process

The encryption process itself shall be located in the upper part of the MAC layer, which itself is the lower part of layer 2. Situating the encryption process at this point, prior to channel coding at the transmitting end and after channel decoding at the receiving end, enables the MAC headers to be left unencrypted. This allows the appropriate channel coding to be used, and enables receiving parties to determine the applicability of a message received over air for them, and so enables them to apply the correct key for the decryption process. Figure 48 illustrates this interconnection.

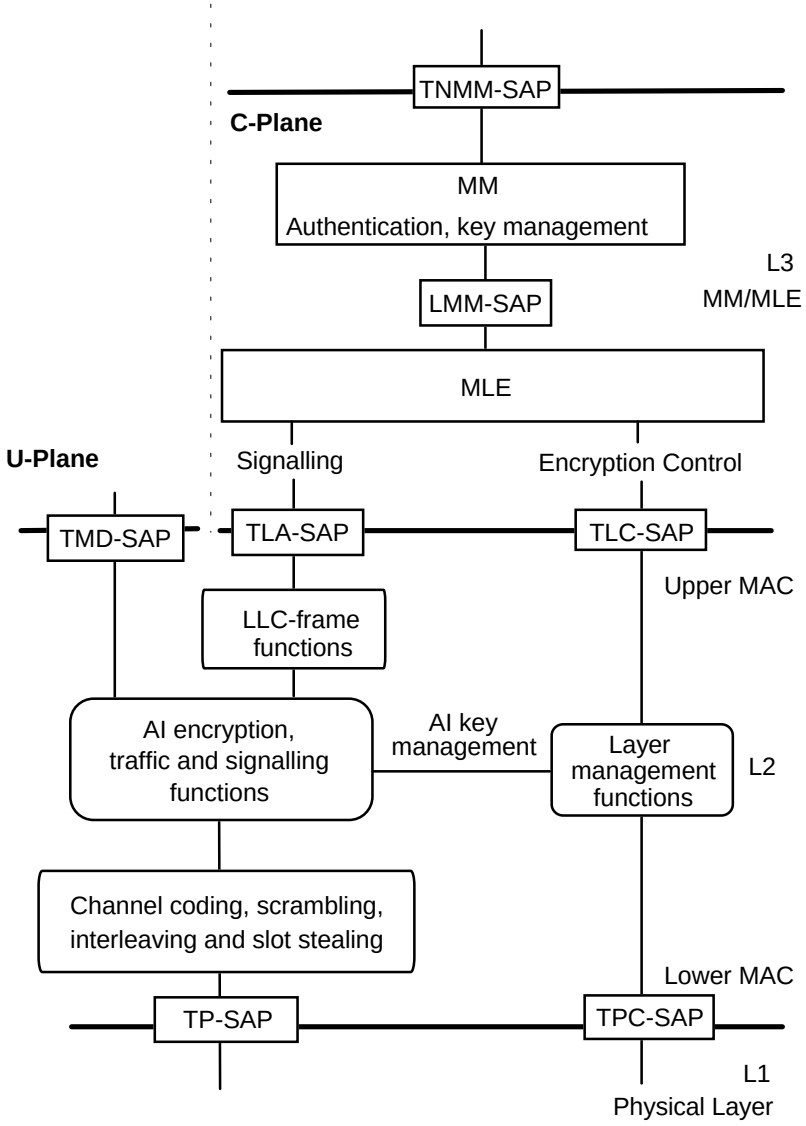


Figure 48: Relationship of security functions to layers functions in MS

6.7 Encryption control

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

6.7.1 Data to be encrypted

6.7.1.1 Downlink control channel requirements

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

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

- when broadcast the PDU D-NWRK-BROADCAST shall be sent in clear.

If D-NWRK BROADCAST is given as part of the neighbour cell data in an individually addressed message it shall be in the same encryption state as any other individually addressed message.

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

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 ETS 300 392-2 [2], subclause 21.4.3.1) all information from the channel allocation flag element shall be encrypted. The channel allocation flag shall be included in the data to be encrypted;

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

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

The KSG shall be initialized as described in subclause 6.2.2.1 using the frame and slot numbering system.

