ETSI TS 100 392-7 V4.1.1 (2022-10)

TECHNICAL SPECIFICATION

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

Reference

RTS/TCCE-06208

Keywords

security, TETRA, V+D

ETSI

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

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee TETRA and Critical Communications Evolution (TCCE).

The present document is part 7 of a multi-part deliverable covering the Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D), Release 2, as identified below:

Part 1: "General network design";

Part 2: "Air Interface (AI)";

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

Part 4: "Gateways basic operation";

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

Part 7: "Security";

Part 9: "General requirements for supplementary services";

Part 10: "Supplementary services stage 1";

Part 11: "Supplementary services stage 2";

Part 12: "Supplementary services stage 3";

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

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

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

Part 16: "Network Performance Metrics";

Part 17: "TETRA V+D and DMO specifications";

Part 18: "Air interface optimized applications";

Part 19: "Interworking between TETRA and Broadband systems".

NOTE 1: Part 3, sub-parts 6 and 7 (Speech format implementation), part 4, sub-part 3 (Data networks gateway), part 10, sub-part 15 (Transfer of control), part 13 (SDL) and part 14 (PICS) of this multi-part deliverable are in status "historical" and are not maintained.

NOTE 2: Some parts are also published as Technical Specifications such as ETSI TS 100 392-7 (the present document) and those may be the latest version of the document.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

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

The present 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 for the Inter-System Interface (ISI).

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

- authentication of an MS by the TETRA infrastructure;
- authentication of the TETRA infrastructure by an MS;
- mutual authentication of MS and TETRA infrastructure.

The key management mechanisms specified in clause 4 enable the provision of key material for the air interface encryption mechanisms specified in clause 6.

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. Encryption mechanisms and control protocol are specified for two different air interface encryption algorithm sets.

Annex A specifies the Protocol Data Units and Information Elements required to fulfil the protocols specified in clauses 4, 5 and 6. Annex B specifies boundary conditions, dimensioning and summaries of the cryptographic algorithms, parameters and processes specified in the present document. Annex C specifies timer values used within the protocols. Annex D provides considerations for a transition process between the usage of encryption algorithms from different air interface encryption algorithm sets.

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

The detail description of the Authentication Centre is outside the scope of the present document.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE 1: Some referenced ENs are also published as Technical Specifications. In all cases, the latest version of such a document, either EN or TS, should be taken as the referenced document.

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

NOTE 2: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

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

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

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

[4] ETSI EN 300 812-3: "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 3: Integrated Circuit (IC); Physical, logical and TSIM application characteristics".

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

[6] ETSI EN 302 109: "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption".

[7] ETSI EN 300 392-12-22: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 12: Supplementary services stage 3; Sub-part 22: Dynamic Group Number Assignment (DGNA)".

[8] ETSI EN 300 392-3-5: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 5: Additional Network Feature for Mobility Management (ANF-ISIMM)".

[9] ETSI EN 300 396-1: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 1: General network design".

[10] ETSI ES 200 812-2: "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (TSIM-ME) interface; Part 2: Universal Integrated Circuit Card (UICC); Characteristics of the TSIM application".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI ETS 300 392-2 (1996): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

[i.2] ETSI ETS 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

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

[i.4] ETSI EN 300 392-7 (V2.2.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[i.5] ETSI EN 300 392-7 (V2.1.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[i.6] ETSI TS 100 392-18-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D) and Direct Mode Operation (DMO); Part 18: Air interface optimized applications; Sub-part 1: Location Information Protocol (LIP)".

[i.7] ETSI EN 300 392-10-21: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 21: Ambience Listening (AL)".

[i.8] ETSI TS 100 392-7 (V2.4.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[i.9] ETSI EN 300 392-7 (V3.1.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[i.10] ETSI TS 101 053-1: "Rules for the management of the TETRA standard encryption algorithms; Part 1: TEA1".

[i.11] ETSI TS 101 053-2: "Rules for the management of the TETRA standard encryption algorithms; Part 2: TEA2".

[i.12] ETSI TS 101 053-3: "Rules for the management of the TETRA standard encryption algorithms; Part 3: TEA3".

[i.13] ETSI TS 101 053-4: "Rules for the management of the TETRA standard encryption algorithms; Part 4: TEA4".

[i.14] ETSI TS 101 052: "Rules for the management of the TETRA standard authentication and key management algorithm set TAA1".

[i.15] ETSI TS 101 053-5: "TCCE Security (TCCE); Rules for the management of the TETRA standard encryption algorithms; Part 5: TEA5".

[i.16] ETSI TS 101 053-6: "TCCE Security (TCCE); Rules for the management of the TETRA standard encryption algorithms; Part 6: TEA6".

[i.17] ETSI TS 101 053-7: "TCCE Security (TCCE); Rules for the management of the TETRA standard encryption algorithms; Part 7: TEA7".

[i.18] ETSI TS 101 052-2: "TCCE Security (TCCE); Rules for the management of the TETRA standard authentication and key management algorithm set TAA2".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

All SwMI MNI: network address used to signal to an MS that the current transaction is applied to parameters stored by the MS for use in all SwMIs

NOTE: The All SwMI MNI is encoded as all binary ones ($11…11_2$).

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

authentication Key (K or K2): primary secret, the knowledge of which has to be demonstrated for authentication

authentication session: period between consecutive successful authentication operations

CCK Identifier (CCK-id): identification of the key within an LA, where the key may be a CCK or CCKX

Cipher Key (CK): value that is used to determine the transformation of plain text to cipher text in a cryptographic algorithm

cipher text: data produced through the use of encipherment

NOTE: The semantic content of the resulting data is not available (see ISO 7498-2 [3]).

class: See security class.

Common Cipher Key (CCK): cipher key that is generated by the infrastructure to protect group addressed signalling and traffic where an air interface encryption algorithm from TEA set A is in use

NOTE: CCK can also be used to protect SSI identities (ESI) in layer 2.

Conventional Access (CA): method of operation in which a phase modulation carrier is used as the main carrier

NOTE: See ETSI EN 300 392-2 [2].

Crypto Management Group (CMG): group of MSs with common key material

crypto period: length of time during which a specific key is in use

DCK forwarding: action of the SwMI whereby a DCK or DCKX that has already been established with an MS is sent to a cell defined by the MS, at the request of the MS

NOTE: The purpose is to allow the MS to subsequently perform reselection to that cell and use encrypted location updating.

DCK retrieval: action of the SwMI whereby a DCK or DCKX that has already been established with an MS is sent to a cell to which the MS location updates, without any previous knowledge that the MS is going to perform location updating to that cell

NOTE: The purpose is to allow the MS to perform encrypted location updating on that cell without any prior forwarding transaction. The SwMI may be able to perform DCK retrieval of a DCK or DCKX during initial registration, during cell reselection, or both.

decipherment: reversal of a corresponding reversible encipherment

NOTE: See ISO 7498-2 [3].

Derived Cipher Key (DCK): key generated during authentication for use in protection of individually addressed signalling and traffic where an air interface encryption algorithm from TEA set A is in use

Direct Access (DA): method of operation in which a QAM carrier is used as the main carrier

NOTE: See ETSI EN 300 392-2 [2].

encipherment: cryptographic transformation of data to produce cipher text

NOTE: See ISO 7498-2 [3].

Encryption Cipher Key (ECK): cipher key that is used as input to the encryption algorithm where an air interface encryption algorithm from TEA set A is in use

NOTE: This key is derived from one of SCK, DCK, MGCK or CCK and modified using an algorithm by the broadcast data of the serving cell where an air interface encryption algorithm from TEA set A is in use. There is no equivalent where an air interface encryption algorithm from TEA set B is in use.

encryption mode: choice between static (security class 2 using SCK or SCKX) and dynamic (security class 3 using DCK/CCK or DCKX/CCKX) 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

NOTE: Defined in ETSI EN 302 109 [6].

Extended Cipher Key (CKX): value that is used to determine the transformation of plain text to cipher text in a cryptographic algorithm where an air interface encryption algorithm from TEA set B is in use

Extended Common Cipher Key (CCKX): cipher key that is generated by the infrastructure to protect group addressed signalling and traffic where an air interface encryption algorithm from TEA set B is in use

NOTE: CCKX can also be used to protect SSI identities (ESI or MAE) in layer 2.

Extended Derived Cipher Key (DCKX): key generated during authentication for use in protection of individually addressed signalling and traffic where an air interface encryption algorithm from TEA set B is in use

Extended Group Cipher Key (GCKX): cipher key known by the infrastructure and MS to protect group addressed signalling and traffic where an air interface encryption algorithm from TEA set B is in use

Extended Group Session Key for OTAR (EGSKO or GSKOX): cipher key used for the distribution of keys to groups of MSs

Extended Modified Group Cipher Key (MGCKX): cipher key known by the infrastructure and MS to protect group addressed signalling and traffic that is composed algorithmically from CCKX and GCKX where an air interface encryption algorithm from TEA set B is in use

Extended Session Key for OTAR (KSOX): derived from a MS's authentication key and a random seed for OTAR where an air interface encryption algorithm from TEA set B is in use

NOTE: KSOX is used to protect the transfer of the Extended Static Cipher Key, Extended Group Cipher Key and Extended Group Session Key for OTAR.

Extended Session Key for OTAR for a visited network (KSOXv): key derived from an MS's authentication key and a random seed for OTAR that is used for OTAR in a visited network where an air interface encryption algorithm from TEA set B is in use

NOTE: KSOXv may be used to protect the transfer of the Extended Static Cipher Key, Extended Group Cipher Key and Extended Group Session Key for OTAR in a visited network. It may be sent from the home network to a visited network.

Extended Static Cipher Key (SCKX): predetermined cipher key that may be used to provide confidentiality in class 2 systems with a corresponding algorithm and may also be used in DMO or for fallback where an air interface encryption algorithm from TEA set B is in use

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

NOTE: The fallback key is an SCK where an air interface algorithm from TEA set A is in use, and an SCKX where an air interface algorithm from TEA set B is in use.

Group Cipher Key (GCK): cipher key known by the infrastructure and MS to protect group addressed signalling and traffic where an air interface encryption algorithm from TEA set A is in use

NOTE: Not used directly at the air interface but modified by CCK to give a Modified Group Cipher Key (MGCK).

Group Session Key for OTAR (GSKO): cipher key used to derive EGSKO for the distribution of keys to groups of MSs where an air interface encryption algorithm from TEA set A is in use

home network or **home SwMI:** network or SwMI where an MS has its subscription

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

Key Association Group (KAG): set of keys associated with one or more GSSIs at different periods of time

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

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

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

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

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

Manipulation Flag (MF): flag used to indicate that a sealed cipher key (CCK, SCK, GCK, GSKO, CCKX, SCKX, GCKX or GSKOX) has been incorrectly recovered

Modified Group Cipher Key (MGCK): cipher key known by the infrastructure and MS to protect group addressed signalling and traffic that is composed algorithmically from CCK and GCK where an air interface encryption algorithm from TEA set A is in use

Open MNI: network address used in conjunction with an open group address, which allows communication with any users who have selected the same DMO frequency

NOTE 1: The open MNI is encoded as all binary ones ($11\ldots11_2$).

NOTE 2: The open MNI is described in ETSI EN 300 396-1 [9].

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

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

plain text: un-encrypted source data

NOTE: 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 an MS or in an MS to authenticate the infrastructure, respectively

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

Random Seed for OTAR (RSO): random value used to derive a session key for OTAR from an MS's authentication key

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

Response (RES1, RES2): value calculated in the MS from RAND1 and the KS to prove the authenticity of an MS to the infrastructure or by the infrastructure from RAND2 and the KS' to prove its authenticity to an MS, respectively

SCK-set: collective term for a group of up to 32 SCK and/or SCKX which may be held by an MS

NOTE: An SCK set may contain SCKs or SCKXs or both SCKs and SCKXs.

Sealed Cipher Key (SxCK or SxCKX): cipher key that has been cryptographically protected

NOTE: In the above definition x refers to Common, Group, Static.

security class 1, 2 or 3: classification of terminal and SwMI encryption and authentication support

NOTE: See Table 4.1.

Session Authentication Key (KS, KS'): key generated from the authentication key and a random seed for authentication that is used for authentication in the home network

Session Authentication Key for a visited network (KSv, KSv'): key generated from the authentication key and a random seed for authentication that is used for authentication in a visited network

NOTE: It is sent from the home network to a visited network.

Session Key for OTAR (KSO): derived from a MS's authentication key and a random seed for OTAR where an air interface encryption algorithm from TEA set A is in use

NOTE: KSO is used to protect the transfer of the Static Cipher Key, Group Cipher Key and Group Session Key for OTAR.

Session Key for OTAR for a visited network (KSOv): key derived from an MS's authentication key and a random seed for OTAR that is used for OTAR in a visited network where an air interface encryption algorithm from TEA set A is in use

NOTE: KSOv may be used to protect the transfer of the Static Cipher Key, Group Cipher Key and Group Session Key for OTAR in a visited network. It may be sent from the home network to a visited network.

Session key modifier key (GCK0 or GCKX0): key used by an algorithm (TA101, TA102 or TA103) to modify the session keys KS, KS', KSO or KSOX when transferring keys over the ISI, designated as GCK0 or GCKX0 to allow use of GCK or GCKX OTAR mechanisms

Static Cipher Key (SCK): predetermined cipher key that may be used to provide confidentiality in class 2 systems with a corresponding algorithm and may also be used in DMO or for fallback where an air interface encryption algorithm from TEA set A is in use

TEA set A: set of air interface encryption algorithms comprising TEA1, TEA2, TEA3 and TEA4

TEA set B: set of air interface encryption algorithms comprising TEA5, TEA6 and TEA7

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): key 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)

visited SwMI: SwMI which is not the home SwMI of the MS receiving service on that SwMI

3.2 Symbols

Void.

3.3 Abbreviations

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

AACH	Access Assignment CHannel
AC	Authentication Code
ACK	ACKnowledgement
AESI	Alias Encrypted Short Identity
AI	Air Interface
AIE	Air Interface Encryption
ASCII	American Standard Code for Information Interchange
ASSI	Alias Short Subscriber Identity
AuC	Authentication Centre
BNCH	Broadcast Network CHannel
BS	Base Station
BSCH	Broadcast Synchronization CHannel
CA	Conventional Access
CC	Colour Code
CCK	Common Cipher Key
CCK-id	CCK-identifier
CCKX	Extended Common Cipher Key
CK	Cipher Key
CKX	Extended Cipher Key
CMCE	Circuit Mode Control Entity
CMG	Crypto Management Group
CN	Carrier Number
C-PLANE	Control-PLANE
CR	Change Request
DA	Direct Access

DCK	Derived Cipher Key

NOTE: DCK1 and DCK2 are components of the Derived Cipher Key.

DCKX	Extended Derived Cipher Key
DGNA	Dynamic Group Number Assignment
DM	Direct Mode
DMAC	Downlink MAC
DMO	Direct Mode Operation
DM-SCK	SCK used in Direct Mode operation

NOTE: May also apply to an SCKX used in Direct Mode operation.

D-NWRK	Downlink-NetWoRK
DQPSK	Differential Quadrature Phase Shift Keying
ECK	Encryption Cipher Key
EGSKO	Extended Group Session Key for OTAR
ESI	Encrypted Short Identity
FACCH	Fast Associated Control CHannel
FEC	Forward Error Correction
GCK	Group Cipher Key
GCK0	Group Cipher Key number 0
GCKN	Group Cipher Key Number
GCK-VN	GCK-Version Number
GCKX	Extended Group Cipher Key
GCKX0	Extended Group Cipher Key number 0
GESI	Group Encrypted Short Identity
GSKO	Group Session Key for OTAR
GSKO-VN	GSKO-Version Number
GSKOX	Extended Group Session Key for OTAR
GSSI	Group Short Subscriber Identity
GTSI	Group TETRA Subscriber Identity
HLAV	High Location Area Value
hSwMI	home SwMI
HW	HardWare
IE	Information Element
IESI	Individual Encrypted Short Identity
ISI	Inter-System Interface
ISSI	Individual Short Subscriber Identity
ITSI	Individual TETRA Subscriber Identity
IV	Initialization Value
K	authentication Key
K2	authentication Key
KAG	Key Association Group
KS, KS'	Session authentication Key
KSG	Key Stream Generator
KSO	Session Key for OTAR
KSOv	Session Key for OTAR for a visited network
KSOX	Extended Session Key for OTAR
KSOXv	Extended Session Key for OTAR for a visited network
KSS	Key Stream Segment
KSv, KSv'	Session Authentication Key for a visited network
LA	Location Area
LA-id	Location Area-identifier
LIP	Location Information Protocol
LLAV	Low Location Area Value
LLC	Logical Link Control
LMM	Link entity Mobility Management
MAC	Medium Access Control
MAE	MAC Address Encryption
MCC	Mobile Country Code
MCCH	Main Control CHannel
MF	Manipulation Flag

MGCK	Modified Group Cipher Key
MGCKX	Extended Modified Group Cipher Key
MLE	Mobile Link Entity
MM	Mobility Management
MMI	Man-Machine Interface
MNC	Mobile Network Code
MNI	Mobile Network Identity
MNIv	Mobile Network Identity of a visited network
MS	Mobile Station
MSC	Message Sequence Chart
N/A	Not Applicable
OTAR	Over The Air Re-keying
PDU	Protocol Data Unit
PEI	Peripheral Equipment Interface
PIN	Personal Identification Number
QAM	Quadrature Amplitude Modulation
Q/D	QAM/Downlink
RA	Registered Area
RAND	RANDom challenge
RAND1	RANDom challenge 1
RAND2	RANDom challenge 2
RES	RESponse
RES1	RESponse 1
RES2	RESponse 2
RS	Random Seed
RSO	Random Seed for OTAR
RX	Receiver
SACCH	Slow Associated Control CHannel
SAP	Service Access Point
SCCH	Secondary Control CHannel
SCCK	Sealed Common Cipher Key
SCCKX	Sealed Extended Common Cipher Key
SCH	Signalling CHannel
SCH/F	Full Slot Signalling Channel
SCH/HD	Half-slot Downlink Signalling Channel
SCH/HU	Half-slot Uplink Signalling Channel
SCH-Q	Signalling CHannel, QAM
SCK	Static Cipher Key
SCKN	Static Cipher Key Number
SCK-VN	SCK-Version Number
SCKX	Extended Static Cipher Key
SDL	Specification and Description Language
SDMO	Secure Direct Mode Operation
SDU	Service Data Unit
SGCK	Sealed Group Cipher Key
SGCKX	Sealed Extended Group Cipher Key
SGSKO	Sealed Group Session Key for OTAR
SGSKOX	Sealed Extended Group Session Key for OTAR
SICH-Q	Slot Information CHannel, QAM
SIM	Subscriber Identity Module
SMI	Short Management Identity
SNDCP	SubNetwork Dependent Convergence Protocol
SSCK	Sealed Static Cipher Key
SSCKX	Sealed Extended Static Cipher Key
SS-DGNA	Supplementary Service Dynamic Group Number Assignment
SSI	Short Subscriber Identity
STCH	STealing CHannel
SW	SoftWare
SwMI	Switching and Management Infrastructure
TA	TETRA Algorithm

NOTE: Used with specific numeric algorithm identity e.g. TA11.

TAA	TETRA Authentication Algorithm

NOTE: Used with specific numeric algorithm set identity e.g. TAA1.

TCH	Traffic CHannel
TCH/2.4	Traffic CHannel for 2,4 kbs circuit mode data
TCH/4.8	Traffic CHannel for 4,8 kbs circuit mode data
TCH/7.2	Traffic CHannel for 7,2 kbs circuit mode data
TEA	TETRA Encryption Algorithm

NOTE: Used with specific numeric algorithm identity e.g. TEA1.

TEI	TETRA Equipment Identity
TL	TETRA LLC
TLC-SAP	TETRA LLC Service Access Point C
TMB-SAP	TETRA MAC Service Access Point B
TMC-SAP	TETRA MAC Service Access Point C
TMO	Trunked Mode Operation
TM-SCK	SCK or SCKX used in Trunked Mode operation

NOTE: TM-SCK may apply to an SCK or an SCKX used in Trunked Mode operation.

TM-SDU	TETRA MAC-Signalling Data Unit
TNMM	TETRA Network Mobility Management (refers to the SAP)
TSIM	TETRA Subscriber Identity Module
TX	Transmitter
UAK	User Authentication Key
UICC	Universal Integrated Circuit Card
UL	UpLink
U-PLANE	User-PLANE
USSI	Unexchanged Short Subscriber Identity
V-ASSI	Visitor Alias Short Subscriber Identity
(V)ASSI	ASSI or V-ASSI
V-GSSI	Visitor Group Short Subscriber Identity
VN	Version Number
vSwMI	visited SwMI
XRES	eXpected RESponse
XRES1	eXpected RESponse 1
XRES2	eXpected RESponse 2

4 Air Interface authentication and key management mechanisms

4.a General

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

4.0 Security classes

TETRA security is defined in terms of class. Each class has associated features that are mandatory or optional and are summarized in Table 4.1.

Table 4.1: Summary of Security features in TETRA by class

Class	Authentication	OTAR	Encryption	Enable-Disable
	Clause 4	**Clause 4**	**Clause 6**	**Clause 5**
1	O	O (see note 3)	-	O
2	O	O	M	O
3	M (see note 1)	M (see note 2)	M	O†
KEY: M = Mandatory O = Optional - = Does not apply † = Recommended				
NOTE 1: Authentication is required for generation of DCK or DCKX. NOTE 2: OTAR for CCK or CCKX is mandatory, other key management OTAR mechanisms are optional. NOTE 3: Required if key material is either distributed in preparation for security class transition, or during cell reselection to a cell of a different security class.				

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

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

- class 1 only;
- class 2 only;
- class 2 and class 1;
- class 3 only; or
- class 3 and class 1.

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

4.1 Air interface authentication mechanisms

4.1.1 Overview

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

The authenticating parties shall be the authentication centre of the Switching and Management Infrastructure (SwMI) and the Mobile Station (MS). The MS is considered, for the purposes of authentication, to represent the user as defined by the Individual TETRA Subscriber Identity (ITSI). The design of the SwMI is not specified, but some other entity such as a Base Station (BS) may carry out the authentication protocol on behalf of the Authentication Centre. This entity is assumed to be trusted by the SwMI and the authentication exchange proves knowledge given to this entity by the authentication centre. This knowledge shall be the session authentication key (KS). This ensures that the authentication key of the MS is never visible outside the Authentication Centre.

An MS that supports authentication shall be provisioned with a single authentication key, K or K2. The SwMI shall be provisioned with the same single key as the MS, which therefore may be either K or K2. The use of K or K2 in authentication and key management transactions is described in the following clauses. 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.

NOTE: The SwMI controls access to the network and not the authentication process (i.e. successful authentication is not sufficient to guarantee access to the SwMI).

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

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

4.1.1a Authentication and key management algorithms

TETRA supports standard algorithms for authentication and key management, which are specified in the TAA1 and TAA2 algorithm sets. Any use of a proprietary authentication and key management algorithm set is outside the scope of the present document.

NOTE: There is no mechanism by which a BS and MS can indicate that a proprietary authentication or key management algorithm set is in use.

The TETRA standard authentication and key management algorithm sets TAA1 and TAA2 are only available on a restricted basis. The rules for management of the TAA1 algorithm set are specified in ETSI TS 101 052 [i.14], and the rules for management of the TAA2 algorithm set are specified in ETSI TS 101 052-2 [i.18]. The Confidentiality and Restricted Usage Undertaking for these algorithm sets can be found on the ETSI Web Portal (http://www.etsi.org/algorithms).

Annex B lists the parameters for each of the algorithms in the TAA1 and TAA2 sets, and provides their allocation to the TAA1 and TAA2 sets.

Algorithms in the TAA1 and TAA2 sets provide key management for the air interface encryption algorithms. There are two sets of air interface encryption algorithms, TEA set A and TEA set B, where TEA set A contains the TEA1, TEA2, TEA3 and TEA4 algorithms, and TEA set B contains the TEA5, TEA6 and TEA7 algorithms. These are described in clause 6. An MS that supports authentication and key management algorithms in the TAA2 set of algorithms, and supports air interface encryption algorithms from TEA set B shall be provisioned with authentication key K2.

4.1.2 Authentication of an MS

In this clause, a mechanism is described that shall be used to achieve the authentication of an MS by the SwMI. This shall be done using a challenge response protocol, with session authentication key(s) derived from an authentication key (K or K2) that shall be shared by the MS and the infrastructure. The session authentication key(s) shall be provided by an authentication centre of the home system.

The computation of the session authentication key(s) shall be carried out by an algorithm, TA11 or TA13. TA11 is used where the MS has been provisioned with key K, and TA13 is used where the MS has been provisioned with key K2. The computation of the response shall be done by another algorithm, TA12 or TA15. TA12 also produces a derived cipher key.

The SwMI shall generate a random number as a challenge RAND1.

If the MS is provisioned with an authentication key K, a single session key KS shall be used with algorithm TA12. The MS shall compute a response, RES1, and the SwMI shall compute an expected response, XRES1. MS and SwMI may compute DCK1 using algorithm TA12.

If the MS is provisioned with an authentication key K2, and negotiates security class 1 operation, the MS may use a single session key KS with algorithm TA12 to compute RES1, and the SwMI shall likewise compute an expected response XRES1. If the SwMI is aware that the MS is provisioned with authentication key K2 and both SwMI and MS are configured to use TA15 for authentication for security class 1 operation, the MS shall use two session key KS and KS' with algorithm TA15 to compute RES1, and the SwMI shall likewise compute an expected response XRES1.

NOTE 1: RAND1 values should be non-repeating, and it should be difficult to predict the value of RAND1 chosen by the SwMI, as the authentication response RES1 and the derived cipher key DCK1 or DCKX both depend on RAND1.

NOTE 2: RAND1 should not be set to zero (i.e. all bits of RAND1 should not be set to 0_2). If the MS receives a RAND1 with value zero, the MS may consider abandoning the authentication, or performing cell reselection, or some other action outside the scope of the present document. It is advisable that the SwMI ensures that RAND1 is not set to zero to avoid such an outcome.

NOTE 3: An MS that is configured to permit negotiation of security class 1, security class 2 or security class 3 with a SwMI may be configured to adopt TA15 for authentication of the MS following the first successful negotiation of a KSG from TEA set B with that SwMI.

If the MS is provisioned with an authentication key K2, and negotiates security class 2 or security class 3 operation using an algorithm from TEA set A, the MS shall use a single session key KS with algorithm TA12 to compute RES1, and the SwMI shall likewise compute an expected response XRES1. MS and SwMI may compute DCK1 using algorithm TA12.

If the MS is provisioned with an authentication key K2 and negotiates security class 2 or security class 3 operation using an algorithm from TEA set B, two session keys KS and KS' shall be used with algorithm TA15. The MS shall compute a response, RES1, and the SwMI shall likewise compute an expected response, XRES1.

The SwMI on receipt of RES1 from the MS shall compare it with XRES1. If the values are equal the result R1 shall be set to TRUE, else the result R1 shall be set to FALSE.

NOTE 4: DCK1 may be used as an encryption key where one of the air interface encryption algorithms in TEA set A is in use. See clause 6 for more information.

The process is summarized in Figures 4.1, 4.1a and 4.1b.

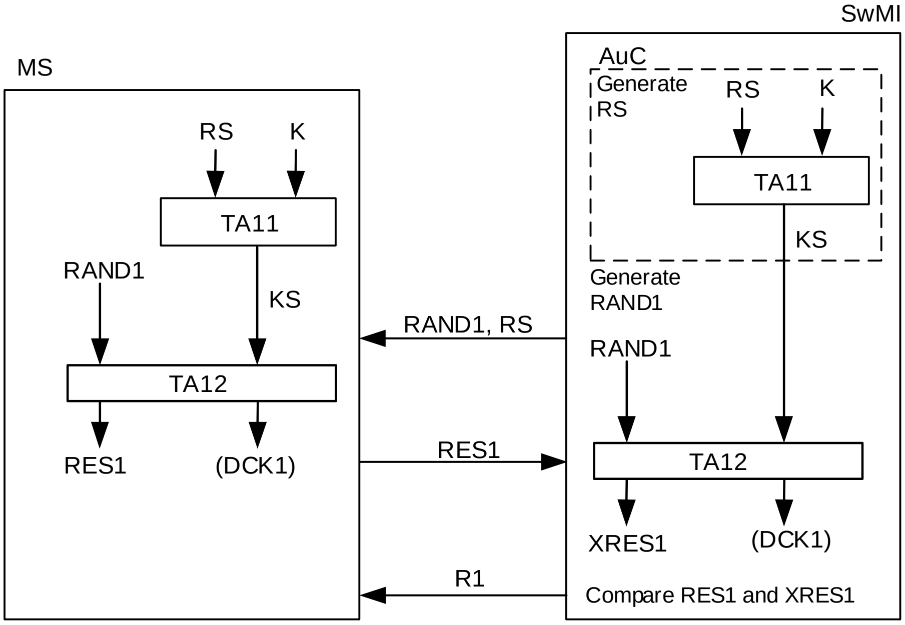


Figure 4.1: Authentication of an MS by the infrastructure using authentication key K

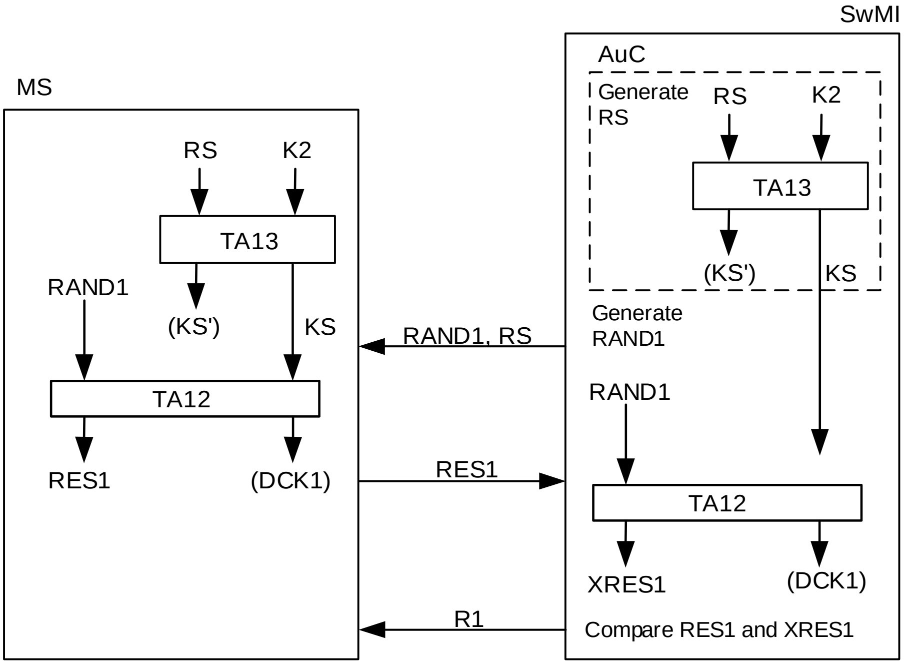


Figure 4.1a: Authentication of an MS by the infrastructure using authentication key K2 where an algorithm from TEA set A is negotiated

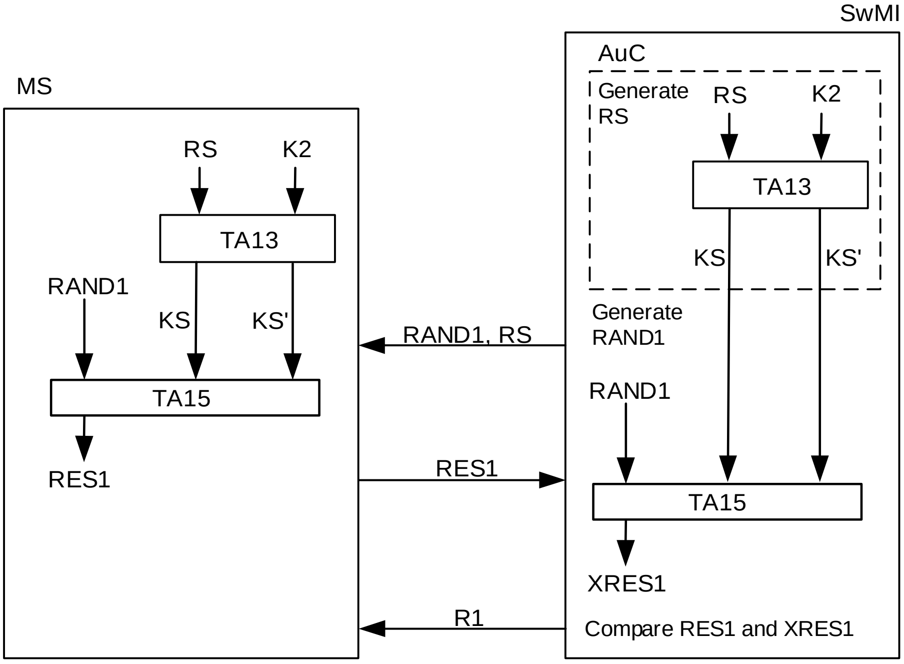


Figure 4.1b: Authentication of an MS by the infrastructure using authentication key K2 where an algorithm from TEA set B is negotiated

For authentication of the MS in security class 1 operation, Figure 4.1, Figure 4.1a or Figure 4.1b may apply, depending on the authentication key provisioned in the MS and on the SwMI configuration, as described in the previous paragraphs.

4.1.3 Authentication of the infrastructure

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

NOTE 1: RAND2 values should be non-repeating, and it should be difficult to predict the value of RAND2 chosen by the MS, as the authentication response RES2 and the derived cipher key DCK2 or DCKX both depend on RAND2.

NOTE 2: RAND2 should not be set to zero (i.e. all bits of RAND2 should not be set to 0_2). If the SwMI receives a RAND2 with value zero, the SwMI may consider abandoning the authentication, or rejecting the MS from the cell, or some other action outside the scope of the present document. It is advisable that the MS ensures that RAND2 is not set to zero to avoid such an outcome.

NOTE 3: DCK2 may be used as an encryption key where an air interface encryption algorithm from TEA set A is in use. See clause 6 for more information.

The same authentication key (K or K2) shall be used as in the case of authentication of the MS by the infrastructure together with a random seed RS.If the MS is provisioned with an authentication key K, a session key KS' that is different to the session key KS used for authentication of the MS shall be generated using algorithm TA21. The SwMI shall compute a response RES2 using RAND2 and KS' with algorithm TA22, and the MS shall compute an expected response XRES2 in the same way. MS and SwMI may compute DCK2 using algorithm TA22.

If the MS is provisioned with an authentication key K2, and negotiates security class 1 operation, the SwMI may use a single session key KS' that is different to the session key KS used for authentication of the MS with algorithm TA22 to compute RES2, and the MS shall likewise compute an expected response XRES2. If the SwMI is aware that the MS is provisioned with authentication key K2 and both SwMI and MS are configured to use TA23 for authentication for security class 1 operation, the SwMI shall use two session key KS and KS' with algorithm TA23 to compute RES2, and the MS shall likewise compute an expected response XRES2.

NOTE 4: An MS that is configured to permit negotiation of any of security class 1, security class 2 or security class 3 with a SwMI may be configured to adopt TA23 for authentication of the SwMI following the first successful negotiation of a KSG from TEA set B with that SwMI.

If the MS is provisioned with an authentication key K2 and negotiates security class 2 or security class 3 operation using an algorithm from TEA set A, a session key KS' that is different to the session key KS used for authentication of the MS shall be generated using algorithm TA13. The SwMI shall compute a response RES2 using RAND2 and KS' with algorithm TA22, and the MS shall compute an expected response XRES2 in the same way. MS and SwMI may compute DCK2 using algorithm TA22.

If the MS is provisioned with an authentication key K2 and negotiates security class 2 or security class 3 operation using an algorithm from TEA set B, two session keys KS and KS' shall be generated using algorithm TA13. The session keys KS and KS' are the same as those used for authentication of the MS, but algorithm TA23 calculates a different RES from that calculated by algorithm TA15. The SwMI shall compute a response RES2, and the MS shall compute an expected response XRES2 using RAND2 and KS' as inputs to TA23.

In either case, the MS validates that RES2 calculated by the SwMI is equal to XRES2 calculated by the MS and shall set R2 to TRUE if so, otherwise the result R2 shall be set to FALSE if they are not equal.

The process is summarized in Figures 4.2, 4.2a and 4.2b.

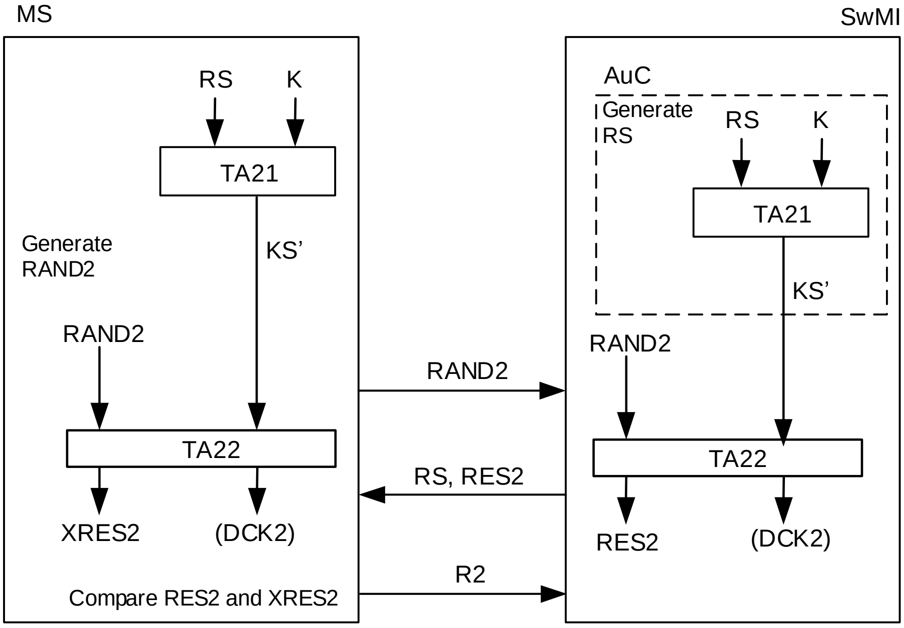


Figure 4.2: Authentication of the infrastructure by an MS using authentication key K

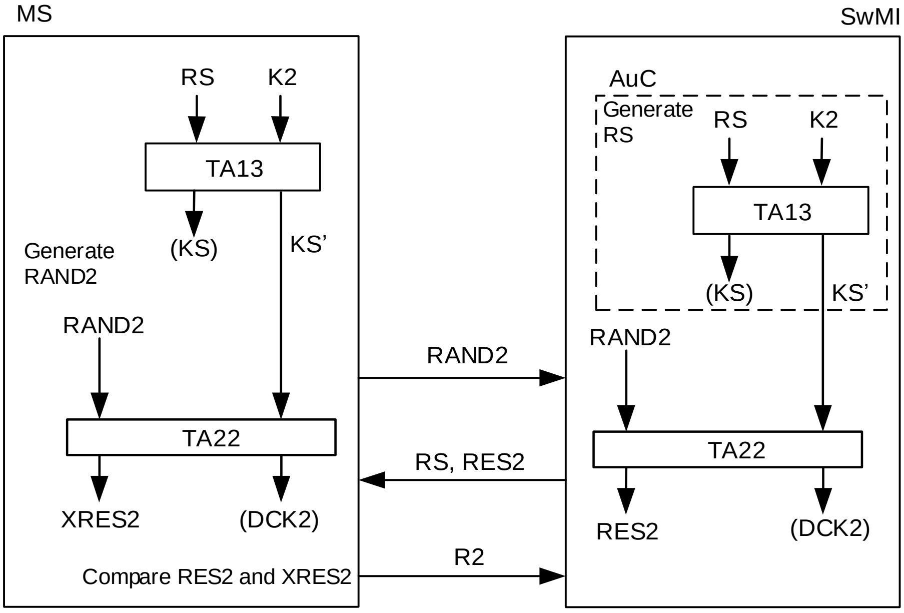


Figure 4.2a: Authentication of the infrastructure by an MS using authentication key K2 where an algorithm from TEA set A is negotiated

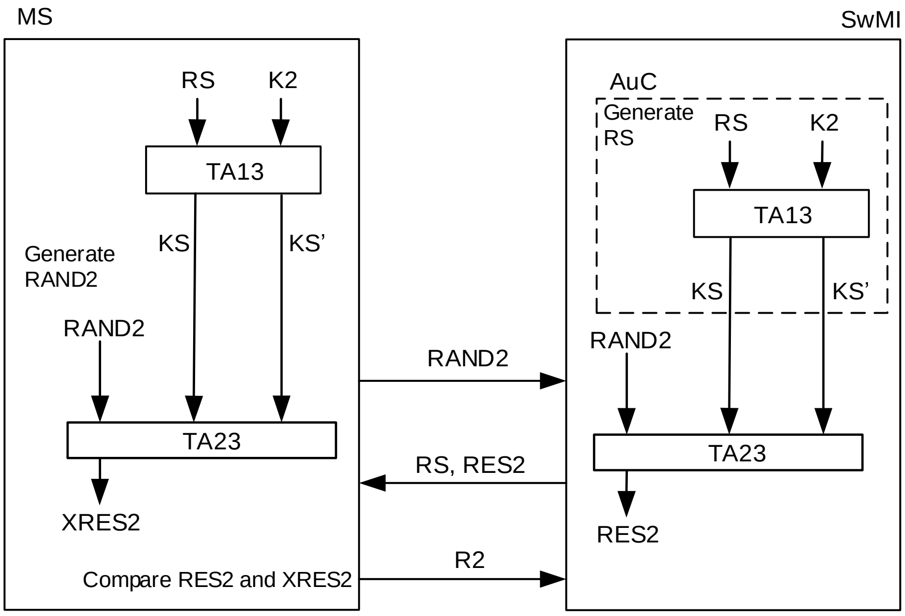


Figure 4.2b: Authentication of the infrastructure by an MS using authentication key K2 where an algorithm from TEA set B is negotiated

For authentication of the infrastructure in security class 1 operation, Figure 4.2, Figure 4.2a or Figure 4.2b may apply, depending on the authentication key provisioned in the MS and on the SwMI configuration, as described in the previous paragraphs.

4.1.4 Mutual authentication of MS and infrastructure

Mutual authentication of MS and infrastructure shall be achieved using a confirmed three pass mechanism. The algorithms and key K or K2 used shall be the same as those used in the one way authentication described in the previous clauses. The decision to make the authentication mutual shall be made by the first party to be challenged, not the initial challenging party. Thus mutual authentication shall be started as a one way authentication by the first challenging party, and then made mutual by the responding party. It is recommended that authentications are always made mutual by the responding party.

If the first challenging party does not support mutual authentication, then it may immediately conclude the authentication exchange by indicating a successful authentication result to the responding party. When the MS is the responding party, it determines whether or not to remain on the serving cell.

In the event that the first authentication fails, the second authentication shall be abandoned. However, if the first challenge is ignored by the initial challenged party, then the initial challenged party may instead challenge the initial challenging party. When the MS is the initial challenging party, it determines whether or not to remain on the serving cell. If the authentication was initiated by the SwMI, and the MS is provisioned with K, the SwMI 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'.

If the authentication was initiated by the SwMI, and the MS is provisioned with K2, the SwMI shall use K2 and one random seed RS with algorithm TA13 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 also run TA13 to generate session key KS and KS'.

If the MS is negotiating an algorithm from TEA set A, both MS and SwMI shall run algorithm TA12. If the MS is negotiating an algorithm from TEA set B, both MS and SwMI shall run algorithm TA15. 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 is provisioned with K and has not already done so.

If the MS is negotiating an algorithm from TEA set A, 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. If the MS is negotiating an algorithm from TEA set B, the SwMI shall then run TA23 to produce its response to the MS's challenge RES2. RES2 is sent to the MS, which shall also run TA23 to produce expected response XRES2. The MS on receipt of RES2 from the SwMI shall compare it with XRES2. If the values are equal the result R2 shall be set to TRUE, else the result R2 shall be set to FALSE. If R2 is TRUE mutual authentication will have been achieved.

If the MS is negotiating security class 1 operation, the MS shall generate RES1 and XRES2 according to the MS provisioning of K or K2, and the SwMI shall generate XRES1 and RES2 according to the SwMI awareness of the MS provisioning of K or K2 (e.g. by SwMI configuration), using the following keys and algorithms:

- MS is provisioned with K: KS and TA12, KS' and TA22;
- MS is provisioned with K2: KS and TA15, KS' and TA23;
- MS is provisioned with K2 but not configured to use TA15 and TA23: KS and TA12, KS' and TA22.

In either case, each party shall compare RES with XRES, and shall indicate the success of the authentication of the other party by setting R1 or R2, as described above.

NOTE 1: An MS that is configured to permit negotiation of any of security class 1, security class 2 or security class 3 with a SwMI may be configured to adopt TA15 and 23 for mutual authentication following the first successful negotiation of a KSG from TEA set B with that SwMI.

NOTE 2: Each party should choose a different RAND from the other party, i.e. RAND1 should not be equal to RAND2. If the second party challenges the first party with the same value of RAND that was provided by the first party, the first party may decide to abandon the authentication and restart the authentication process, or take some other action outside the scope of the present document.

NOTE 3: Both RAND1 and RAND2 should be unpredictable and non-repeating.

NOTE 4: Neither RAND1 nor RAND2 should be zero (i.e. all bits of RAND should not be set to 0_2). If either party receives a RAND set to zero, that party may consider restarting the authentication process or performing some other action (see clause 4.1.2 note 2 and clause 4.1.3 note 2).

NOTE 5: If configuration is incorrect and one party chooses to use TA12 and TA22, and the other party chooses to use TA15 and TA13, authentication will fail.

Algorithms TA12 and TA22 produce DCK1 and DCK2 respectively; these may 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 resulting DCK may be used as a cipher key when an air interface encryption algorithm from TEA set A is in use. The algorithm TB4 and the alternative extended derived cipher key DCKX that is used when one of air interface encryption algorithm set B is in use are described in clause 4.2.1.

The process is shown in Figure 4.3 and Figure 4.3a below.

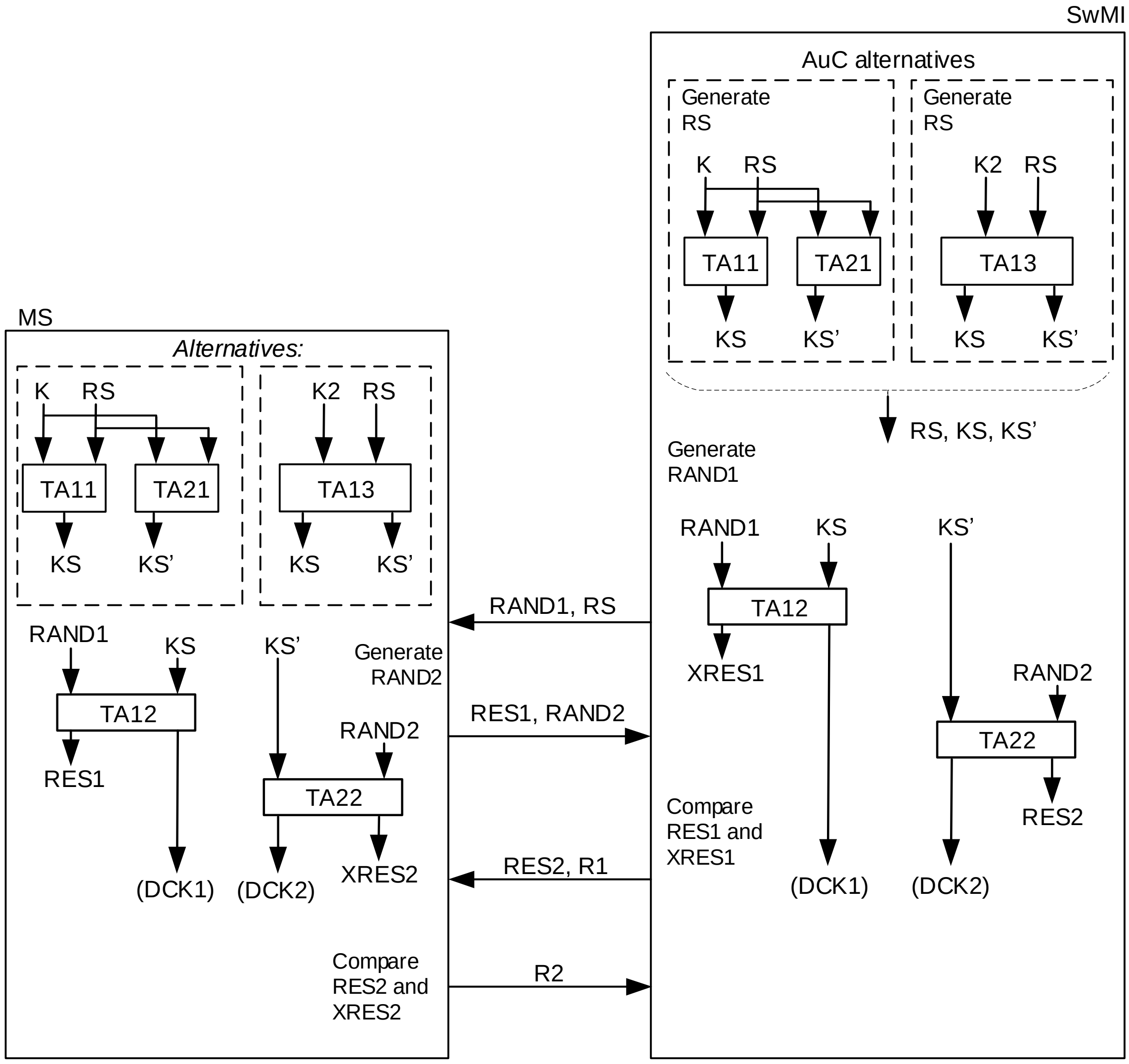


Figure 4.3: Mutual authentication initiated by SwMI where an algorithm from TEA set A is negotiated

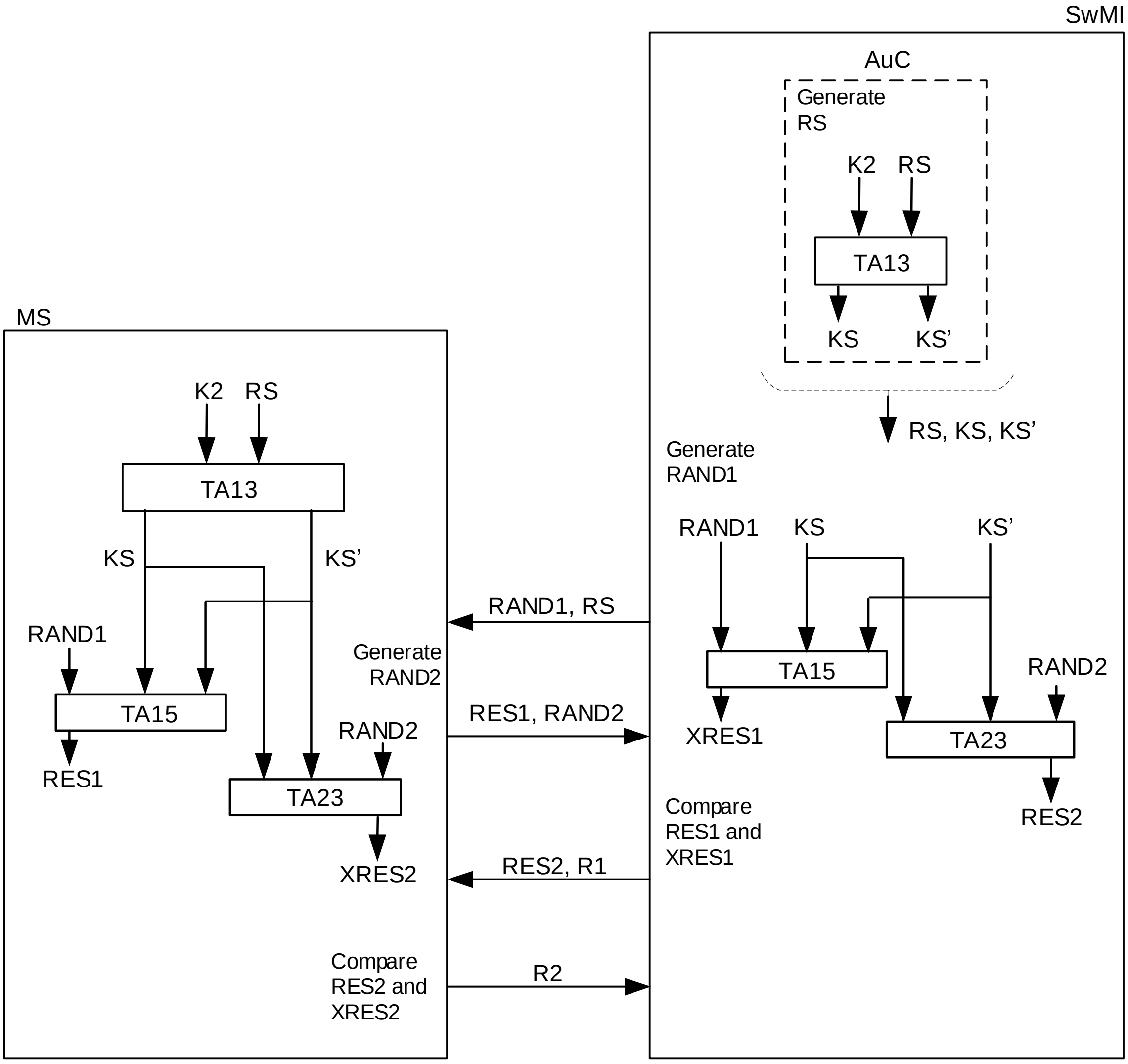


Figure 4.3a: Mutual authentication initiated by SwMI where an algorithm from TEA set B is negotiated

For mutual authentication in security class 1 operation, either Figure 4.3 or Figure 4.3a may apply, depending on the authentication key provisioned in the MS and on the SwMI configuration, as described in the previous paragraphs.

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 4.4 and Figure 4.4a below.

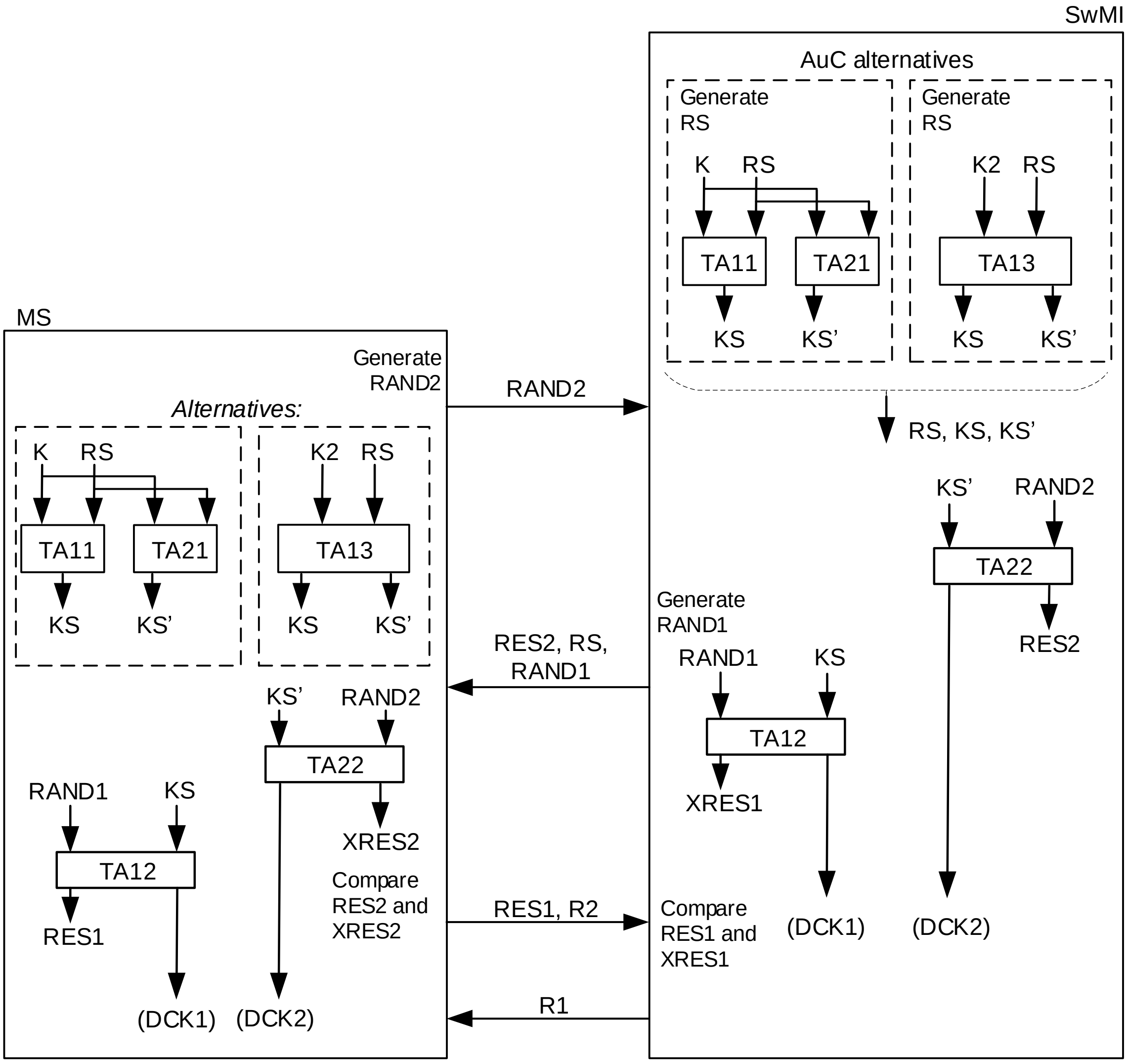


Figure 4.4: Mutual authentication initiated by MS where an algorithm from TEA set A is negotiated

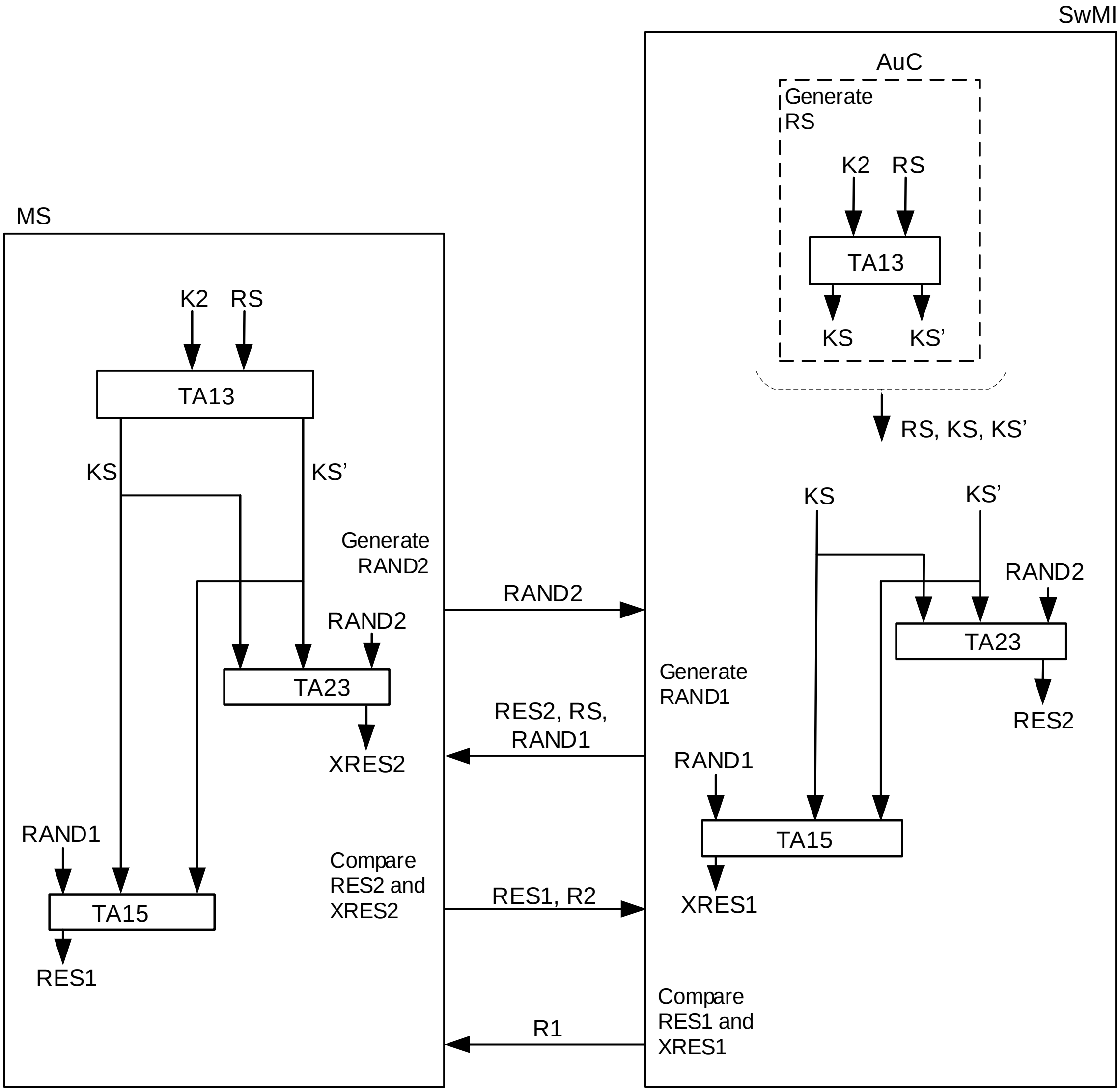


Figure 4.4a: Mutual authentication initiated by MS where an algorithm from TEA set B is negotiated

For mutual authentication in security class 1 operation, either Figure 4.4 or Figure 4.4a may apply, depending on the authentication key provisioned in the MS and on the SwMI configuration, as described in the previous paragraphs.

4.1.5 The authentication key

The ITSI and its associated user should be authenticated by a process that is carried out in the MS, as described in clause 4.1.2. To provide against misuse of lost, or stolen, MS, and to authenticate the user to the MS, the user should be required to make an input before the authentication key (K or K2) is available and valid for use. The authentication key 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).

4.1.6 Equipment authentication

The authentication of the TETRA Equipment Identity (TEI) is outside the scope of the present document. However, the protocol described in clause 4.4 provides a mechanism whereby the BS may demand an MS to provide TEI and other security related information, including version numbers of the hardware and software which comprise the MS, as part of the registration exchange.

4.1.6a Request for information related to an MS

The BS may request security related information from the MS as part of the registration process. The BS may explicitly request hardware and software version number information and model number information, and may also request the list of air interface encryption algorithms contained in the MS. An MS that is capable of providing this information shall make the BS aware during the registration process when registering for security class 3 security on the home network that it can accept such a request. The MS may respond with version number information for hardware and software, may also respond with model number information, may also respond with air interface encryption algorithm information, and may provide a list of KSGs supported; the MS may also volunteer additional information. The BS may also request TEI information as part of this process.

If the MS already knows that the SwMI supports the U-INFORMATION PROVIDE PDU (e.g. by configuration, or because the MS has previously received a "Security downlink" information element from the present SwMI having one or more of the "TEI request flag", the "Model number information request flag", the "HW SW version request flag" and/or "AI algorithm information request flag" set) the MS may send the U-INFORMATION PROVIDE PDU on an unsolicited basis following an exceptional event, for example a software or configuration change.

NOTE: Although hardware and software version number information is not used directly in TETRA security protocols, it is considered sensitive and therefore is categorized as security related information.

The format of version number and additional information shall be 8 bit ASCII encoded text information, which is provided together with a length field. Up to 63 characters of text may be provided within each set of information. The MS designer is therefore able to encode the information in a manner most suitable for the MS.

As all such information is considered to be sensitive, the MS should not provide the information unless operating with air interface encryption, i.e. in security class 2 or security class 3.

4.1.7 Authentication of an MS when migrated

When migrated the mechanism to achieve the authentication of an MS by the SwMI described in clause 4.1.2 is modified as shown in this clause.

An MS provisioned with authentication key K may migrate to a SwMI that requires the MS to use an air interface encryption algorithm from either TEA set A or TEA set B. Similarly, an MS provisioned with authentication key K2 may also migrate to a SwMI that requires the MS to use an air interface encryption algorithm from either TEA set A or TEA set B.

The session key KS generated by TA11 or TA13 in the home SwMI, using an RS randomly generated by the home SwMI, as defined in clause 4.1.2 shall be modified as a visitor session authentication key (KSv). KSv shall be provided by the home system to the visited system. The computation of KSv shall be carried out by an algorithm, TA101 or TA102, modifying the KS produced by algorithm TA11 or TA13. A second session key KSv' may be generated in a similar manner from KS' using TA101 or TA102 and provided to the visited system by the home system where the visited system requires the use of an algorithm from TEA set B for air interface encryption.

TA101 is used when the MS is provisioned with K or K2 and last negotiated one of the air interface encryption algorithms from TEA set A with the home SwMI, and has been provided with GCK0 (a designated session key modifier key). TA102 is used when the MS is provisioned with K2 and has last negotiated one of the air interface encryption algorithms from TEA set B with the home SwMI, and has been provided with GCKX0 (a designated session key modifier key).The inputs to TA101 shall be the MNI of the visited network, GCK0 and KS (the output of TA11 or TA13). The inputs to TA102 shall be the MNI of the visited network, GCKX0 and KS or KS' (the outputs of TA13). KSv, KSv' where applicable and RS shall be sent to the visited SwMI by the home SwMI.

When the value of GCK0 or GCKX0 is zero (i.e. the key designated as GCK0 consists of 80 zeros or the key designated as GCKX0 consists of 192 zeros), or if either the MS or the home SwMI does not support the use of GCK0 or GCKX0, the algorithms TA101 or TA102 shall not be invoked and KSv shall have the same value as KS, and KSv' where applicable shall have the same value as KS'.

If the visited SwMI requires the use of a KSG from TEA set A and supports authentication of an MS, the home SwMI shall transfer session key KSv to the visited SwMI. The home SwMI may also need to transfer session key KSv' to the visited SwMI if authentication of the SwMI or mutual authentication is required by the migrating MS and/or visited SwMI. If the visited SwMI requires the use of a KSG from TEA set B and supports authentication of the MS, the home SwMI shall transfer both session keys KSv and KSv' to the visited SwMI.

NOTE: The protocol for transfer of KSv and KSv' is described in ETSI EN 300 392-3-5 [8].

The process is summarized in Figure 4.5 for the case where the MS is required to use TEA set A in the visited SwMI. The cases where the MS last used TEA set A with the home SwMI (and so GCK0 and TA101 are used) and where the MS last used TEA set B with the home SwMI (and so GCKX0 and TA102 are used) are shown.

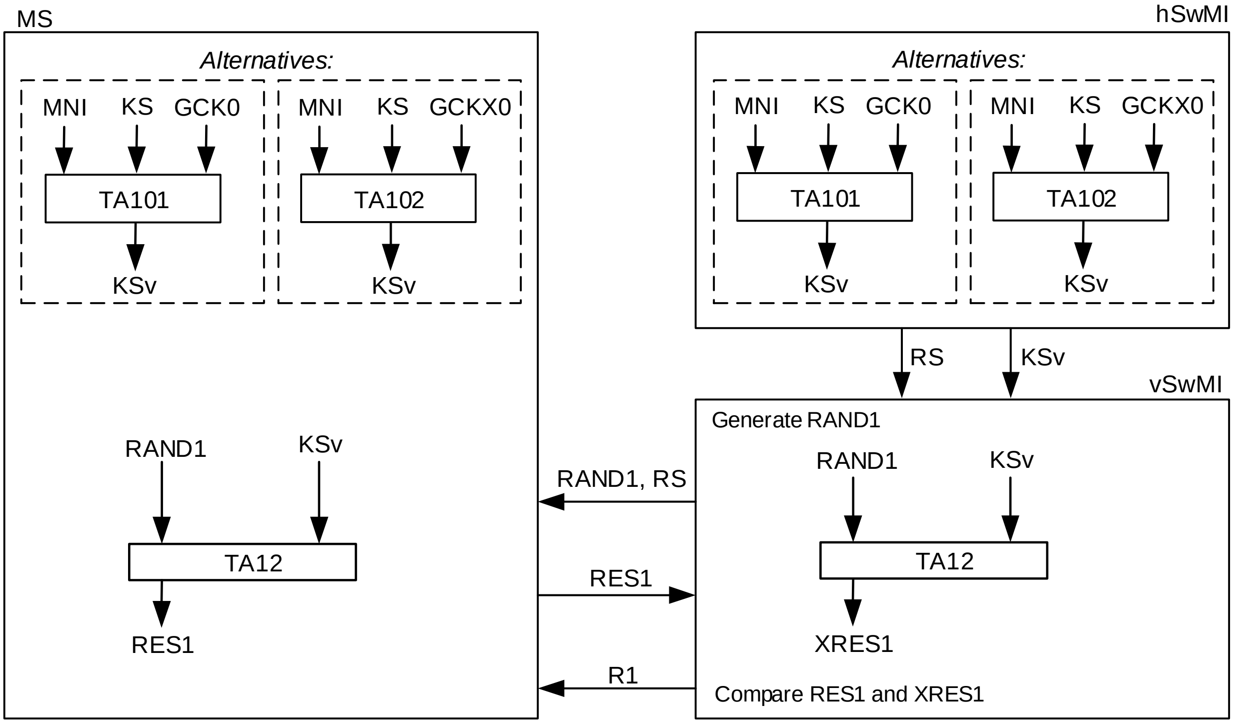


Figure 4.5: Authentication of a visited MS by the infrastructure where TEA set A is in use in the visited SwMI

Figure 4.5a shows the case where the MS last negotiated TEA set B with the home SwMI, and is required to use TEA set B with the visited SwMI.

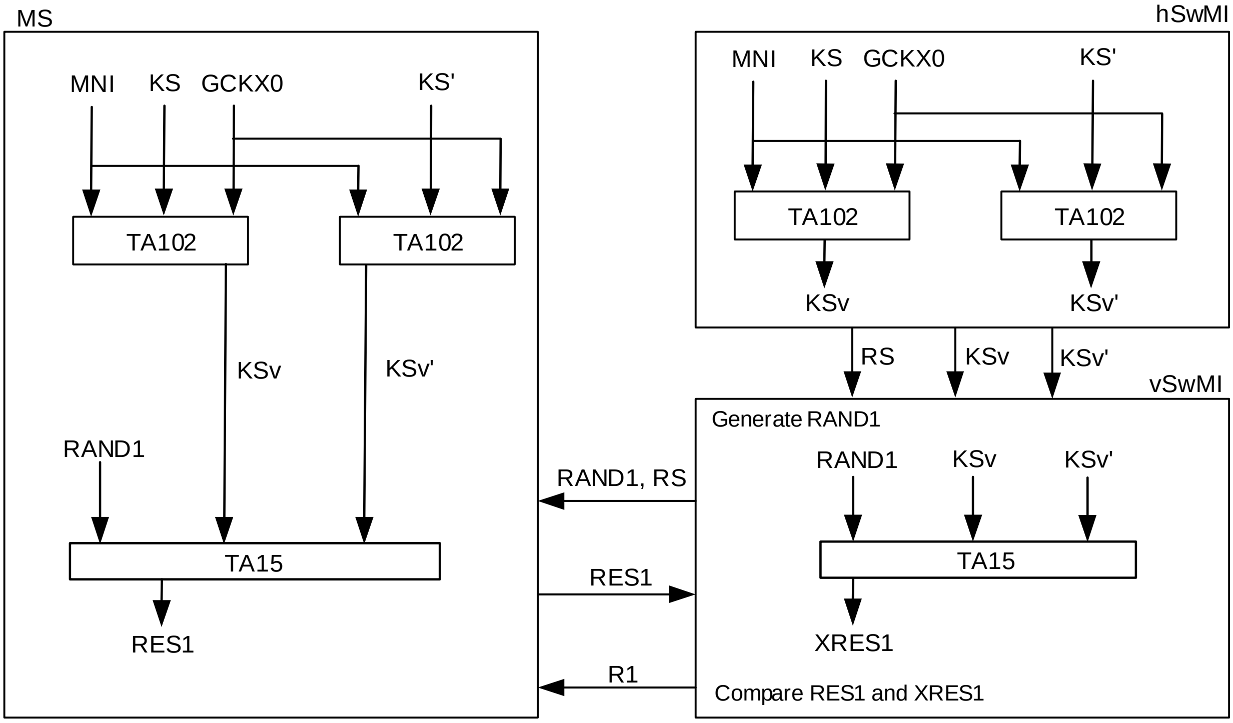


Figure 4.5a: Authentication of a visited MS by the infrastructure where the MS last negotiated TEA set B with the home SwMI and TEA set B is in use in the visited SwMI

Figure 4.5b shows the case where the MS last negotiated TEA set A with the home SwMI, and is required to use TEA set B with the visited SwMI.

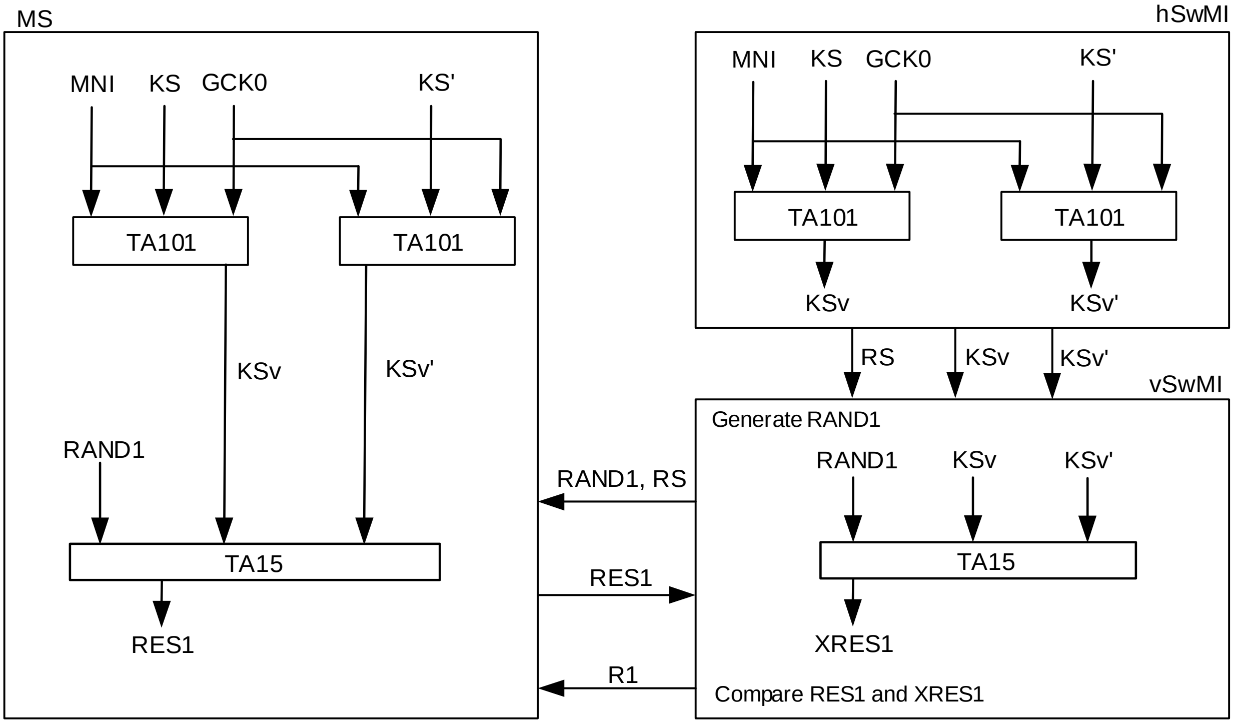


Figure 4.5b: Authentication of a visited MS by the infrastructure where the MS last negotiated TEA set A with the home SwMI and TEA set B is in use in the visited SwMI

4.1.8 Authentication of the home SwMI when migrated

When migrated the mechanism to achieve the authentication of the home SwMI by an MS as described in clause 4.1.3 is modified as shown in this clause.

NOTE 1: The authentication mechanism explicitly authenticates the home SwMI (holder of K or K2) and if successful implies that the visited SwMI is trusted (through the ISI) by the home SwMI.

The session key KS' generated by TA21 or TA13 in the home SwMI, using an RS randomly generated by the home SwMI, as defined in clause 4.1.3 shall be modified as a visitor session authentication key (KSv'). KSv' shall be provided by the home system to the visited system. The computation of KSv' shall be carried out by an algorithm, TA101 or TA102, modifying the KS' produced by algorithm TA21 or TA13. A second session key KSv may be generated in a similar manner from KS using TA101 or TA102 and provided to the visited system by the home system where the visited system requires the use of an algorithm from TEA set B for air interface encryption.

TA101 is used when the MS last negotiated one of the air interface encryption algorithms from TEA set A with the home SwMI and has been provided with GCK0 (a designated session key modifier key). TA102 is used when the MS is provisioned with K2 and has last negotiated one of the air interface encryption algorithms from TEA set B with the home SwMI and has been provided with GCKX0 (a designated session key modifier key).

The inputs to TA101 shall be the MNI of the visited network designated MNIv, GCK0 and KS' (the output of TA21). The inputs to TA102 shall be the MNI of the visited network designated MNIv, GCKX0 (a designated session key modifier key) and KS' or KS (the outputs of TA13). The process is summarized in Figure 4.6. KSv', KSv where applicable and RS shall be sent to the visited SwMI by the home SwMI.

When the value of GCK0 or GCKX0 is zero (i.e. the key designated as GCK0 consists of 80 zeros or the key designated as GCKX0 consists of 192 zeros), or if either the MS or the home SwMI does not support the use of GCK0 or GCKX0, the algorithms TA101 or TA102 shall not be invoked and KSv' shall have the same value as KS', and KSv where applicable shall have the same value as KS.

If the visited SwMI requires the use of a KSG from TEA set A and supports authentication of the SwMI, the home SwMI shall transfer session key KSv' to the visited SwMI. In this case, the home SwMI may also need to transfer session key KSv to the visited SwMI if authentication of the MS or mutual authentication is required by the visited SwMI. If the visited SwMI requires the use of a KSG from TEA set B and supports authentication of the SwMI, the home SwMI shall transfer both session keys KSv and KSv' to the visited SwMI.

NOTE 2: The protocol for transfer of KSv' and KSv is described in ETSI EN 300 392-3-5 [8].

The process is summarized in Figure 4.6 for the case where the MS is required to use TEA set A in the visited SwMI. The cases where the MS last used TEA set A with the home SwMI (and so GCK0 and TA101 are used) and where the MS last used TEA set B with the home SwMI (and so GCKX0 and TA102 are used) are shown.

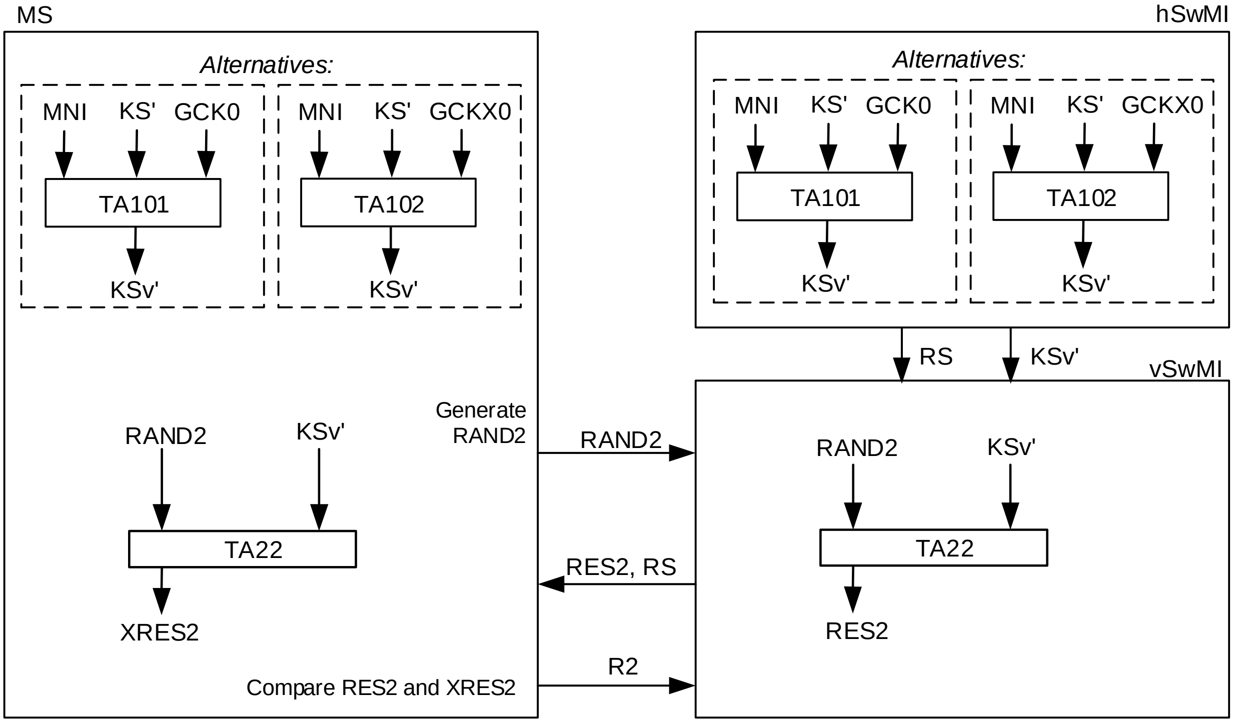


Figure 4.6: Authentication of the infrastructure by a visiting MS where TEA set A is in use in the visited SwMI

Figure 4.6a shows the case where the MS last negotiated TEA set B with the home SwMI, and is required to use TEA set B with the visited SwMI.

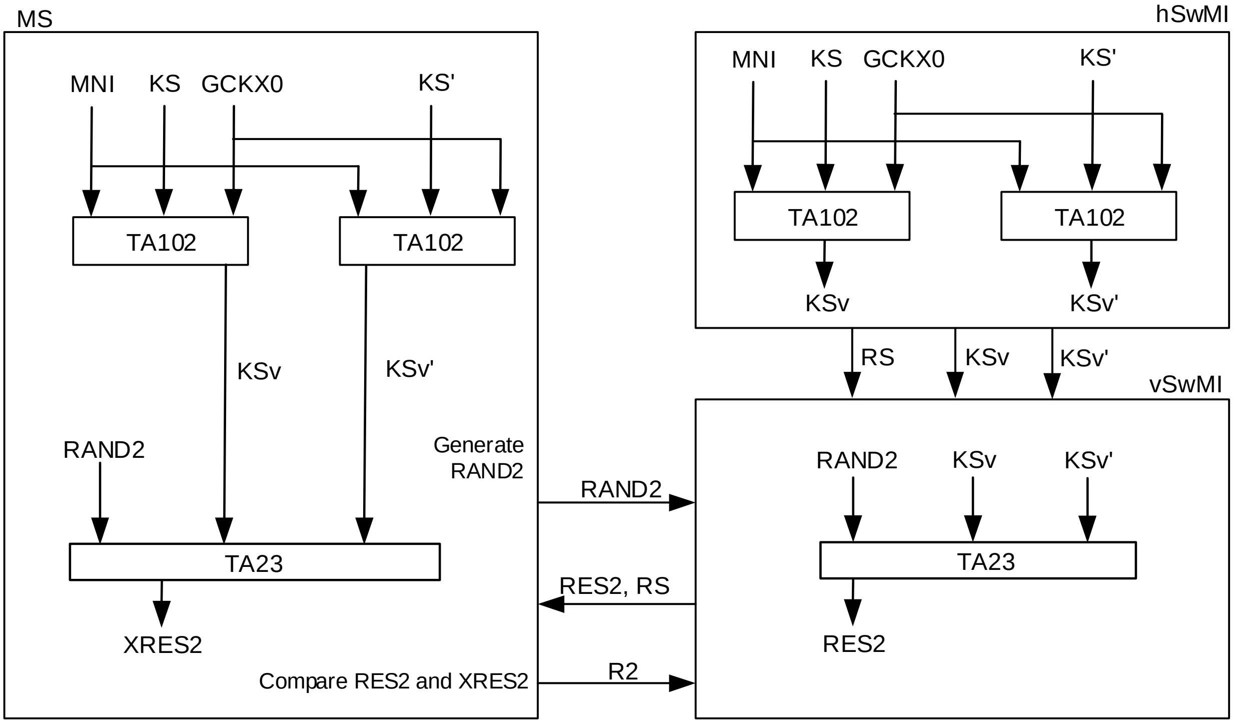


Figure 4.6a: Authentication of the infrastructure by a visiting MS where the MS last negotiated TEA set B with the home SwMI and TEA set B is in use in the visited SwMI

Figure 4.6b shows the case where the MS last negotiated TEA set A with the home SwMI, and is required to use TEA set B with the visited SwMI.

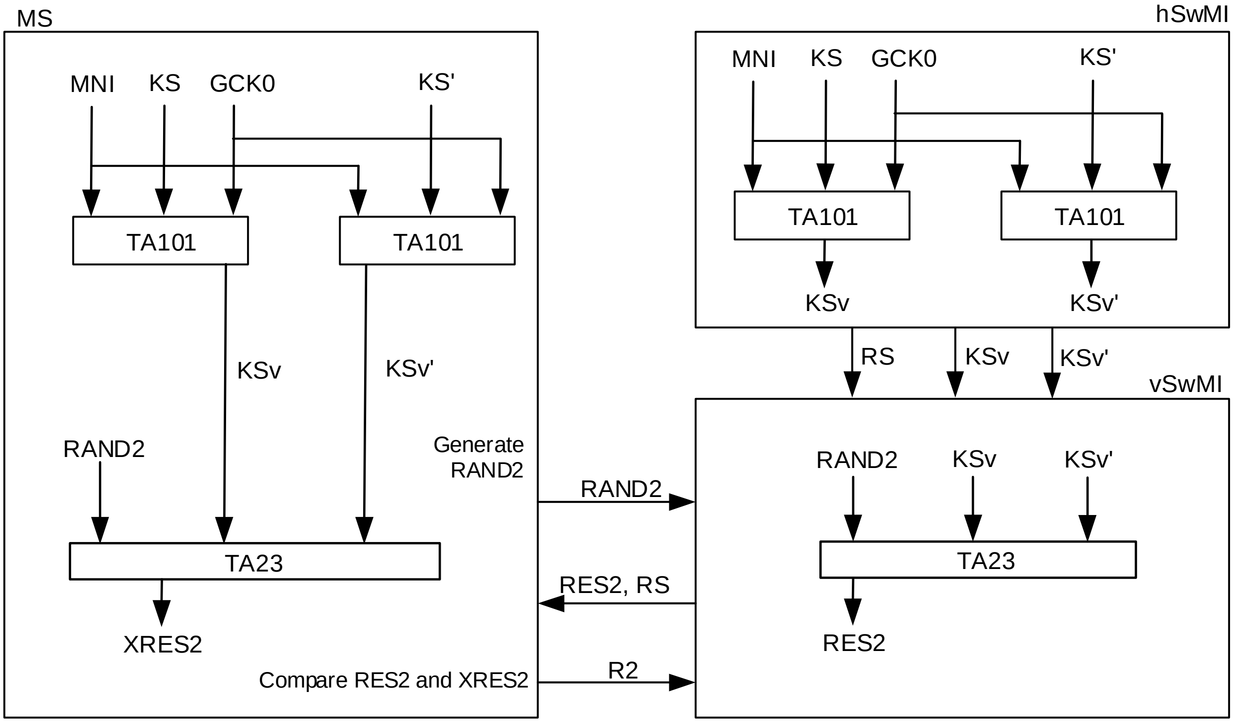


Figure 4.6b: Authentication of the infrastructure by a visiting MS where the MS last negotiated TEA set A with the home SwMI and TEA set B is in use in the visited SwMI

4.1.9 Mutual Authentication of MS and infrastructure when migrated

When migrated, the mechanism to achieve the mutual authentication of the MS and SwMI described in clause 4.1.4 is modified as shown in this clause.

The session key KS generated by TA11 or TA13 by the home SwMI and the session key KS' generated by TA21 or TA13 by the home SwMI, using a single RS randomly generated by the home SwMI, shall both be modified to produce visitor session authentication keys (KSv and KSv'). KSv and KSv' shall be provided by the home system to the visited system. The computation of KSv and KSv' shall be carried out by an algorithm, TA101 or TA102. The inputs to TA101 or TA102 shall be the MNI of the visited network, GCK0 or GCKX0 (a designated session key modifier key) and KS (the output of TA11 or TA13, where KSv is required) or KS' (the output of TA21 or TA13, where KSv' is required). KSv, KSv' and RS shall be sent to the visited SwMI by the home SwMI.

TA101 and GCK0 are used when the MS last negotiated one of the air interface encryption algorithms from TEA set A with the home SwMI, and TA102 and GCKX0 are used when the MS last negotiated one of the air interface encryption algorithms from TEA set B with the home SwMI.

The process shall be similar to that shown in Figures 4.3, 4.3a, 4.4 and 4.4a in clause 4.1.4, with KS and KS' replaced by KSv and KSv' respectively as the inputs to TA12 and TA22 or to TA15 and TA23.

When the value of GCK0 or GCKX0 is zero (i.e. the key designated as GCK0 consists of 80 zeros or the key designated as GCKX0 consists of 192 zeros), or if either the MS or the home SwMI does not support the use of GCK0 or GCKX0, the algorithms TA101 or TA102 shall not be invoked and KSv/KSv' shall have the same value as KS/KS'.

4.2 Air Interface key management mechanisms

4.2.0 General

Five types of key are managed over the air interface:

- the Derived Cipher Key, which may be a DCK or an extended DCK (DCKX);
- the Common Cipher Key, which may be a CCK or an extended CCK (CCKX);

- the Group Cipher Key, which may be a GCK or an extended GCK (GCKX);
- the Group Session Key for OTAR, which may be a GSKO or an extended GSKO (GSKOX); and
- the Static Cipher Key, which may be an SCK or an extended SCK (SCKX).

The Encrypted Short Identity (ESI) mechanism is also described in this clause. Generation of DCK or DCKX is linked to the authentication exchange described in clause 4.1. Clauses 4.2.2 to 4.2.5 describe over the air re-keying (OTAR) that is used to exchange the remainder of these keys.

4.2.1 The Derived Cipher Key

4.2.1.1 DCK and DCKX overview

DCK and extended DCK DCKX are only used in class 3 cells. DCK shall be used where one of the air interface encryption algorithms from TEA set A is in use. DCKX shall be used where one of the air interface encryption algorithms from TEA set B is in use. DCK or DCKX is derived from the authentication process by both the MS and the infrastructure: see clause 4.1.

If DCK or DCKX is used for key sealing (OTAR of CCK or CCKX, see clause 4.2.3) the DCK or DCKX should always be generated during authentication irrespective of the security class of the cell.

4.2.1.2 DCK derivation

The DCK shall be derived from its two parts DCK1 and DCK2 by the algorithm TB4, as shown in Figure 4.7, where an air interface encryption algorithm from TEA set A is in use. DCK1 is generated by successful authentication of the MS by the infrastructure, and DCK2 is generated by successful authentication of the infrastructure by the MS. Mutual authentication generates both DCK1 and DCK2.

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

In case of unilateral authentication, either DCK1 or DCK2 shall be set to zero: DCK2 = 0 for an authentication of the MS by the infrastructure; DCK1 = 0 for an authentication of the infrastructure by the MS.

If mutual authentication is requested by the MS, but the SwMI does not support mutual authentication and instead concludes the authentication, then DCK2 shall be set to "0" when deriving DCK using TB4.

If mutual authentication is requested by the SwMI, but the MS does not support mutual authentication and instead concludes the authentication, then DCK1 shall be set to "0" when deriving DCK using TB4.

If MS initiated authentication is ignored by the SwMI, and instead only SwMI initiated authentication is performed, then DCK2 shall be set to "0" when deriving DCK using TB4.

If SwMI initiated authentication is ignored by the MS, and instead only MS initiated authentication is performed, then DCK1 shall be set to "0" when deriving DCK using TB4.

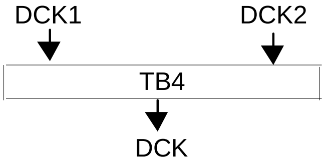


Figure 4.7: Derivation of the DCK from its two parts

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

4.2.1.3 DCKX derivation

The DCKX is generated by algorithm TA14 with the values of KS, KS', RAND1 and RAND2 that are used for authentication acting as inputs, where an air interface encryption algorithm from TEA set B is in use. This is illustrated in Figure 4.7a below.

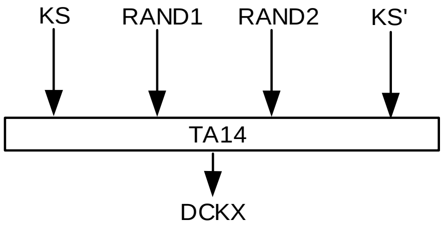


Figure 4.7a: Derivation of the DCKX during authentication

If authentication of the MS is initiated by the SwMI and the MS does not make the authentication mutual, RAND2 shall be set to zero (i.e. all bits of RAND2 shall be set to 0_2).

If authentication of the SwMI is initiated by the MS and the SwMI does not make the authentication mutual, RAND1 shall be set to zero (i.e. all bits of RAND1 shall be set to 0_2).

4.2.1.4 Usage of DCK and DCKX

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

4.2.1.5 Validity of DCK and DCKX

A DCK or DCKX is valid within one network only. If the MS detaches from the network, it may store its current DCK or DCKX to allow it to use security class 3 encryption on its next attempt at attachment on the same network. The MS may store the last DCK or DCKX used for each network if has attached to more than one network. If it does this, it shall store each DCK or DCKX with reference to the MNI of the relevant network so that it may attempt to use only the correct DCK or DCKX for a particular network.

4.2.2 The Group Cipher Key

4.2.2.0 General

GCK and extended GCK (GCKX) are only used on class 3 cells. GCK is used where one of the air interface encryption algorithms from TEA set A is in use. GCKX is used where one of the air interface encryption algorithms from TEA set B is in use.

The GCK or GCKX shall be known to the infrastructure and distributed to the MSs. GCK and GCKX shall not be used directly by the air interface encryption unit. Within each LA, either the GCK shall be modified by CCK (see clause 4.2.3) using algorithm TA71 to provide a Modified GCK (MGCK) for use on the air interface, or the GCKX shall be modified by CCKX (see clause 4.2.3) using algorithm TA72 to produce the MGCKX for use on the air interface. The process is shown in Figure 4.8.

If GCK or GCKX is not defined for a group, the value of MGCK shall be equal to that of CCK or the value of MGCKX shall be equal to that of CCKX, and algorithms TA71 or TA72 shall not be invoked.

Use of GCK or GCKX shall be determined by the security policy of the serving SwMI and shall only be valid for use by groups in that SwMI. If a group migrates to a visited SwMI, the use of GCK or GCKX in that group while migrated shall be determined by the security policy of the visited SwMI.

NOTE 1: SwMIs may agree to apply the same security policy to a particular group. The process to achieve this is outside the scope of the present document.

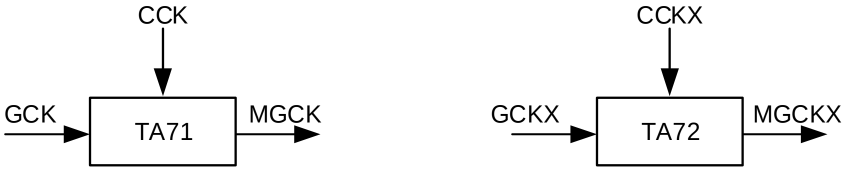


Figure 4.8: Generation of MGCK from GCK and CCK and MGCKX from GCKX and CCKX

One GCK or GCKX may be associated with more than one group. A GCK Number (GCKN) associated with each GCK and each GCKX can be used to identify association with multiple groups. The values of GCKN should be unique between all MSs sharing the same sets of GCK and GCKX. The MS shall consider a GCK or a GCKX and the corresponding identifying GCKN as valid only within one network. The MS may hold more than one set of GCKs or GCKXs with their associated GCKNs for use in more than one network; in this case the MS shall reference the GCKN to the MNI of the network in which the GCKN is valid. The association of GCK or GCKX to groups may be changed by the OTAR service to allow automatic key management to take place.

A GCK or GCKX shall be associated with a GCK Version Number (GCK-VN) as well as a GCKN. The GCK-VN allows identified key material for each GCK or GCKX to be changed at intervals and therefore to manage crypto periods for GCKs, whilst retaining the same association of GCKN to groups. The SwMI may indicate the version of GCK in use to MSs by indicating the GCK-VN in the D-CK CHANGE DEMAND PDU, as described in clause 4.5.5, and may coordinate GCK-VNs between GCKNs such that several or all GCKNs have the same active GCK-VN.

The same GCKN may be allocated to both a GCK and a GCKX, but in this case the GCK-VNs of the GCK and GCKX shall be different.

NOTE 2: This could allow the SwMI and MS to transition to use of a different air interface encryption algorithm at the start of a new crypto period, when the GCK or GCKX with the later GCK-VN is activated.

4.2.2.0a Validity of GCK and GCKX

A SwMI shall only distribute a GCK or GCKX to an MS by OTAR where that GCK or GCKX is valid in that SwMI. GCKs and GCKXs shall not be distributed by OTAR for use in a different SwMI.

4.2.2.0b Distribution of GCK

When distributing GCK to an individual MS by an OTAR mechanism (algorithms TA81 and TA82) to an MS that is provisioned with authentication key K, a session key for OTAR (KSO) may be used to protect the GCK, alternatively an Extended Group Session Key for OTAR (EGSKO) derived from a Group Session Key for OTAR (GSKO) may be used. The signalling shall indicate the sealing key in use. KSO shall be individual to each MS and shall be derived from an MS's authentication key (K) and a random seed RSO with algorithm TA41.