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

6.7.1.3 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 state of encryption on the U-plane shall follow the state of encryption of the C-plane signalling message which causes the switch to the U-plane (see ETS 300 392-2 [2], subclauses 14.5.1.4 and 14.5.2.4).

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

6.7.2 Service description and primitives

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

6.7.2.1 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 93: TNMM-REGISTRATION parameters (c.f. ETS 300 392-2 [2], subclause 15.3.3.7)

Parameter	Request	Indication	Confirm
Registration Status	-	M	M
Registration Reject Cause (note 1)	-	C	-
Registration Type	M	-	-
Location Area (note 2)	C	-	-
MCC (note 3)	C	-	-
MNC (note 3)	C	-	-
ISSI or ASSI or USSI (note 4)	M	-	-
Group identities	-	O	O
Group identity request	O	-	-
Group identity attach/detach mode	O	O	O
Group identity report	O	-	-
Encryption control	M	M	M
KSG number	-	O	O
Key: M = Mandatory; C = Conditional; O = Optional NOTE 1: Shall be present if Registration Status = "failure". NOTE 2: Shall be present if Registration Type = "No new ITSI - forward registration". NOTE 3: Shall be present if Registration Type = "New ITSI" or Registration Type = "No new ITSI - forward registration". NOTE 4: A previously established and valid ASSI may be used to prevent exposure of the ITSI at registration.			

6.7.2.2 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 SYS-INFO PDU.

The MAC shall indicate to MM if the short CCK-id or short CSCK version number (in the MAC RESOURCE PDU) does not correspond to the CCK idneitfier or SCK version number 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 94: 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
MGCK (note 2)	C		-
GTSI (note 3)	C		-
xSSI (note 5)	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;
DCK, xSSI pair;
CCK, CCK-id, LA-id;
MGCK, GTSI.

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 ETS 300 392-2 [2], clause 21.

The corresponding MLE-ENCRYPTION request and indication should be passed through the LLC in a transparent way by using TL-ENCRYPTION request and indication respectively at the TLC-SAP, the boundary between the MLE and LLC. Similarly, the LLC should exchange the TM-ENCRYPTION request and indication at the TMC-SAP, the boundary between the LLC and the MAC.

The MAC shall indicate to MM/MLE the CCK-id of the current CCK in use in the LA.

Encryption shall be performed in the upper MAC before FEC and interleaving.

6.7.3 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 subclauses.

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 shall 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.

6.7.4 PDUs for cipher negotiation

Ciphering elements shall be contained in the U_LOCATION_UPDATE-DEMAND, and the D_LOCATION_UPDATE-REJECT PDUs to permit negotiation of encryption parameters. These PDUs are described in ETS 300 392-2 [2], subclause 16.9.

The definition of reject cause from ETS 300 392-2 [2], subclause 16.10.42, is extended as follows:

Table 95: Reject Cause element contents

Information element	Length	Value	Remark
Reject Cause	5	10010_2	Ciphering required

The MS-MM may suggest initial encryption parameters in the U-LOCATION UPDATE DEMAND PDU. The MS-MM shall assume that these parameters are acceptable and inform the MAC to use these parameters with the MLE-Encryption primitive. If the parameters are not acceptable the BS-MM shall reject them using the D-LOCATION-UPDATE REJECT with reject cause set to one of:

- no cipher KSG;
- identified cipher KSG not available;
- requested cipher key not available;
- identified cipher key not available;
- ciphering required.

If the encryption parameters are rejected the MS-MM shall use MLE-ENCRYPTION to inform the MAC to modify the parameters in accordance with the D-LOCATION UPDATE REJECT reject cause.

If the reject cause is "ciphering required" the MS may choose a set of parameters and send a new U-LOCATION UPDATE DEMAND or it may initiate the authentication process using the U-AUTHENTICATE DEMAND exchange described in subclause 4.4.7.