If an MS is provisioned with authentication key K2 and has negotiated an encryption algorithm from TEA set A, the KSO used to protect the GCK shall be derived from an extended session key for OTAR KSOX by algorithm TA104, and then the GCK shall be sealed using algorithm TA81. In this case, KSOX is derived from authentication key K2 and a random seed for OTAR RSO using algorithm TA42. Alternatively, an EGSKO derived from a GSKO may be used to protect the GCK.

When distributing a GCK to a group by OTAR an EGSKO derived from GSKO shall be used as the sealing key.

A GCK may be distributed by a vSwMI to an MS that has migrated to that vSwMI. The mechanism is described in clause 4.2.5a.

4.2.2.0c Distribution of GCKX

When distributing GCKX to an individual MS by an OTAR mechanism (algorithms TA83 and TA84) an Extended Session Key for OTAR (KSOX) may be used to protect the GCKX, alternatively an Extended Group Session Key for OTAR (GSKOX) may be used. The signalling shall indicate the sealing key in use. KSOX shall be individual to each MS and shall be derived from an MS's authentication key (K2) and a random seed RSO with algorithm TA42.

When distributing a GCKX to a group by OTAR a GSKOX shall be used as the sealing key.

A GCKX may be distributed by a vSwMI to an MS that has migrated to that vSwMI. The mechanism is described in clause 4.2.5a.

4.2.2.0d Decryption of sealed GCK and GCKX

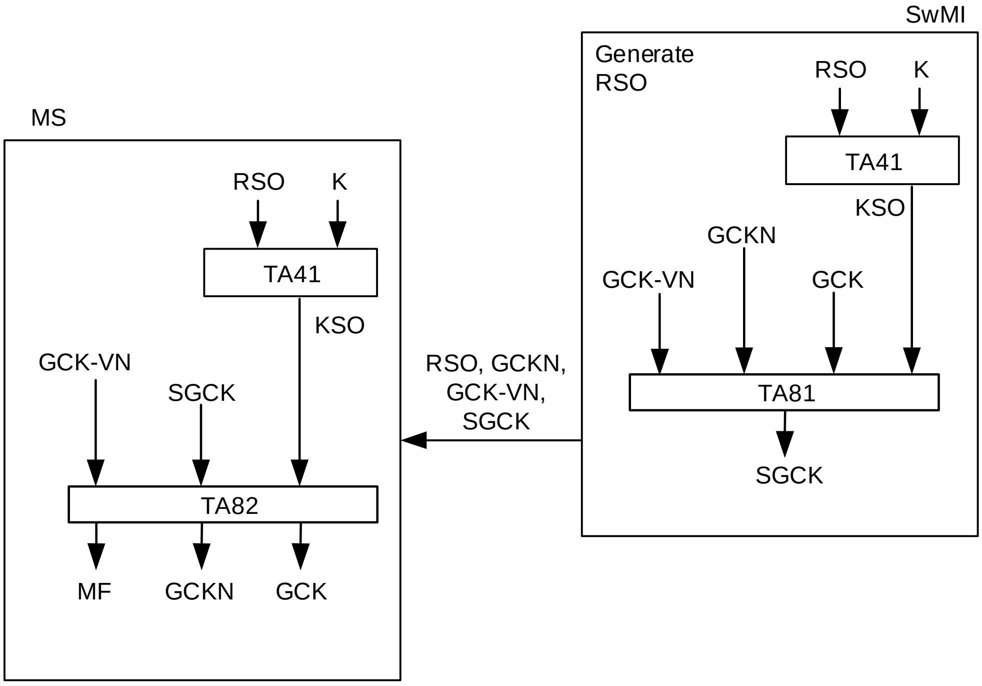
To allow the sealed GCK and GCKX to be decrypted by the MS, algorithm TA81 has an inverse TA82, and algorithm TA83 has an inverse TA84. To allow the MS to discover if GCK or GCKX has been corrupted due to transmission errors or manipulation, TA81 and TA83 introduce some redundancy into the Sealed Group Cipher Key (SGCK or SGCKX). Algorithms TA81 and TA83 take the Group Cipher Key Version Number (GCK-VN) and the Group Cipher Key Number (GCKN), as additional inputs. The GCK-VN is also provided to algorithms TA82 and 84. The redundancy is checked by TA82 or TA84 respectively. A detected manipulation shall be indicated by setting the manipulation flag MF.

If MF is TRUE the recovered key shall be discarded.

The MS is also provided with the GCKN during OTAR transmission in the D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE PDUs, independently of its recovery by TA82 or TA84. The MS should check the value of GCKN output by TA82 or TA84 against the independently provided value in the D-OTAR PDU, and should discard the recovered key if there is a mismatch.

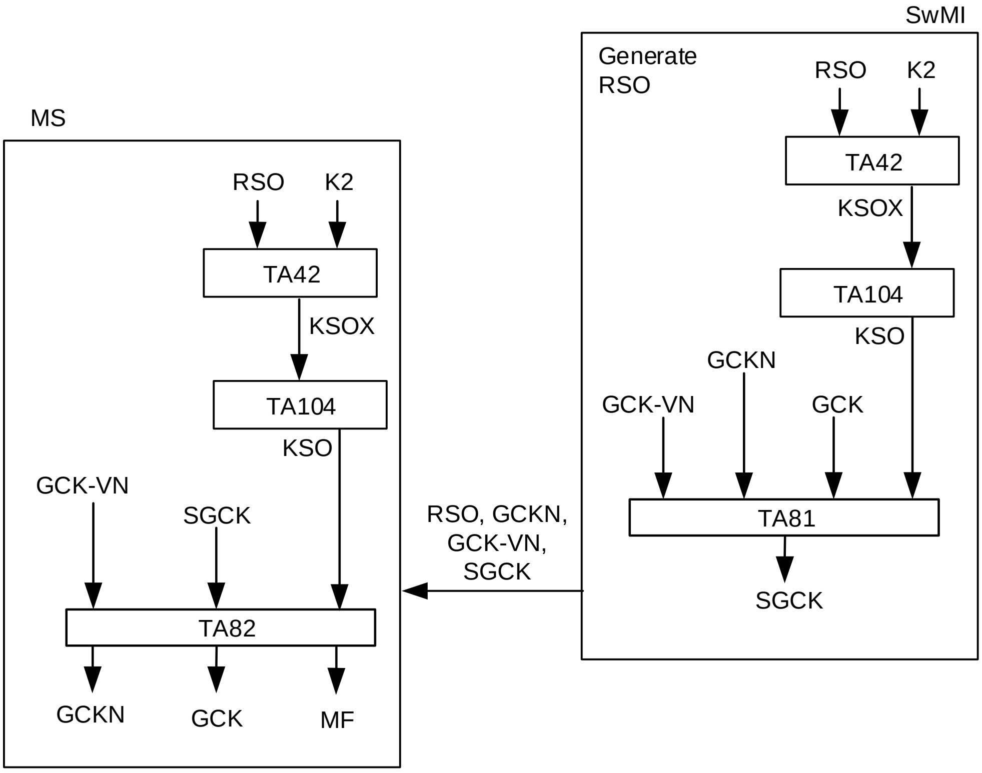
4.2.2.0e Summary of GCK distribution process

The process is summarized in Figures 4.9, 4.9a and 4.9b below.



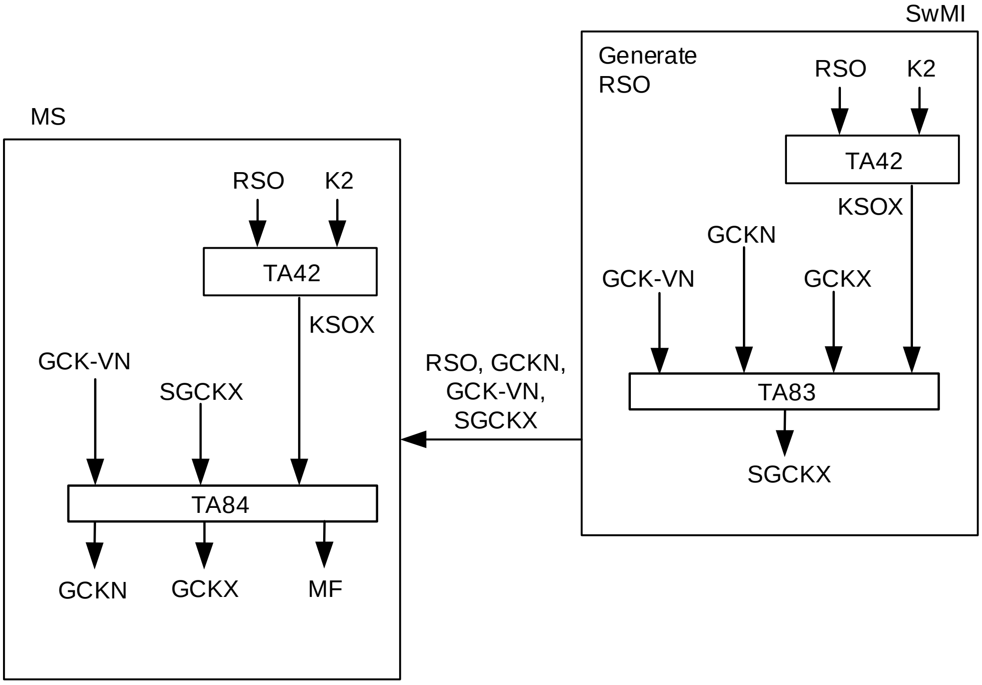
NOTE: EGSKO is input to TA81 and TA82 instead of KSO for distribution to a group, and may be input to TA81 and TA82 instead of KSO for distribution to an individual MS.

Figure 4.9: Distribution of a GCK to an MS that is provisioned with K



NOTE: Alternatively, EGSKO may be input to TA81 and TA82 instead of KSO

Figure 4.9a: Distribution of a GCK to an MS that is provisioned with K2



NOTE: GSKOX is input to TA83 and TA84 instead of KSOX for distribution to a group, and may be input to TA83 and TA84 instead of KSOX for distribution to an individual MS.

Figure 4.9b: Distribution of a GCKX to an MS

4.2.2.1 Session key modifiers GCK0 and GCKX0

Where the MS uses one of the air interface encryption algorithms from TEA set A with the home SwMI, the session key modifier GCK0 may be used in conjunction with algorithm TA101 in the authentication process when the MS is migrated as described in clause 4.1. GCK0 may also be used in the OTAR process to provide keys to the MS when migrated, as described in clause 4.2.5a.

Where the MS uses one of the air interface encryption algorithms from TEA set B with the home SwMI, the session key modifier GCKX0 may be used in conjunction with algorithm TA102 in the authentication process when the MS is migrated as described in clause 4.1. GCKX0 may also be used in conjunction with algorithm TA103 in the OTAR process to provide keys to the MS when migrated, as described in clause 4.2.5a.

GCK0 and GCKX0 may be distributed to MSs by the same OTAR mechanisms and algorithms that are used to distribute GCK and GCKX respectively. If distributed by OTAR, they may be protected by a session key for OTAR (KSO or KSOX), or by an EGSKO derived from GSKO or a GSKOX as described in clause 4.2.2.0b and 4.2.2.0c. The session key modifier shall be identified by a specific GCKN = 0 to distinguish it from GCK or GCKX whilst allowing it to use the same distribution mechanisms.

GCK0 and GCKX0 shall only be distributed to the MS by OTAR while the MS is operational in its home SwMI.

A specific value of GCK0 = 0 (all 80 bits set to 0) or GCKX0 = 0 (all 192 bits set to 0) shall cause the key modification algorithms TA101, TA102 or TA103 to not be invoked in the case that key modification in a visited SwMI is not required.

4.2.3 The Common Cipher Key

4.2.3.1 CCK and CCKX usage

CCK and the Extended CCK (CCKX) are only used in class 3 cells.

CCK and CCKX are used to give protection of voice, data, and signalling sequences between the infrastructure and an MS when using group addresses (including the broadcast address) on the downlink either as a key modifier of GCK or GCKX (see clause 4.2.2) or as a standalone key. In addition CCK or CCKX is used to generate ESI as described in clause 4.2.6, or CCKX is used to apply the MAE mechanism as described in clause 6.7.1.2a. The CCK or CCKX shall be generated by the infrastructure and distributed to the MSs. A CCK or CCKX may be used in more than one LA or there may be a distinct CCK or CCKX for every LA in the system.

The CCK is used when any of the air interface encryption algorithms from TEA set A is in use for air interface encryption. There shall only be one CCK in use in an LA, even if a SwMI uses more than one algorithm from TEA set A in that LA. The CCKX is used when any of the air interface encryption algorithms from TEA set B is in use for air interface encryption. There shall only be one CCKX in use in an LA, even if a SwMI uses more than one algorithm from TEA set B in that LA. If a SwMI uses at least one algorithm from TEA set A and at least one algorithm from TEA set B in any LA, there may be one CCK and one CCKX in use in that LA. If the SwMI uses an algorithm from TEA set A and an algorithm from TEA set B in the same LA, the SwMI shall derive the CCK used with the algorithm from TEA set A from the CCKX used with the algorithm from TEA set B using algorithm TA106.

NOTE 1: It is not recommended to use more than one algorithm from TEA set A in the same LA, and not recommended to use more than one algorithm from TEA set B in the same LA. It is also not recommended to use an algorithm from TEA set A in the same LA as an algorithm from TEA set B, except in exceptional circumstances such as transition between air interface encryption algorithms.

NOTE 2: If the SwMI uses different algorithms from TEA set A in different LAs, it is recommended that different CCKs are used in those different LAs. Similarly, if the SwMI uses different algorithms from TEA set B in different LAs, it is recommended that different CCKXs are used in those different LAs.

NOTE 3: If the SwMI supports more than one algorithm in the same LA (whether those algorithms are from the same or different TEA sets), transmissions sent to the broadcast address should be sent in clear to avoid any erroneous operation if an MS fails to decrypt a broadcast transmission sent with a different algorithm to that negotiated by the MS. See clause 6.3.1.

4.2.3.2 CCK and CCKX identification

CCK and CCKX are uniquely identified by the combination of LA-id and CCK-id. Where a CCK or a CCKX applies to many LAs the CCK-id shall be the same in each LA.

There shall only be one CCK-id in use in any LA. If one of the algorithms from TEA set A is in use in the same LA as one of the algorithms from TEA set B, the same CCK-id shall apply to CCK and to CCKX. In this case, when a new CCK(X) is to be distributed, the SwMI shall distribute both the new CCK and the new CCKX to those MSs that require them, and shall activate the new CCK and new CCKX at the same time.

4.2.3.3 CCK and CCKX distribution

The MS may request the CCK or CCKX 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. The CCKX may be transmitted in encrypted form using algorithm TA33 and DCKX as the sealing key. To allow the CCK or CCKX to be decrypted by the MS, algorithm TA31 has an inverse TA32 and TA33 has an inverse TA34. To allow the MS to discover if CCK or CCKX has been corrupted due to transmission errors or manipulation, TA31 and TA33 introduce some redundancy into the Sealed Common Cipher Key (SCCK) or Sealed Extended Common Cipher Key (SCCKX). The redundancy is checked by TA32 or TA34 respectively.
A detected manipulation shall be indicated by setting the manipulation flag MF.

If MF is true the recovered key shall be discarded.

The infrastructure may change the CCK or CCKX 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 input to algorithms TA31 and TA32 or to algorithms TA33 and TA34 to the effect that decryption of the correct CCK or CCKX shall only be possible if the correct CCK-id has been received. CCK-id shall be referenced by one bit in the encryption mode element of the MAC RESOURCE PDU of the encrypted message to select the active CCK or CCKX. The value of this bit shall equal the value of the least significant bit of CCK-id. The method of determining a valid CCK-id and, therefore, of identifying a replay is outside the scope of the present document.

The process is summarized in Figure 4.10 and Figure 4.10a below.

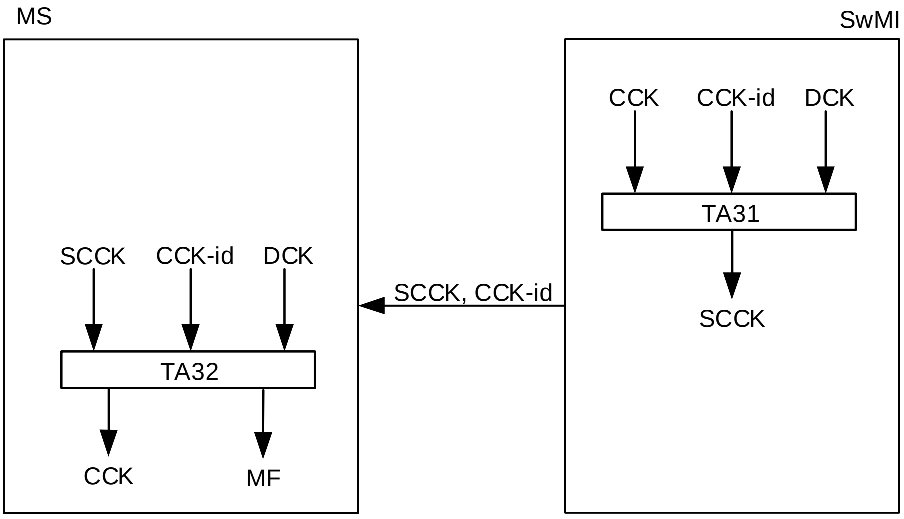


Figure 4.10: Distribution of a common cipher key

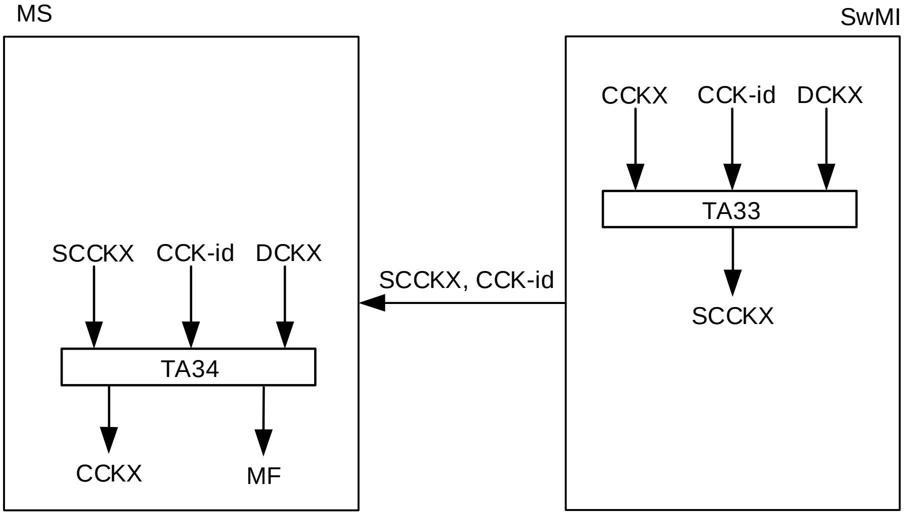


Figure 4.10a: Distribution of an extended common cipher key

4.2.3.4 CCK and CCKX validity

A CCK or CCKX is valid within the specified LAs in one network only. If the MS detaches from the network, it may store one or more CCKs or CCKXs to allow it to use security class 3 encryption on its next attempt at attachment to the same network. The MS may store the CCKs or CCKXs used for more than one network if has attached to more than one network. If it does this, it shall store each CCK or CCKX with reference to the MNI of the relevant network as well as reference to the relevant LAs, so that it shall only attempt to use the correct CCK or CCKX for a particular network.

4.2.4 The Static Cipher Key

4.2.4.0 General

SCK and the Extended SCK (SCKX) are used on class 2 cells and in Direct Mode operations (see ETSI EN 300 396-6 [5]). SCK or SCKX may also be used for encryption in a cell that normally operates in class 3 but is in fallback mode. In a security class 2 cell, SCK or SCKX is used to generate ESI as described in clause 4.2.6, or SCKX is used to apply the MAE mechanism as described in clause 6.7.1.2a. SCK is used where one of the air interface encryption algorithms from TEA set A is in use. SCKX is used where one of the air interface encryption algorithms from TEA set B is in use.

SCK or SCKX is used to protect voice, data, and signalling sequences between the infrastructure and an individual MS or groups of MSs in a security class 2 cell. There shall be up to 32 Static Cipher Keys available to each ITSI for use with one MNI, where each of the 32 may be an SCK or an SCKX. SCK or SCKX shall be a fixed value that should be known to the infrastructure and every MS. These keys are termed "static" because they are not generated or changed by the authentication exchange. Each SCK or SCKX is identified by an SCK Number, SCKN.

The SCK is used when any of the air interface encryption algorithms from TEA set A is in use for air interface encryption on a cell operating in security class 2. If a SwMI uses more than one algorithm from TEA set A in any LA, there shall still only be one SCK in use in that LA. The SCKX is used when any of the air interface encryption algorithms from TEA set B is in use for air interface encryption on a cell operating in security class 2. If a SwMI uses more than one algorithm from TEA set B in any LA, there shall still be only one SCKX in use in that LA. If a SwMI uses at least one algorithm from TEA set A and at least one algorithm from TEA set B in any LA, there may be one SCK and one SCKX in use in that LA. If the SwMI uses an algorithm from TEA set A and an algorithm from TEA set B in the same LA, the SwMI shall derive the SCK used with the algorithm from TEA set A from the SCKX used with the algorithm from TEA set B using algorithm TA106.

Where an infrastructure uses security class 3 normally, but may use security class 2 in a fallback mode, two specific SCKNs (see clause 4.2.4.0b) with value 31 and 32 are reserved for security class 2 fallback use. An infrastructure that only uses class 2 may use any SCKN for SCKs or SCKXs.

SCKs and SCKXs may be associated with one or more groups for encryption in DMO (see ETSI EN 300 396-6 [5]). The association principle is described in clause 4.2.4.1.

SCK and SCKX may also be deleted from the MS by the key deletion procedures in clause 4.5.9.

4.2.4.0a SCK sets

SCK shall be a member of an SCK set containing up to 32 keys, where each of these keys may either be an SCK or an SCKX, and each shall be identified by its position in the SCK set (SCK Number (SCKN)). One SCK set is valid for use with one MNI. An MS may store more than one SCK set, and shall reference each SCK set to the MNI of the network where the SCK applies. The MNI may be the 'Open MNI', in which case the SCK set shall only be used with GTSIs containing the 'Open MNI'. 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 using algorithms TA51 and TA52. SCKXs may be protected for distribution using algorithms TA53 and TA54.

4.2.4.0b SCK and SCKX identification

An SCK or SCKX shall be identified by two numbers:

- The SCK Number (SCKN) shall address one of the 32 SCKs or SCKXs stored in an SCK set in an MS. The SCK Version Number (SCK-VN) shall identify the version of each of the 32 SCKs or SCKXs and should be incremented for each new key identified with the same SCKN.

- SCK-VN may be used to protect the distribution of the SCKs against replay. The method of determining a valid SCK-VN and, therefore, of identifying a replay is outside the scope of the present document. The SCKN is input to TA51 and TA53 and output from TA52 and TA54.

A key identified by an SCKN may be an SCK or an SCKX. Therefore, SCKs and SCKXs may be contained within the same SCK set. An SCK with an allocated SCKN and SCK-VN may be replaced by an SCKX with the same SCKN and different SCK-VN, and an SCKX with allocated SCKN and SCK-VN may be replaced by an SCK with the same SCKN and different SCK-VN.

SCKNs 1 to 30 may be used for DMO. SCKNs 1 to 32 may be used in TMO on a network that only uses security class 2. SCKNs 31 and 32 may be used for a network that normally uses security class 3, but that uses security class 2 in a fallback mode. If a network uses an encryption algorithm from TEA set A and an encryption algorithm from TEA set B on the same BS, an SCK and an SCKX may be in use in the same cell. As the BS can only indicate that a single SCKN with a specific version number SCK-VN is in use, the SCK and the SCKX used with the two algorithms in this case shall have the same SCKN and SCK-VN. Therefore the SCK set assigned to an MS that negotiates an algorithm from TEA set A with the SwMI shall be different from the SCK set assigned to an MS that negotiates an algorithm from TEA set B with the SwMI, as each set will contain a different key assigned to the same SCKN and SCK-VN.

SCK-VN shall be referenced by one bit in the encryption mode element of the MAC RESOURCE PDU of the encrypted message to select the active SCK or SCKX. The value of this bit shall equal the value of the least significant bit of SCK-VN.

4.2.4.0c Distribution of SCK

When distributing SCK to an individual by an OTAR mechanism (algorithms TA51 and TA52) to an MS that has negotiated an encryption algorithm from TEA set A and is provisioned with K, a Session Key for OTAR (KSO) may be used to protect the SCK, alternatively an Extended Group Session Key for OTAR (EGSKO) derived from a Group Session Key for OTAR (GSKO) may be used. The signalling shall indicate the sealing key in use. KSO shall be individual to each MS and shall be derived from an MS's authentication key K and a random seed for OTAR RSO, using algorithm TA41.

If an MS is provisioned with authentication key K2 and has negotiated an encryption algorithm from TEA set A, the KSO used to protect the SCK shall be derived from an Extended Session Key for OTAR KSOX by algorithm TA104, and then the SCK shall be sealed using algorithm TA51. In this case, KSOX is derived from authentication key K2 and a Random Seed for OTAR (RSO) using algorithm TA42. Alternatively, an EGSKO derived from a GSKO may be used to protect the SCK.

When distributing an SCK to a group by OTAR and where an encryption algorithm from TEA set A is in use, an EGSKO derived from GSKO shall be used as the sealing key, as described in clause 4.2.5, whether the MS is provisioned with K or provisioned with K2.

An SCK may be distributed to an MS that has negotiated an encryption algorithm from TEA set B and is therefore provisioned with K2. In this case, the KSO used to protect the SCK shall be derived from a KSOX by algorithm TA104, where KSOX is derived from authentication key K2 and a Random Seed for OTAR (RSO) using algorithm TA42, and then the SCK shall be sealed using algorithm TA51. The SCK may also be sealed for distribution to a group of MSs. In this case, the SCK shall be sealed using an EGSKO derived from a GSKOX by algorithm TA104, instead of by a KSO.

NOTE: As described in the previous paragraphs, the sealing mechanisms for SCK when distributed to a group of MSs that are provisioned with K2 are different depending on whether an MS has negotiated an encryption algorithm from TEA set A or from TEA set B. This allows MSs that are provisioned with K2 but have negotiated an algorithm from TEA set A to use the same GSKO and CMG GSSI as MSs that are provisioned with K. It also allows MSs that have negotiated an algorithm from TEA set B to use the same GSKOX to distribute SCK as is used to distribute SCKXs and GCKXs.

The OTAR protocol for distributing SCKs indicates the air interface encryption algorithm for which the SCK is to be used.

An SCK may be distributed to an MS that has migrated. The mechanism is described in clause 4.2.5a.

4.2.4.0d Distribution of SCKX

When distributing an SCKX to an individual MS by an OTAR mechanism (algorithms TA53 and TA54) a Session Key for OTAR KSOX may be used to protect the SCKX, alternatively an extended Group Session Key for OTAR GSKOX may be used. The signalling shall indicate the sealing key in use. KSOX shall be individual to each MS and shall be derived from an MS's authentication key K2 and a Random Seed for OTAR (RSO) using algorithm TA42.

When distributing an SCKX to a group by OTAR a GSKOX shall be used as the sealing key, as described in clause 4.2.5.

The OTAR protocol for distributing SCKs and SCKXs indicates the air interface encryption algorithm for which the SCK or SCKX is to be used.

An SCKX may be distributed to an MS that has migrated. The mechanism is described in clause 4.2.5a.

4.2.4.0e Decryption of sealed SCK and SCKX

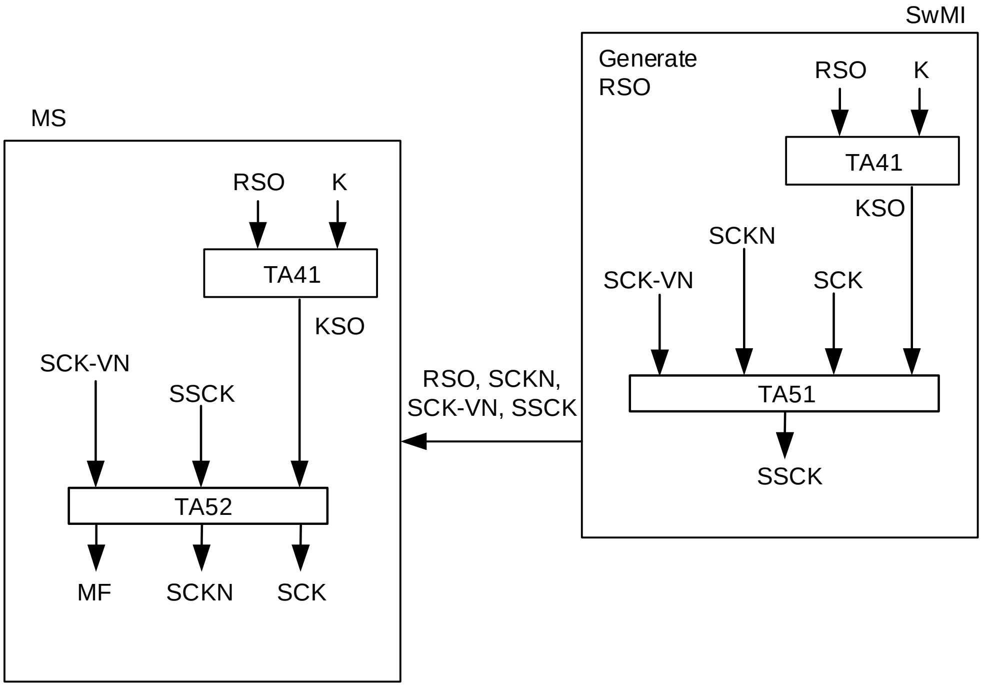
The result of the application of TA51 to SCK, SCK-VN, KSO (or KSOv when migrated) and SCKN shall be a Sealed Static Cipher Key (SSCK). To allow recovery of sealed SCK and SCKN sent to an individual MS at the MS, SCK-VN and RSO shall be distributed together with SSCK. Similarly, application of TA53 to SCKX, SCK-VN, KSOX (or KSOXv when migrated) and SCKN shall be an Extended Sealed Static Cipher Key (SSCKX). To allow recovery of sealed SCKX and SCKN sent to an individual MS at the MS, SCK-VN and RSO shall be distributed together with SSCKX. Alternatively, the GSKO-VN of the GSKO used to seal the SCK or the GSKO-VN of the GSKOX used to seal the SCKX shall be provided where the sealed SCK or SCKX is sent to a group of MSs.

To allow the MS to discover if SCK or SCKX has been corrupted due to transmission errors or manipulation, TA51 and TA53 introduce some redundancy into the Sealed Static Cipher Key (SSCK or SSCKX). Algorithms TA51 and TA53 take the Static Cipher Key Version Number (SCK-VN) and the Static Cipher Key Number (SCKN), as additional inputs. The SCK-VN is also provided to algorithms TA52 and 54. The redundancy is checked by TA52 or TA54 respectively. A detected manipulation shall be indicated by setting the manipulation flag MF.

When distributing an SCK or SCKX by OTAR, the MNI for the TMO network or DMO network in which the SCK or SCKX applies shall be provided in the OTAR transaction if that network is different from the serving network. If an SCK or SCKX is for use in a DMO network that uses the "Open MNI", the "Open MNI" value shall be provided in the transaction.

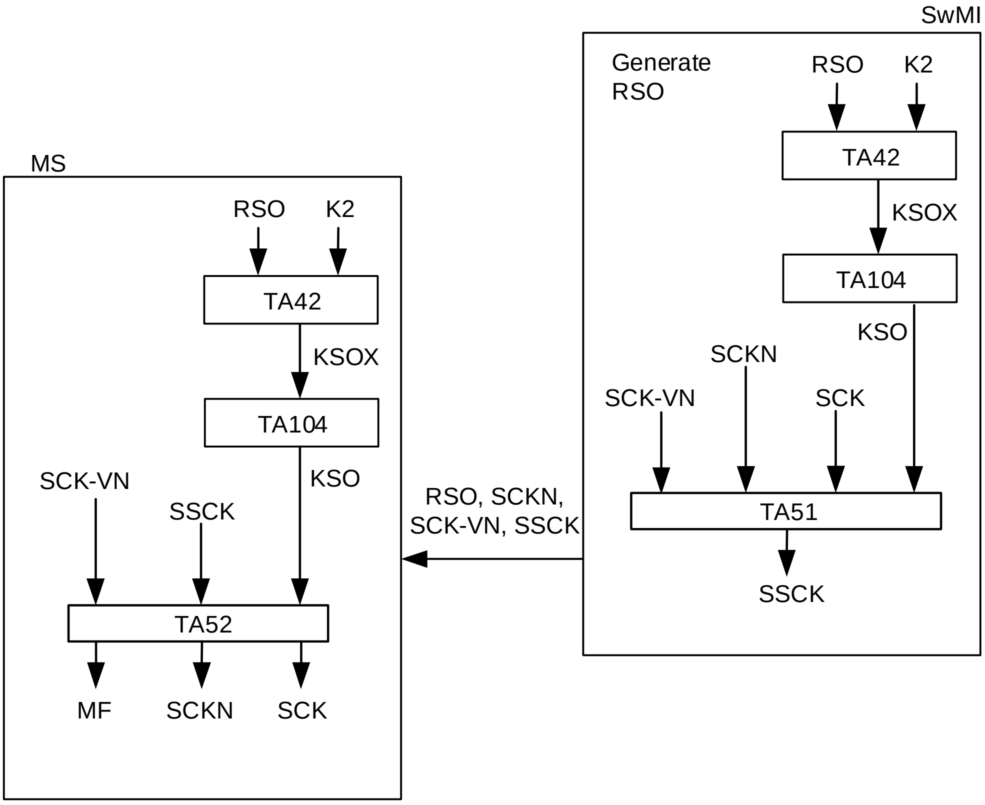
4.2.4.0f Summary of SCK distribution process

Distribution of SCK to an MS is shown in Figure 4.11 and Figure 4.11a, and distribution of an SCKX to an MS is shown in Figure 4.11b.



NOTE: EGSKO is input to TA51 and TA52 instead of KSO for distribution to a group, and may be input to TA51 and TA52 instead of KSO for distribution to an individual MS.

Figure 4.11: Distribution of SCK to an MS that is provisioned with K

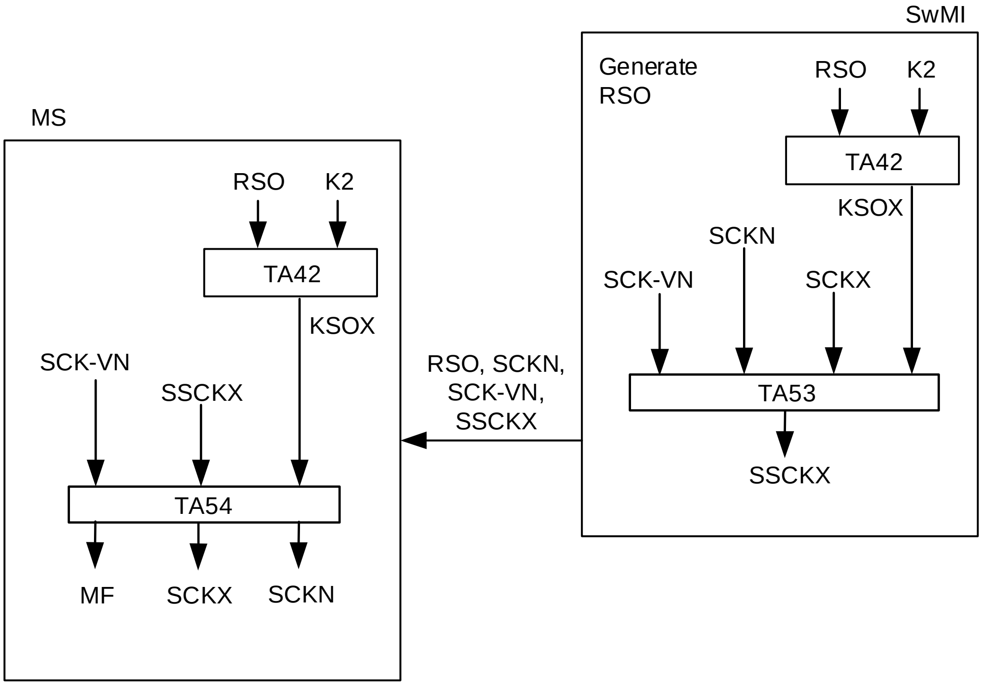


NOTE 1: In the case of SCK distribution to a group where TEA set A is in use, EGSKO derived from GSKO is input to TA51 and TA52 instead of KSO.

NOTE 2: In the case of SCK distribution to a group where TEA set B is in use, EGSKO derived from GSKOX using TA104 is input to TA51 and TA52 instead of KSO.

NOTE 3: EGSKO may also be input to TA51 and TA52 instead of KSO for distribution of SCK to an individual MS

Figure 4.11a: Distribution of SCK to an MS that is provisioned with K2



NOTE: In the case of SCKX distribution to a group, GSKOX is input to TA53 and TA54 instead of KSOX. GSKOX may also be input to TA53 and TA54 instead of KSOX for distribution to an individual MS.

Figure 4.11b: Distribution of SCKX to an MS

4.2.4.1 SCK association for DMO use

4.2.4.1.0 General

The OTAR service provided in TMO may also be used to provide key management for DMO. The OTAR service allows SCKs and SCKXs to be provided for use in DMO, and for one or more provided SCKs or SCKXs to be associated with one or more groups in DMO. The purpose of associating more than one SCK or SCKX with a DMO group is to allow different SCKs or SCKXs to be active at different periods of time in DMO. Associations can be formed for single SCKs or SCKXs or for SCK subsets, where an SCK subset may include SCKs or SCKXs or both.

To allow the OTAR service to provide SCKs or SCKXs for use in more than one DMO network, the MNI for the intended network shall be provided with the association if the DMO network has a different MNI from the serving network. The MNI provided with the association shall also be used to specify the SCK set from which the associated SCK or SCKX is to be taken. It shall not be possible to associate an SCK or SCKX from one SCK set, identified by an MNI, for use in a different network to that of the SCK set, i.e. the MNIs of the SCK set and the network in which the association applies shall be the same.

4.2.4.1.1 DMO SCK subset grouping

For each DMO group call where encryption is to be applied, the MS should have a means to associate one or more SCKs or SCKXs with the GTSI to be called. The means of associating SCKs and SCKXs with GTSIs may be achieved using air interface signalling.

An SCK or SCKX should have a defined lifetime or crypto period. At the end of this crypto period, it should be replaced. Replacement is achieved when the MS selects a different SCK or SCKX for transmission. However, as DMO is an uncontrolled environment, different MSs may change their SCK or SCKX selection at different times. To overcome the possibilities for communication failure, SCKs and SCKXs may be grouped into one or more subsets to facilitate the key management process. The SCKs and SCKXs within a subset shall all be taken from the same SCK set, and therefore shall all be associated with the same MNI.

Keys in different subsets associated with the same GTSI(s) are referred to by the term Key Association Group (KAG). The MS shall consider one SCK or SCKX of the KAG as current and shall use this SCK or SCKX as the key for transmission. Any SCK or SCKX of the KAG may be used for reception. The SCKs and SCKXs within a KAG shall all be taken from the same SCK set, and therefore shall all be associated with the same MNI.

EXAMPLE 1: If SCKN#3, SCKN#13, SCKN#23 are members of the same KAG and an MS transmits using SCKN#13 then it shall also be prepared to receive using SCKN#3, SCKN#13, SCKN#23.

A KAG should only contain SCKs or SCKXs but not both, and all keys within a KAG should be associated with the same KSG. However, exceptionally a KAG may contain both SCKs and SCKXs if an MS needs to transition to use of a different air interface encryption algorithm at the start of a new crypto period. In this case, the SCK(s) shall be associated with a KSG in TEA set A, and the SCKXs associated with a KSG in TEA set B.

NOTE: Considerations for transition from a KSG in TEA set A to a KSG in TEA set B are provided in Annex D of the present document.

An SCK subset may contain both SCKs and SCKXs, for example if an MS needs to communicate with different groups of MSs that use different air interface encryption algorithms. Each SCK or SCKX is associated with an air interface encryption algorithm by the OTAR signalling that provides the SCK or SCKX.

The SCKs or SCKXs within the subsets can be activated separately or synchronized and activated together. If an entire subset of SCKs and SCKXs is to be activated together, the crypto periods of all SCKs and all SCKXs in the subset shall be the same, and the SCK-VNs of all SCKs and all SCKXs in a subset shall also be the same.

Subset groups shall be identified by the SCK subset grouping type as shown in Table 4.2 and the membership of each resulting subset shall be identified as shown in Table 4.3.

The SCK subset numbering shall be determined by the SCK subset grouping type. In all cases, SCK subset grouping type = 1 corresponds to the subset with SCKN = 1 as the first value. Other SCK subset grouping types are determined according to Table 4.3.

Table 4.2: SCK subset grouping type definitions

SCK subset grouping type	Maximum number of SCK subsets (n)	Maximum number of SCKs and SCKXs per subset (m)	Remarks
0	1	30	Default.
1	2	15	
2	3	10	Suited for past-present-future mode of operation.
3	4	7	Only 28 keys of 30 are associated to groups.
4	5	6	
5	6	5	
6	7	4	Only 28 keys of 30 are associated to groups.
7	10	3	
8	15	2	
9	30	1	
NOTE: The maximum number of SCKs and SCKXs per subset is limited to 30, as SCKNs 31 and 32 are reserved for TMO use.			

Table 4.3: Membership by SCKN value of each subset of each SCK subset grouping type

SCK subset number	SCK subset grouping type							
	1	2	3	4	5	6	7	8
1	1 to 15	1 to 10	1 to 7	1 to 6	1 to 5	1 to 4	1 to 3	1 to 2
2	16 to 30	11 to 20	8 to 14	7 to 12	6 to 10	5 to 8	4 to 6	3 to 4
3	X	21 to 30	15 to 21	13 to 18	11 to 15	9 to 12	7 to 9	5 to 6
4	X	X	22 to 28	19 to 24	16 to 20	13 to 16	10 to 12	7 to 8
5	X	X	X	25 to 30	21 to 25	17 to 20	13 to 15	9 to 10
6	X	X	X	X	26 to 30	21 to 24	16 to 18	11 to 12
7	X	X	X	X	X	25 to 28	19 to 21	13 to 14
8	X	X	X	X	X	X	22 to 24	15 to 16
9	X	X	X	X	X	X	25 to 27	17 to 18
10	X	X	X	X	X	X	28 to 30	19 to 20
11	X	X	X	X	X	X	X	21 to 22
12	X	X	X	X	X	X	X	23 to 24
13	X	X	X	X	X	X	X	25 to 26
14	X	X	X	X	X	X	X	27 to 28
15	X	X	X	X	X	X	X	29 to 30
NOTE 1: For SCK subset grouping type = 9 (not shown), 30 subsets of 1 key each, the SCK subset number is equal to the SCKN, i.e. SCK subset number = 1 signifies SCKN = 1 and so on. NOTE 2: A table entry given by "X" indicates an illegal value that shall not be used. NOTE 3: For SCK subset grouping type = 0 (not shown), 1 subset of 30 keys, the SCK subset number is always 1.								

All SCKNs in a KAG shall be associated with a GTSI by implication when the SCKN in that KAG that is in subset#1 is associated with that GTSI.

The association of SCKNs within a KAG with any GTSI can also be determined from the following formula:

where:

- SCK(i) are the members of a KAG;
- SCK(f) is the associated SCKN in the first subset; and
- there are (n) subsets, each containing (m) member SCKs or SCKXs.

Then:

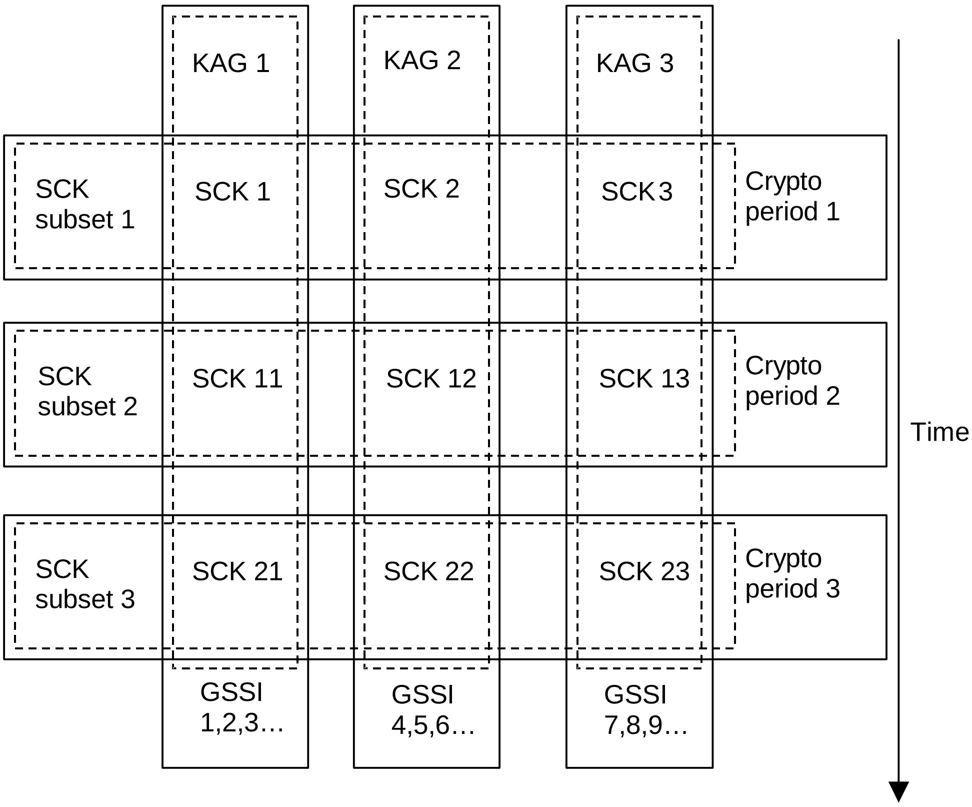
```
For j = 0 to (n-1)
{
    i = f + m × j
}
```

EXAMPLE 2: Associating GTSI#22 with SCKN#3 in SCK subset grouping type 2 implies association of SCKN#3, SCKN#13 and SCKN#23 with GTSI#22, i.e. SCKN#3, SCKN#13, SCKN#23 are members of the same KAG.

EXAMPLE 3: Associating GTSI#22 with SCKN#3 in SCK subset grouping type 4 implies association of SCKN#3, SCKN#9, SCKN#15, SCKN#21 and SCKN#27 with GTSI#22, i.e. SCKN#3, SCKN#9, SCKN#15, SCKN#21 and SCKN#27 are members of the same KAG.

EXAMPLE 4: If SCK subset grouping type = 2 (corresponding to 3 subsets of 10 keys), then n = 3, m = 10, and if f = 5, then SCKN = 5, SCKN = 15 and SCKN = 25 shall be associated with the same GTSI and are members of the same KAG.

EXAMPLE 5: Figure 4.12 shows an example of key association for SCK subset grouping type = 2.



NOTE: GSSI is used in this figure to represent GTSI.

Figure 4.12: Example of key association for SCK subset grouping type = 2

4.2.5 The Group Session Key for OTAR

4.2.5.0 General

In some cases keys may need to be distributed to groups as identified by GTSI. In order to allow the sealing mechanisms described in clauses 4.2.2 and 4.2.4 to operate, KSO shall be replaced by an Extended Group Session Key for OTAR. An extended Group Session Key for OTAR may be an EGSKO derived using algorithm TB7 from a Group Session Key for OTAR (GSKO), which is used to provide cipher keys for use with one of the air interface encryption algorithms from TEA set A, or may be a GSKOX which is used to provide cipher keys for use with one of the air interface encryption algorithms from TEA set B.

4.2.5.0a Validity of GSKO and GSKOX

The MS shall consider a GSKO or GSKOX as valid only within one network. The MS may hold different GSKOs or GSKOXs for use in more than one network; in this case the MS shall reference the GSKO or GSKOX to the MNI of the network in which the GSKO or GSKOX is valid. The MS may only hold either GSKO or GSKOX for use with one network, and shall not store both a GSKO and GSKOX for that network. Whether the MS holds GSKO or GSKOX valid for a particular network is dependent on the KSG negotiated by the MS with the SwMI for use on that network. If the MS has negotiated a KSG from TEA set A it may only hold GSKO, and if the MS has negotiated a KSG from TEA set B it may only hold GSKOX. The SwMI may use the GSKO to distribute SCKs for use in networks other than the serving network, or the GSKOX to distribute SCKXs for use in networks other than the serving network, however the GSKO or GSKOX valid in the serving network shall be used to protect those keys.

A GSKO or GSKOX is associated with a version number GSKO-VN. An MS may hold more than one version of GSKO or GSKOX distinguished by version number to allow change of active GSKO or GSKOX at the end of a crypto period.

4.2.5.0b Distribution of GSKO and GSKOX

The SwMI shall only provide a GSKO or GSKOX that is valid in the serving network.

When distributing GSKO by an OTAR mechanism (algorithms TA91 and TA92) a session key for OTAR (KSO) shall be used to protect the GSKO. KSO shall be individual to each MS and shall be derived from an MS's authentication key (K) and a random seed RSO with algorithm TA41, as for distribution of SCK and GCK. If an MS is provisioned with authentication key K2, KSO is derived from KSOX using algorithm TA104, where KSOX is derived from K2 and a random seed RSO using algorithm TA42.