7 End-to-end encryption

7.1 Introduction

End-to-end encryption algorithms and key management are outside the scope of this ETS. This subclause describes a standard mechanism for synchronization of the encryption system that may be employed when using a synchronous stream cipher. The mechanism also permits transmission of encryption related and other signalling information. The mechanism shall apply only to U-plane traffic and U-plane signalling. The method described shall use the Stealing Channel, STCH, for synchronization during transmission (see ETS 300 392-2 [2], subclause 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 49 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.

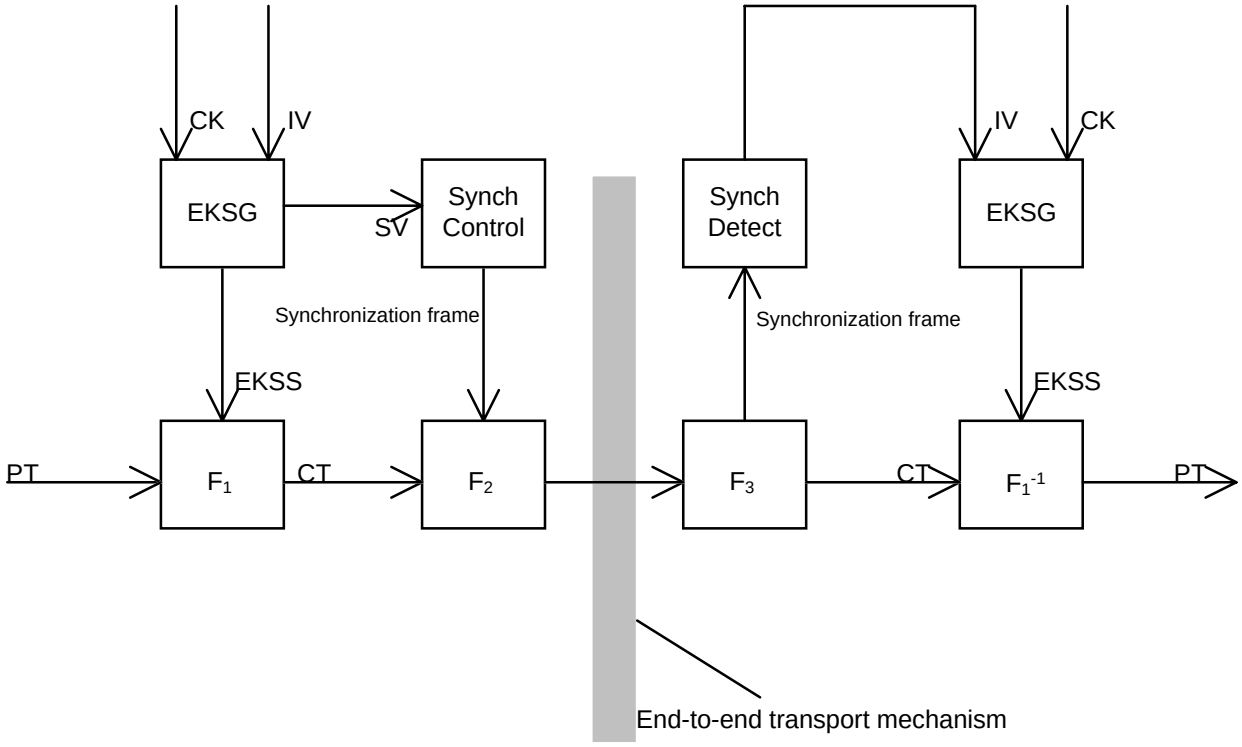


Figure 49: Functional diagram of voice encryption and decryption mechanisms

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

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

7.2.1 Protection against replay

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

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

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

7.3 Data encryption mechanism

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

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

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

7.4 Exchange of information between encryption units

Two different cases shall be identified by an appropriate MAC header (see subclause 7.4.2):

- synchronization information in clear; or
- encrypted information.

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

7.4.1 Synchronization of encryption units

Figure 49 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 ETS 300 392-2 [2], subclause 23.8.4).

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

Table 96 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 96: 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 97 shows the parameters of the TMD-REPORT primitive that shall be used for any further communication from MAC to the U-plane.