When distributing GSKOX by an OTAR mechanism (algorithms TA93 and TA94) a session key for OTAR (KSOX) shall be used to protect the GSKOX. KSOX shall be individual to each MS and shall be derived from an MS's authentication key (K2) and a random seed RSO with algorithm TA42, as for distribution of SCKX and GCKX.

The GSKO or GSKOX has an associated version number, GSKO-VN, which can be used for replay protection.

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

Algorithm TA93 is used with GSKOX, KSOX and GSKO-VN as inputs to produce a sealed key SGSKOX for transmission to an MS. Recovery of GSKOX from SGSKOX is achieved using algorithm TA94 in conjunction with KSOX and GSKO-VN as inputs. A manipulation flag MF provides assurance of correct recovery.

The process is summarized in Figures 4.13, 4.13a and 4.13b below.

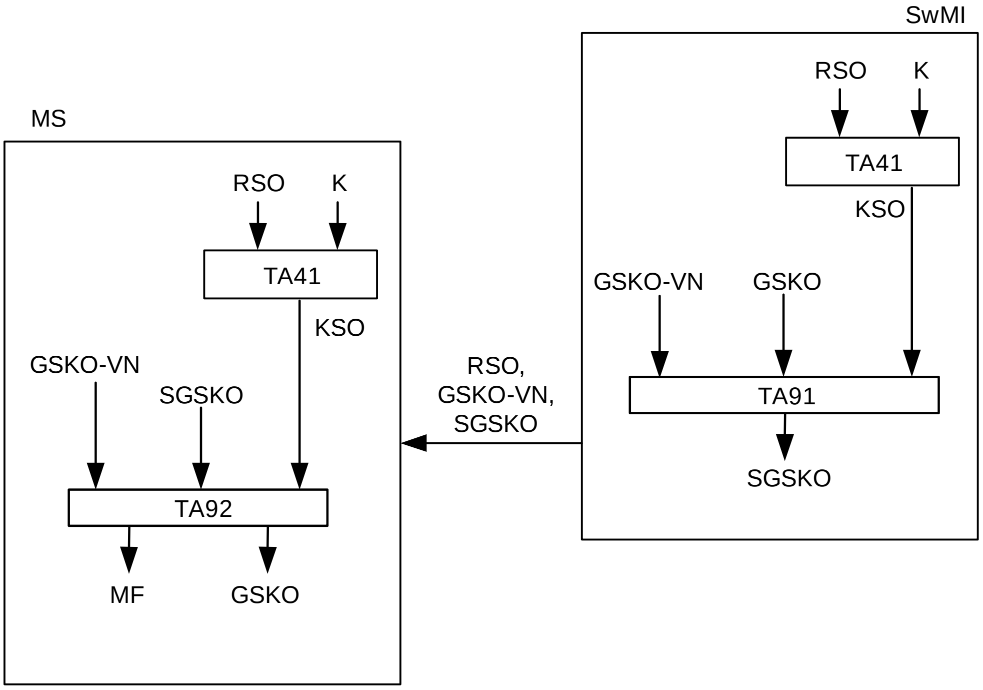


Figure 4.13: Distribution of GSKO to an MS that is provisioned with K

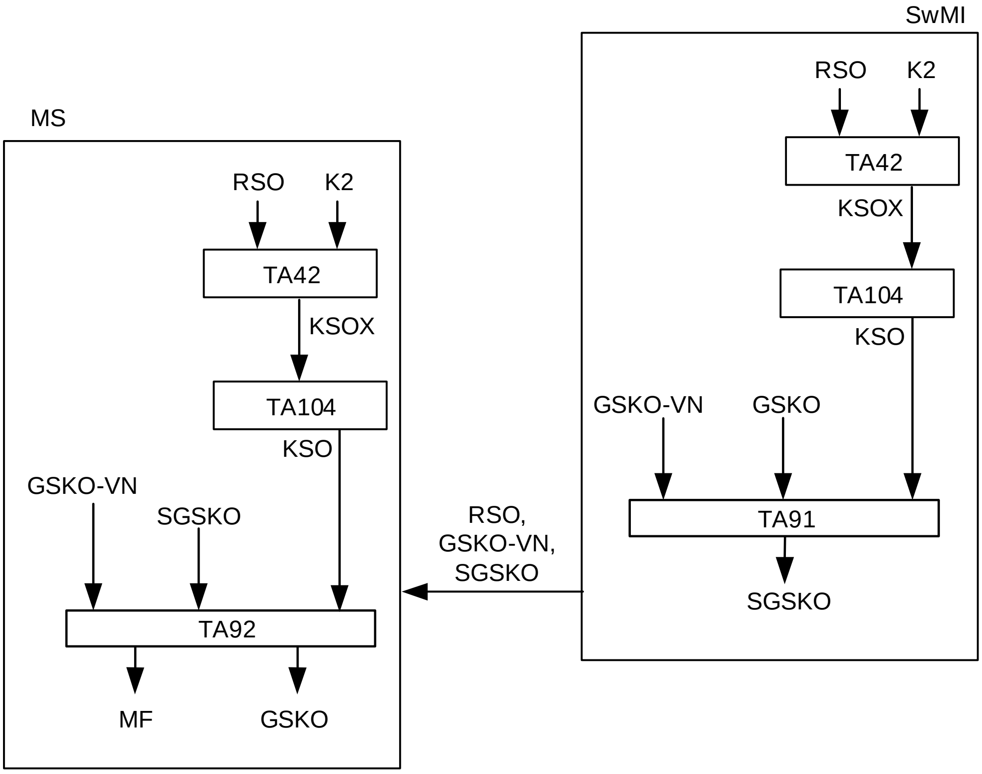


Figure 4.13a: Distribution of a GSKO to an MS that is provisioned with K2

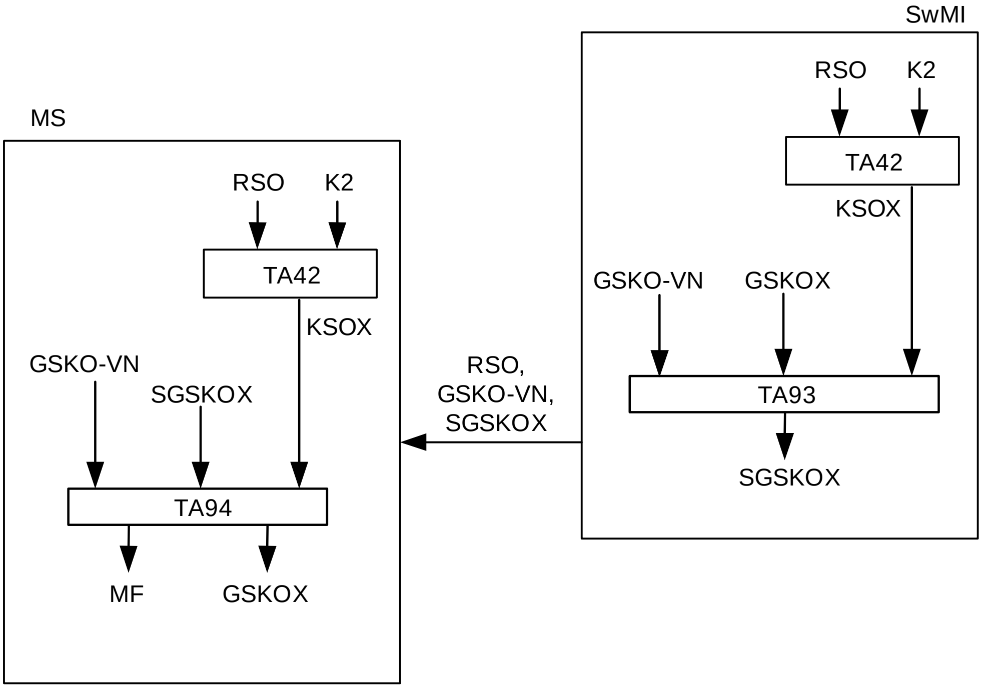


Figure 4.13b: Distribution of GSKOX to an MS

4.2.5.1 SCK and SCKX distribution to groups with OTAR

When distributing SCK to a group EGSKO shall be used in place of KSO as input to algorithms TA51 and TA52. Signalling shall indicate if the distributed SCK is sealed with EGSKO instead of KSO (refer to Figure 4.11). In this case the mechanism shall be as shown in Figure 4.11 with TA41 not invoked and KSO replaced by EGSKO.

EGSKO is derived from GSKO using algorithm TB7 as shown in Figure 4.14.

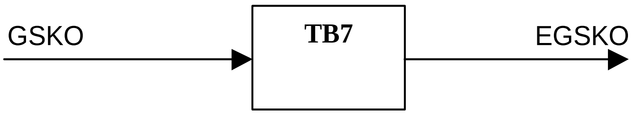


Figure 4.14: Generation of EGSKO using TB7

When distributing SCKX to a group, GSKOX shall be used in place of KSOX as input to algorithms TA53 and TA54. Signalling shall indicate if the distributed SCKX is sealed with GSKOX instead of KSOX (refer to Figure 4.11b). In this case the mechanism shall be as shown in Figure 4.11b with TA42 not invoked and KSOX replaced by GSKOX.

4.2.5.2 GCK and GCKX distribution to groups with OTAR

When distributing GCK to a group, EGSKO shall be used in place of KSO as input to algorithms TA81 and TA82. Signalling shall indicate that the distributed GCK is sealed with EGSKO. In this case the mechanism shall be as shown in Figure 4.9 with TA41 not invoked and KSO replaced by EGSKO.

When distributing GCKX to a group, GSKOX shall be used in place of KSOX as input to algorithms TA83 and TA84. Signalling shall indicate that the distributed GCKX is sealed with GSKOX. In this case the mechanism shall be as shown in Figure 4.9a with TA42 not invoked and KSOX replaced by GSKOX.

4.2.5.3 Rules for MS response to group key distribution

Where a key is provided to the MS using a group addressed transmission, and using the GSKO or GSKOX for key encryption, the MS shall determine whether to respond to the group addressed OTAR distribution as follows:

- if the transmission explicitly requires MSs to respond, each MS shall respond to inform the SwMI of the success (or failure) of the transaction following expiry of timer T371 that is set to a random value on receipt of the OTAR provision;
- if the transmission does not explicitly require MSs to respond, an MS shall respond following the expiry of T371 on receipt of the OTAR provision, only if the transmission provides that MS with a key or a version of a key that the MS does not have stored;
- if the transmission does not explicitly require MSs to respond, and the transmission does not provide an MS with a key or a version of a key that the MS does not have stored, that MS shall not respond.

The maximum value to which the timer T371 may be set by the MS is provided by the SwMI.

If an MS is required to respond for one of the reasons given above, but needs to leave the SwMI by sending ITSI-Detach signalling the MS shall consider T371 to have terminated at this point, and should send the response to the OTAR signalling before detaching from the SwMI.

NOTE: If the MS is unable to send the response there is no requirement to store the response.

4.2.5a OTAR of migrated MS

4.2.5a.1 Visited Session Keys for OTAR

When distributing GCK, SCK or GSKO to a migrated MS, a visited session key for OTAR KSOv shall be used instead of KSO, if the Cipher Key CK is to be sealed by an individual session key. An EGSKO valid in the visited SwMI may alternatively be used instead of KSOv when distributing SCK or GCK to an individual MS or to a group of MSs. Similarly, when distributing GCKX, SCKX or GSKOX to an MS who has migrated, an extended visited session key for OTAR KSOXv shall be used instead of KSOX, if the extended Cipher Key CKX is to be sealed by an individual session key. A GSKOX valid in the visited SwMI may alternatively be used instead of KSOXv when distributing SCKX or GCKX to an individual MS or to a group of MSs.

4.2.5a.2 Derivation of KSOv

KSOv may be derived by the home SwMI by modifying KSO in an algorithm TA101, and may be provided to the visited SwMI. The inputs to TA101 shall be the MNI of the visited network designated MNIv, GCK0 (a designated session key modifier key) and KSO (the output of TA41).

The process is illustrated in Figure 4.14a below.

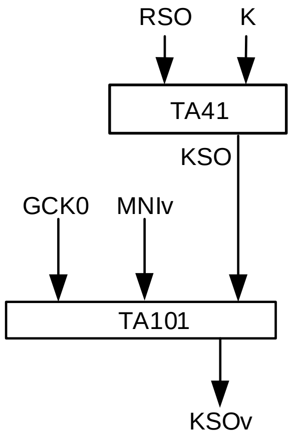


Figure 4.14a: Derivation of KSOv from KSO

When the value of GCK0 is zero (i.e. the key designated as GCK0 consists of 80 zeros), or if either the MS or the home SwMI does not support the use of GCK0, algorithm TA101 shall not be invoked and KSOv shall have the same value as KSO.

4.2.5a.3 Derivation of KSOXv

KSOXv may be derived by the home SwMI by modifying KSOX in an algorithm TA103, and may be provided to the visited SwMI. The inputs to TA103 shall be the MNI of the visited network designated MNIv, GCKX0 (a designated session key modifier key) and KSOX (the output of TA42).

The process is illustrated in Figure 4.14b below.

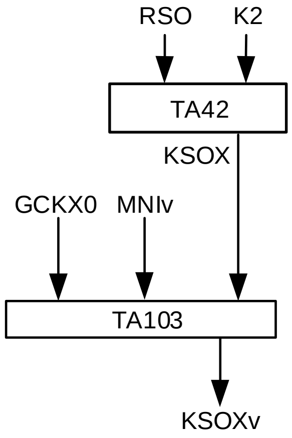


Figure 4.14b: Derivation of KSOXv from KSO

When the value of GCKX0 is zero (i.e. the key designated as GCKX0 consists of 192 zeros), or if either the MS or the home SwMI does not support the use of GCKX0, algorithm TA103 shall not be invoked and KSOXv shall have the same value as KSOX.

4.2.5a.4 OTAR of CKX to migrated MS where home SwMI supports an air interface encryption algorithm from TEA set A

If the MS last negotiated one of algorithms from TEA set A with the home SwMI but is required to use one of the algorithms from TEA set B by the visited SwMI and if OTAR of CKX is required in the visited SwMI, the home SwMI may provide the visited SwMI with a KSOv to enable OTAR in the visited SwMI. The visited SwMI shall derive a KSOXv for the use of OTAR in that visited SwMI from the provided KSOv using algorithm TA105. When a sealed CKX is provided to the MS by the visited SwMI together with the RSO and CK-VN, the MS shall derive the same KSOXv by first generating a KSOv using the RSO provided in the OTAR transaction using algorithm TA41 and key K, and then shall derive a KSOXv using TA105; the KSOXv is used to decrypt the provided sealed CKX.

NOTE 1: The CKX is sealed with a key derived from a shorter key encryption key (KSOv) than the CKX. The security policy of the vSwMI should take this into account.

Key modification of the KSOv may be applied by the home SwMI using GCK0 and algorithm TA101 prior to providing the KSOv to the visited SwMI, and in this case the MS shall also apply key modification using GCK0 and TA101 to the KSOv before deriving the KSOXv using algorithm TA105. The process is illustrated in Figure 4.14c below.

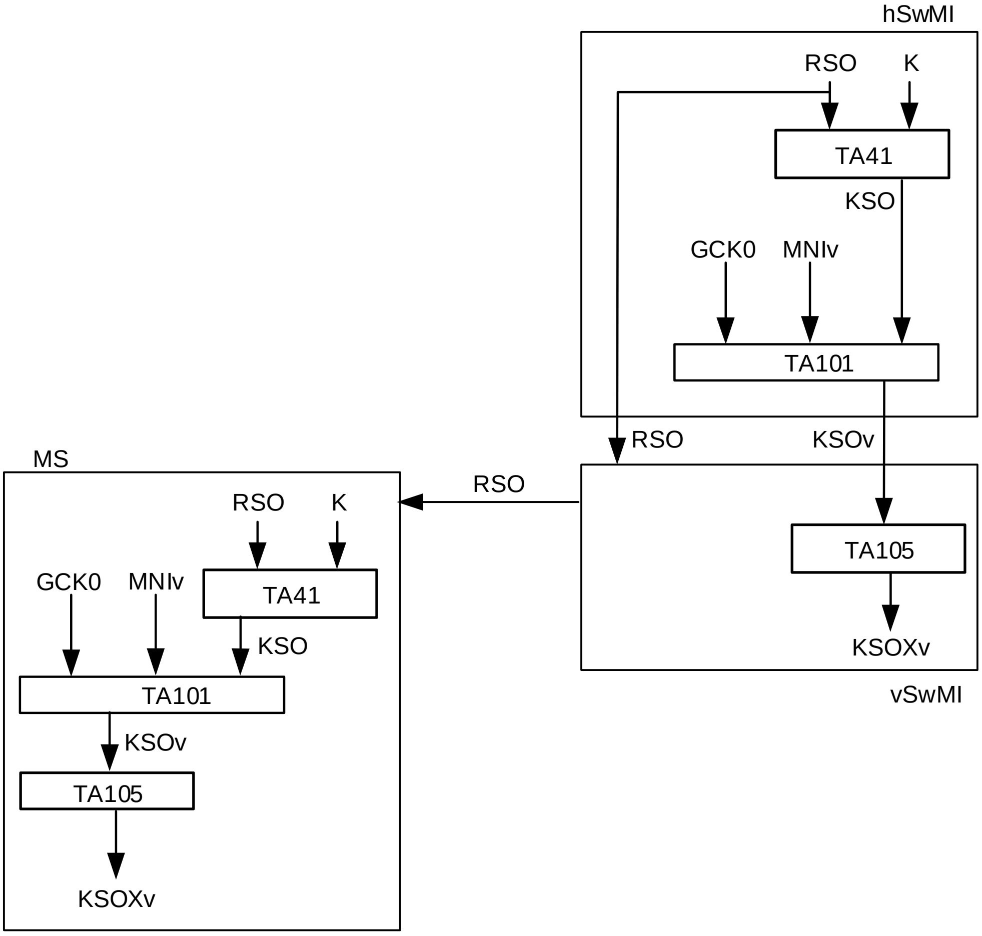


Figure 4.14c: Derivation of KSOX to where MS uses an algorithm from TEA set A in home SwMI

NOTE 2: The MS negotiates the algorithm in use in the visited SwMI according to the mechanisms described in clause 6.

NOTE 3: The means by which the home SwMI decides whether to provide a KSO or a KSOX to the visited SwMI to permit OTAR of a migrating MS is outside the scope of the present document.

4.2.5a.5 OTAR of CK to migrated MS where home SwMI supports an air interface encryption algorithm from TEA set B

If the MS last negotiated one of the algorithms from TEA set B with the home SwMI but is required to use one of the algorithms from TEA set A by the visited SwMI and if OTAR of CK is required in the visited SwMI, the home SwMI may provide the visited SwMI with a KSOv to enable OTAR in the visited SwMI. The home SwMI shall derive a KSOv for the use of OTAR in the visited SwMI by first generating a KSOXv for the MS using the key K2 of the MS and random seed RSO with algorithm TA42, and then shall derive the KSOv using algorithm TA104. KSOv shall be provided to the visited SwMI together with RSO. When a sealed CK is provided to the MS by the visited SwMI together with the RSO and CK-VN, the MS shall derive the same KSOv as that provided to the visited SwMI by first generating a KSOXv using the RSO provided in the OTAR transaction using algorithm TA42 and key K2, and then shall derive a KSOv using TA104; the KSOv is used to decrypt the provided sealed CK.

Key modification of the KSOXv may be applied by the home SwMI using GCKX0 and algorithm TA103 prior to deriving the KSOv that is provided to the visited SwMI, and in this case the MS shall also apply key modification using GCKX0 and TA103 to the KSOXv before deriving the KSOv using algorithm TA104. The process is illustrated in Figure 4.14d below.

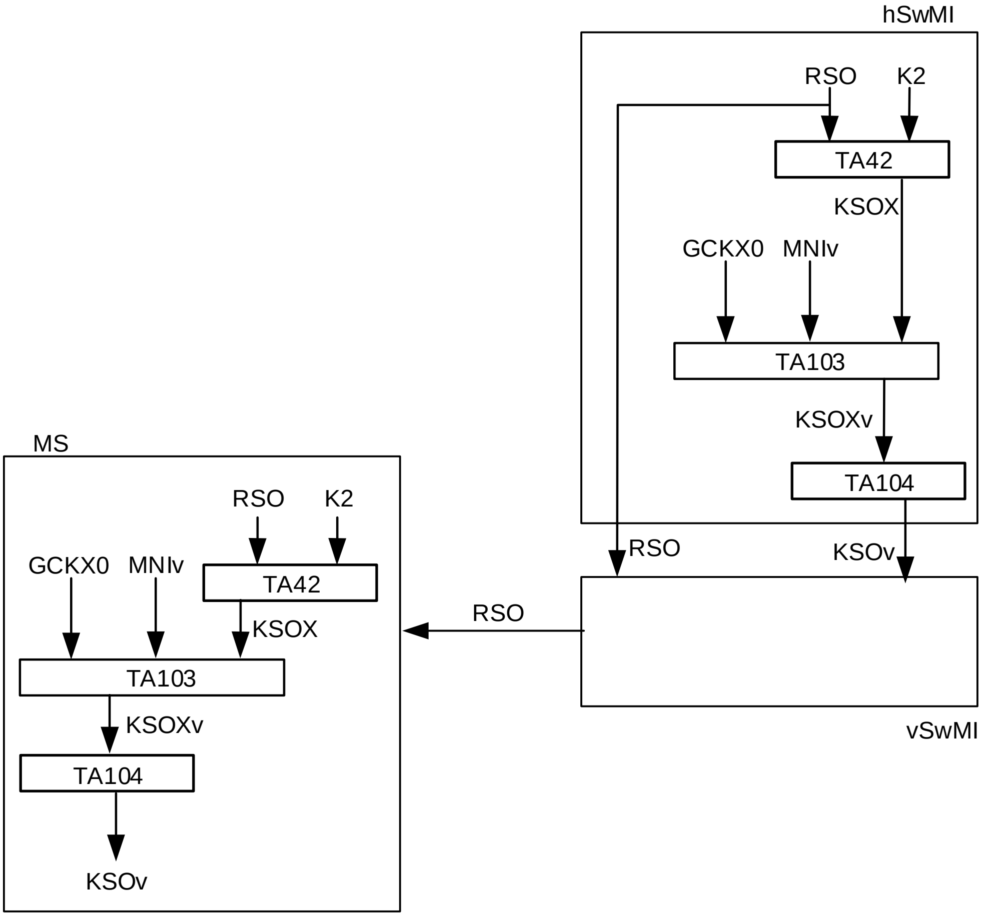


Figure 4.14d: Derivation of KSO where MS uses an algorithm from TEA set B in the home SwMI

NOTE 1: The MS negotiates the algorithm in use in the visited SwMI according to the mechanisms described in clause 6.

NOTE 2: The means by which the SwMI decides whether to provide a KSO or a KSOX to permit OTAR of a migrating MS is outside the scope of the present document.

4.2.6 Encrypted Short Identity (ESI) mechanism

The ESI mechanism provides 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 ETSI EN 300 392-1 [1], clause 7.

NOTE 1: 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 SSI types.

NOTE 2: The broadcast address as defined in ETSI EN 300 392-1 [1] is a reserved value of the group address so ESI applies to it.

The ESI mechanism may be used where MSs have negotiated a KSG from TEA set A or a KSG from TEA set B (see clause 6.3.1). Where all MSs in a cell or in a SwMI have negotiated a single KSG from TEA set B, the ESI mechanism described in this clause may be replaced by the MAC Address Encryption (MAE) mechanism described in clause 6.7.1.2a, in which case the ESI mechanism described in this clause shall not be applied.

NOTE 3: If more than one KSG from TEA set B is in use in an LA, the ESI mechanism needs to be used.

This clause describes a mechanism that allows the encryption of the SSI segment of addresses used by layer 2. The event label and usage marker shall not be encrypted by this mechanism. USSI and SMI shall not be encrypted by this mechanism. The mechanism is valid only for networks with air interface encryption applied. The mechanism shall be integrated with the use of CCK within a location area in cells of security class 3, or with SCK for cells of security class 2. Whenever encrypted signalling is used, indicated by setting the "Encrypted flag" in uplink MAC PDUs and by the "Encryption mode" element in downlink MAC PDUs, the ESI shall be sent instead of the true identity.

Where any MS served by a BS in an LA has negotiated a KSG from TEA set A, all BSs and all MSs in the LA shall use ESI with TA61 for identity encryption, as shown in Figure 4.15. An MS negotiating a KSG from TEA set A at initial registration shall use TA61 identity encryption. A BS shall indicate the use of TA61 identity encryption to an MS that negotiates a KSG from TEA set B by setting the "Identity encryption" element to "1" in the "Security downlink" element sent to the MS in the D-LOCATION UPDATE ACCEPT PDU at initial registration to the network (ITSI-Attach). In this case, the "Security downlink" element shall be included in the D-LOCATION UPDATE ACCEPT PDU sent at initial registration, and the "Additional security" element shall be set to "1" to permit inclusion of the "Identity encryption" element, even if the BS does not need to send cipher keys to the MS. The MS shall store this setting and shall continue to use TA61 encryption for entire period of registration with the network on any LA. In order to make use of TA61, the MS shall derive CCK from CCKX or SCK from SCKX as shown in Figure 4.15a.

NOTE 4: Subsequent transmissions of D-LOCATION UPDATE ACCEPT PDU by a BS, e.g. when the MS performs cell reselection, do not need to include the "Security downlink" element and therefore do not need to indicate the setting of "Identity encryption". Therefore the MS needs to maintain the stored value of "Identity encryption" received at initial registration. However, if the BS needs to send a D-LOCATION UPDATE ACCEPT PDU containing a "Security downlink" element with "Additonal security" set, e.g. to send the MS new cipher keys for use on a new cell when performing cell reselection, the BS needs to set the "Identity encryption" element to the same value that was set during initial registration.

Where all MSs served by the BS have negotiated a KSG from TEA set B, the BS and all MSs may use the MAE mechanism specified in clause 6.7.1.2a instead of the ESI mechanism specified in this clause. In this case, the BS shall indicate use of the MAE mechanism by setting the "Identity encryption" element to "0" if it is sent in "Security downlink" within a D-LOCATION UPDATE ACCEPT PDU at initial registration with the network (ITSI-Attach). If the "Identity encryption" element is not included in "Security downlink" because "Additional security" is set to "0", or if "Security downlink" is not included in the D-LOCATION UPDATE ACCEPT PDU sent at initial registration, an MS negotiating a KSG from TEA set B shall likewise make use of the MAE mechanism and shall store this setting for the entire period of registration with the network.

NOTE 5: As the identity encryption mechanism used by an MS is maintained on cell reselection, it is likely that a region or an entire network will need to use TA61 identity encryption unless all MSs served by the BSs in that region or network have negotiated KSGs from TEA set B. Annex D describes considerations for transition from use of TEA set A to use of TEA set B in a network.

The ESI mechanism uses algorithm TA61 as shown in Figure 4.15.

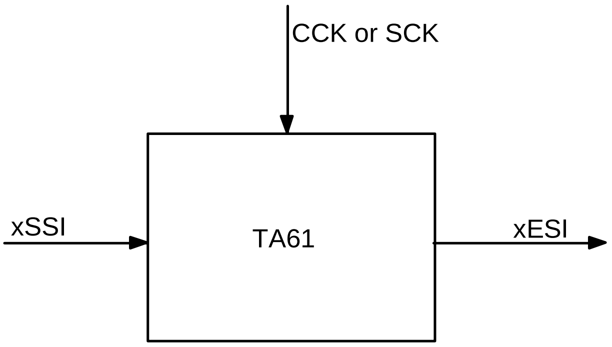


Figure 4.15: Generation of ESI from SSI and a cipher key

An MS that has negotiated a KSG from TEA set B but that has been instructed to use TA61 identity encryption shall derive the CCK from CCKX or shall derive SCK from SCKX using algorithm TA106. The key derivation and identity encryption mechanism in this case is shown in Figure 4.15a.

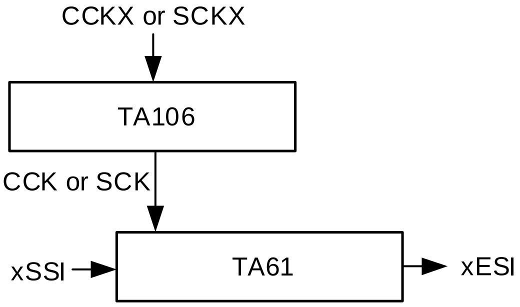


Figure 4.15a: Generation of ESI using TA61 by an MS negotiating a KSG from TEA set B

xSSI are all short addresses valid for the MS (ISSI, GSSI, ASSI, V-ASSI, V-GSSI). The output xESI (IESI, GESI, AESI, V-AESI, V-GESI) shall be a cryptographic address. Only MSs in a location area with the correct values of CCK or SCK shall be able to identify messages addressed for their attention.

If the PDU is encrypted either ESI or MAE shall be used in that PDU. The use of signalling for AI encryption management is more fully described in clause 6.5.

4.2.7 Encryption Cipher Key

Where an air interface encryption algorithm from TEA set A is in use, the Encryption Cipher Key (ECK) shall be derived using algorithm TB5 (Figure 4.16) from a selected CK. The CK shall be one of DCK, CCK, MGCK in class 3 cells, and shall be SCK in class 2 cells. TB5 combines CK with CN, CC and LA identifier to produce ECK. This is to prevent attacks on the encryption process by replaying cipher text to eliminate the keystream, and to prevent keystream replay within the repeat period of the frame numbering system.

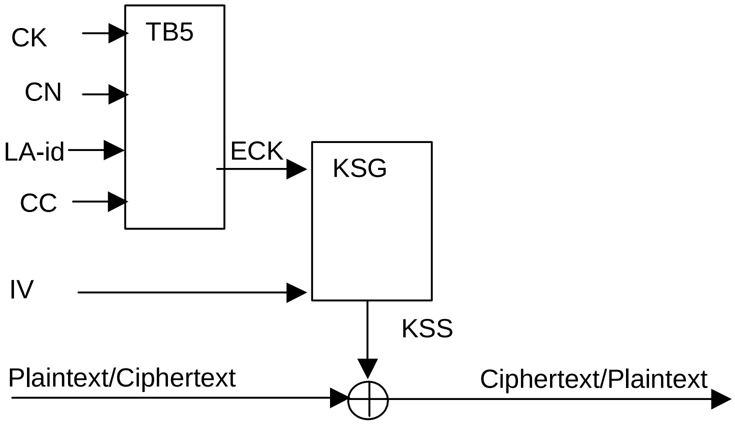


Figure 4.16: Use of TB5 to generate ECK

Where an air interface encryption algorithm from TEA set B is in use, no equivalent ECK generation algorithm is used, as parameters including CN, CC and LA-id are directly input as part of the initialization vector to the KSG (see clause 6).

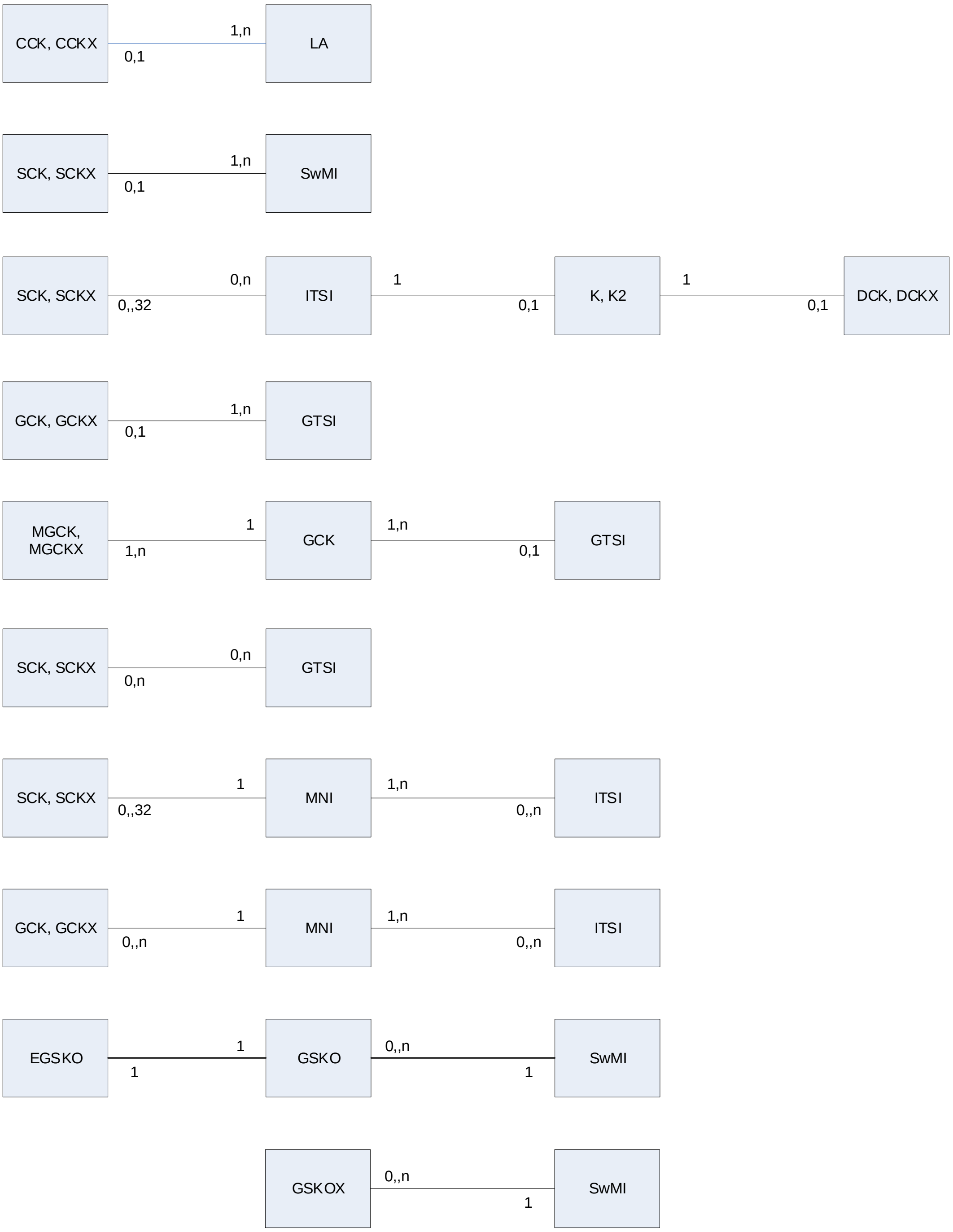
4.2.8 Summary of AI key management mechanisms

Table 4.4 summarizes the pre-conditions and lifetimes for each key.

Table 4.4: Cipher Key pre-conditions and lifetime

Key	Pre-condition	Lifetime (see note 6)
K, K2	None	ITSI (see note 1, note 2)
DCK, DCKX	Authentication	Authentication session (see note 3)
CCK, CCKX	Authentication	Not defined (see note 4)
SCK, SCKX	None	Not defined (see note 2, note 5)
GCK, GCKX	None	Not defined (see note 2, note 5)
MGCK, MGCKX	Authentication	As per CCK
GSKO, GSKOX	None	Not defined (see note 1, note 5)
GCK0, GCKX0	None	Not defined (see note 2, note 5)
NOTE 1: If OTAR is used for GSKO then K is required, and if OTAR is used for GSKOX then K2 is required. NOTE 2: K or GSKO is required for OTAR of SCK and GCK in class 2 and class 3, and K2 or GSKOX is required for OTAR of SCKX and GCKX. NOTE 3: In an MS DCK or DCKX may be deleted on power down, but shall be retained if encrypted registration is required. NOTE 4: CCK or CCKX may be deleted from the MS on power down, but shall be retained if encrypted registration is required. NOTE 5: Generally long life. NOTE 6: Refer to clause 5 for considerations of key storage resulting from invocation of the enable-disable protocols.		

Figure 4.17 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 combined total of SCKs and SCKXs associated with it per MNI.
NOTE 2: An SCK or SCKX may be associated with 0,1 or many ITSIs (in the diagram "n" represents this).
NOTE 3: An LA may only use one CCK and/or one CCKX at any one time.
NOTE 4: A CCK or CCKX may be used in more than one LA (represented by "n").
NOTE 5: An ITSI may have 0 or 1 key, either K or K2.
NOTE 6: Key K or K2 shall only be associated with 1 ITSI.
NOTE 7: A SwMI shall only use one SCK or SCKX at any one time except during key changeover periods (see also clause 6.5).
NOTE 8: An SCK or SCKX may be used in more than one SwMI.
NOTE 9: A GCK or GCKX may be associated with 1 or many GTSIs.
NOTE 10: A GTSI may have 0 or 1 active GCK or GCKX associated with it. A GTSI may have more than one version of GCK or GCKX associated with it for the purposes of key changeover.
NOTE 11: A GCK may have several MGCKs associated with it, if CCK is different in different LAs. Similarly, a GCKX may have several MGCKXs associated with it, if CCKX is different in different LAs.
NOTE 12: One or several SCKs or SCKXs may be associated with 0, 1 or many GTSIs for DMO only.

NOTE 13: A GTSI may have 0 or 1 active SCK or SCKX associated with it for DMO only, and may have many SCKs or SCKXs associated with the GTSI to enable key changeover.
NOTE 14: An ITSI may have 0, 1 or many sets of SCKs and SCKXs, and GCKs and GCKXs for use with different MNIs.
NOTE 15: A GCK or GCKX is valid within one SwMI only.
NOTE 16: An SCK or SCKX is valid within one SwMI or one DMO MNI only.
NOTE 17: A GSKO or GSKOX is valid within one SwMI only.
NOTE 18: The diagram does not show transient cases where more than one version of a key may be in use.

Figure 4.17: 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 (see also Table 4.5):

- 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 4.5: TNMM AUTHENTICATE service primitives

Generic name	Specific name	Parameters
TNMM-AUTHENTICATE	Indication	Result, reason
TNMM-AUTHENTICATE	Confirm	Result
TNMM-AUTHENTICATE	Request	Configure

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

- result =
  - success;
  - failure of MS authentication;
  - failure of SwMI authentication;
- reason =
  - authentication pending;
- configure =
  - authenticate SwMI now;
  - never mutually authenticate;
  - always mutually authenticate;
  - never authenticate during location update;
  - always authenticate during location update;
  - authenticate only in ITSI-Attach form of location update.

4.3.2 Static Cipher Key transfer primitives

A service shall be provided to allow an application to receive new SCKs or SCKXs either on demand or initiated by the SwMI. The primitives required shall be as follows (see also Table 4.6):

- 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 or SCKX requested. More than one SCK or SCKX may be requested in one transaction.

Table 4.6: TNMM SCK service primitives

Generic name	Specific name	Parameters
TNMM-SCK	Indication	SCKN, SCK-VN, GTSI
TNMM-SCK	Confirm	Result
TNMM-SCK	Request	SCKN

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

- result =
  - SCK or SCKX received successfully;
  - SCK or SCKX failed to decrypt;
  - SwMI Unable to provide SCK or SCKX;
- SCKN =
  - SCK number 1;
  - SCK number 2;
  - SCK number 3;
  - …;
  - SCK number 32;
- SCK-VN =
  - 0;
  - …;
  - 2^{16}-1;
- GTSI =
  - 1;
  - 2;
  - …;
  - 2^{48}-2;

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

4.3.3 Group Cipher Key transfer primitives

A service shall be provided to allow an application to receive new GCKs or GCKXs either on demand or initiated by the SwMI. The primitives required shall be as follows (see also Table 4.7):

- TNMM-GCK indication shall be used to provide the MS application with the GCKN, optionally the GTSI, and GCK-VN of the key received.
- TNMM-GCK confirm shall be used by the MS application to confirm that the key information received is acceptable, or provide the reject reasons if not.
- TNMM-GCK request shall be used to request the distribution of a new group cipher key. It shall contain either the address (GTSI) for the GCK or GCKX requested or the GCKN for the GCK or GCKX requested.

Table 4.7: TNMM GCK service primitives

Generic name	Specific name	Parameters
TNMM-GCK	Indication	GTSI, GCK-VN, GCKN
TNMM-GCK	Confirm	Result
TNMM-GCK	Request	GTSI, GCKN

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

- result =
  - GCK or GCKX received successfully;
  - GCK or GCKX failed to decrypt;
  - SwMI Unable to provide GCK or GCKX;
- GTSI =
  - 1;
  - 2;
  - …;
  - 2^{48}-2;

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

- GCK-VN =
  - 0;
  - …;
  - 2^{16}-1;
- GCKN =
  - 0;
  - 1;
  - 2;
  - …;
  - 2^{16}-1.

4.3.4 Group Session Key for OTAR transfer primitives

A service shall be provided to allow an application to receive new GSKO or GSKOX either on demand or initiated by the SwMI. The primitives required shall be as follows (see also Table 4.8):

- TNMM-GSKO indication shall be used to provide the MS application with the GSKO-VN of each key received.
- TNMM-GSKO confirm shall be used by the MS application to confirm that the key information received is acceptable, or provide the reject reasons if not.
- TNMM-GSKO request shall be used to request the distribution of a new Group Session Key for OTAR.

Table 4.8: TNMM GSKO service primitives

Generic name	Specific name	Parameters
TNMM-GSKO	Indication	GSKO-VN
TNMM-GSKO	Confirm	Result
TNMM-GSKO	Request	

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

- result =
  - GSKO or GSKOX received successfully;
  - GSKO or GSKOX failed to decrypt;
  - SwMI Unable to provide GSKO or GSKOX;
- GSKO-VN =
  - 0;
  - …;
  - 2^{16}-1.

4.4 Authentication protocol

4.4.1 Authentication state transitions

Figure 4.18 and Figure 4.19 give an overview of the received PDUs that result in a change of authentication state.

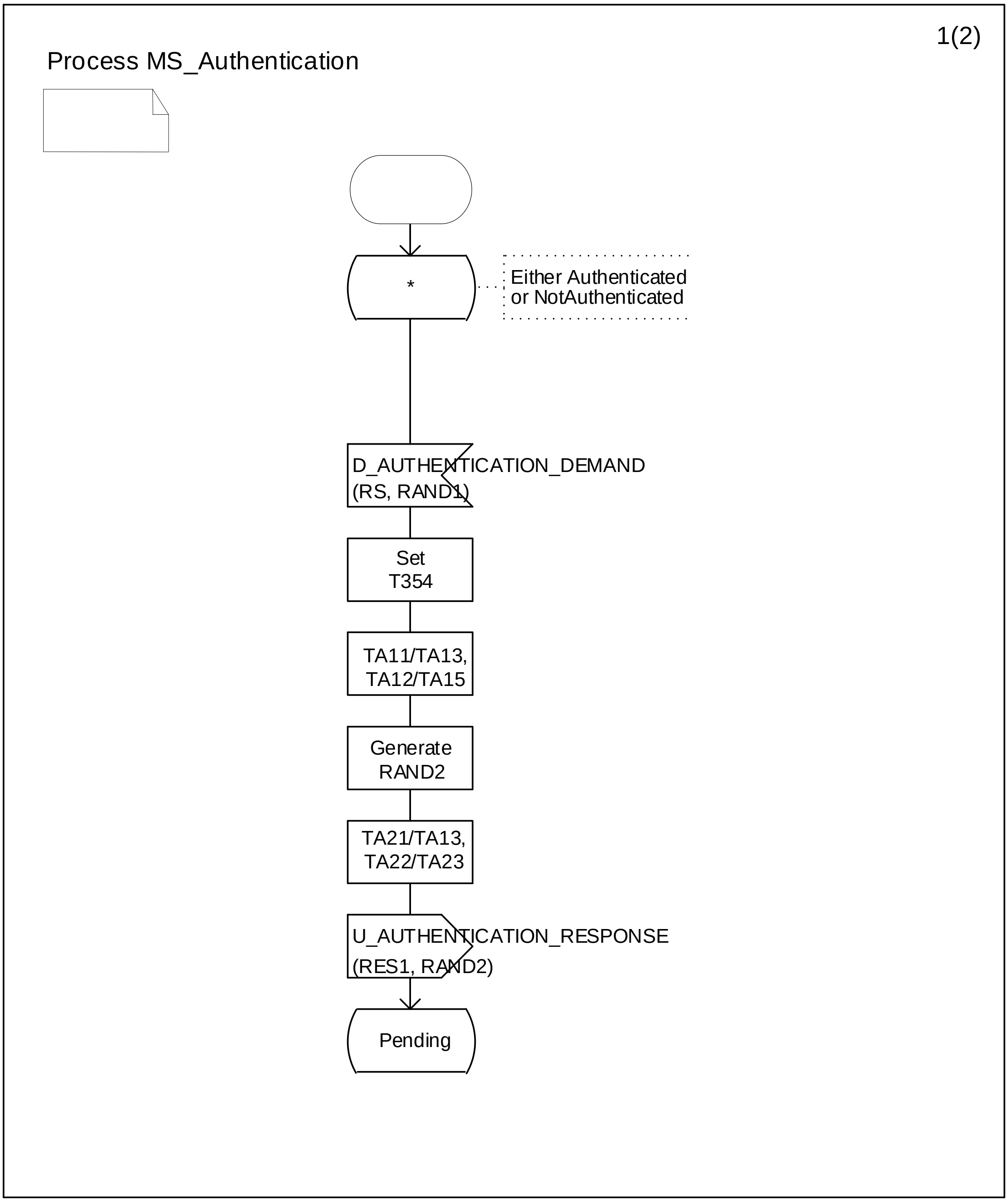
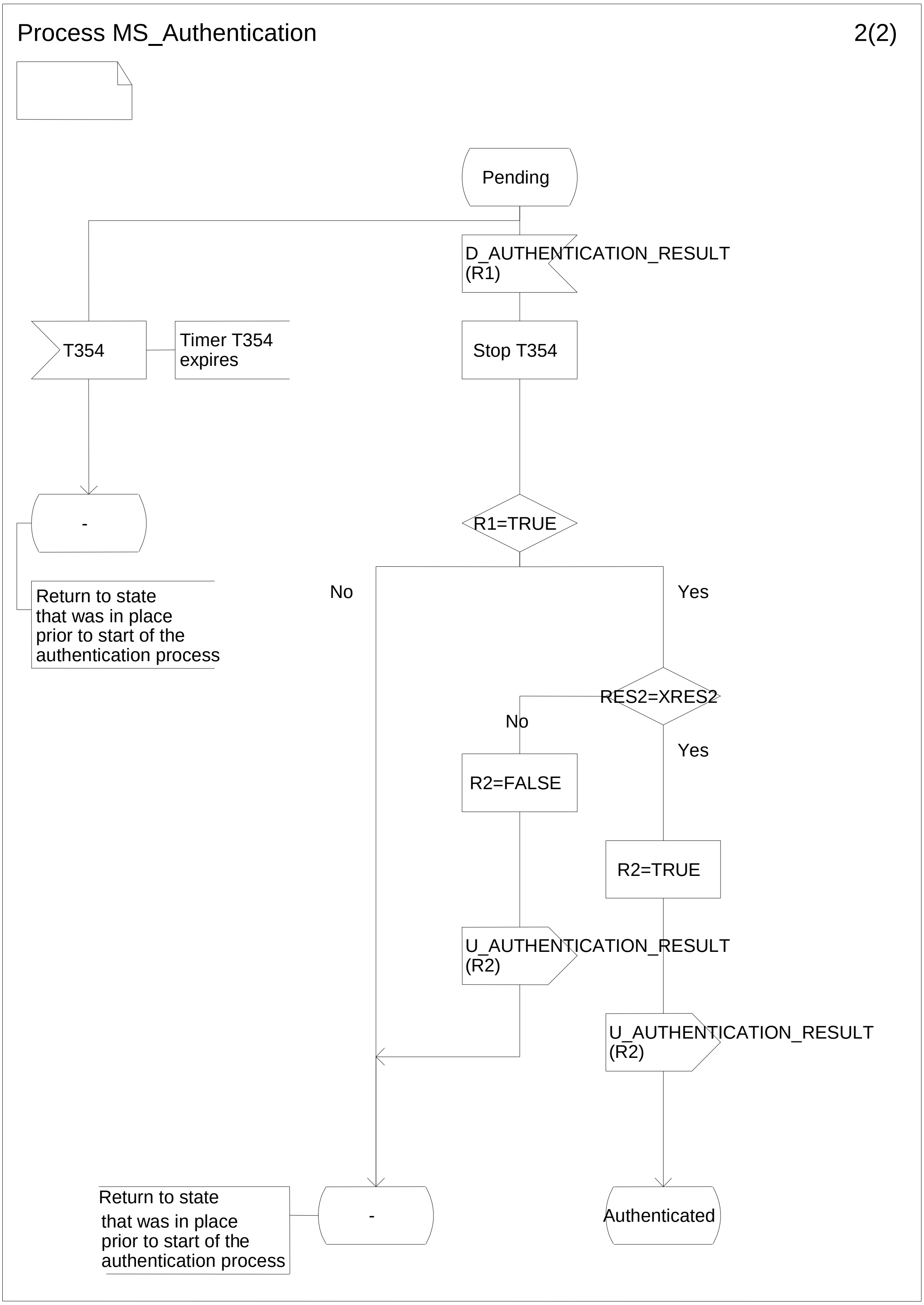


Figure 4.18: SDL process diagram for SwMI initiated authentication made mutual by MS (page 1 of 2)



Authenticated =	The MS has performed a successful authentication sequence.
Not authenticated =	The MS has not yet been authenticated.
Pending =	An authentication sequence has begun and not yet completed. If a new authentication is started then any pending authentication shall be abandoned.

Figure 4.19: SDL process diagram for SwMI initiated authentication made mutual by MS (page 2 of 2)

4.4.2 Authentication protocol sequences and operations

4.4.2.0 General

The air interface authentication protocol shall use the Mobility Management (MM) service of layer 3 in the TETRA protocol stack (see ETSI EN 300 392-2 [2], clause 15).

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

- if an authentication procedure fails, or fails to complete within time T354, the authenticating parties shall each revert to the same authentication state and set of encryption keys that were in place prior to the start of the authentication procedure;
- if an MS initiated authentication procedure as part of a registration procedure fails to complete within time T354, or if retries of an MS initiated authentication procedure as part of or outside a registration procedure fail, the MS may consider taking further action such as cell reselection;
- if an MS initiated authentication procedure as part of a registration procedure to a new cell fails to complete within time T354, or if the authentication procedure itself fails, the SwMI should not cancel the registration of the MS with the last known serving BS of that MS;
- if a SwMI initiated authentication procedure as part of or outside a registration procedure, excluding within a registration procedure to a new cell, fails to complete within time T354, the SwMI may consider taking further action such as retrying the procedure or deregistering or rejecting the MS;
- if a SwMI initiated authentication procedure as part of an MS initiated registration procedure to a new cell fails, the SwMI should not cancel the registration of the MS with the last known serving BS of that MS, and may consider attempting a registration and/or authentication procedure with the MS on the last known serving BS of that MS before taking further action;
- if DCK is to be used for AI encryption then CCK shall be used to generate ESI and MGCK where used (class 3 cell);
- if DCKX is to be used for AI encryption then CCKX shall be used to generate MGCKX where used (class 3 cell), and CCK or CCKX shall be used to generate ESI or as the input to the MAE mechanism;
- if authentication is performed during a U-PLANE transmission the DCK or DCKX change shall take place according to the criteria given in clause 4.5.5.1;
- authentication should be carried out using a previously established encryption key where possible (changeover of DCK or DCKX may be applied at the points shown in the MSCs of this clause);
- the encryption state (clear or encrypted) shall not be changed during location update signalling. The change (if required) shall be made when both the authentication sequence has been completed and the location update has been accepted.

An authentication exchange can be requested, either explicitly or as part of the registration procedure and can be initiated by either the MS or SwMI. The initiating side shall send an "AUTHENTICATION DEMAND" PDU that shall always be answered by the other side with either an "AUTHENTICATION RESPONSE" or an "AUTHENTICATION REJECT" PDU. Success or failure of the authentication shall be communicated by a specific "AUTHENTICATION RESULT" PDU. If an MS is not currently involved in an authentication exchange it shall ignore any authentication results or rejections addressed to the MS.

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

If the mutual authentication flag is set and an air interface encryption algorithm from TEA set A is in use, then the recipient knows to use DCK1 and DCK2 as input to TB4. If the mutual authentication flag is not set then TB4 is run with one of DCK1 or DCK2 set to zero as stated as clause 4.2.1. Thus, if "MS to SwMI" authentication is followed at some later time by "SwMI to MS" authentication, the first exchange will produce a DCK with DCK2 set to zero, and the second exchange will produce a DCK with DCK1 set to zero. If the mutual authentication flag is used and the authentication made mutual, as described above and in clause 4.1.4, then DCK is an algorithmic combination of DCK1 and DCK2.

If the mutual authentication flag is set and an air interface encryption algorithm from TEA set B is in use, then the recipient knows to use RAND1 and RAND2 as inputs to TA14 to generate the DCKX. If the mutual authentication flag is not set then one of RAND1 or RAND2 is set to zero as stated as clause 4.2.1.3. Thus, if "MS to SwMI" authentication is followed at some later time by "SwMI to MS" authentication, the first exchange will produce a DCKX derived with RAND1 set to zero, and the second exchange will produce a DCKX derived with RAND2 set to zero. If the mutual authentication flag is used and the authentication made mutual, as described above and in clause 4.1.4, then DCKX is derived using both RAND1 and RAND2.

After a successful authentication exchange, both MS and SwMI shall replace the derived cipher key, DCK or DCKX with the newly calculated key.

On sending of an authentication challenge the MS or SwMI shall start timer T354. On receipt of an authentication challenge the MS or SwMI shall start timer T354. If a location update procedure is ongoing and timer T351 is running, then T351 shall be stopped and T354 shall apply; in this case T354 shall not be stopped until the completion of the location update procedure.

When T354 expires the MS and SwMI shall revert to the state that existed prior to the initiating authentication challenge and if encryption in security class 3 is applied, shall revert to the DCK or DCKX that was in use prior to the initiation of the authentication procedure. Repeated expiry of T354 may be used as a reason by the MS to select an alternative cell. Repeated expiry of T354 may be used as a reason by the SwMI to initiate further procedures including SwMI initiated authentication and/or registration procedures, and may lead to the SwMI rejecting the MS following failures in SwMI initiated procedures.

If the MS receives a D-AUTHENTICATION RESULT PDU containing a value of R1 set to "Authentication failed" the MS MM may send the MS MLE an MLE-UPDATE request primitive with reject cause "LA rejection" so that the MS MLE initiates cell reselection as defined in ETSI EN 300 392-2 [2], clause 18.3.4.7. If the MS decides to initiate cell selection at this stage, it shall treat this as though it received a D-LOCATION UPDATE REJECT PDU with reject cause "Authentication failure (system rejection)", and shall count this towards the maximum permitted number of system rejections, as described in ETSI EN 300 392-2 [2], clause 16.4.1.1.

NOTE: If the MS does not leave the current cell when it receives a value of R1 set to "Authentication failed", it may subsequently be instructed to leave the cell by receipt of a D-LOCATION UPDATE REJECT PDU.

If the MS receives an incorrect RES2 value in a D-AUTHENTICATION RESPONSE PDU or a D-AUTHENTICATION RESULT PDU, the MS MM service shall send the SwMI a U-AUTHENTICATION RESULT PDU with R2 set to "Authentication failed". The MS shall send the MS MLE service an MLE-UPDATE request primitive with reject cause "LA rejection" so that the MS MLE initiates cell reselection as defined in ETSI EN 300 392-2 [2], clause 18.3.4.7. The MS shall treat this as though it received a D-LOCATION UPDATE REJECT PDU with reject cause "Authentication failure (system rejection)", and shall count this towards the maximum permitted number of system rejections, as described in ETSI EN 300 392-2 [2], clause 16.4.1.1.

If the MS sends the SwMI a U-AUTHENTICATION DEMAND PDU and the MS receives in reply a D-AUTHENTICATION REJECT PDU, the MS MM may send the MS MLE an MLE-UPDATE request primitive with reject cause "LA rejection" so that the MS MLE initiates cell reselection as defined in ETSI EN 300 392-2 [2], clause 18.3.4.7.

If the MS attempts to make an authentication challenge mutual by sending the SwMI a U-AUTHENTICATION RESPONSE PDU that includes a RAND2 information element, and if the MS receives in reply a D-AUTHENTICATION RESULT PDU that does not contain a RES2 information element the MS MM may send the MS MLE an MLE-UPDATE request primitive with reject cause "LA rejection" so that the MS MLE initiates cell reselection as defined in ETSI EN 300 392-2 [2], clause 18.3.4.7.

4.4.2.1 MSCs for authentication

This clause presents Message Sequence Charts (MSCs) for the authentication protocol to enable the mechanisms described in clause 4.1 (the figures are identified in Table 4.9).

Table 4.9: Authentication protocol MSC locations

Case	Title	Figure number
1	SwMI authenticates MS	Figure 4.20
2	MS authenticates SwMI	Figure 4.21
3	Authentication initiated by SwMI and made mutual by the MS	Figure 4.22
4	Authentication initiated by MS and made mutual by the SwMI	Figure 4.23
5	SwMI rejects authentication demand from MS	Figure 4.24
6	MS rejects authentication demand from SwMI	Figure 4.25

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

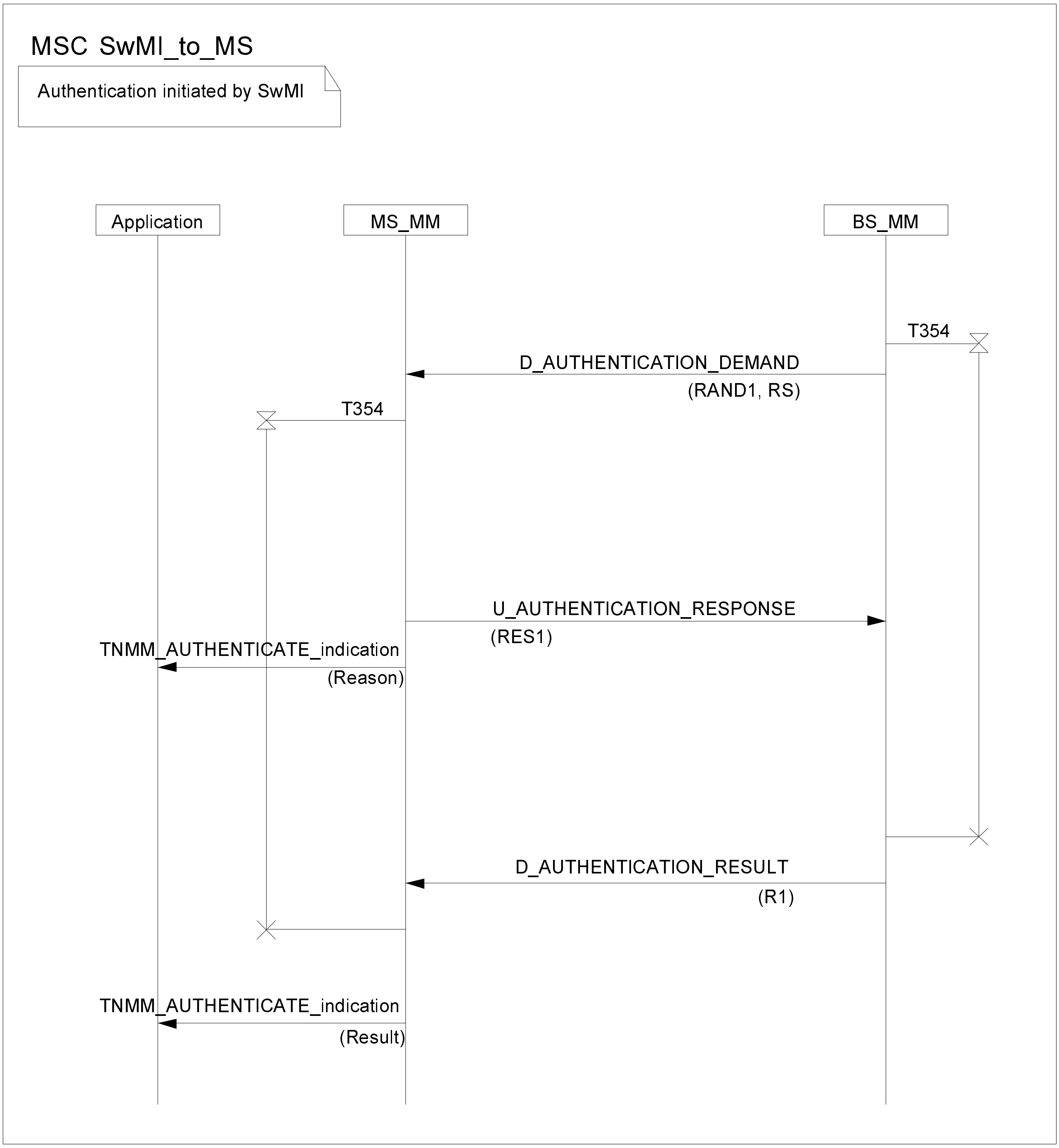


Figure 4.20: Authentication of MS by SwMI

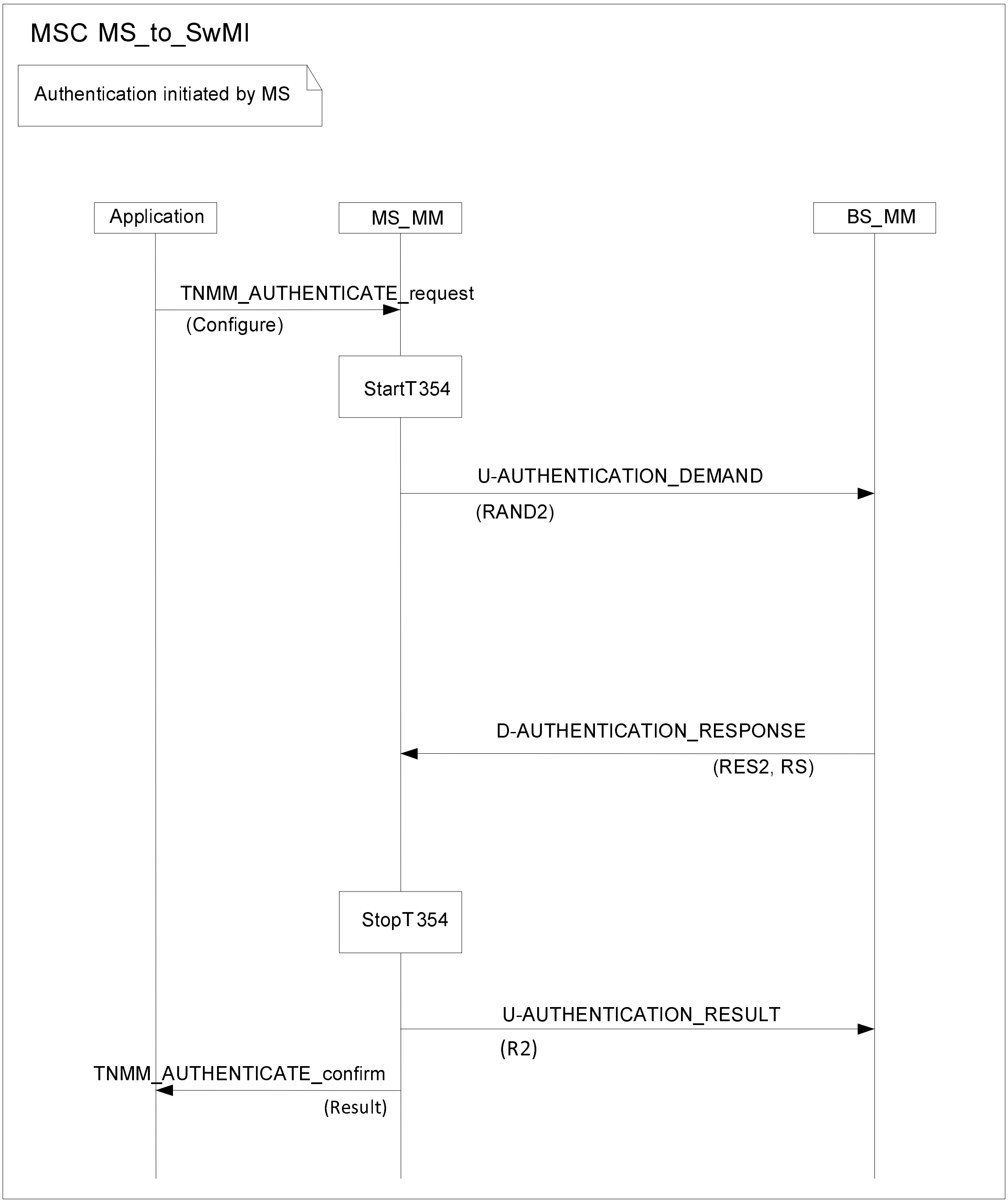


Figure 4.21: Authentication of the SwMI by the MS

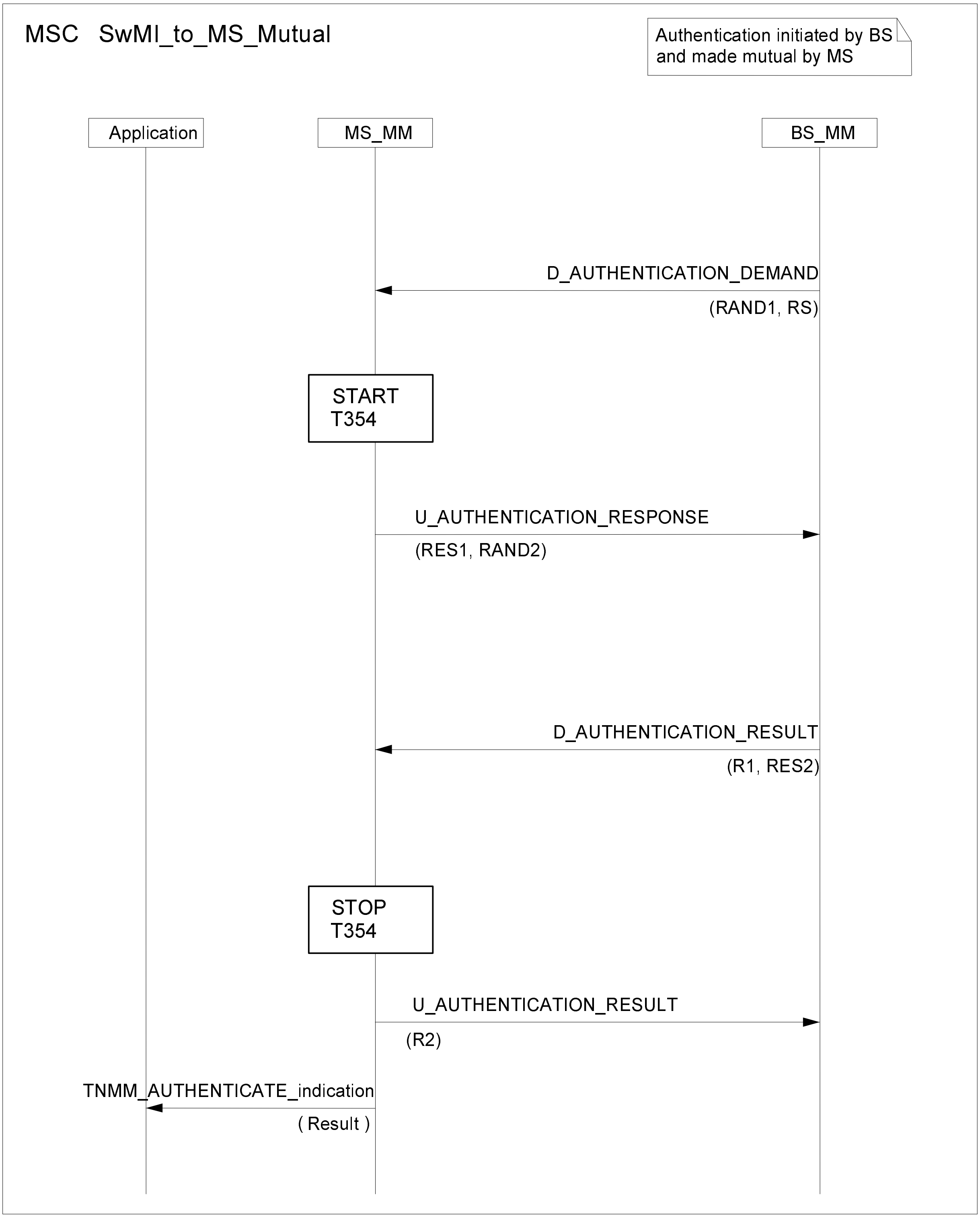


Figure 4.22: Authentication initiated by SwMI and made mutual by the MS

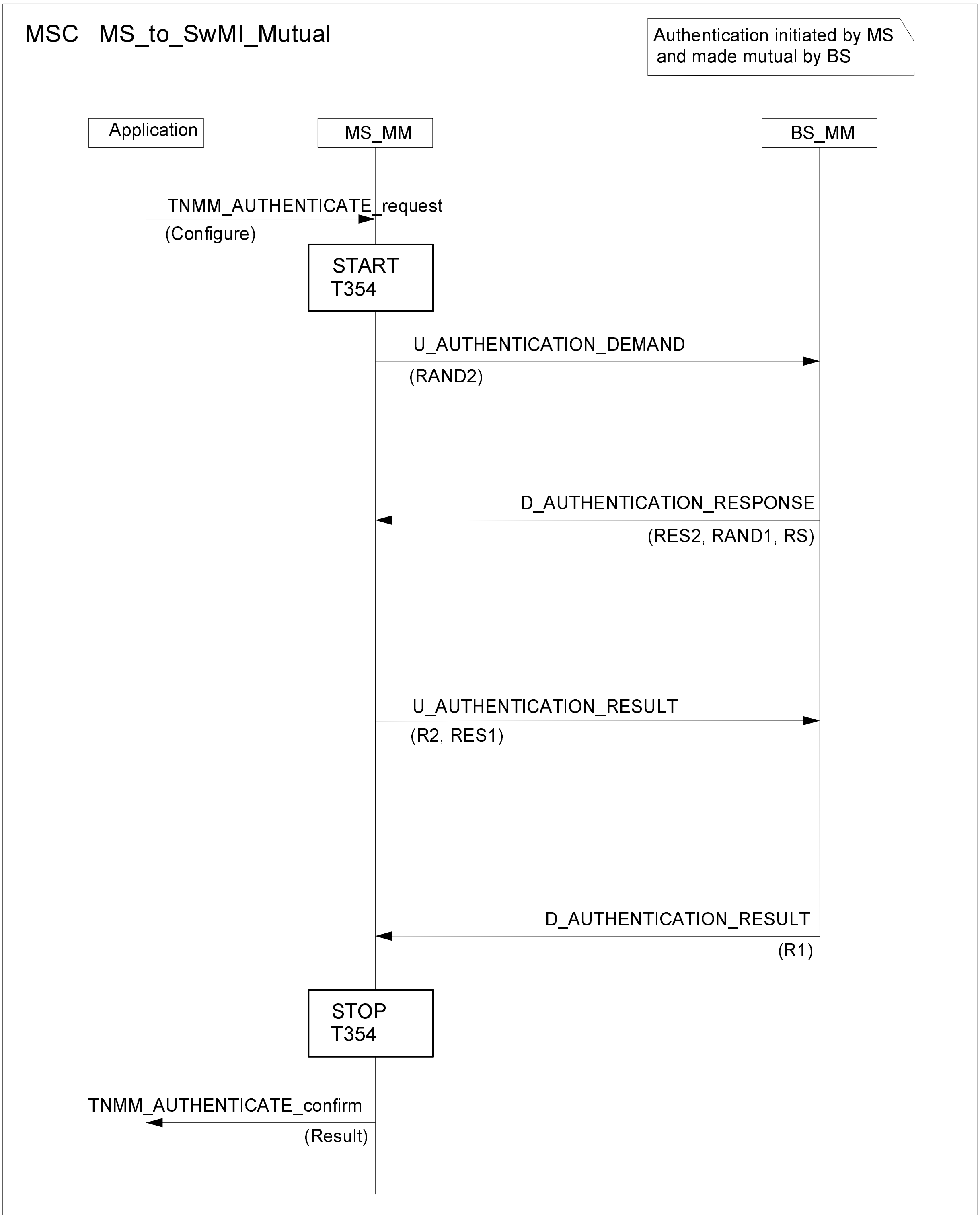


Figure 4.23: Authentication initiated by MS and made mutual by the SwMI

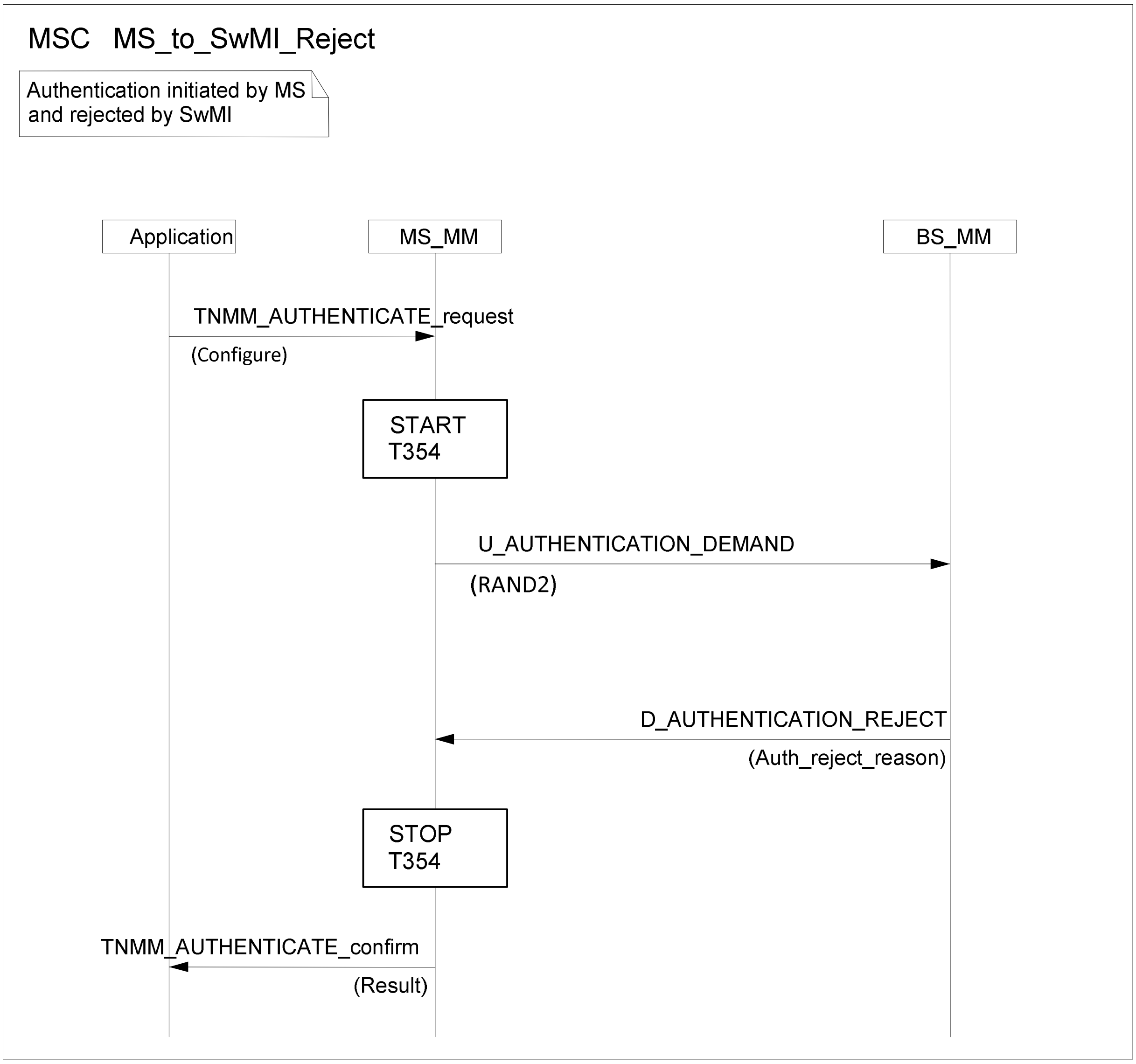


Figure 4.24: Authentication initiated by MS and rejected by SwMI

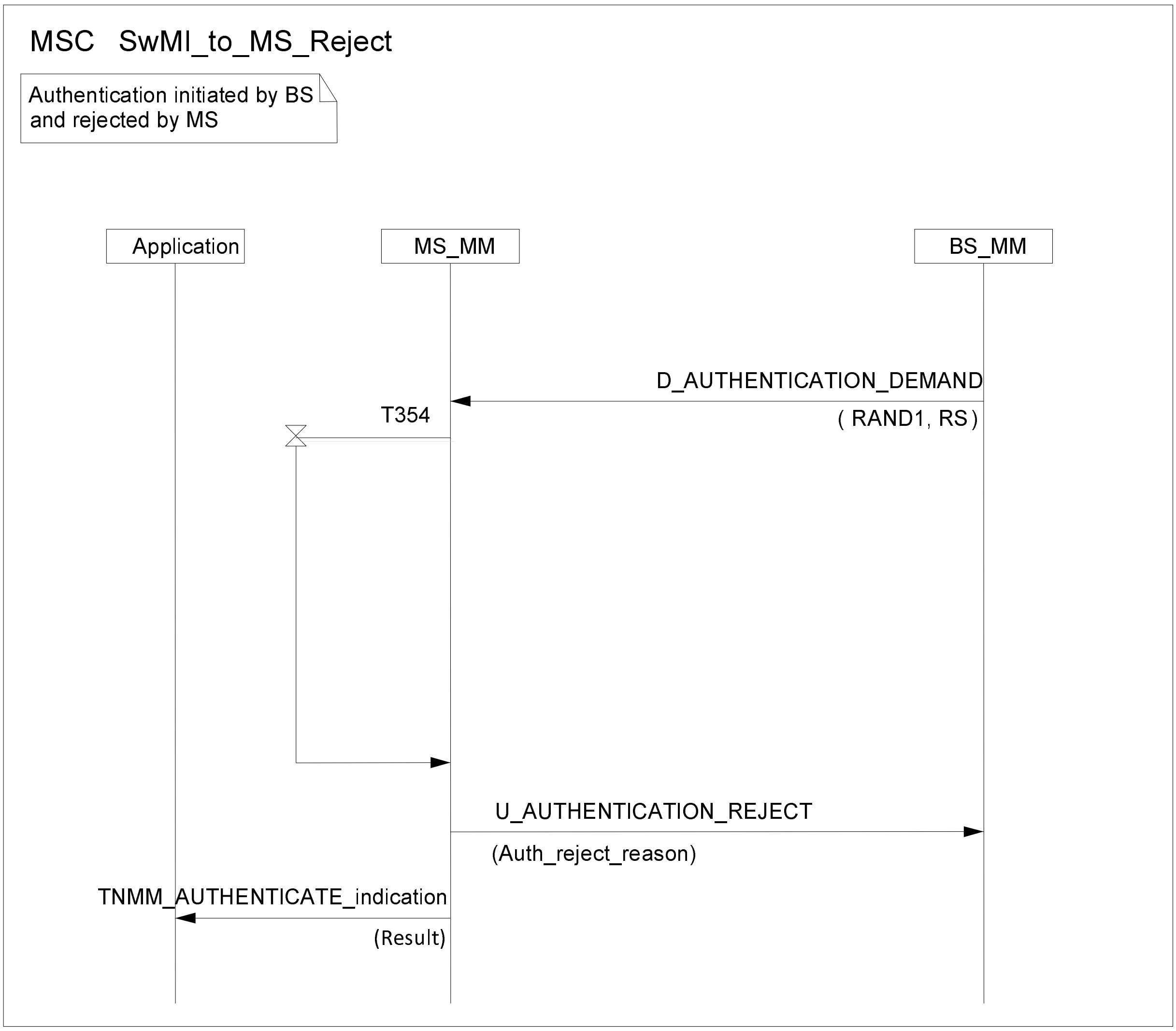


Figure 4.25: Authentication initiated by SwMI and rejected by MS

4.4.2.2 MSCs for authentication and security type-3 elements

The type-3 PDU elements "Authentication uplink" contained in the U-LOCATION UPDATE DEMAND and "Authentication downlink" or "Security downlink" contained in the D-LOCATION UPDATE ACCEPT PDUs allow authentication and CK or CKX key provision to be initiated by the MS. The SwMI then is able to provide the CK or CKX for the current LA (of which the serving cell is a member) to the registering MS.

The cipher key being requested in the "Authentication uplink" shall be qualified by the security class element in the ciphering parameters, i.e.:

- if the MS requests the CK in the "Authentication uplink", and the ciphering parameters information element indicates security class 2, then the SwMI shall infer that the MS is requesting the SCK or SCKX in current use;
- if the MS requests the CK in the "Authentication uplink", and the ciphering parameters information element indicates security class 3, then the SwMI shall infer that the MS is requesting the CCK or CCKX.

The key being requested in the "Authentication uplink" shall also be qualified by the KSG number element in the ciphering parameters provided that the requested KSG is acceptable to the SwMI, i.e.:

- if the MS requests the CK in the "Authentication uplink", and is requesting a KSG number representing an air interface encryption algorithm from TEA set A, the SwMI shall infer that the MS is requesting a CCK or SCK;

- if the MS requests the CK in the "Authentication uplink", and is requesting a KSG number representing an air interface encryption algorithm from TEA set B, the SwMI shall infer that the MS is requesting a CCKX or SCKX.

NOTE 1: If the KSG proposed by the MS is not acceptable to the SwMI, KSG negotiation takes place according to clause 6.6.2 of the present document, and cipher keys are not provided until an acceptable KSG has been successfully negotiated.

Where the negotiated KSG is a KSG from TEA set A, the SwMI may provide CK information using the "Authentication downlink" or "Security downlink" information element. However, the SwMI shall only send the "Security downlink" element to the MS if it is aware that the MS supports reception of this element. Where the negotiated KSG is a KSG from TEA set B, the SwMI shall only use the "Security downlink" information element to provide CK information.

NOTE 2: Whether the MS is provisioned with a K or K2 authentication key may be an indication of whether the MS supports "Security downlink" when a KSG from TEA set A is negotiated.

The MS should store which KSG is negotiated with the SwMI, and propose that KSG first on next registration with that SwMI. If the SwMI requires that the MS negotiates a different KSG to that last negotiated with that SwMI, any stored CCK/CCKX(s), TM-SCK/SCKX(s), GCK/GCKX(s) and GSKO/GSKOX associated with that SwMI should be deleted, and the MS should update its record of the last KSG negotiated with that SwMI. See clause 6.6.2.1 for more information.

When the SwMI provides CK information in the "Authentication downlink" or "Security downlink", the SwMI may provide additional CK or CKX material as well as that requested in the "Authentication uplink", i.e.:

- if the MS requests the CCK in the "Authentication uplink", the SwMI may provide the CCK and the SCK in the "Authentication downlink" or "Security downlink";
- if the MS requests the CCKX in the "Authentication uplink", the SwMI may provide the CCKX and the SCKX in the "Security downlink";
- if the MS requests the SCK in the "Authentication uplink", the SwMI may provide the SCK and the CCK in the "Authentication downlink" or "Security downlink";
- if the MS requests the SCKX in the "Authentication uplink", the SwMI may provide the SCKX and the CCKX in the "Security downlink".

NOTE 3: "Authentication downlink" does not support transmission of sealed CCKX or SCKX.

NOTE 4: The SwMI may restrict the number of keys provided in the "Security downlink" element in the D-LOCATION UPDATE ACCEPT PDU depending on the amount of additional information that is to be sent in the PDU, and the capacity of the channel in use. Whether the current and future CCKX and current and future SCKX can be sent together in the "Security downlink" element on a phase modulation channel depends on which other type 2 and type 3 elements are sent in the D-LOCATION UPDATE ACCEPT PDU. If more keys need to be provided than can be sent in this PDU, additional D-OTAR PDUs may be sent.

The "Authentication downlink" may also contain a demand for the MS to provide its TEI. The "Security downlink" may also contain a demand for the MS to provide its TEI and/or hardware or software version number, and/or other security related information. It is recommended that such information is only requested if encryption is applied (i.e. in class 2 and class 3 systems).

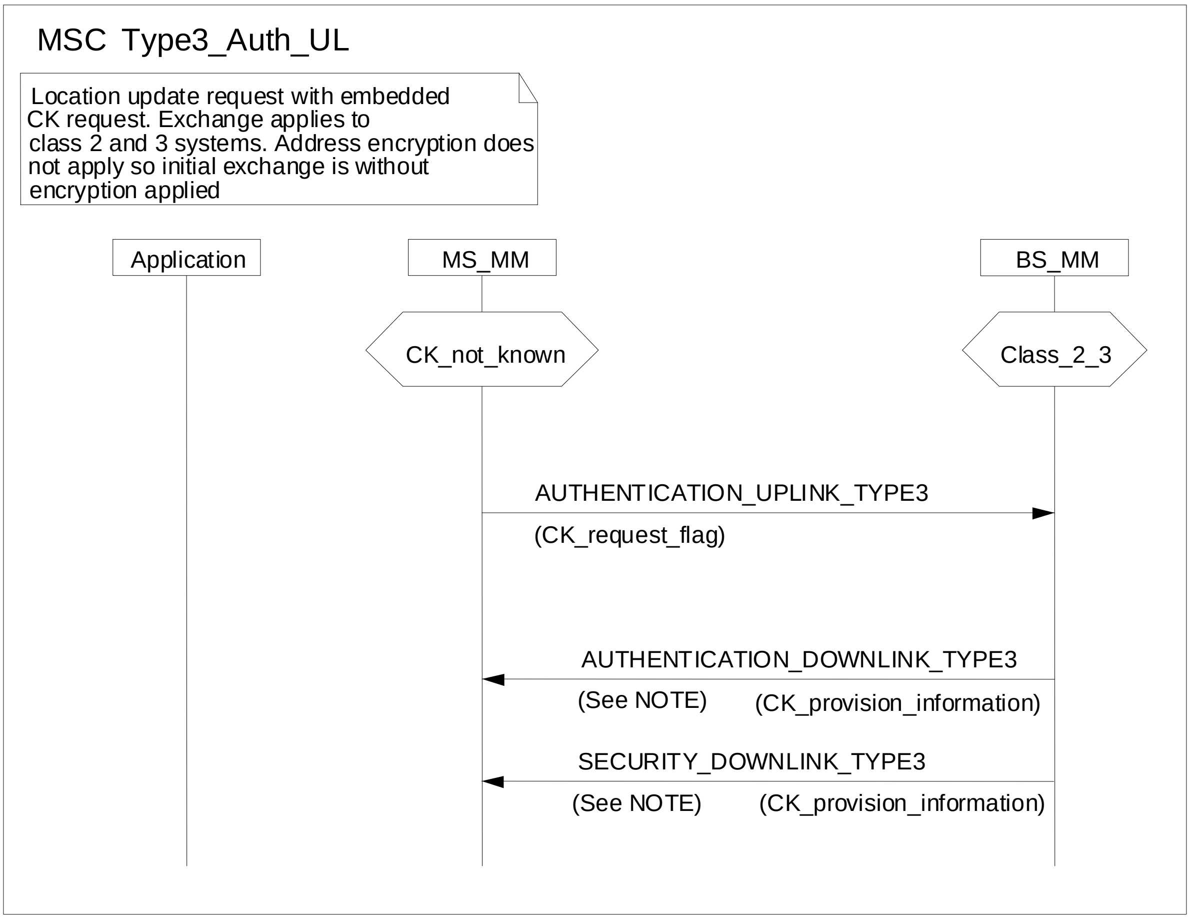
The SwMI may send one or both of the "Authentication downlink" and the "Security downlink" in a D-LOCATION UPDATE ACCEPT PDU. The SwMI shall only send the "Security downlink" element to the MS if it is aware that the MS supports reception of this element. Only one of these elements shall contain CK information if both elements are included in the same D-LOCATION UPDATE ACCEPT PDU.

NOTE 5: Both elements contain the same Authentication result.

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

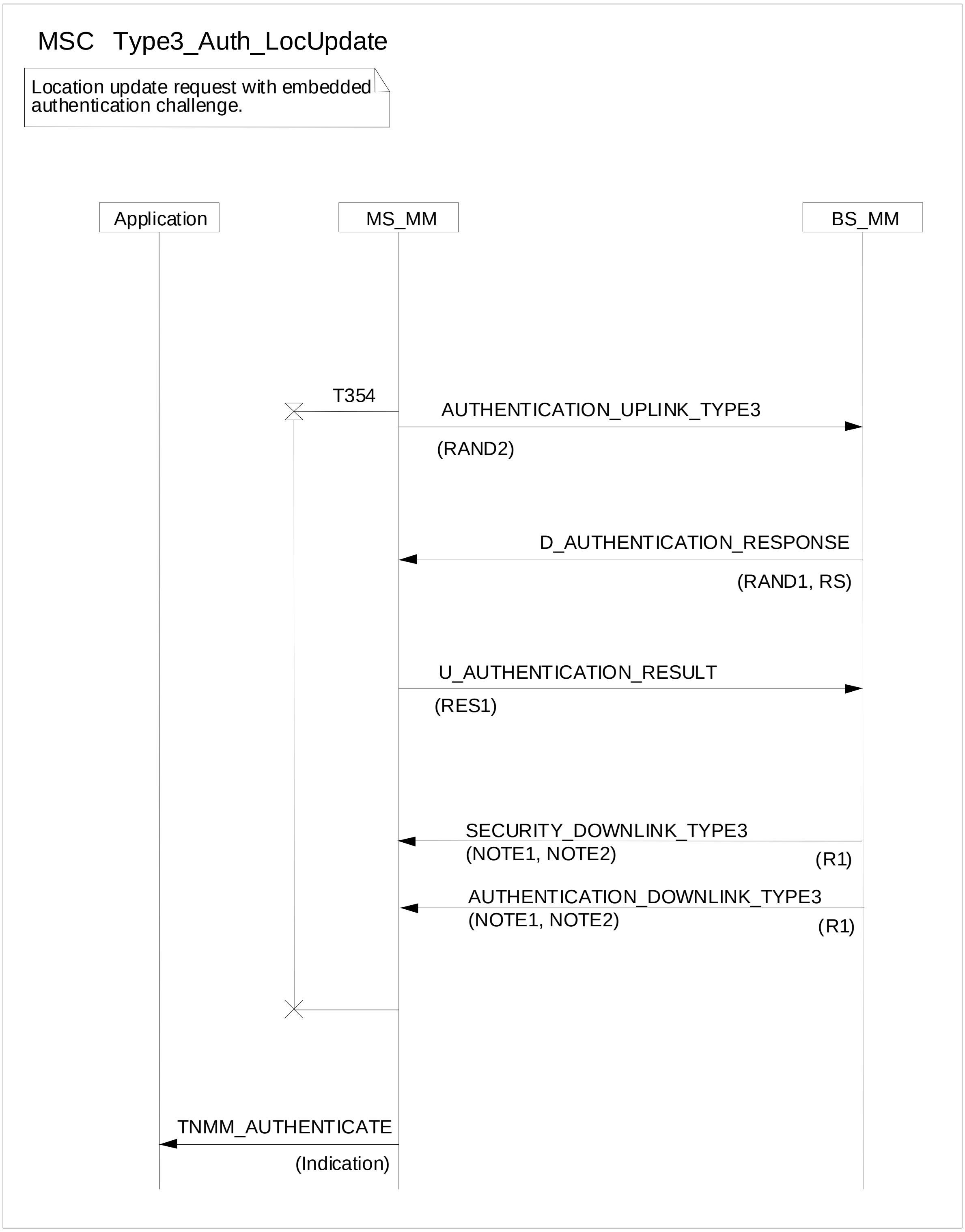
- MS initiated location update request with embedded CK request and SwMI CK provision (Figure 4.26);
- MS initiated location update request with embedded Authentication challenge (Figure 4.27);

- MS initiated location update request, followed by Authentication challenge from the SwMI made mutual by the MS (Figure 4.27a).


MSC Type3_Auth_UL
Location update request with embedded CK request. Exchange applies to class 2 and 3 systems. Address encryption does not apply so initial exchange is without encryption applied
Application
MS_MM
BS_MM
CK_not_known
Class_2_3
AUTHENTICATION_UPLINK_TYPE3
(CK_request_flag)
AUTHENTICATION_DOWNLINK_TYPE3
(See NOTE)
(CK_provision_information)
SECURITY_DOWNLINK_TYPE3
(See NOTE)
(CK_provision_information)

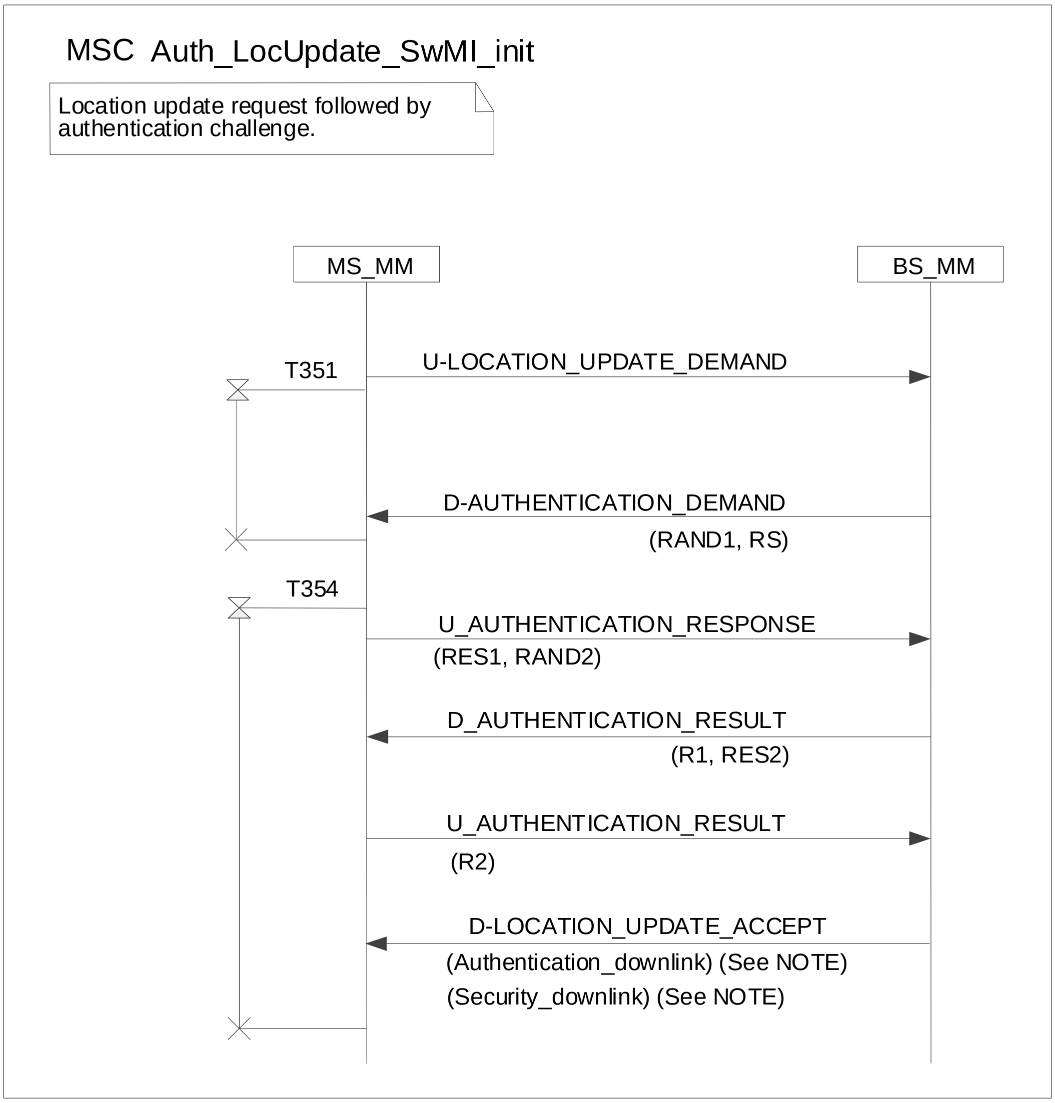
NOTE: Either one of or both of "Authentication downlink" and "Security downlink" may be included in the PDU.

Figure 4.26: CK provision during location update



NOTE 1: If D-LOCATION UPDATE ACCEPT is received R1 may be ignored.
NOTE 2: Either one of or both of "Authentication downlink" and "Security downlink" may be included in the PDU.

Figure 4.27: MS initiated authentication during location update


MSC Auth_LocUpdate_SwMI_init
Location update request followed by authentication challenge.
MS_MM
BS_MM
T351
U-LOCATION_UPDATE_DEMAND
D-AUTHENTICATION_DEMAND
(RAND1, RS)
T354
U_AUTHENTICATION_RESPONSE
(RES1, RAND2)
D_AUTHENTICATION_RESULT
(R1, RES2)
U_AUTHENTICATION_RESULT
(R2)
D-LOCATION_UPDATE_ACCEPT
(Authentication_downlink) (See NOTE)
(Security_downlink) (See NOTE)

NOTE: Either one of or both of "Authentication downlink" and "Security downlink" may be included in the PDU.

Figure 4.27a: SwMI initiated authentication during location update, made mutual by MS

4.4.2.3 Control of authentication timer T354 at MS

The timer shall be started under the following conditions:

- on sending of U-AUTHENTICATION DEMAND;
- on receipt of D-AUTHENTICATION DEMAND; and
- on sending of U-LOCATION UPDATE DEMAND containing an Authentication challenge in the type-3 element "Authentication uplink".

The timer shall be stopped (cancelled) under the following conditions where authentication takes place outside a location update procedure:

- on receipt of D-AUTHENTICATION RESULT for SwMI initiated unilateral authentication, and for authentication initiated by the MS but made mutual by the SwMI;
- on sending of U-AUTHENTICATION RESULT for MS initiated unilateral authentication, and for authentication initiated by the SwMI but made mutual by the MS;
- on sending of U-AUTHENTICATION REJECT;

- on receipt of D-AUTHENTICATION REJECT.