Table 97: Parameters used in the TMD-REPORT primitive

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

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

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

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

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 96 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 97 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 92 should be followed, however no more than four half-slots should be stolen per second:

Table 98: Maximum average frequency of stealing

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

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

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

If the encryption unit steals a frame it shall update the header of the stolen frame and set HSI to HIGH in 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 50 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.

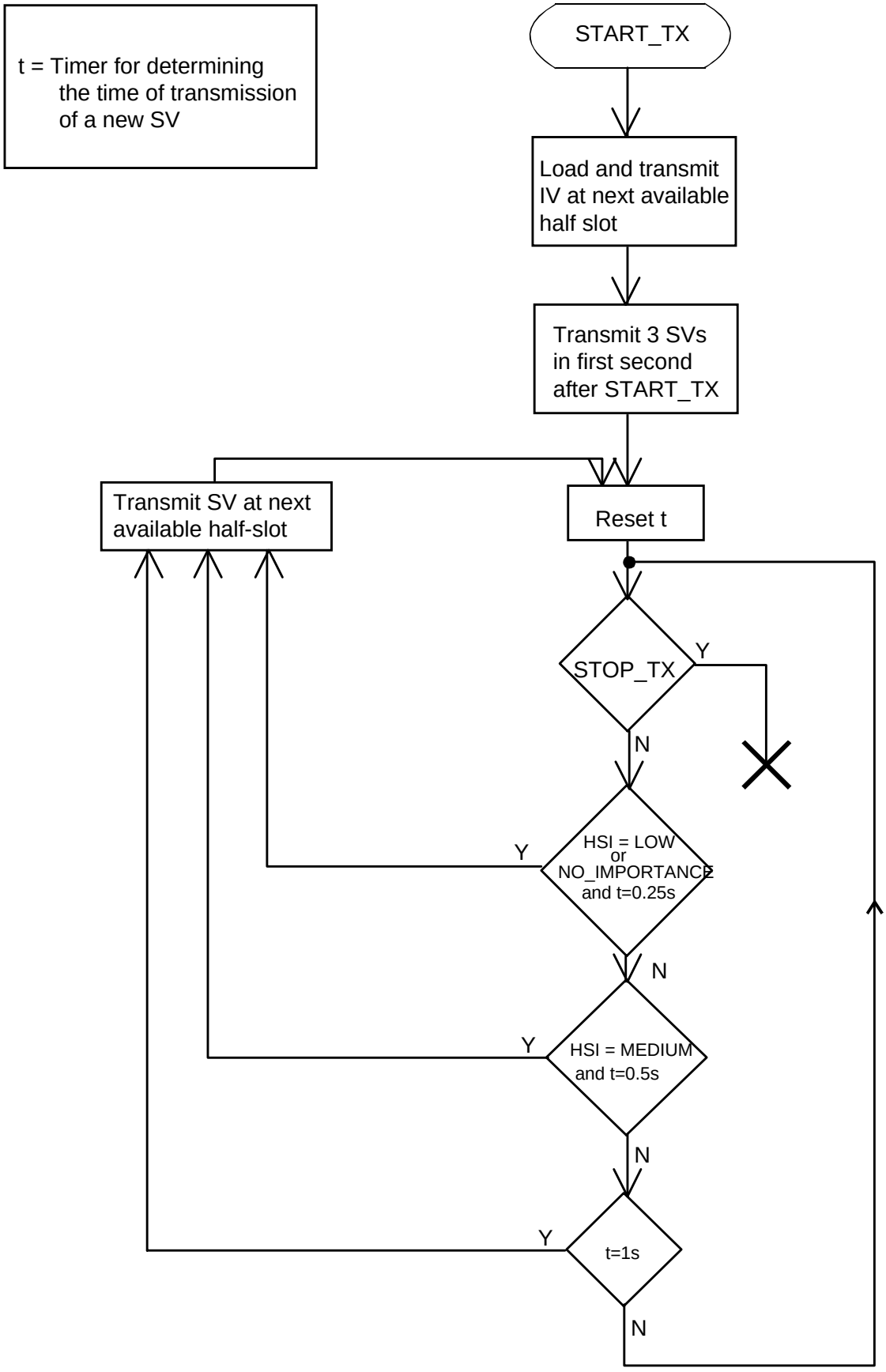


Figure 50: Flow chart of an example transmitter "sync-control" process

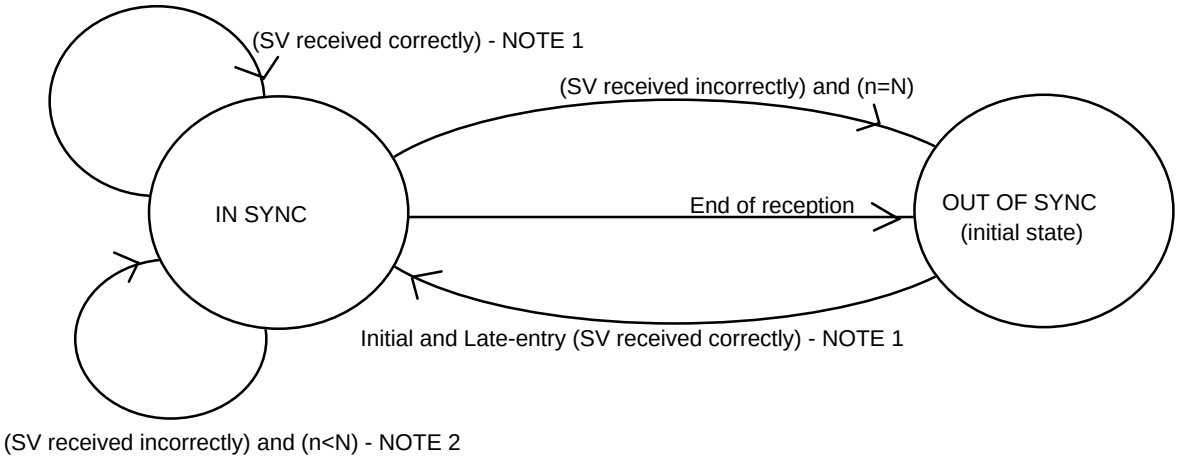
7.4.4 Reception

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 51 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 51: 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 99 defines the format of a stolen frame (half-slot):

Table 99: 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 94) indicates the terminating devices for stolen frames based upon the values of HSSE and SHSI where a codec is present:

Table 100: U-plane terminating devices for stolen frames

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

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

7.5 Location of security components in the functional architecture

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

Figure 52 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.