The timer shall be stopped (cancelled) under the following conditions where authentication takes place within a location update procedure:

- on receipt of D-LOCATION UPDATE REJECT;
- on receipt of D-LOCATION UPDATE ACCEPT containing the type-3 element "Authentication downlink"; and
- on receipt of D-LOCATION UPDATE ACCEPT where T354 has replaced T351.

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

4.4a Information request protocol

The BS may request security related information from the MS by including one or both of the optional "Authentication downlink" or "Security downlink" information elements in the D-LOCATION UPDATE ACCEPT sent at the completion of a successful registration to a cell, and setting an appropriate flag within the chosen element. The BS shall not send the "Security downlink" element to the MS unless it is aware that the MS is capable of receiving this element, either by positive indication of support from an MS when performing an ITSI-Attach in a security class 3 system, by the MS negotiating a KSG from TEA set B, or due to some configuration mechanism outside the scope of the present document. The BS should not make this request at every location update, and should not make such requests more than once between location updates where an ITSI-Attach is performed.

NOTE 1: It is advisable that the BS does not request this information following every ITSI-Attach, and only requests the information when needed by the network operator. Requesting information during ITSI-Attach should be avoided due to potential air interface loading issues, especially where authentication and key provision take place.

When the MS performs ITSI-attachment requesting security class 3 operation on the home network, the MS shall indicate its capability to respond to information requests which are made using the "Security downlink" element by setting the "Security information protocol" element contained in the "Ciphering parameters" element sent in the U-LOCATION UPDATE DEMAND PDU to "supported". If the MS requests security class 3 operation on a visited network, it may indicate this capability, depending on its security policy.

The BS may request the TEI by setting the "TEI request flag" in the "Authentication downlink" element or in the "Security downlink" element. The BS may request model number information from the MS by setting the "Model number request" flag in the "Security downlink" element. The BS may request information on hardware and software version numbers from the MS by setting the "HW SW version request" flag in the "Security downlink" element. The BS may request air encryption algorithm information from the MS by setting the "AI algorithm information request flag" in the "Security Downlink" element. The BS may request several or all four of the TEI, model number information, hardware and software version numbers or air interface encryption algorithm information by sending the "Security downlink" element in the D-LOCATION UPDATE ACCEPT PDU.

If the BS requested the TEI using the "Authentication downlink" element, the MS may respond with the U-TEI PROVIDE PDU, containing the TEI. If the MS cannot provide the TEI, it shall send no response. The MS shall not send the U-INFORMATION PROVIDE PDU in response to a request for TEI made using the "Authentication downlink" element.

The BS should not request the TEI using both the "Authentication downlink" and "Security downlink" elements in the same D-LOCATION UPDATE ACCEPT PDU. However if the BS did request the TEI in both downlink type-3 elements, the MS should respond with both the U-TEI PROVIDE and U-INFORMATION PROVIDE PDUs, both containing the TEI.

If the BS requested TEI, model number, version number or air interface algorithm information by setting the required flags in the "Security downlink" element, the MS may reply by sending the U-INFORMATION PROVIDE PDU containing the required information. The MS should normally only provide information that has been requested by the BS, however in exceptional circumstances, additional information may be provided within the U-INFORMATION PROVIDE PDU, whilst that PDU is providing a response to a request for other information.

NOTE 2: Such an exceptional circumstance might be to inform the SwMI of some software or configuration change which has taken place since the last time that the SwMI requested security related information from the MS.

The MS may also send an unsolicited U-INFORMATION PROVIDE following a successful registration with ITSI-attach in exceptional circumstances. An example exceptional circumstance could be to indicate to the SwMI that a software or major configuration change has taken place, without the SwMI needing to poll the MS at every registration to find out if this has been done. The MS should only send such unsolicited information once on the first ITSI-attach following the change, to prevent unnecessary loading on the air interface. Also, the MS should only send such unsolicited information if it already knows that the SwMI supports the U-INFORMATION-PROVIDE PDU (e.g. by configuration, or because the MS has previously received a "Security downlink" information element from the present SwMI having one or more of the "TEI request flag", the "Model number information request flag", the "HW SW version request flag" and/or "AI algorithm information request flag" set).

NOTE 3: A SwMI supporting TEA set B needs to support the use of "Security downlink" in order to provide cipher keys to an MS at ITSI-attach. If such a SwMI does not support the information request protocol, it should discard the U-INFORMATION_PROVIDE.

If the BS requested air interface encryption algorithm information, and the MS is unable or unwilling to provide air interface encryption algorithm information, or is a security class 1 MS and does not support air interface encryption, it shall set the "AI algorithm information present" to a value of "AI algorithm information is not included". In this case, the "Number of KSGs present" and "KSG Number" elements shall be omitted from the PDU.

NOTE 4: An MS may be unwilling to provide detailed AI algorithm information dependent on its security policy, for example if operating on a visited SwMI.

If the MS is able to provide air interface encryption algorithm information and contains one or more KSGs, the MS shall set the "AI algorithm information present" to a value of "AI algorithm information is included", shall set the "Number of KSGs present" element to the number of KSGs that the MS contains (1 or more), and shall list the algorithms by sending a number of different "KSG number" elements, where the number of elements provided is equal to the value of the "Number of KSGs present" element. In this case, the MS shall send the KSGs as a list with the lowest value KSG sent first.

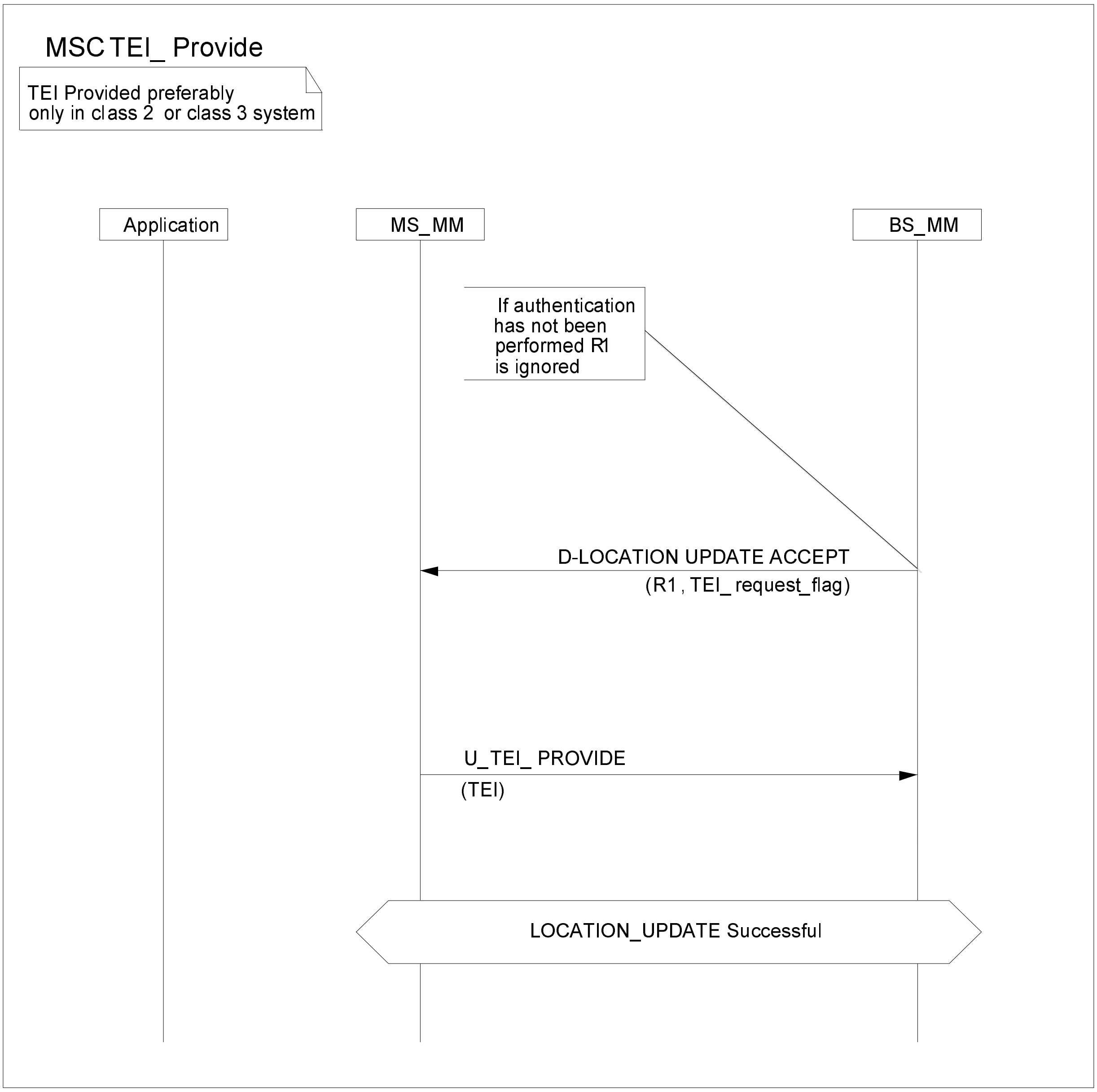
NOTE 5: The value for each KSG is defined in clause A.8.41.

If the MS is unable to send any information in response to a request for model number, version number, air interface algorithm information or TEI, it may send a U-INFORMATION PROVIDE PDU with no contents (i.e. with each of the "information present" elements set to "no information present"). It may also decide not to send a response. The MS shall not send a U-TEI PROVIDE PDU in response to the "Security downlink" element.

If the information that the MS intends to send causes the PDU to become too large (e.g. to exceed the capacity of a MAC PDU, or some other pre-determined limit), the MS may send multiple U-INFORMATION PROVIDE PDUs. In this case, all PDUs except for the last sent by the MS shall set the "further information follows" flag to "1", and the last PDU sent by the MS shall have the "further information follows" flag set to "0". If only one U-INFORMATION PROVIDE PDU is sent, the "further information follows" flag shall be set to "0".

If the authentication process has failed because the BS provided an incorrect response to the MS's challenge, the MS shall not provide any information to the BS.

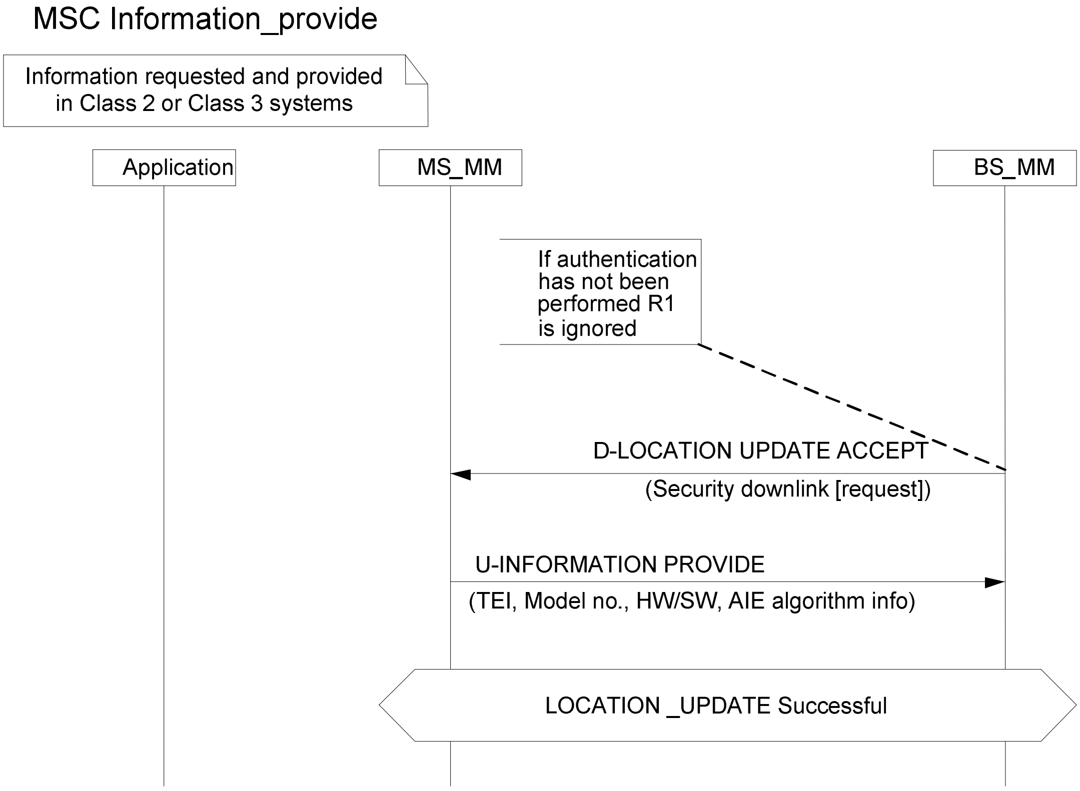
Figure 4.28 shows the MSC for requesting TEI using the "Authentication downlink" element.


MSC TEI_ Provide
TEI Provided preferably only in class 2 or class 3 system
Application
MS_MM
BS_MM
If authentication has not been performed R1 is ignored
D-LOCATION UPDATE ACCEPT
(R1 , TEI_ request_flag)
U_TEI_ PROVIDE
(TEI)
LOCATION_UPDATE Successful

NOTE: If D-LOCATION UPDATE ACCEPT is received R1 may be ignored.

Figure 4.28: TEI Provision in class 2 or 3 system

Figure 4.29 shows the MSC where information such as TEI, Model number, HW/SW version number and/or AI algorithm information is requested using the "Security downlink" element.


MSC Information_provide
Information requested and provided in Class 2 or Class 3 systems
Application
MS_MM
BS_MM
If authentication has not been performed R1 is ignored
D-LOCATION UPDATE ACCEPT
(Security downlink [request])
U-INFORMATION PROVIDE
(TEI, Model no., HW/SW, AIE algorithm info)
LOCATION _UPDATE Successful

NOTE: If D-LOCATION UPDATE ACCEPT is received R1 may be ignored.

Figure 4.29: Information Provision in class 2 or 3 system

4.5 OTAR protocols

4.5.1 Common Cipher Key delivery - protocol functions

4.5.1.0 General

CCK is a cipher key linked to the use of air interface encryption with DCK. CCKX is a cipher key linked to the use of air interface encryption with DCKX. This clause describes the key management protocols used to support the algorithms and mechanisms described in clause 4.2.3. CCK or CCKX is required prior to enabling encrypted air interface services on a cell as it is linked to the ESI and MAE mechanisms used for layer 2 addressing (see clauses 4.2.6 and 6.7.1.2a).

CCK and CCKX shall be delivered over the air interface using the mechanisms and protocols described in this clause, and by the registration and authentication procedures defined in clause 4.4.2. A CCK shall be delivered to an MS that has successfully negotiated a KSG in TEA set A, and a CCKX shall be delivered to an MS that has successfully negotiated a KSG in TEA set B. A CCK shall not be delivered to an MS that has negotiated a KSG in TEA set B, and a CCKX shall not be delivered to an MS that has negotiated a KSG in TEA set A. When scanning a cell prior to registration an MS shall receive the CCK-id and LA-id of the CCK or CCKX in use on that cell in the SYSINFO, SYSINFO-DA or SYSINFO-Q broadcast PDUs. If the CCK or CCKX so identified is not known to the MS it shall request the CCK or CCKX either through its current serving cell or at the new cell using the protocols defined in the present document. If a cell has both a CCK and a CCKX in use at the same time for use by different sets of MSs, the same CCK-id shall apply to both the CCK and the CCKX.

The SwMI can deliver to all registered MSs a CCK or CCKX (whichever is appropriate for the negotiated KSG) for future use.

When delivering a CCK or CCKX the SwMI shall indicate the LAs for which the CCK or CCKX 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 or CCKX by a list the list shall include the corresponding LA identity.

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

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

The CCK or CCKX may be provided explicitly by the SwMI using the D-OTAR CCKX PROVIDE PDU, the D-OTAR NEWCELL-X PDU, or may be provided during the registration procedure using the MM type 3 element "Security downlink" contained in D-LOCATION UPDATE ACCEPT PDU.

An MS may explicitly request a CCK or CCKX from the SwMI using the U-OTAR CCK DEMANDPDU, or the U-OTAR PREPARE PDU, or CCK or CCKX may be requested during the registration procedure using the MM type 3 element "Authentication uplink" contained in U-LOCATION UPDATE DEMAND PDU.

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

4.5.1.1 SwMI-initiated CCK and CCKX provision

The scenario in Figure 4.30 shows how the SwMI can distribute new CCK or CCKX information. The SwMI can initiate CCK or CCKX provision at any time when the MS is registered on the cell. The SwMI may provide the CCK or CCKX of the current cell or the CCK or CCKX of any other cell. The LAs for which the CCK or CCKX is valid are always identified in the D-OTAR CCK PROVIDE PDU or D-OTAR CCKX PROVIDE PDU in the CCK information element.

The normal message sequence in this case shall be according to Figure 4.30.

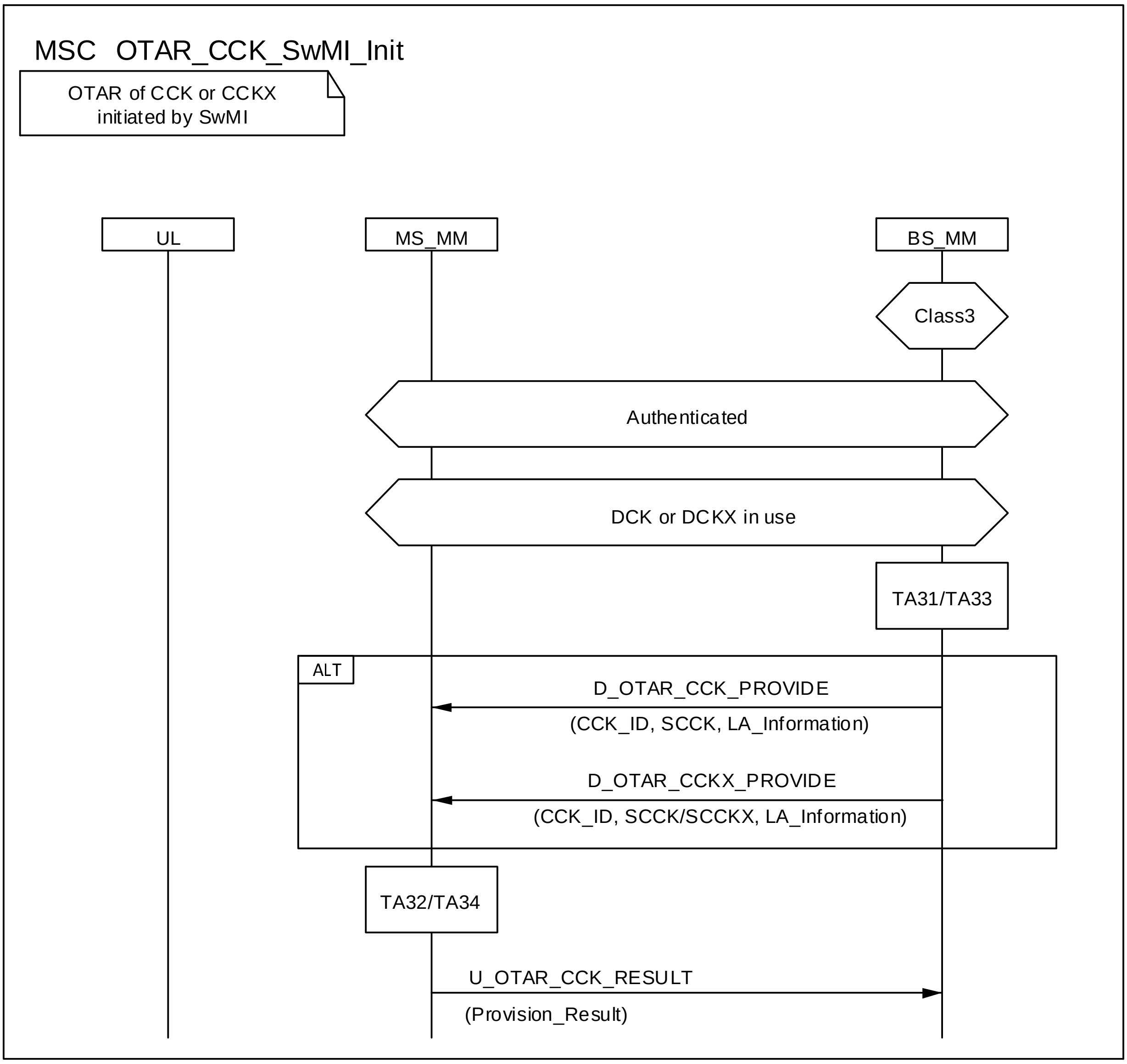


Figure 4.30: SwMI Initiated CCK or CCKX provision

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

The normal message sequence in this case shall be according to Figure 4.31.

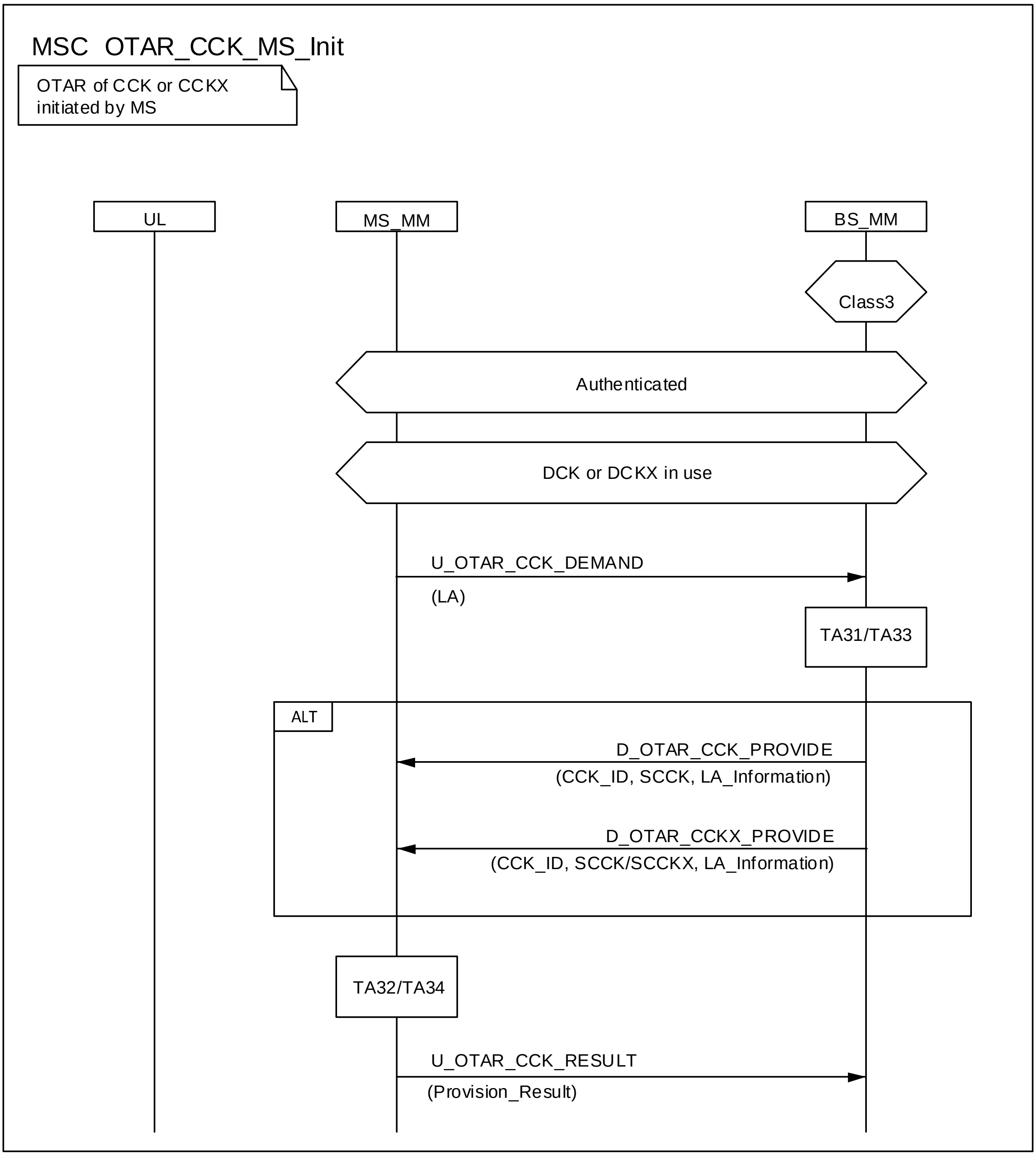


Figure 4.31: MS-initiated CCK or CCKX provision

4.5.1.3 MS-initiated CCK or CCKX 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 or CCKX for the new cell, or to forward register to a new cell using the announced type 1 cell re-selection mechanism. In order to support encrypted cell change to class 3 cells the U-PREPARE PDU may carry an U-OTAR CCK DEMANDPDU.

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

1) MS required to register:

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

2) MS not required to register:

   - the CCK request shall be sent in the U-OTAR CCK DEMANDPDU 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 or CCKX and DCK or DCKX 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 or CCKX of the new cell from its current serving cell by sending U-OTAR CCK DEMANDwith LA = LA of new cell. The U-OTAR CCK DEMANDPDU may be sent in the U-PREPARE PDU, in case MS is allowed to make the announced cell re-selection. The MS shall assume that DCK or DCKX is valid in the new cell.

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

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

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

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

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

4.5.2 OTAR protocol functions - Static Cipher Key

4.5.2.0 General

Up to seven SCKs may be distributed to the MS using the D-OTAR SCK PROVIDE PDU, and up to seven SCKs or SCKXs may be distributed to the MS using the D-OTAR SCKX PROVIDE PDU.

NOTE 1: The SwMI may provide fewer SCKXs to limit the maximum size of the D-OTAR SCKX PROVIDE PDU, depending on the capacity of channel in use. A limit of four SCKXs is advisable when using a phase modulation channel.

The provision may be started automatically by the SwMI or in response to a request from the MS using the U-OTAR SCK DEMANDPDU. The SwMI may take any knowledge that it has of the capabilities of the MS into account when deciding whether to provide SCKs using the D-OTAR SCK PROVIDE PDU or the D-OTAR SCKX PROVIDE PDU. SCKXs shall only be provided in the D-OTAR SCKX PROVIDE PDU.

The "SCK Use" element contained in each "SCK Key and Identifier" or "SCKX Key and Identifier" element within the PROVIDE PDUs shall be used by the MS to determine whether a particular SCK or SCKX is to be used in TMO or in DMO. The received value for the "SCK Use" element for a provided SCK or SCKX shall overwrite any previous value held by the MS for that SCK or SCKX. The most common cases are described by the MSCs and protocol description in clauses 4.5.2.1, 4.5.2.2, 4.5.2.3 and 4.5.2.4. An MS may request, and a SwMI may provide, SCKs or SCKXs to be used with more than one air interface encryption algorithm. A U-OTAR SCK DEMANDPDU shall only request SCKs or SCKXs to be used with a single KSG. A D-OTAR SCK PROVIDE PDU or D-OTAR SCKX PROVIDE PDU shall only provide SCKs or SCKXs for use with a single KSG. The KSG is identified in the "KSG number" element in the U-OTAR SCK DEMAND, D-OTAR SCK PROVIDE and D-OTAR SCKX PROVIDE PDUs. Multiple PDUs shall be sent if an MS is to be provided with keys to be used with more than one KSG. SCKs shall only be requested and provided where a KSG number indicating an air interface encryption algorithm in TEA set A is applicable. SCKXs shall only be requested and provided where a KSG number indicating an air interface encryption algorithm in TEA set B is applicable.

NOTE 2: The indication of KSG number permits an SCK set provided to an MS that has negotiated a KSG from TEA set B to contain both SCKs and SCKXs, and to support air interface encryption algorithms from TEA set A and from TEA set B. There is no equivalent mechanism to support provision of SCKXs to an MS that has negotiated a KSG from TEA set A.

A SwMI may provide an SCK or SCKX with an SCKN that has been requested by the MS, but assigned to a different KSG to that requested by the MS. In this case, the MS shall consider the KSG provided by the SwMI to be valid for that SCKN, and shall replace any previous association of SCK or SCKX to KSG for that SCKN.

The MS shall send the U-OTAR SCK RESULT PDU according to the rules below.

- For MS requests and where the SwMI provides keys individually addressed to the MS a result shall always be sent (Figure 4.32). When the SwMI responds individually addressed to the MS, the SwMI shall set the "Acknowledgement Flag" in the D-OTAR SCK PROVIDE or D-OTAR SCKX PROVIDE PDU to "Acknowledgement required" and "Explicit Response" to "Response to be sent whether state changed or not". However, the SwMI may provide keys addressed to a CMG GTSI, in response to an MS's individual request, in which case the MS shall interrogate the value of the "Acknowledgement Flag" to determine if an acknowledgement is required. If an acknowledgement is required the MS shall also interrogate the "Explicit Response" element in the D-OTAR SCK PROVIDE or D-OTAR SCKX PROVIDE PDU. If set to "Response to be sent whether state changed or not" the MS shall respond whether the key provide changes the MS state or not; if set to "Response to be sent only if state of MS is changed", the MS shall only respond if the SwMI provides a key or key version that the MS did not previously have.

- For SwMI provision to a single MS a response shall always be sent (Figure 4.33). The SwMI shall set "Acknowledgement Flag" to "Acknowledgement required" and Explicit Response to "Response to be sent whether state changed or not" when sending D-OTAR SCK PROVIDE or D-OTAR SCKX PROVIDE PDU to a single MS.

- For SwMI provision to CMG GTSI (Figure 4.34) the MS shall interrogate the value of the "Acknowledgement Flag" to determine if an acknowledgement is required. If an acknowledgement is required the MS shall also interrogate the "Explicit Response" element in the D-OTAR SCK PROVIDE or D-OTAR SCKX PROVIDE PDU. If set to "Response to be sent whether state changed or not" the MS shall respond whether the key provide changes the MS state or not; if set to "Response to be sent only if state of MS is changed", the MS shall only respond if the SwMI provides a key or key version that the MS did not previously have.

In all cases, all SCKs or SCKXs requested by the MS or provided by the SwMI in a single PDU shall belong to the same network, either the serving network in which case the "Address extension" element shall not be included, or any other network in which case the "Address extension" element shall be included and shall identify the network in which the SCKs or SCKXs are to be used. The "Address extension" element may also be used to specify the 'Open MNI' where SCKs or SCKXs are to be used with GTSIs containing the 'Open MNI'.

4.5.2.1 MS requests provision of SCK(s) or SCKX(s)

The scenario in Figure 4.32 shows the case where the MS requests provision of one or more SCKs or SCKXs in use on a system. The normal message sequence in this case shall be according to Figure 4.32 that shows the invocation of algorithms at each of MS and BS to satisfy the request.

NOTE: Figure 4.32 shows individual encryption of SCK using KSO and the alternative encryption of SCKX using KSOX, however use of GSKO or GSKOX as shown in Figure 4.34 is also possible for an individually or group addressed OTAR transmission. If the MS has migrated, KSO or KSOX (where used) is replaced by KSOv or KSOXv respectively.

The SwMI shall respond with the requested keys using the D-OTAR SCK PROVIDE PDU or D-OTAR SCKX PROVIDE PDU, together with the SCKN and SCK-VN information. The MS shall respond and inform the SwMI of the success or failure of the OTAR using the U-OTAR SCK RESULT PDU in accordance with the rules mentioned in clause 4.5.2. In case of failure, it shall indicate the reason, which may include failure to decrypt the key, or SwMI provided the wrong key.

For individual provision of SCKs or SCKXs to an MS, the "Max response timer value" element in the provision PDU shall be set to "0".

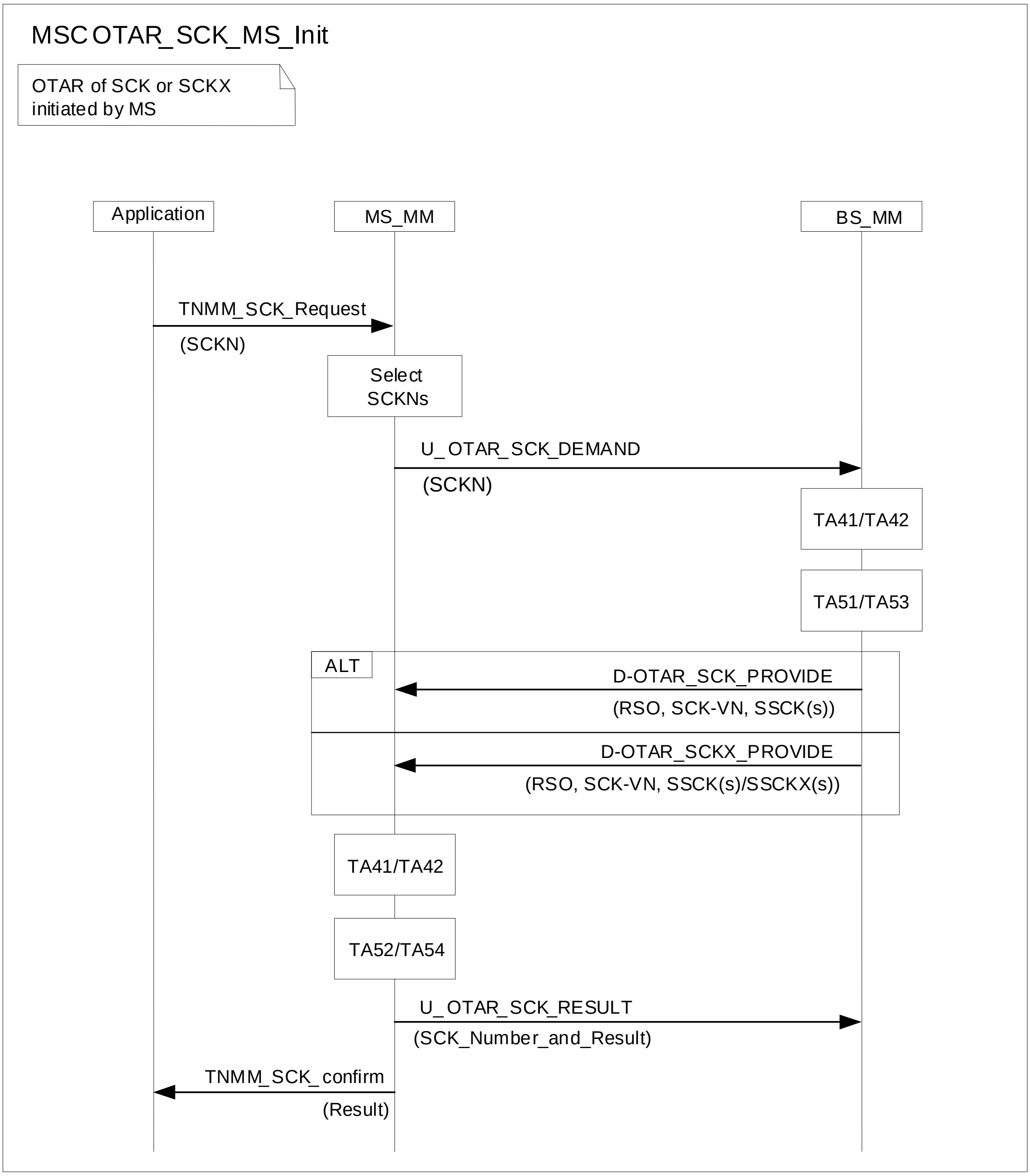


Figure 4.32: SCK or SCKX delivery initiated by MS to an individual

4.5.2.2 SwMI provides SCK(s) or SCKX(s) to individual MS

The scenario in Figure 4.33 shows the case where the SwMI provides one or more SCK(s) or SCKX(s) to an MS without the MS first requesting SCK provision. The SwMI may initiate this procedure at any time.

NOTE: Figure 4.33 shows individual encryption of SCK using KSO or SCKX using KSOX, however use of GSKO or GSKOX as shown in Figure 4.34 is also possible for an individually or group addressed OTAR transmission. If the MS has migrated, KSO (where used) is replaced by KSOv or KSOX is replaced by KSOXv.

For individual provision of SCKs or SCKXs to an MS, the "Max response timer value" element in the provision PDU shall be set to "0".

The MS shall respond and inform the SwMI of the success or failure of the OTAR using the U-OTAR SCK RESULT PDU. The options are as detailed in clause 4.5.2.1.

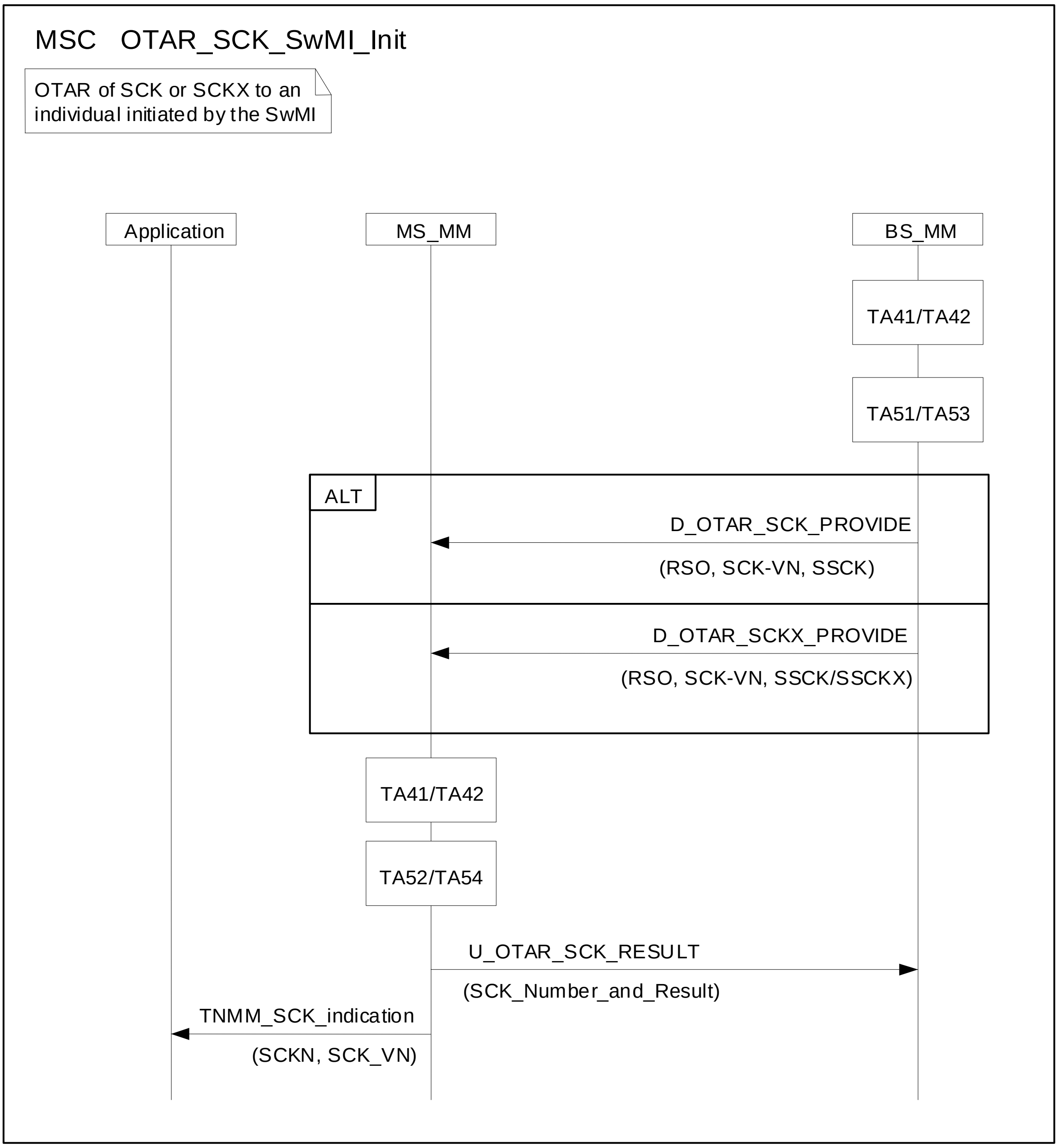


Figure 4.33: SCK or SCKX delivery to an individual initiated by SwMI

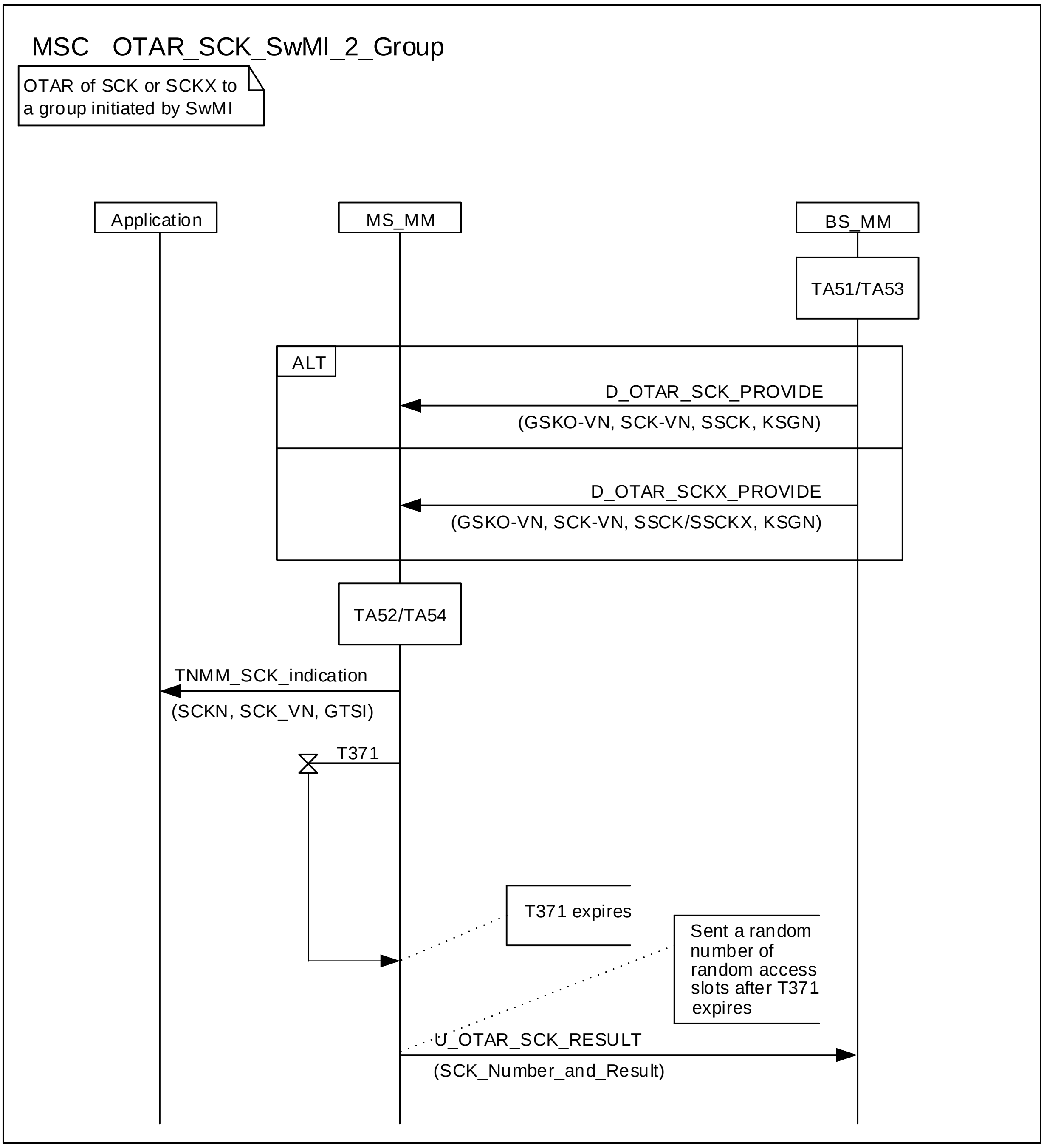
4.5.2.3 SwMI provides SCK(s) or SCKX(s) to group of MSs

In the case of group addressed delivery of SCK, BS_MM and MS_MM shall not run TA41, but shall use EGSKO as input to TA51 and TA52. In the case of group addressed delivery of SCKX, BS_MM and MS_MM shall not run TA42, but shall use GSKOX as input to TA53 and TA54. The U-OTAR SCK RESULT PDU shall be sent from MS to SwMI following the expiry of random timer T371 provided that the "Acknowledgement Flag" in the D-OTAR SCK PROVIDE or D-OTAR SCKX PROVIDE PDU is set to "Acknowledgement required" and either the key material provided is not currently stored in the MS, or the "Explicit response" element of the D-OTAR SCK PROVIDE or D-OTAR SCKX PROVIDE PDU is set to "Response to be sent whether state changed or not". T371 is started on reception of the D-OTAR SCK PROVIDE or D-OTAR SCKX PROVIDE PDU.

T371 is a timer with a value randomized to fall within the range 1 s and a maximum value that is signalled by the SwMI in the "Max response timer value" element of the PDU. This maximum value may be up to 65 535 s (18,2 hours). The MS shall select a value in this range when setting T371. When T371 expires the MS shall wait a further random number of random access signalling slots before sending the U-OTAR SCK RESULT PDU. The procedure for randomly selecting the signalling slot shall follow the procedure for "Choosing from a new access frame" as defined in ETSI EN 300 392-2 [2], clause 23.5.1.4.6. If the MS needs to leave the SwMI by sending ITSI-Detach signalling the MS shall consider T371 to have terminated and shall send the U-OTAR SCK RESULT PDU before detaching from the SwMI.

The scenario in Figure 4.34 shows the case where the SwMI provides one or more SCK(s) or SCKX(s) to a group of MSs identified by GTSI. The SwMI may initiate this procedure at any time.

The normal message sequence in this case shall be according to Figure 4.34.


MSC OTAR_SCK_SwMI_2_Group
OTAR of SCK or SCKX to a group initiated by SwMI
Application
MS_MM
BS_MM
TA51/TA53
ALT
D_OTAR_SCK_PROVIDE
(GSKO-VN, SCK-VN, SSCK, KSGN)
D_OTAR_SCKX_PROVIDE
(GSKO-VN, SCK-VN, SSCK/SSCKX, KSGN)
TA52/TA54
TNMM_SCK_indication
(SCKN, SCK_VN, GTSI)
T371
T371 expires
Sent a random number of random access slots after T371 expires
U_OTAR_SCK_RESULT
(SCK_Number_and_Result)

NOTE: Although SCK or SCKX is sealed by the group key, the D-OTAR SCK PROVIDE or D-OTAR SCKX PROVIDE PDU may be distributed to either a group or an individual address and encrypted appropriately.

Figure 4.34: SCK or SCKX delivery to a group initiated by SwMI

4.5.2.4 SwMI rejects provision of SCK or SCKX

If the SwMI is unable to provide an SCK or an SCKX the provision request shall be explicitly rejected using the D-OTAR SCK REJECT PDU indicating the reason for rejection. The SwMI shall indicate to the MS how long the MS shall wait before retrying a request for SCK or SCKX by setting the value of the "OTAR retry interval" element. The behaviour of the MS shall be as described in clause 4.5.12.

4.5.3 OTAR protocol functions - Group Cipher Key

4.5.3.0 General

Up to seven GCKs or GCKXs may be distributed to the MS using the D-OTAR GCK PROVIDE PDU or the D-OTAR GCKX 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 DEMANDPDU. The most common cases are described by the MSCs and protocol description in the present clause.

NOTE: The SwMI may provide fewer GCKXs to limit the maximum size of the D-OTAR GCKX PROVIDE PDU, depending on the capacity of channel in use. A limit of four GCKXs is advisable when using a phase modulation channel.

The MS shall send U-OTAR GCK RESULT PDU according to the rules below:

- For MS requests, and where the SwMI provides keys individually addressed to the MS, a result shall be sent (Figure 4.35 and Figure 4.36). When the SwMI responds individually addressed to the MS, the SwMI shall set "Acknowledgement Flag" in the D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE PDU to "Acknowledgement required" and "Explicit Response" to "Response to be sent whether state changed or not". However, the SwMI may provide keys addressed to a CMG GTSI, in response to an MS's individual request, in which case the MS shall interrogate the value of the "Acknowledgement Flag" in the D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE PDU to determine if an acknowledgement is required. If an acknowledgement is required the MS shall also interrogate the "Explicit Response" element in the D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE PDU. If set to "Response to be sent whether state changed or not" the MS shall respond whether the key provide changes the MS state or not; if set to "Response to be sent only if state of MS is changed", the MS shall only respond if the SwMI provides a key or key version that the MS did not previously have.

- For SwMI provision to a single MS a response shall always be sent (Figure 4.35). The SwMI shall set "Acknowledgement Flag" to "Acknowledgement required" and "Explicit Response" to "Response to be sent whether state changed or not" when sending the D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE PDU to a single MS.

- For SwMI provision to a CMG GTSI the MS shall interrogate the value of the "Acknowledgement Flag" to determine if an acknowledgement is required. If an acknowledgement is required the MS shall also interrogate the "Explicit Response" element in the D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE PDU. If set to "Response to be sent whether state changed or not" the MS shall respond whether the key provide changes the MS state or not; if set to "Response to be sent only if state of MS is changed", the MS shall only respond if the SwMI provides a key or key version that the MS did not previously have.