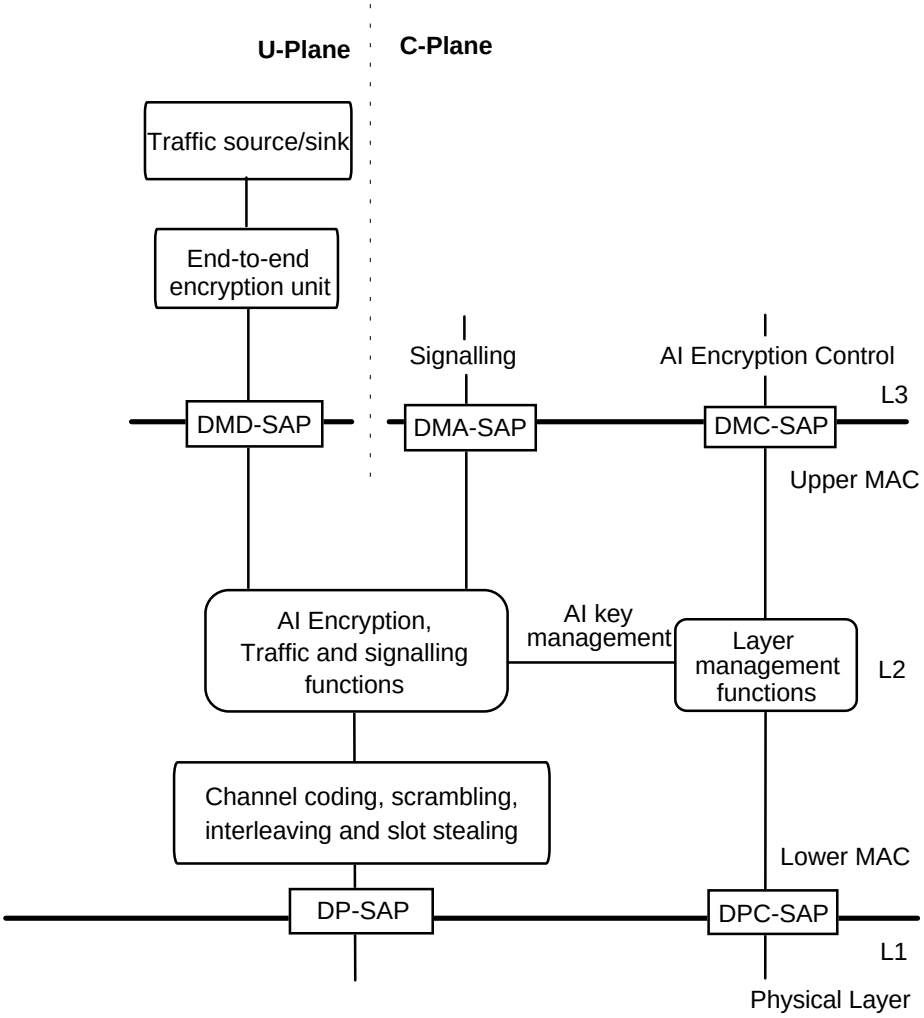


Figure 52: Position of end-to-end encryption unit in MS

The services offered on the U-Plane side, as shown in figure 52, may be further expanded as shown in figure 53.

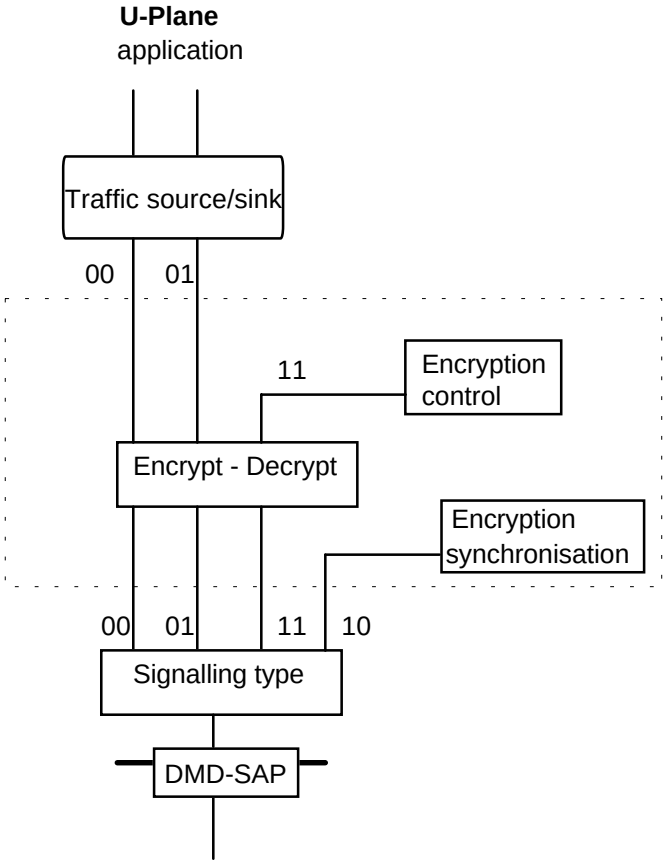


Figure 53: Functional model of the encryption unit

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.

The definition of user defined data type 4, given in ETS 300 392-2 [2], subclause 14.8.52 shall be replaced by the definition given in table 101:

Table 101: User defined data-4 element contents

Information element	Length	Value	Remark
SDS type 4 header	8	00000000_2	Reserved for future expansion
		00000001_2	End to end encryption key management
		others	Available for other applications
Data	0-2039	varies	All values available for the user application (see note)
NOTE: The length of the data element is as defined in ETS 300 392-2 [2], subclause 14.8.52, with the first byte reserved as a header.			

Annex A (informative): 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".

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

History

Document history			
December 1996	First Edition		
May 1999	Public Enquiry	PE 9940:	1999-05-05 to 1999-10-01