In all cases, all GCKs or GCKXs requested by the MS or provided by the SwMI in a single PDU shall be valid in the same network which shall be the serving network. There is no "Address extension" element in the PDU.

All GCKs or GCKXs provided by the SwMI in a single PDU shall apply to the same KSG, indicated by the "KSG number" element in the PDU. The SwMI shall not provide GCKs or GCKXs to an MS that are for use with a different KSG to the KSG negotiated by the MS.

4.5.3.1 MS requests provision of GCK or GCKX

The scenario in Figure 4.35 shows the case where the MS requests provision of a GCK or GCKX for a group. The MS may initiate this procedure in accordance with clause 4.5.14.

The MS may request GCKs or GCKXs associated with one or more GSSIs in which case it shall send a U-OTAR GCK DEMAND PDU to the SwMI indicating that it is requesting GCKs or GCKXs referenced by one or more GSSIs and shall include the GSSIs or GTSIs of the requested group(s). Alternatively, the MS may request a new version of one or more GCKs or GCKXs that it already possesses, or that it expects due to a Key Association. In this case, it shall send a U-OTAR GCK DEMANDPDU to the SwMI indicating that it is requesting one or more GCKs or GCKXs referenced by GCKNs, and shall include the GCKNs of the requested key(s). The MS may request GCKs or GCKXs referenced by GSSIs and GCKs or GCKXs referenced by GCKNs in the same PDU; however the total number of requests shall not exceed seven in a single U-OTAR GCK DEMANDPDU.

All GCKs or GCKXs requested in a single PDU shall belong to the same network which shall be the serving network.

The normal message sequence in this case shall be according to Figure 4.35.

NOTE: Figure 4.35 shows individual encryption of GCK using KSO or of GCKX using KSOX, however use of GSKO or GSKOX as shown in Figure 4.37 is also possible for an individually or group addressed OTAR transmission. If the MS has migrated, KSO (where used) is replaced by KSOv, or KSOX (where used) is replaced by KSOXv.

For individual provision of GCKs to an MS using KSO or KSOX (or KSOv or KSOXv if migrated) as the sealing key, the "Max response timer value" element in the provision PDU shall be set to indicate "Immediate response".

The SwMI shall respond with the requested keys using the D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE PDU, together with the GCKN and GCK-VN information. The MS shall respond and inform the SwMI of the success or failure of the OTAR using the U-OTAR GCK RESULT PDU in accordance with the rules in clause 4.5.3. In case of failure, it shall indicate the reason, which may include failure to decrypt key, or SwMI provided the wrong key.

The MS shall only request GCKs or GCKXs for the KSG that has been negotiated with the SwMI.

If the KSG identified in the U-OTAR GCK DEMAND PDU is invalid the SwMI shall respond with error indication "KSG number not supported" in the D-OTAR GCK REJECT PDU.

If the KSG identified in the D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE PDU is invalid the MS shall respond with error indication "KSG number not supported" in the U-OTAR GCK RESULT PDU.

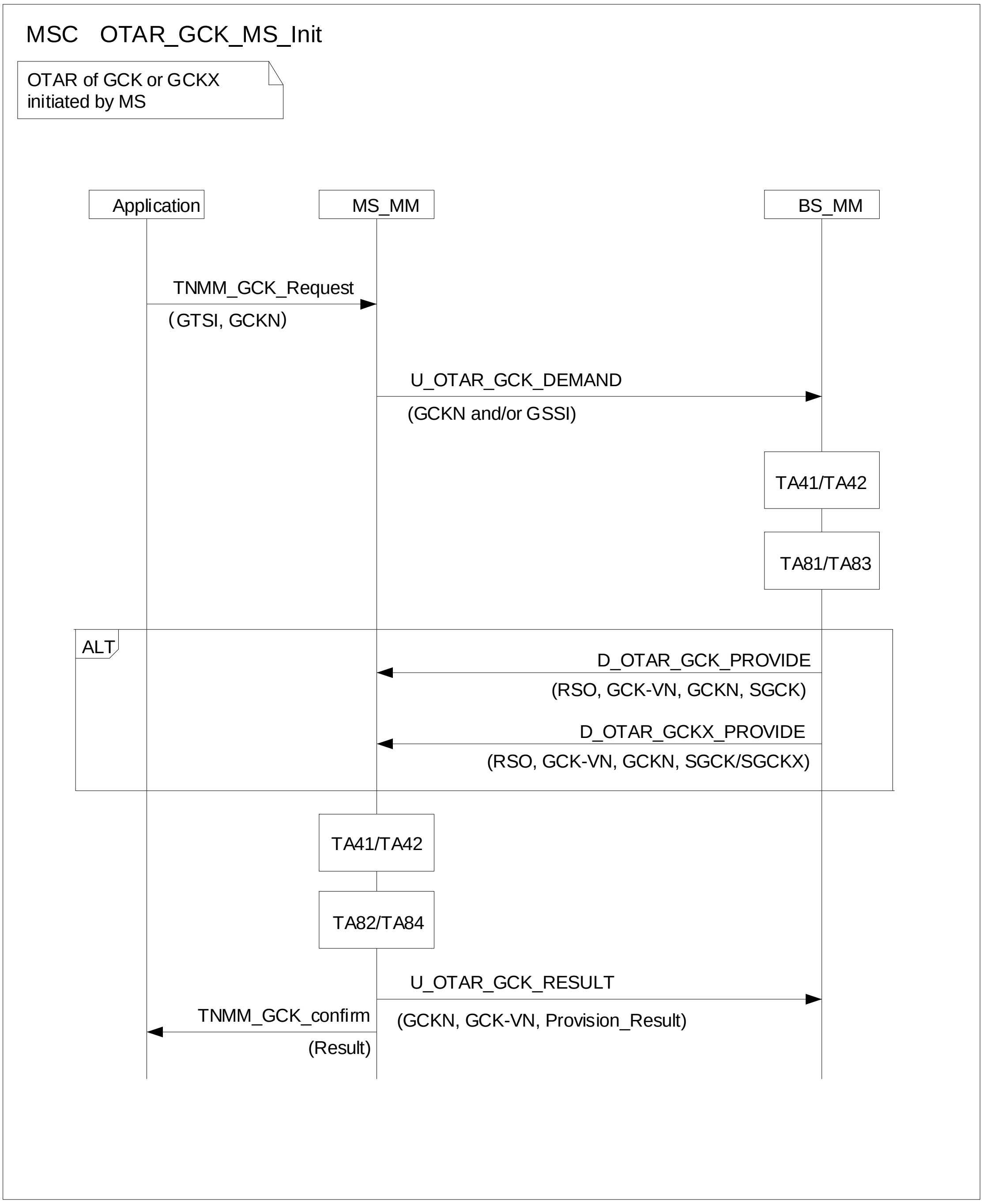


Figure 4.35: GCK or GCKX delivery initiated by MS to an individual

4.5.3.2 SwMI provides GCK or GCKX to an individual MS

The scenario in Figure 4.36 shows the case where the SwMI provides a GCK or GCKX to an MS without the MS first requesting GCK or GCKX provision. The SwMI may initiate this procedure at any time. The SwMI shall provide the GCK or GCKX to the MS using the D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE PDU. The SwMI may provide one or more GCKs or GCKXs, each associated with a specific GSSI, in which case the "Group Association" element in the PDU shall indicate "GSSI" and the SwMI shall provide the GSSI. Alternatively, the GCK(s) or GCKX(s) may be either newer versions of a GCK or GCKX that the MS already possesses, or new GCK(s) or GCKX(s) which will subsequently be associated with one or more GSSIs. In this alternative case the "Group Association" element in the PDU shall indicate "GCKN" and the SwMI shall provide the GCKN relevant to the GCK or GCKX.

The normal message sequence in this case shall be according to Figure 4.36.

NOTE: Figure 4.36 shows individual encryption of GCK or GCKX using KSO, however use of GSKO or GSKOX as shown in Figure 4.37 is also possible for an individually or group addressed OTAR transmission. If the MS has migrated, KSO (where used) is replaced by KSOv, or KSOX (where used) is replaced by KSOXv.

For individual provision of GCKs or GCKXs to an MS using KSO or KSOX (or KSOv or KSOXv if migrated) as the sealing key, the "Max response timer value" element in the provision PDU shall be set to indicate "Immediate response". The MS shall respond and inform the SwMI of the success or failure of the OTAR using the U-OTAR GCK RESULT PDU. The options are as detailed in clause 4.5.3.1.

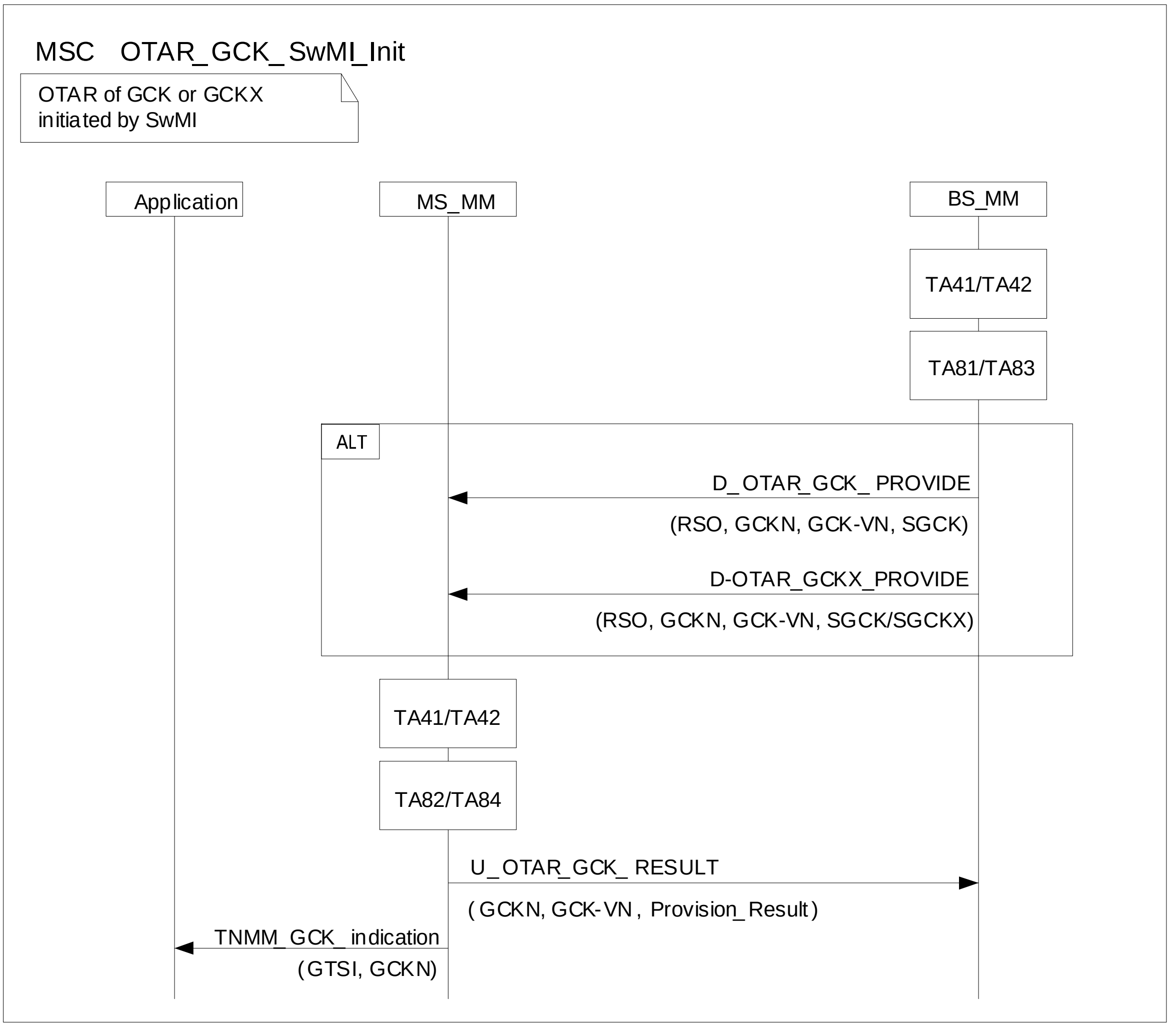


Figure 4.36: GCK or GCKX delivery initiated by SwMI to an individual

4.5.3.3 SwMI provides GCK or GCKX to a group of MSs

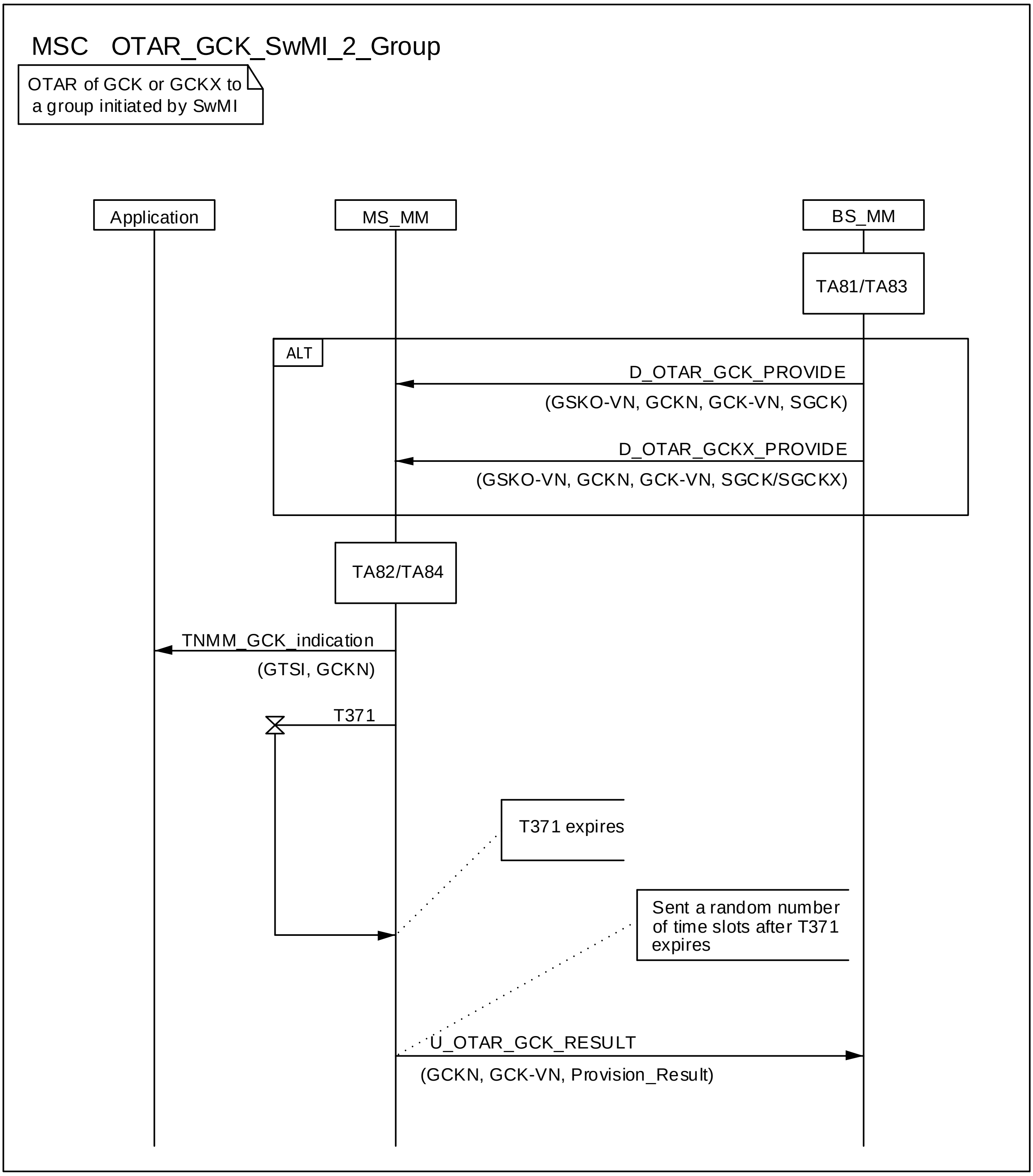
In the case of group sealed delivery of GCK, BS_MM and MS_MM shall not run TA41, but shall use EGSKO as input to TA81 and TA82.

In the case of group sealed delivery of GCKX, BS_MM and MS_MM shall not run TA42, but shall use GSKOX as input to TA83 and TA84.

The U-OTAR GCK RESULT PDU shall be sent from MS to SwMI following the expiry of random timer T371 provided that the "Acknowledgement Flag" in the D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE PDU is set to "Acknowledgement required" and either the key material provided is not currently stored in the MS, or the "Explicit response" element of the D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE PDU is set to "Response to be sent whether state changed or not". T371 is started on reception of the D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE PDU.

T371 is a timer with a value randomized to fall within the range 1 s and a maximum value that is signalled by the SwMI in the "Max response timer value" element of the PDU. This maximum value may be up to 65 535 s (18,2 hours). The MS shall select a value in this range when setting T371. When T371 expires the MS shall wait a further random number of random access signalling slots before sending the U-OTAR GCK RESULT PDU. The procedure for randomly selecting the signalling slot shall follow the procedure for "Choosing from a new access frame" as defined in ETSI EN 300 392-2 [2], clause 23.5.1.4.6. If the MS needs to leave the SwMI by sending ITSI-Detach signalling the MS shall consider T371 to have terminated and shall send the U-OTAR GCK RESULT PDU before detaching from the SwMI.

The normal message sequence in this case shall be according to Figure 4.37.


MSC OTAR_GCK_SwMI_2_Group
OTAR of GCK or GCKX to a group initiated by SwMI
Application
MS_MM
BS_MM
TA81/TA83
ALT
D_OTAR_GCK_PROVIDE
(GSKO-VN, GCKN, GCK-VN, SGCK)
D_OTAR_GCKX_PROVIDE
(GSKO-VN, GCKN, GCK-VN, SGCK/SGCKX)
TA82/TA84
TNMM_GCK_indication
(GTSI, GCKN)
T371
T371 expires
Sent a random number of time slots after T371 expires
U_OTAR_GCK_RESULT
(GCKN, GCK-VN, Provision_Result)

NOTE: Although GCK or GCKX is sealed by the group key, the D-OTAR GCK PROVIDE may be distributed to either a group or an individual address and encrypted appropriately.

Figure 4.37: GCK delivery to a group initiated by SwMI

4.5.3.4 SwMI rejects provision of GCK or GCKX

If the SwMI is unable to provide a GCK or GCKX the provision request shall be explicitly rejected using the D-OTAR GCK REJECT PDU indicating the reason for rejection. The SwMI shall indicate to the MS how long the MS shall wait before retrying a request for GCK or GCKX by setting the value of the "OTAR retry interval" element. The behaviour of the MS shall be as described in clause 4.5.12.

4.5.4 Cipher key association to group address

4.5.4.0 General

When provisioning a GSSI into an MS's group database using SS-DGNA, the SwMI may provide a "GCK Association" and/or "SCK Association" by including the "Security Related Information" element in D-FACILITY (ASSIGN) PDU. The "Security Related Information" element is specified in clause A.8.77b.

Table 4.10: Void

When performing group attachment, the SwMI may provide a "GCK Association" and/or "SCK Association" by including a new "Group Identity Security Related Information" element in D-ATTACH/DETACH GROUP IDENTITY, D-ATTACH/DETACH GROUP IDENTITY ACK and D-LOCATION UPDATE ACCEPT. The "Group Identity Security Related Information" is specified in clause A.8.31a.

Table 4.11: Void

4.5.4.1 Static Cipher Key association for DMO

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

The SwMI may request that the MS associates a particular SCK or SCKX (identified by SCKN) with up to 30 groups (identified by the "Number of groups" element of the D-OTAR KEY ASSOCIATE DEMAND PDU) for which the GSSI of each is listed, or for a range of groups identified by the first and last GSSIs in the range. In this case the key-type element of the D-OTAR KEY ASSOCIATE DEMAND PDU shall be set to SCK.

The SwMI may request that the MS associates more than one SCK or SCKX to one or more groups, where the SCKs or SCKXs are members of the same KAG in different SCK subsets. In this case, it will also identify the structure of the subsets and the member SCK or SCKX to be associated. This is described in clause 4.5.4.2.

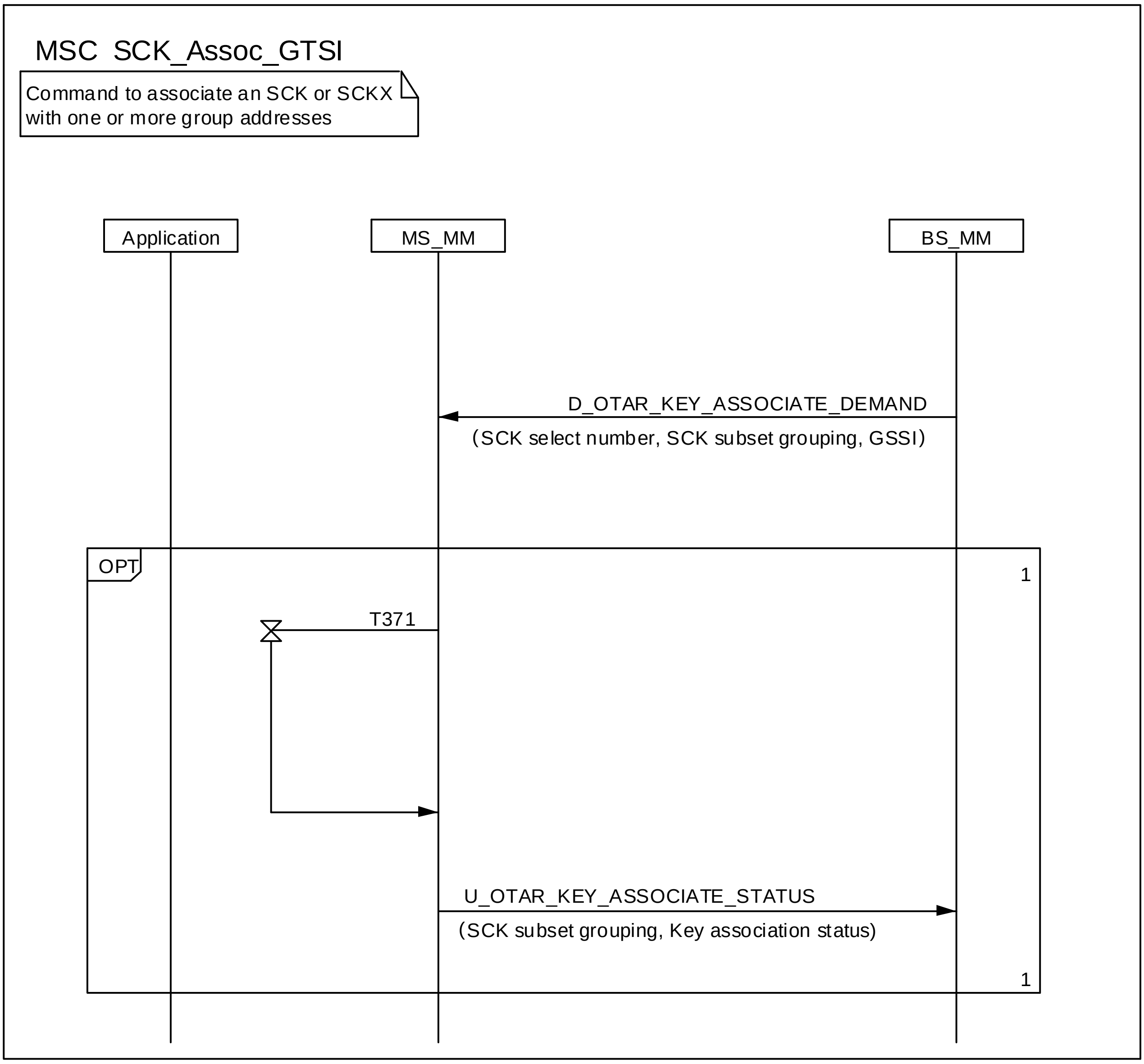
The SwMI may request that the MS associates one or more SCKs or SCKXs to one or more groups where those groups belong to a different network, i.e. the requested DMO network has a different MNI to that of the SwMI. In this case, the SwMI shall indicate the network code of the relevant network using the "Address extension" element in the D-OTAR KEY ASSOCIATE DEMAND PDU. The SCK set from which the SCKs or SCKXs are taken and the DMO network shall have the same MNI, which shall be that indicated by the "Address extension" element.

A later association shall take precedence over an earlier association. This allows the SwMI to make associations to ranges and sub-ranges of groups. The SwMI may associate one key with a wide range of groups, and then make an association of a second key with a narrower range within the first range. In this case, the first association still applies over the wide range with the exception of the narrow range, where the second later association shall apply.

The SwMI may also demand that groups be associated to SCKs or SCKXs by groups of MSs. In this case, the D-OTAR KEY ASSOCIATE DEMAND PDU is addressed to the group of MSs. If the "Acknowledgement Flag" element is set to indicate "Acknowledgement required" the MS shall respond on expiry of random timer T371 provided that either the key association is new to the MS, or provided that the "Explicit response" element of the D-OTAR KEY ASSOCIATE DEMAND PDU is set to "Response to be sent whether state changed or not". If so the MS shall start random timer T371 on reception of the D-OTAR KEY ASSOCIATE DEMAND PDU and send the U-OTAR KEY ASSOCIATE STATUS on expiry of T371. If the "Explicit response" element is set to "0" (i.e. "Response to be sent only if the state has changed"), and the D-OTAR KEY ASSOCIATE DEMAND PDU does not change the MS's state (it already has the key association being signalled) it shall not send acknowledgement. If the MS needs to detach from the SwMI before sending the acknowledgement to the SwMI, it shall consider T371 to have expired and shall send the acknowledgement before detaching. T371 is described in clause 4.5.2.3. If the MS is unable to send the Result PDU before detaching, it should store the PDU and send it next time it attaches to the SwMI, even if is switched off and on again in the meantime.

The value of T371 shall be provided to the MS by the SwMI in the "Max response timer value" element. If the PDU is individually addressed to a single MS, this element shall be set to "0".

The normal message sequence in this case shall be according to Figure 4.38.

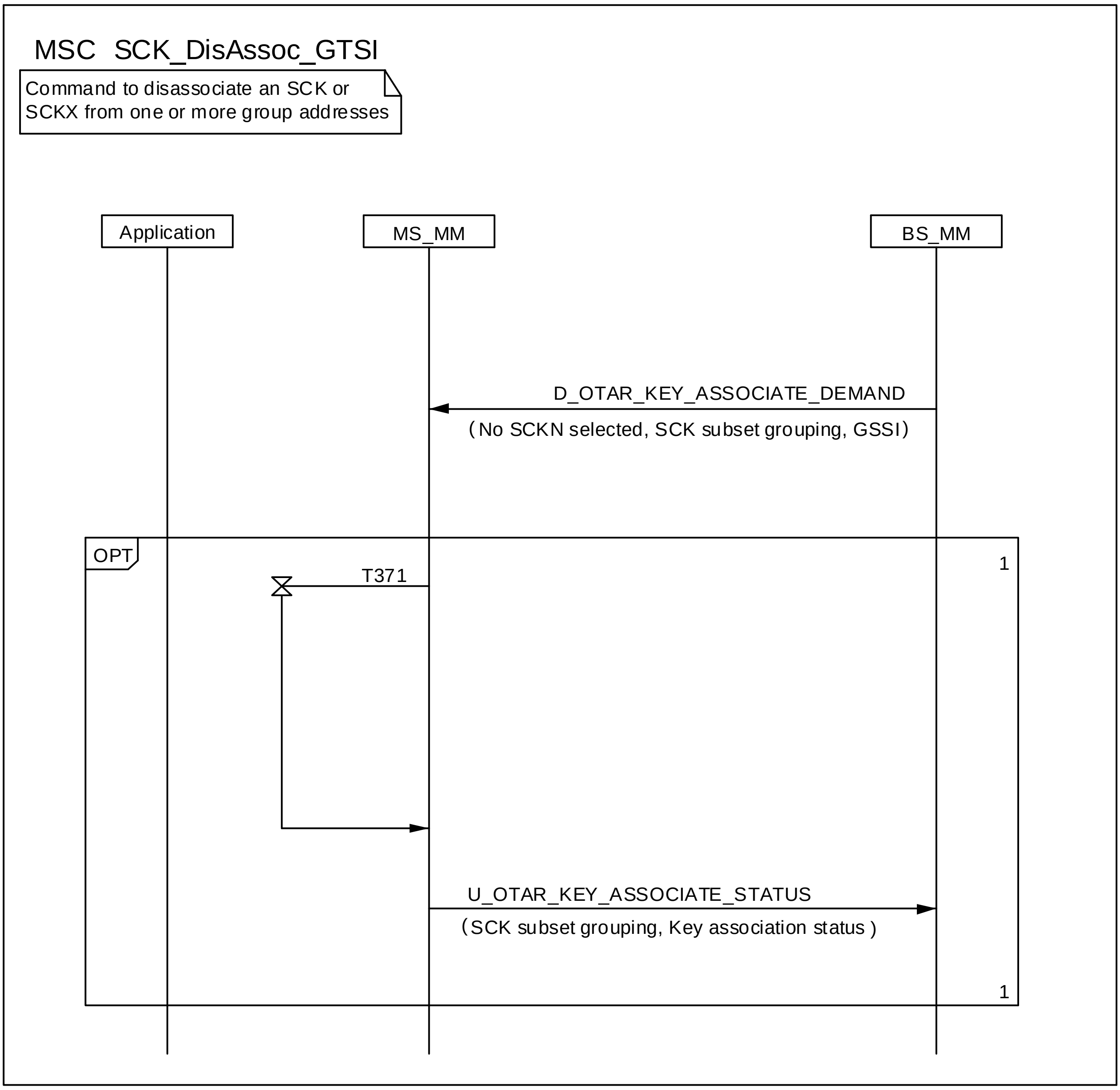

MSC SCK_Assoc_GTSI
Command to associate an SCK or SCKX with one or more group addresses
Application
MS_MM
BS_MM
D_OTAR_KEY_ASSOCIATE_DEMAND
(SCK select number, SCK subset grouping, GSSI)
OPT
1
T371
U_OTAR_KEY_ASSOCIATE_STATUS
(SCK subset grouping, Key association status)
1

NOTE: The optional sequence is employed if the rules for sending U-OTAR KEY ASSOCIATE STATUS defined in clause 4.5.4.1 are enabled.

Figure 4.38: SCK or SCKX association by SwMI

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

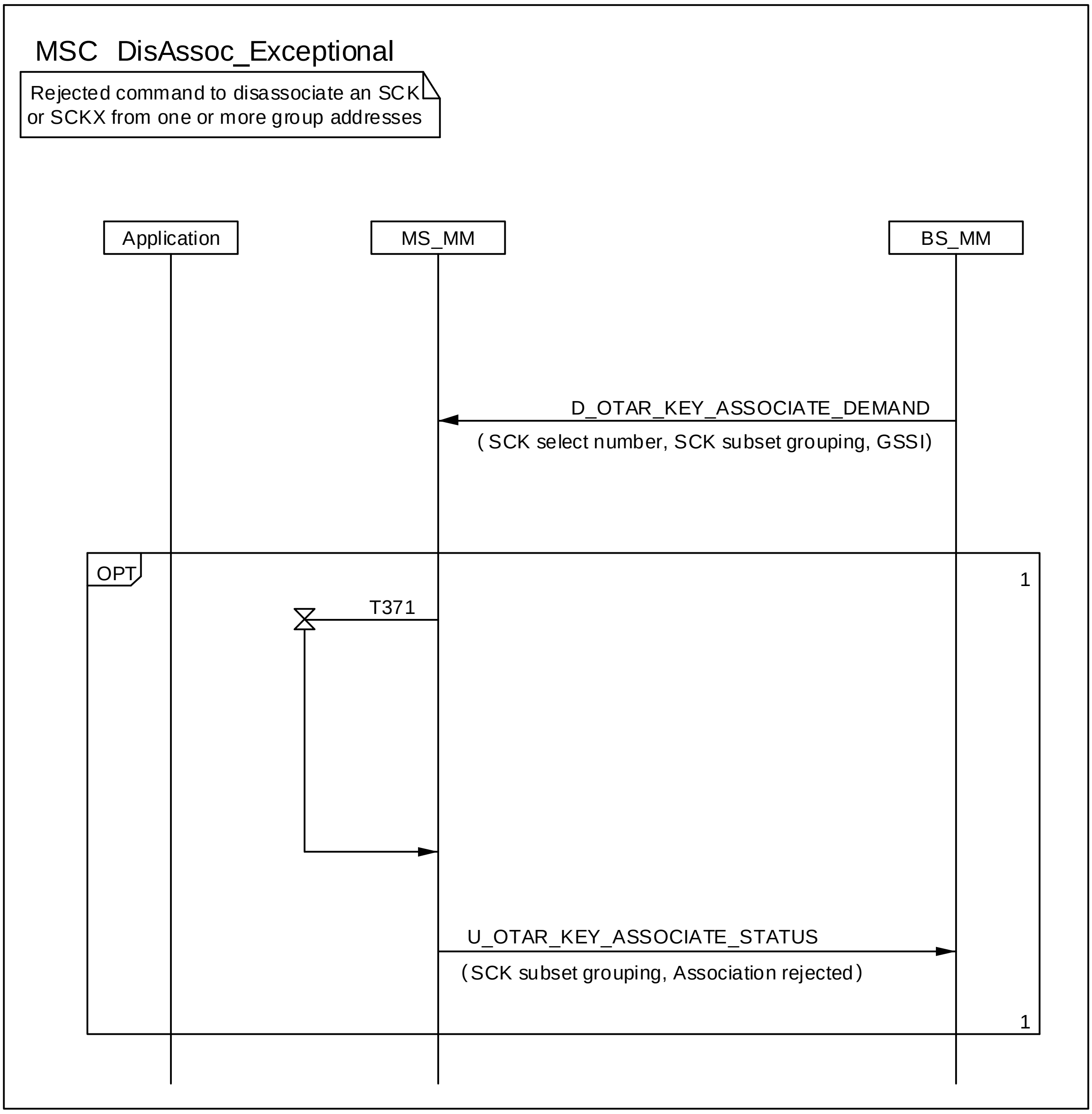
The normal message sequence in this case shall be according to Figure 4.39.


MSC SCK_DisAssoc_GTSI
Command to disassociate an SCK or SCKX from one or more group addresses
Application
MS_MM
BS_MM
D_OTAR_KEY_ASSOCIATE_DEMAND
(No SCKN selected, SCK subset grouping, GSSI)
OPT
1
T371
U_OTAR_KEY_ASSOCIATE_STATUS
(SCK subset grouping, Key association status)
1

NOTE: The optional sequence is employed if the rules for sending U-OTAR KEY ASSOCIATE STATUS defined in clause 4.5.4.1 are enabled.

Figure 4.39: SCK or SCKX disassociation by SwMI

If in either case, the SwMI requests the MS to associate keys with GSSIs that the MS does not possess, the MS can reject the association and indicate the status of this back to the SwMI. If the SwMI requests the MS to associate keys with a range of GSSIs, and the MS does not have GSSIs either at the end points of the range, or elsewhere in the range, it should still accept and maintain this association in case groups are subsequently loaded within this range.


MSC DisAssoc_Exceptional
Rejected command to disassociate an SCK or SCKX from one or more group addresses
Application
MS_MM
BS_MM
D_OTAR_KEY_ASSOCIATE_DEMAND
(SCK select number, SCK subset grouping, GSSI)
OPT
1
T371
U_OTAR_KEY_ASSOCIATE_STATUS
(SCK subset grouping, Association rejected)
1

NOTE: The optional sequence is employed if the rules for sending U-OTAR KEY ASSOCIATE STATUS defined in clause 4.5.4.1 are enabled.

Figure 4.40: Rejection of SCK or SCKX disassociation

4.5.4.2 Group Cipher Key association

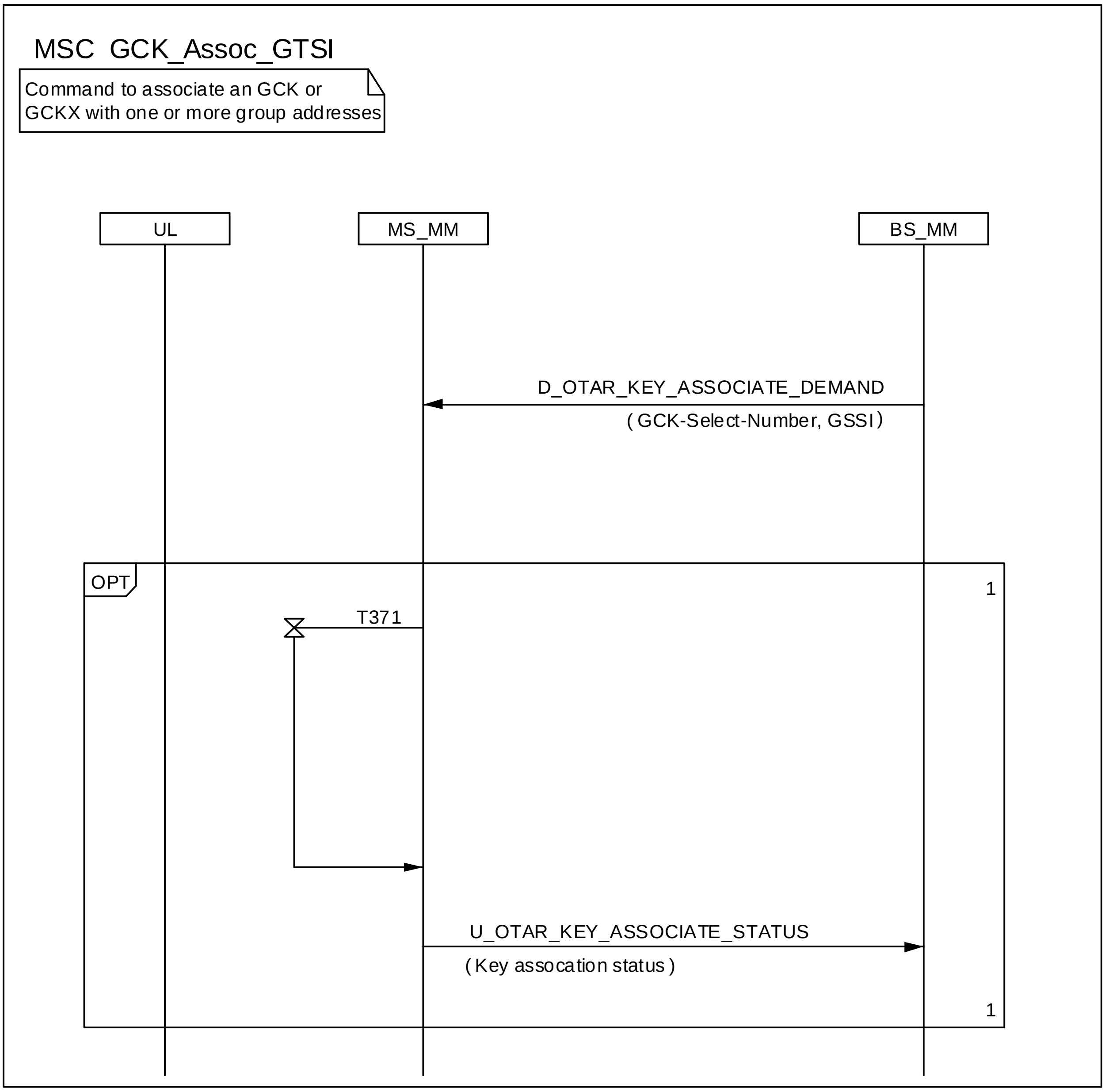
The scenario in Figure 4.41 shows the case where the SwMI requests the MS to associate a GCK or GCKX (which the MS already has) with between 1 and 30 groups or a range of groups where the ends of the range are identified by a lower and higher value of GSSI.

The SwMI may request that the MS associates GCKs or GCKXs to groups where those groups are home to a different network, i.e. the MNI of the group is different to that of the serving SwMI. The GCKs or GCKXs are valid for use on the serving SwMI only. In this case, the "Address extension" element is used to indicate the identity of the network which is home to the group for which the association shall be valid. The association shall only be valid in the serving network.

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

The value of T371 shall be provided to the MS by the SwMI in the "Max response timer value" element. If the PDU is individually addressed to a single MS, this element shall be set to "0".

The normal message sequence in this case shall be according to Figure 4.41.


MSC GCK_Assoc_GTSI
Command to associate an GCK or GCKX with one or more group addresses
UL
MS_MM
BS_MM
D_OTAR_KEY_ASSOCIATE_DEMAND
(GCK-Select-Number, GSSI)
OPT
1
T371
U_OTAR_KEY_ASSOCIATE_STATUS
(Key assocation status)
1

NOTE: The optional sequence is employed if the rules for sending U-OTAR KEY ASSOCIATE STATUS defined in clause 4.5.4.2 are enabled.

Figure 4.41: GCK and GCKX association by SwMI

The SwMI may demand that the GCKs or GCKXs currently associated with the groups are disassociated forcing the groups to revert to using CCK (for security class 3 systems). This is done by setting the "GCK select number" element to the value for "No GCKN selected".

If in either case, the SwMI requests the MS to associate keys with GSSIs that the MS does not possess, the MS can reject the association and indicate the status of this back to the SwMI. If the SwMI requests the MS to associate keys with a range of GSSIs, and the MS does not have GSSIs either at the end points of the range, or elsewhere in the range, it should still accept and maintain this association in case groups are subsequently loaded within this range.

When using DGNA SS-DGNA defined in ETSI EN 300 392-12-22 [7] the "Security related information" element includes "GCK select number" only to associate a GCK to the address defined in the core of the SS-DGNA message.

4.5.5 Notification of key change over the air

4.5.5.0 General

The MM security function of the BS/SwMI shall use the exchange shown in Figure 4.42 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 4.5.1 to 4.5.3.

The D-CK CHANGE DEMAND/U-CK CHANGE RESULT PDU shall be used to explicitly inform the MS of the time when a key shall be considered valid. The time may be described as either a value representing IV (composed of slot number, frame number, multiframe number and hyper frame number), or a time based upon TETRA network time as described in ETSI EN 300 392-2 [2]. The key-id shall be one of CCK-id, SCKN, and GCKN. The scope of the D-CK CHANGE DEMAND/U-CK CHANGE RESULT protocol exchange is the current cell, except where the indicated key type is a DMO-SCK. The D-CK CHANGE DEMAND PDU shall only be used to inform the MS of keys for use on the serving network. Change of active SCKs or SCKXs for use with DMO networks with different MNI from that of the SwMI shall be indicated using the D-DM-SCK ACTIVATE DEMAND PDU. The D-DM-SCK ACTIVATE DEMAND PDU may also be used to indicate active SCKs or SCKXs on DMO networks with the same MNI as the SwMI.

On receipt of the D-CK CHANGE DEMAND or D-DM-SCK ACTIVATE DEMAND PDUs 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 PDU using the U-CK CHANGE RESULT PDU, or acknowledge the D-DM-SCK ACTIVATE DEMAND PDU using the U-DM-SCK ACTIVATE RESULT PDU.

If the MS does not possess the key it shall request the key from the SwMI using the appropriate OTAR request PDU. The MS shall randomize the sending of the OTAR request over the time interval between reception of the D-CK CHANGE DEMAND PDU and the actual time when the change will occur. If the OTAR request is not sent before leaving the cell or detaching from the SwMI the requirement to request the key shall be cancelled.

Acknowledgement of the D-CK CHANGE DEMAND or D-DM-SCK ACTIVATE DEMAND PDUs shall be made for ITSI based key delivery using the U-CK CHANGE RESULT PDU or U-DM-SCK ACTIVATE RESULT PDU by setting the "Acknowledgement flag" element on the downlink PDU to "1". If this is set to "1", the MS shall acknowledge whether the demand changes the MS's state or not.

The D-CK CHANGE DEMAND and D-DM-SCK ACTIVATE DEMAND PDUs may also be transmitted addressed to a group of MSs or the broadcast address. In this case the acknowledgement is optional, either acknowledgement shall not be requested by setting the "Acknowledgement flag" element to FALSE, or if acknowledgement is requested the MS shall start timer T371 with a randomly selected value on receipt of the D-CK CHANGE DEMAND or D-DM-SCK ACTIVATE DEMAND PDUs. However, even if the "Acknowledgement flag" = "1", the MS shall only acknowledge if the D-CK CHANGE DEMAND or D-DM-SCK ACTIVATE DEMAND PDUs change its state, i.e. it has not already received and stored the result of the same key change command. The procedure for randomly selecting the signalling slot shall follow the procedure for "Choosing from a new access frame" as defined in ETSI EN 300 392-2 [2], clause 23.5.1.4.6. On expiry of T371, the MS responds with a U-CK CHANGE RESULT PDU or D-DM-SCK ACTIVATE DEMAND as appropriate. The value of T371 shall be such that the acknowledgement is received by the SwMI before the time that the key becomes valid.

The value of T371 shall be randomized over the time interval between receipt of the PDU and the time identified in the PDU for the key change.

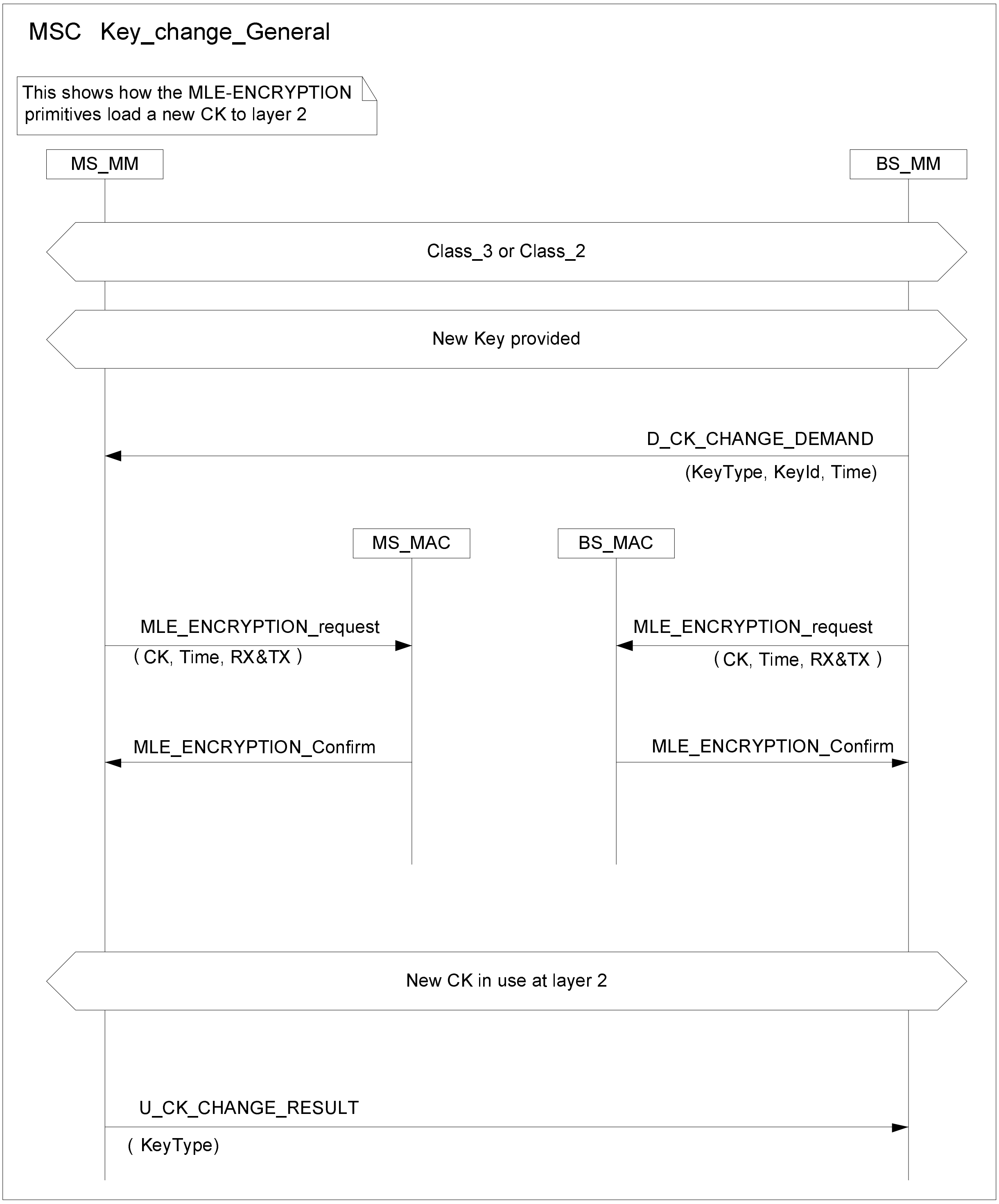


Figure 4.42: Key change protocol

4.5.5.1 Change of Derived Cipher Key

The DCK or DCKX shall be changed explicitly using the authentication protocols described in clause 4.4.2.

The DCK or DCKX in use shall change at the following times:

- on successful authentication;
- if a DCK or DCKX 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.

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

4.5.5.2 Change of Common Cipher Key

The SwMI may administer the change of CCK or CCKX using the D-CK CHANGE DEMAND PDU. Each cell in an LA shall update the CCK or CCKX in use as indicated in the D-CK CHANGE DEMAND PDU.

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

The SwMI MM shall notify all MSs in the cell of the new CCK-id in the SYSINFO, SYSINFO-DA or SYSINFO-Q broadcast and in the header of the MAC-RESOURCE PDU described in clause 6.5.1.

When the SwMI changes the CCK or CCKX for downlink, it will still receive two slots where ESIs are encrypted with the old CCK or CCKX on the uplink (or where the MAE mechanism is applied with the old CCKX in these two slots). For the duration of these two slots the SwMI shall use old CCK or CCKX for decrypting ESI or MAE addresses in the uplink and new CCK or CCKX for encrypting in the downlink.

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

4.5.5.3 Change of Group Cipher Key

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

The SwMI may choose to link the crypto-periods of all GCKs and GCKXs on the network, in this case all GCKs and GCKXs have the same GCK-VN and only one GCK-VN need be conveyed to the MS. If the SwMI supports the latter mechanism, a short GCK-VN (representing the 2 least significant bits of the GCK-VN) shall be conveyed in the "Security Information Element" of SYSINFO, SYSINFO-DA or SYSINFO-Q, with the full GCK-VN provided using the D-CK CHANGE DEMAND PDU with "Key Change Type" of "All GCKs".

4.5.5.4 Change of Static Cipher Key for TMO

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

The SwMI MM shall notify all MSs in the cell of the new SCKN/SCK-VN in the SYSINFO, SYSINFO-DA or SYSINFO-Q broadcast, and SCK-VN in the header of the MAC-RESOURCE PDU described in clause 6.5.1.

When the SwMI changes the SCK or SCKX for downlink, it will still receive two slots encrypted with the old SCK or SCKX. For the duration of these two slots the SwMI shall use old SCK or SCKX for decrypting ESI or MAE addresses and message contents in the uplink and new SCK or SCKX for encrypting in the downlink.

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

4.5.5.5 Change of Static Cipher Key for DMO

The "SCK use" element in the OTAR SCK PROVIDE or D-OTAR SCKX Provide PDU shall indicate whether the SCK or SCKX is to be used for DMO or TMO operation. The SwMI may use the D-CK CHANGE DEMAND PDU to inform the MS which SCK(s) or SCKX(s) are in use for Direct Mode Operation (DMO) provided the MNI of the relevant DMO GTSIs is the same as the MNI of the SwMI. The use of SCK or SCKX in DMO shall be indicated in the "SCK use" element. The change of SCK or SCKX may be immediate or may instead occur on a specific IV/network time. The SwMI may indicate whether one or several specific SCKs or SCKXs are to be used, or whether a complete subset of SCKs or SCKXs is to be used. In the latter case, the SwMI shall indicate the relevant subset. If a complete subset is to be changed at the same time, the SwMI shall ensure that the SCK-VNs of all SCKs or SCKXs in the subset are the same. The SCK-VN common to all SCKs or SCKXs to be made active shall be included in the D-CK CHANGE DEMAND PDU.

The SwMI may indicate a change in DMO SCK or SCKX for use in a DMO network with a different MNI to that of the SwMI. In this case, the SwMI shall use the D-DM-SCK ACTIVATE DEMAND PDU, and shall indicate the MNI using the "Address extension" element in the PDU. The D-DM-SCK ACTIVATE DEMAND PDU may also be used to indicate active SCKs or SCKXs on DMO networks with the same MNI as the SwMI as an alternative to the D-CK CHANGE DEMAND PDU.

If an MS receives a D-CK CHANGE DEMAND PDU and does not have the SCK-VN for either an individual SCK or SCKX, or for a subset of SCKs or SCKXs, then it may request OTAR of new SCKs or SCKXs.

4.5.5.6 Synchronization of Cipher Key Change

When the D-CK CHANGE DEMAND PDU is used to indicate a change of cipher key or security class of the LA, the "Time Type" element shall be used to indicate the exact moment of change and may take one of the following forms:

- **Absolute IV:** the SwMI shall activate the new cipher key on the indicated IV. In this case all 16 bits of the hyperframe number shall be used;

- **Network time:** the SwMI shall activate the new cipher key on the Network time. If the Network time falls between slot boundaries, the SwMI shall round up to the next slot number of the downlink; or

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

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

4.5.6 Security class change

4.5.6.0 General

The SwMI may send the D-CK CHANGE DEMAND PDU on control channels and on assigned channels to invoke transitions between any of the following security classes:

- Security class 1;

- Security class 2;

- Security class 3 without GCK or GCKX;

- Security class 3 with GCK or GCKX.

NOTE: Conceptually, "Security class 3 with GCK or GCKX" is treated as a separate security class.

The scope of the D-CK CHANGE DEMAND/U-CK CHANGE RESULT protocol exchange when used to indicated security class change is the current cell on the serving network only.

In order to avoid unnecessary re-registration attempts by registered MS during security class changes (described above), the following behaviour is expected from the MS:

- If an MS had registered with **Ciphering On** in security class 2, or security class 3, or security class 3 with GCK or GCKX, and the cell subsequently transitions to security class 1, then the MS shall temporarily override its registered ciphering mode with **Ciphering Off**, and shall remain registered providing it supports security class 1. Furthermore, if the cell subsequently transitions to security class 2, or security class 3, or security class 3 with GCK or GCKX, then the MS shall resume its previous ciphering mode (i.e. prior to the override) of **Ciphering On,** and shall remain registered providing it supports the new security class and possesses the relevant key material for that security class. However, if the MS is unable to support the resumed ciphering mode of Ciphering On in the new security class, then the MS shall either re-register to request Ciphering Off or perform cell re-selection, whichever is most appropriate.

- If an MS had registered with **Ciphering On** in security class 2, or security class 3, or security class 3 with GCK or GCKX, and the cell subsequently transitions to security class 2, or security class 3, or security class 3 with GCK or GCKX, then the MS shall continue to use the existing ciphering mode of **Ciphering On**, and shall remain registered providing it supports the new security class and possesses the relevant key material for that security class. However, if the MS is unable to support the same ciphering mode of Ciphering On in the new security class, then the MS shall either re-register to request Ciphering Off or perform cell re-selection, whichever is most appropriate.

- If an MS had registered with **Ciphering Off** in security class 2, or security class 3, or security class 3 with GCK or GCKX, and the cell subsequently transitions to security class 1, or security class 2, or security class 3, or security class 3 with GCK or GCKX, then the MS shall continue to use the existing ciphering mode of **Ciphering Off**. However, if the MS needs to change its ciphering mode to Ciphering On following the security class change, then the MS shall either re-register to request Ciphering On or perform cell re-selection, whichever is most appropriate.

- If an MS had registered with **Ciphering Off** in security class 1 and the cell subsequently transitions to security class 2, or security class 3, or security class 3 with GCK or GCKX, then the MS shall re-register to negotiate a ciphering mode that is acceptable to the SwMI which may result in the MS continuing to use Ciphering Off.

- If the MS supports the new security class but needs to obtain the relevant key material, then the MS shall re-register to obtain the keys through OTAR.

- If the MS does not support the new security class or does not support OTAR of the relevant key material then the MS shall invoke cell re-selection procedures.

4.5.6.1 Change of security class to security class 1

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

The SwMI shall set the "Change of security class" element of the D-CK CHANGE DEMAND PDU to "Transition to security class 1", and set the "Key change type" element to "No cipher key".

4.5.6.2 Change of security class to security class 2

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

The SwMI shall set the "Change of security class" element of the D-CK CHANGE DEMAND PDU to "Transition to security class 2", and set the "Key change type" element to "SCK/SCKX" and set the "SCK use element" to "TMO".

4.5.6.3 Change of security class to security class 3

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

The SwMI shall set the "Change of security class" element of the D-CK CHANGE DEMAND PDU to "Transition to security class 3", and set the "Key change type" element to "CCK/CCKX".

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

4.5.6.4 Change of security class to security class 3 with GCK or GCKX

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

The SwMI shall set the "Change of security class" element of the D-CK CHANGE DEMAND PDU to "Transition to security class 3", and set the "Key change type" element to "Class 3 CCK(X) and GCK(X) activation".

4.5.7 Notification of key in use

When the D-CK CHANGE DEMAND PDU is used to indicate an active cipher key, the "Change of Security Class" element shall indicate "No change of Security Class", and "Time Type" element shall be set to indicate "Currently in use". This may be used by the SwMI to indicate the following information to the MS:

- the current GCK-VN for all GCKs or GCKXs;
- the current SCKN and SCK-VN of a fallback SCK or SCKX for the SwMI;
- the current SCKN and SCK-VN of a DM-SCK(s) or SCKX(s) associated with DMO; or
- the current subset of SCKs or SCKXs for a subset of DM-SCKs or SCKXs associated with DMO.

4.5.8 Notification of GCK or GCKX Activation/Deactivation

When the D-CK CHANGE DEMAND PDU is used to indicate activation or deactivation of GCKs or GCKXs in the cell, the "Key Change Type" shall be set to either "Class 3 CCK(X) and GCK(X) activation" or "CCK/CCKX" respectively. This shall be synchronized with the change of the "GCK Supported" information element in SYSINFO, SYSINFO-DA or SYSINFO-Q PDUs.

4.5.9 Deletion of SCK/SCKX, GCK/GCKX and GSKO/GSKOX

Prior to key deletion using the mechanisms described in this clause there should be no associations to groups for those keys that are to be deleted.

The SwMI should be authenticated by the MS before keys or key associations are deleted, this may be explicit or implicit.

The deletion of the TM-SCK or SCKX in a class 2 SwMI using the mechanisms described in this clause should be carefully considered.

NOTE 1: ETSI EN 300 812-3 [4] and ETSI ES 200 812-2 [10] do not support a delete mechanism.The SwMI may delete SCKs, SCKXs, GCKs, GCKXs, GSKOs or GSKOXs currently contained within an MS by an explicit Key Delete command.

The SwMI shall send a D-OTAR KEY DELETE DEMAND PDU to the MS. The PDU shall be sent to MSs individually, it shall not be sent to groups of MSs. The PDU shall only delete keys which are used in one network, and the "Address extension" element in the PDU shall indicate the relevant network if different from the serving network. If the SwMI requires the MS to delete keys for more than one network, it shall send multiple PDUs, each relevant for a different network except for the case where all keys of a particular type are deleted as described in this clause.

The home SwMI may delete SCKs, SCKXs, GCKs, GCKXs, GSKO or GSKOX in any set in the MS, i.e. associated with any MNI. A visited SwMI shall not be able to delete SCKs, SCKXs, GCKs, GCKXs, GSKOs or GSKOXs that are associated with any MNI except that of that visited SwMI. The MS shall reject any such request from a visited SwMI to delete keys associated with any other MNIs by sending a U-OTAR KEY DELETE RESULT PDU where the "Key delete type" element shall be set to "Key delete extension" and the "Key delete extension type" element shall be set to "Reject". The "Reject reason" element shall be set to "Invalid MNI". The MS shall not delete the requested keys in response to the request of the visited SwMI.

If a single or a list of SCKs or SCKXs is to be deleted, the SwMI shall set the "Key delete type" element to "Individual SCK(s)/SCKX(s)", and shall list the SCKNs of the keys to be deleted. The MS shall delete the required key(s) and shall respond with a U-OTAR KEY DELETE RESULT PDU listing the SCKs that have been deleted. If the MS cannot delete one of the keys, for example if it does not possess the requested key, it shall not include that SCKN in the responding PDU. Therefore, if deletion of a single SCK or SCKX was requested, but the MS does not possess the SCK or SCKX, the "Number of SCKs deleted" element shall be set to zero and no "SCKN" element shall be included in the PDU.

If the SCK set is divided into subsets for DMO use, and a complete KAG is to be deleted (for example to remove all keys associated with a particular GSSI), the SwMI shall set the "Key delete type" to "SCK subset", and shall indicate the number of SCKs or SCKXs to be deleted per subset in the "Number of SCKs deleted" element (which is also the number of SCKN elements to be provided in the PDU). The SCKN elements shall only correspond to the SCKNs in the first subset of SCKs, i.e. the subset with SCKN = 1 as its lowest value. Therefore if multiple SCKNs are included in the PDU, the MS shall delete a number of SCKs or SCKXs equal to the "Number of SCKs deleted" element multiplied by the number of subsets in use.

EXAMPLE: If the SwMI and MS use 3 subsets of 10 keys each, corresponding to "SCK subset grouping type" element value of 010_2, and the SwMI instructs the MS to delete SCKN = 3 and SCKN = 7, (i.e. "Number of SCKs deleted" is 2), the MS shall also delete SCKNs = 13, 17, 23 and 27.

The MS shall respond with the U-OTAR KEY DELETE RESULT PDU indicating the SCKs or SCKXs deleted. It shall indicate to the SwMI the SCK subset grouping in use, and indicate which keys have been deleted by reference to the SCKNs in the first set only. If the MS does not possess any of the sets of members required, it shall omit those SCKNs from the U-OTAR KEY DELETE RESULT PDU.

If the SCK set is divided into subsets for DMO use, and an entire subset is to be deleted, the SwMI shall set the "Key delete type" element value to "SCK subset" to indicate deletion of an entire subset, and shall include the subset grouping and subset number in the corresponding elements. Only one subset shall be deleted by a single PDU, and the SwMI shall send further PDUs if the deletion of more than one subset is required. The MS shall respond with the same element values in the U-OTAR KEY DELETE RESULT PDU. If the MS is not using the subset grouping proposed by the SwMI, it shall not delete the requested SCKs or SCKXs, and it shall instead indicate a mismatch by setting the "SCK subset grouping" element in the U-OTAR KEY DELETE RESULT PDU to "SCK grouping not valid" and the "SCK subset number" element to "0000".

If the SwMI requires the MS to delete all SCKs and/or SCKXs, it shall indicate this by setting the "Key delete type" element to "All SCKs/SCKXs". The MS shall delete all SCKs and/or SCKXs and respond with the same value of "Key delete type" element in the U-OTAR KEY DELETE RESULT PDU. The home SwMI may demand that the MS deletes all SCKs and/or SCKXs associated with a different MNI, in which case the "Key delete type" element shall be set to "All SCKs/SCKXs", and the "Address extension" element shall indicate the MNI of the network with which the SCK set to be deleted is associated.

NOTE 2: Deletion of all SCKs and/or SCKXs associated with the "Open MNI" by this mechanism is not possible, as the "Open MNI" and "All SwMI MNI" are both indicated by all binary ones, $11 \ldots 11_2$, and this value is reserved for deletion of all SCKs associated with all networks (see below). Deletion of SCKs and/or SCKXs associated with the "Open MNI" without deleting SCKs or SCKXs associated with other MNIs needs to be achieved by deleting individual SCKs, by deleting SCK subsets or by deleting KAGs of SCKs.

The MS shall only delete SCKs or SCKXs in the SCK set indicated by the "Address extension" element in the PDU. If there is no "Address extension" element, the MS shall only delete SCKs or SCKXs in the SCK set associated with the serving SwMI.

The home SwMI may also require the MS to delete all SCKs and/or SCKXs for use in all networks. In this case, the SwMI shall include the "Address extension" element in the D-OTAR KEY DELETE DEMAND PDU and shall set it to the value for the "All SwMI MNI" (all binary ones, $11 \ldots 11_2$).

If the SwMI requires the MS to delete one or more GCKs or GCKXs, it shall indicate this by setting the "Key delete type" element to "Individual GCK(s)/GCKX(s)", it shall indicate the number of GCKs or GCKXs to be deleted in the "Number of GCKs deleted" element and list the GCKNs. The MS shall delete all versions (i.e. all corresponding GCK-VNs) of the required GCKN if it has more than one version stored. The MS shall indicate the GCKNs deleted back to the SwMI with the U-OTAR KEY DELETE RESULT PDU. If it cannot delete any of the GCKs or GCKXs because it is not provisioned with them, it shall omit these from the list. Therefore, if deletion of a single GCK or GCKX was requested, but the MS does not possess the GCK or GCKX, the "Number of GCKs deleted" element shall be set to "0000" and no "GCKN" element shall be included in the PDU.

If the SwMI requires the MS to delete all GCKs and/or GCKXs, it shall indicate this by setting the "Key delete type" element to "All GCKs/GCKXs". The MS shall delete all GCKs and/or GCKXs and respond with the same value of "Key delete type" element in the U-OTAR KEY DELETE RESULT PDU.

The home SwMI may delete GCKs that were provisioned for use with other networks. A visited SwMI shall not delete GCKs that were provisioned for use with any network other than that visited SwMI. The MS shall only delete GCKs or GCKXs in the GCK set indicated by the "Address extension" element in the PDU. If there is no "Address extension" element, the MS shall only delete GCKs or GCKXs in the GCK set associated with the serving SwMI.

The home SwMI may also require the MS to delete all GCKs and/or GCKXs for use in all networks. In this case, the SwMI shall include the "Address extension" element in the D-OTAR KEY DELETE DEMAND PDU and shall set it to the value for the "All SwMI MNI" (all binary ones, $11...11_2$).

If the SwMI requires the GSKO or GSKOX to be deleted, it shall indicate this by setting the "Key delete type" element to "GSKO/GSKOX". The MS shall delete the GSKO or GSKOX and respond with the same value of "Key delete type" element in the U-OTAR KEY DELETE RESULT PDU. If the MS contains more than one version of GSKO or GSKOX, it shall delete all versions (i.e. all values of GSKO-VN). It shall additionally send the GSKO-VN in the U-OTAR KEY DELETE RESULT PDU: if more than one version of GSKO-VN was held by the MS, it shall send the highest value of GSKO-VN that it possessed.

The home SwMI may require the MS to delete a GSKO or GSKOX that was for use in a network other than the home network. The SwMI shall indicate the network of the relevant GSKO or GSKOX by use of the "Address extension" element, and the MS will include the same "Address extension" element in its response.

The Home SwMI may also require the MS to delete all GSKOs and/or GSKOXs for use in all networks. In this case, the SwMI shall include the "Address extension" element in the D-OTAR KEY DELETE DEMAND PDU and shall set it to the value for the "All SwMI MNI" (all binary ones, $11...11_2$).

Figure 4.43 shows the message sequence chart for the key deletion protocol.

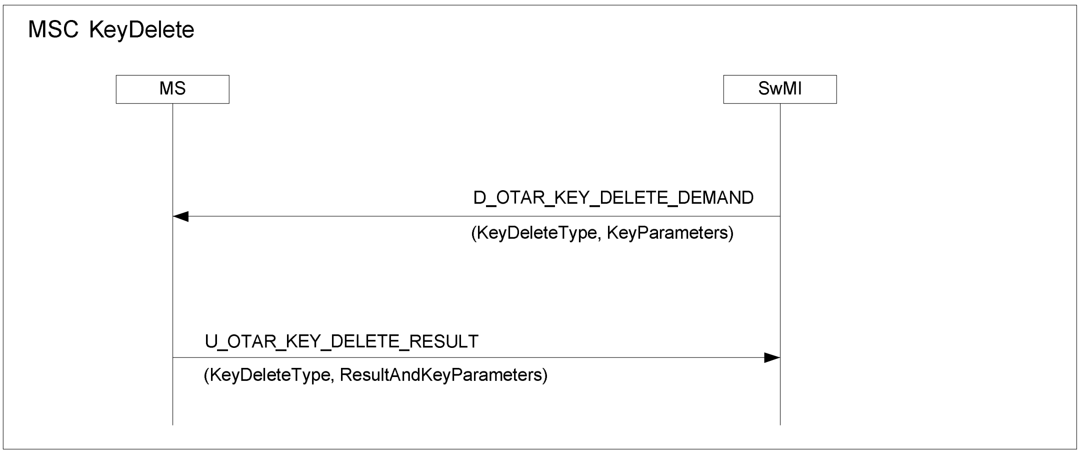

MSC KeyDelete
MS
SwMI
D_OTAR_KEY_DELETE_DEMAND
(KeyDeleteType, KeyParameters)
U_OTAR_KEY_DELETE_RESULT
(KeyDeleteType, ResultAndKeyParameters)

Figure 4.43: Message sequence chart showing key deletion

4.5.10 Air Interface Key Status Enquiry

The SwMI shall be able to discover the current numbers and versions of air interface keys held by an MS by means of a status enquiry. The purpose of this mechanism is to allow a SwMI to maintain a record of the MS keying state, without needing to explicitly update the MS with new key material to force a response, which can make intensive use of air interface bandwidth. The protocol sequence is shown in Figure 4.44.

The SwMI shall send a D-OTAR KEY STATUS DEMAND PDU to the MS. It may be individually or group addressed. The SwMI may request the state of:

- a single SCK or SCKX, specified by SCKN;
- a subset of SCKs or SCKXs used for DMO, identified by the SCK subset grouping pattern used and SCK subset number;
- all SCKs and/or SCKXs held in one network related SCK set in the MS;
- all SCKs and/or SCKXs held in all SCK sets in the MS;
- a single GCK or GCKX, identified by GCKN;
- all GCKs and/or GCKXs held in one network related GCK set in the MS;
- all GCKs and/or GCKXs held in all GCK sets in the MS;
- the GSKO or GSKOX, or multiple versions of GSKOs or GSKOXs related to one network in the MS; or
- all GSKOs and/or GSKOXs held in the MS for use with all networks.

The MS shall respond with a U-OTAR KEY STATUS RESPONSE PDU containing key number (if applicable) and version number of the requested keys, if it has them.

The home SwMI may request the status for keys held in key sets for use in networks other than the serving network by including the "Address extension" element in the PDU to indicate the MNI which specifies the relevant key set. The SwMI may send multiple D-OTAR KEY STATUS DEMAND PDUs, one for each network. The MS shall respond with separate U-OTAR KEY STATUS RESPONSE PDUs for each network. A visited SwMI shall only be able to request the status of keys for use in that SwMI. The MS shall reject any request from a visited SwMI to provide the status of keys associated with any other MNIs by sending a U-OTAR KEY STATUS RESPONSE PDU where the "Key status type" element shall be set to "Reject". The "Reject reason" element shall be set to "Invalid MNI".

If the home SwMI specifically requires to request the status of all keys of a particular type (all SCKs/SCKXs or all GCKs/GCKXs) for all the SCK or GCK sets held in the MS, it may send the D-OTAR KEY STATUS DEMAND PDU to the MS with the "Key status type" element set to "All SCKs/SCKXs" or "All GCKs/GCKXs", and with the "Address extension" element set to the value of the "All SwMI MNI" (all binary ones, $11...11_2$). The MS shall respond with separate U-OTAR KEY STATUS RESPONSE PDUs for each network and shall include the "Address extension" element relevant for that network with each response for all networks other than the serving network. The MS shall reject any request for key status for keys related to all SwMIs if received from a visited SwMI.

If the SwMI requests the status of an individual SCK or SCKX, identified by SCKN, and the MS possesses the SCK or SCKX requested, the MS shall respond setting the "Number of SCK status" element to a value of "1" and shall include a single "SCK data" element containing the SCKN and SCK-VN of that SCK. If the MS does not possess the SCK or SCKX requested, it shall set the "Number of SCK status" element to "0" and shall not provide any "SCK data" element.

If the SwMI requests the status of a subset of SCKs or SCKXs as used for DMO, it shall include the subset grouping pattern in use and the subset number requested. The MS shall respond with the SCK subset grouping and SCK subset number requested, and shall indicate how many SCKs or SCKXs it is providing data for in the "Number of SCK status" element, and shall provide this number of "SCK data" elements, each containing SCKN and SCK-VN for one key. If the MS does not use the SCK subset grouping pattern demanded by the SwMI (i.e. the MS uses a different pattern), it shall set the "SCK subset grouping" element to "SCK grouping not valid" and the "SCK subset number" element to "00000" indicating a grouping mismatch. It shall set the "Number of SCK status" element to "0" and shall not provide any "SCK data" elements. If the MS has the same pattern as indicated by the SwMI, but does not have any keys in the subset, it shall set the "SCK subset grouping" and "SCK subset number" elements to the values in use, shall set the "Number of SCK status" element to "0", and shall not provide any "SCK data" element.

If the SwMI requests the status of all SCKs and/or SCKXs in the MS, the MS shall respond indicating how many SCKs and/or SCKXs it is providing data for in the "Number of SCK status" element, and shall provide this number of "SCK data" elements, each containing SCKN and SCK-VN for one key. If the MS does not possess any SCKs or SCKXs, it shall set the "Number of SCK status" element to "0" and shall not provide any "SCK data" element.

In all cases the "Address extension" element shall be used for requests and responses for status for SCKs and/or SCKXs in sets relating to networks other than the serving network.

If the SwMI requests the status of an individual GCK or GCKX, identified by GCKN, and the MS possesses the GCK or GCKX requested, the MS shall respond setting the "Number of GCK status" element to a value of "1" and shall include a single "GCK data" element containing the GCKN and GCK-VN of that GCK or GCKX. If the MS does not possess the GCK or GCKX requested, it shall set the "Number of GCK status" element to "0" and shall not provide any "GCK data" element.

If the SwMI requests the status of all GCKs and/or GCKXs in the MS, the MS shall respond indicating how many GCKs or GCKXs it is providing data for in the "Number of GCK status" element, and shall provide this number of "GCK data" elements, each containing GCKN and GCK-VN for one key. One PDU allows the MS to give the SwMI the status of 31 GCKs or GCKXs. If the MS possesses more than 31 GCKs and/or GCKXs, it shall send further U-OTAR KEY STATUS RESPONSE PDUs containing the extra GCKNs and GCK-VNs. If the MS does not possess any GCKs or GCKXs, it shall set the "Number of GCK status" element to "0" and shall not provide any "GCK data" element.

In all cases the "Address extension" element shall be used for requests and responses for status for GCKs in sets relating to networks other than the serving network.

NOTE: An MS can only negotiate a single KSG for use with a network, and therefore the response for an MS relating to any network will contain GCKNs and GCK-VNs relating either to GCKs or relating to GCKXs, but not both.

If the SwMI requests the status of the GSKO or GSKOX in the MS, the MS shall respond indicating how many GSKO or GSKOX versions it is providing data for in the "Number of GSKO status" element, and shall provide this number of "GSKO-VN" elements, each containing GSKO-VN for one key. One PDU allows the MS to give the SwMI the status of 3 GSKO-VNs. If the MS possesses more than 3 versions of GSKO or GSKOXs, it shall send further U-OTAR KEY STATUS RESPONSE PDUs containing the extra GSKO-VNs. If the MS does not possess any GSKOs or GSKOXs, it shall set the "Number of GSKO status" element to "0" and shall not provide any "GSKO-VN" element.

If the home SwMI requires the status of GSKOs or GSKOXs held in the MS for use in networks other than the serving network, it shall send one or more key status requests to the MS, where each request refers to a key valid for a single network. The "Address extension" element shall indicate the relevant network if different from the serving network. The MS shall respond to a request for status of GSKO or GSKOX valid for a network other than the serving network including the "Address extension" element referring to the relevant network in its response. A visited SwMI shall only be able to request the status of the GSKO or GSKOX for use in that SwMI. The MS shall reject such a request from a visited SwMI to provide the status of GSKO or GSKOX associated with any other SwMIs.

If the home SwMI specifically requires to request the status of all GSKOs held in the MS for use with all networks, it may send the D-OTAR KEY STATUS DEMAND PDU to the MS with the "Key status type" element set to "GSKO", and with the "Address extension" element set to the value of the "All SwMI MNI" (all binary ones, $11...11_2$). The MS shall respond with separate U-OTAR KEY STATUS RESPONSE PDUs for each network and shall include the "Address extension" element relevant for that network with each response for all networks other than the serving network. The MS shall reject any request for key status related to all SwMIs if received from a visited SwMI.

If the SwMI sends the request to a group of MSs, each MS shall respond on expiry of random timer T371. The SwMI shall send the maximum value of T371 to the MS in the request PDU. If the request is sent to an individual MS, the "Max response timer value" shall be set to "0". If the MS needs to detach from the SwMI before sending the status response to the SwMI, it shall consider T371 to have expired and shall send the response before detaching. T371 is described in clause 4.5.2.3. If the MS is unable to send the response PDU before detaching, it should store the PDU and send it next time it attaches to the SwMI, even if is switched off and on again in the meantime.

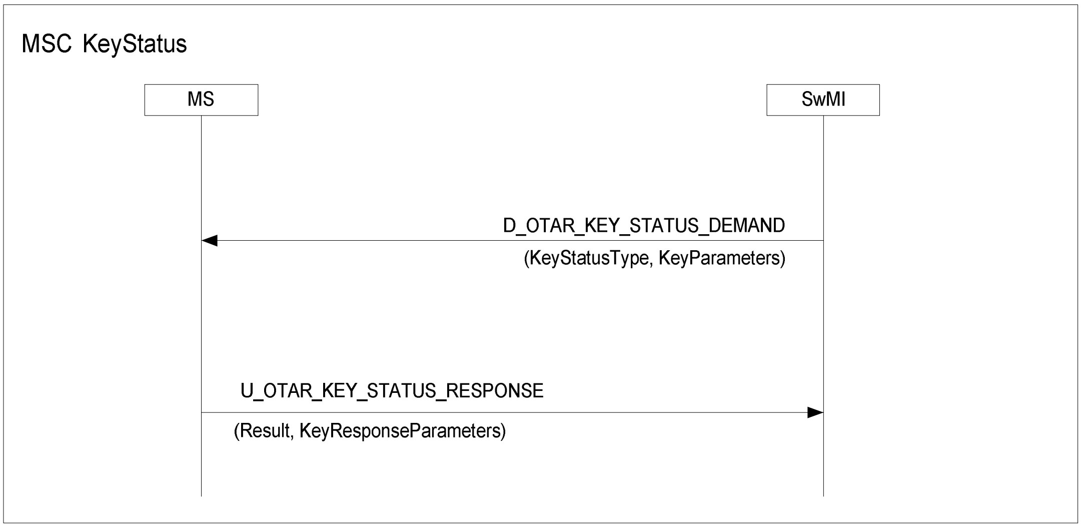

MSC KeyStatus
MS
SwMI
D_OTAR_KEY_STATUS_DEMAND
(KeyStatusType, KeyParameters)
U_OTAR_KEY_STATUS_RESPONSE
(Result, KeyResponseParameters)

Figure 4.44: Message sequence chart of key status inquiry

4.5.11 Crypto management group

Use of CMG is optional but if used shall be as defined in this clause.

A set of MSs with common key material (SCKs, SCKXs, GCKs, GCKXs) shall be considered to be part of the same Crypto Management Group (CMG), and to reduce the load at the air interface, group addressed OTAR signalling shall be sent to the CMG as a whole. The group address may be provisioned over the air interface using the method described in this clause.

The CMG has the following attributes:

- common set of key material (SCKs, SCKXs, GCKs, GCKXs);
- common key encryption key (GSKO or GSKOX);
- common means of addressing for group addressed OTAR (i.e. common GSSI programmed specifically for key management purposes).

An MS shall be a member of zero or only one CMG.

TM-SCK or SCKX and GCK or GCKX identities (SCKN and GCKN) are unique per system irrespective of the number of CMGs in use. If CMGs exist on a system DM-SCK or SCKX identities (SCKN) are unique per CMG, else per system.

To make use of the CMG the MS shall be provided with a GSSI for use with group addressed OTAR. The SwMI may provide this to the MS using D-OTAR CMG GTSI PROVIDE PDU or within D-OTAR GSKO PROVIDE or D-OTAR GSKOX PROVIDE PDUs. The SwMI shall only send these PDUs to an individually addressed MS, and it shall not send these PDUs to a group of MSs. The MS shall respond using U-OTAR CMG GTSI RESULT PDU or U-OTAR GSKO RESULT PDU respectively. The MS shall then act upon OTAR messages sent to this group, as well as to messages sent to the MS's ITSI. It shall ignore OTAR sent to any other group address.

The GTSI used for CMG purposes shall be considered long term and maintained in the MS even when powered down and up again.

If the SwMI wishes to delete the CMG GSSI (or GTSI) in the MS, it shall set the "GSSI" element to "0".

If the MS receives a CMG GTSI from the SwMI that is different to that already stored, or if the SwMI deletes the CMG GTSI from the MS, then the MS shall delete all previously stored DMO SCKs and/or SCKXs (i.e. where $1 \leq \text{SCKN} \leq 30$), GCK and/or GCKX and GSKO or GSKOX material. The fallback SCK or SCKX for TMO (SCKN = 31 or SCKN = 32) should not be deleted.

NOTE: If an MS negotiates a KSG with the SwMI that is different to the last KSG negotiated with that SwMI, the MS should not automatically delete the CMG GSSI that has been stored for use with that SwMI. The SwMI may or may not decide to replace the CMG GSSI in the MS following negotiation of a different KSG.

4.5.12 OTAR retry mechanism

When registered on a cell, the MS shall monitor the "OTAR Retry Interval" element setting, conveyed through transmissions of SCK, SCKX, GCK and GCKX OTAR PROVIDE PDUs, in order for the MS to determine how many hyperframes it shall wait before retrying an OTAR Demand for SCK or SCKX, GSKO or GSKOX, or GCK or GCKX. The SwMI shall also indicate the current OTAR retry interval setting in SCK, GCK and GSKO REJECT PDUs. The last received OTAR retry interval always applies on the serving cell irrespective of whether it arrived in a Provide or Reject PDU.

When the OTAR Retry Interval expires in the MS, and if the MS has not been provided with the requested keys and if the OTAR Retry Interval is different from "Do not retry", it shall re-request the required keys. If the MS is not on the MCCH or SCCH when the OTAR Retry Interval expires, then the MS may either re-request the keys on the present channel (if permitted by prior arrangement with the SwMI) or shall wait until it returns to the MCCH or SCCH. If the MS waits until it returns to the MCCH or SCCH before requesting keys, on return to the MCCH or SCCH the MS shall first randomize over the five multiframes following its return to the MCCH or SCCH and then re-request the keys.

When the OTAR Retry Interval is different from "Do not retry", and the MS sends an OTAR Demand PDU on the MCCH or SCCH and leaves the MCCH or SCCH before receiving a response (Provide or Reject) for the requested key, and if the MS has not been provided with the requested keys on some other channel, then upon return to the MCCH or SCCH, the MS should cancel the OTAR Retry Interval timer, and start a new timer choosing the interval by randomizing over the OTAR Retry Interval. On expiry of this new timer, it should re-request the key at the first opportunity on the MCCH or SCCH following expiry of this random interval if the keys have still not been received at that time. Otherwise the MS shall wait until the expiry of the original OTAR Retry Interval before re-requesting the key (if the key has still not been received at that time).

Where the MS uses random access to re-request the keys, the procedure for randomly selecting the signalling slot shall follow the procedure for "Choosing from a new access frame" as defined in ETSI EN 300 392-2 [2], clause 23.5.1.4.6.

The OTAR Retry Interval setting shall only have relevance to the cell on which it is broadcast; cells that comprise the same SwMI may use different settings. In the absence of any indication of the cell's OTAR Retry Interval setting, the MS shall default to using a setting of "Do not retry". However, if the MS subsequently receives a different OTAR Retry Interval setting from the SwMI, whilst one or more key requests are outstanding, then the MS shall retrospectively apply the newly received setting.

Following cell re-selection, and registration on the new serving cell, the MS may re-request key(s) that are needed and, thereafter, wait the appropriate length of time given by the new serving cell (as previously stated) before retrying its OTAR Demand for SCK or SCKX, GSKO or GSKOX, or GCK or GCKX. In the absence of any indication of the new serving cell's OTAR Retry Interval setting, the MS shall default to using a setting of "Do not retry".

4.5.13 OTAR protocol functions - Group Session Key for OTAR

4.5.13.0 General

A single GSKO may be distributed to the MS using the D-OTAR GSKO PROVIDE PDU or D-OTAR GSKOX PROVIDE PDU, sealed with KSO, or a single GSKOX may be distributed to the MS using the D-OTAR GSKOX PROVIDE PDU, sealed with KSOX. The provision may be started automatically by the SwMI or in response to a request from the MS using the U-OTAR GSKO DEMAND PDU. The D-OTAR GSKO PROVIDE or D-OTAR GSKOX PROVIDE PDU shall also include the GSSI of the Crypto Management Group to which the MS can expect group addressed OTAR relevant to that MS to be addressed. The D-OTAR GSKO PROVIDE or D-OTAR GSKOX PROVIDE PDU shall be individually addressed to the MS, and the MS shall respond with a U-OTAR GSKO RESULT PDU.

If the CMG GSSI provided in the OTAR PROVIDE PDU is different to its previously stored CMG GSSI, the MS shall delete the stored GCKs or GCKXs and DMO-SCKs and/or SCKXs as described in clause 4.5.11.

The MS shall only request and be provided with the GSKO for use on the serving network.

4.5.13.1 MS requests provision of GSKO or GSKOX

The scenario in Figure 4.45 shows the case where the MS requests provision of a GSKO or GSKOX. The MS may initiate this procedure at any time. The MS shall not request a GSKO or GSKOX for use in any network other than the serving network.

The MS may send a U-OTAR GSKO DEMAND PDU to the SwMI. The SwMI shall respond with the requested GSKO or GSKOX using the D-OTAR GSKO PROVIDE or D-OTAR GSKOX PROVIDE PDU, together with the CMG GSSI and GSKO-VN information. The MS shall respond and inform the SwMI of the success or failure of the OTAR using the U-OTAR GSKO RESULT PDU. In case of failure, it shall indicate the reason, which may include failure to decrypt key, or SwMI provided the wrong key.

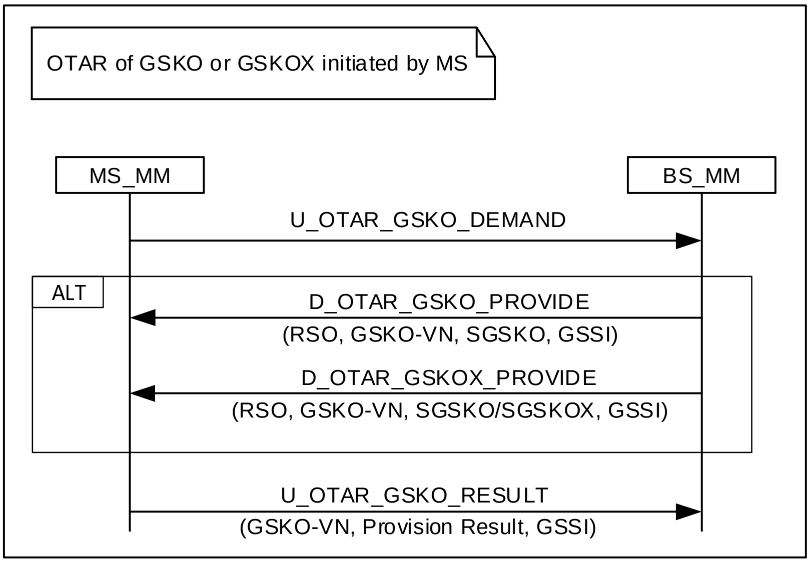

OTAR of GSKO or GSKOX initiated by MS
MS_MM
BS_MM
U_OTAR_GSKO_DEMAND
ALT
D_OTAR_GSKO_PROVIDE
(RSO, GSKO-VN, SGSKO, GSSI)
D_OTAR_GSKOX_PROVIDE
(RSO, GSKO-VN, SGSKO/SGSKOX, GSSI)
U_OTAR_GSKO_RESULT
(GSKO-VN, Provision Result, GSSI)

Figure 4.45: GSKO or GSKOX delivery initiated by MS

4.5.13.2 SwMI provides GSKO or GSKOX to an MS

The scenario in Figure 4.46 shows the case where the SwMI provides a GSKO or GSKOX to an MS without the MS first requesting GSKO or GSKOX provision. The SwMI may initiate this procedure at any time. The SwMI shall provide the GSKO or GSKOX to the MS using the D-OTAR GSKO PROVIDE or D-OTAR GSKOX PROVIDE PDU which includes the CMG GSSI and GSKO-VN information. The MS shall respond and inform the SwMI of the success or failure of the OTAR using the U-OTAR GSKO RESULT PDU. In case of failure, it shall indicate the reason.

The normal message sequence in this case shall be according to Figure 4.46.

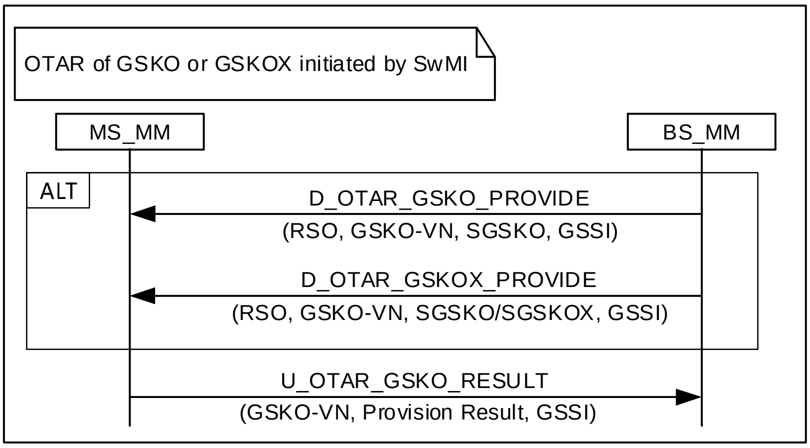

OTAR of GSKO or GSKOX initiated by SwMI
MS_MM
BS_MM
ALT
D_OTAR_GSKO_PROVIDE
(RSO, GSKO-VN, SGSKO, GSSI)
D_OTAR_GSKOX_PROVIDE
(RSO, GSKO-VN, SGSKO/SGSKOX, GSSI)
U_OTAR_GSKO_RESULT
(GSKO-VN, Provision Result, GSSI)

Figure 4.46: GSKO or GSKOX delivery initiated by SwMI

4.5.13.3 SwMI rejects provision of GSKO or GSKOX

If the SwMI is unable to provide a GSKO or GSKOX the provision request shall be explicitly rejected using the D-OTAR GSKO REJECT PDU indicating the reason for rejection. The SwMI shall indicate to the MS how long the MS shall wait before retrying a request for GSKO or GSKOX by setting the value of the "OTAR retry interval" element. The behaviour of the MS shall be as described in clause 4.5.12.

4.5.14 OTAR protocol functions - interaction and queuing

When the MS requires multiple keys, it shall send an OTAR Demand for keys in the following priority order (provided that conditions for requesting the respective keys are met):

- GSKO or GSKOX;
- GCK or GCKX;
- TM-SCK or SCKX;
- DM-SCK or SCKX.

The MS shall not send an OTAR Demand for another key of the same type or of lower priority until it receives a Response (OTAR Provide or Reject) for all the keys included in the previous request, with the exception of transition to security class 2 with Absolute IV where the MS will request the TM-SCK or SCKX regardless of this priority mechanism.

When the MS requires a key of higher importance than one already requested, the MS shall not wait for a response to the previous request.

4.5.15 Session Key for OTAR operations in visited SwMI

4.5.15.1 General

In some cases keys may need to be distributed to MSs that are registered on foreign SwMIs. In order to allow the sealing mechanisms described in clauses 4.2.2, 4.2.4 and 4.2.5 to operate in the visited SwMI the mechanisms described in this clause shall be deployed.

4.5.15.2 Home and visited SwMI use air interface encryption algorithms from the same algorithm set

The session key for OTAR KSO used for distribution of a cipher key for use with an air interface encryption algorithm in TEA set A to a single MS migrated to a visited SwMI where that MS last negotiated an air interface encryption algorithm from TEA set A with the home SwMI shall be modified to become KSOv using algorithm TA101 as shown in Figure 4.47. The inputs to TA101 are the MNI of the visited network MNIv, GCK0 (a designated session key modifier key) and KSO derived from K and RS using algorithm TA41.

The session key for OTAR KSOX used for distribution of a cipher key for use with an air interface encryption algorithm in TEA set B to a single MS migrated to a visited SwMI where that MS last negotiated an air interface encryption algorithm from TEA set B with the home SwMI shall be modified to become KSOXv using algorithm TA103 as shown in Figure 4.47a. The inputs to TA103 are the MNI of the visited network MNIv, GCKX0 (a designated session key modifier key) and KSOX derived from K2 and RS using algorithm TA42.

When the value of GCK0 is zero (i.e. the key designated as GCK0 consists of 80 zeros) , or if either the MS or the home SwMI does not support the use of GCK0, the algorithm TA101 shall not be invoked and KSOv shall have the same value as KSO. Similarly, when the value of GCKX0 is zero (i.e. the key designated as GCK0 consists of 192 zeros) , or if either the MS or the home SwMI does not support the use of GCKX0, the algorithm TA103 shall not be invoked and KSOXv shall have the same value as KSOX.

NOTE 1: KSOv or KSOXv has to be transferred to the visited network identified by MNIv in a secure manner.

NOTE 2: The security policy of the hSwMI should set a limit on the number of uses of KSOv or KSOXv by the vSwMI. The means of managing the limit is outside the scope of the present document.

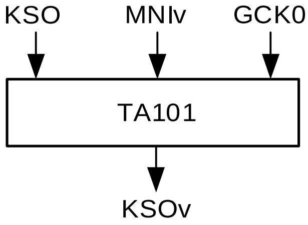


Figure 4.47: Use of TA101 to derive KSOv

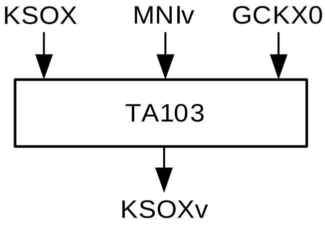


Figure 4.47a: Use of TA103 to derive KSOXv

Where GCK is sealed on the vSwMI algorithm TA81 shall be used by the vSwMI with input KSO replaced by KSOv. Where GCKX is sealed on the vSwMI algorithm TA83 shall be used by the vSwMI with input KSOX replaced by KSOXv. The OTAR protocol between vSwMI and migrating MS follows that specified in clause 4.5.3. The key sealing mechanisms are shown in Figure 4.48.

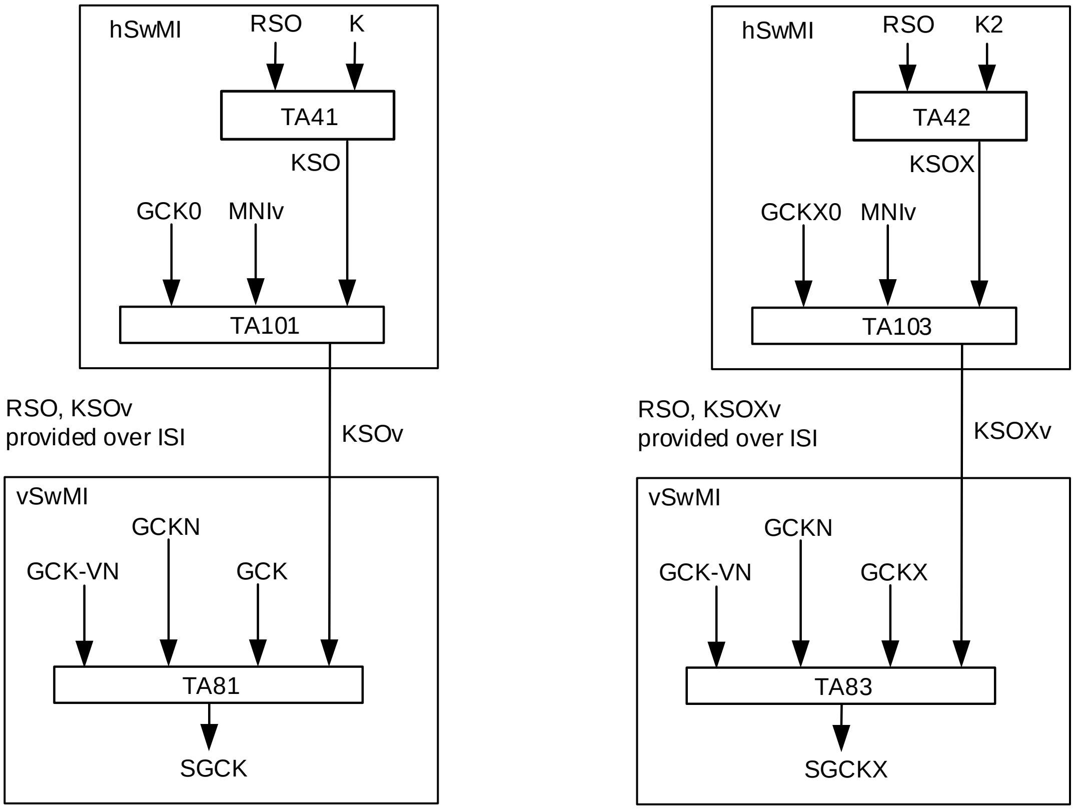


Figure 4.48: Use of KSOv and KSOXv as input to sealing algorithms TA81 and TA83 in vSwMI

Where SCK is sealed on the vSwMI algorithm TA51 shall be used by the vSwMI with input KSO replaced by KSOv. Where SCKX is sealed on the vSwMI algorithm TA53 shall be used by the vSwMI with input KSOX replaced by KSOXv. The OTAR protocol between vSwMI and migrating MS follows that specified in clause 4.5.2. The key sealing mechanisms are shown in Figure 4.49.

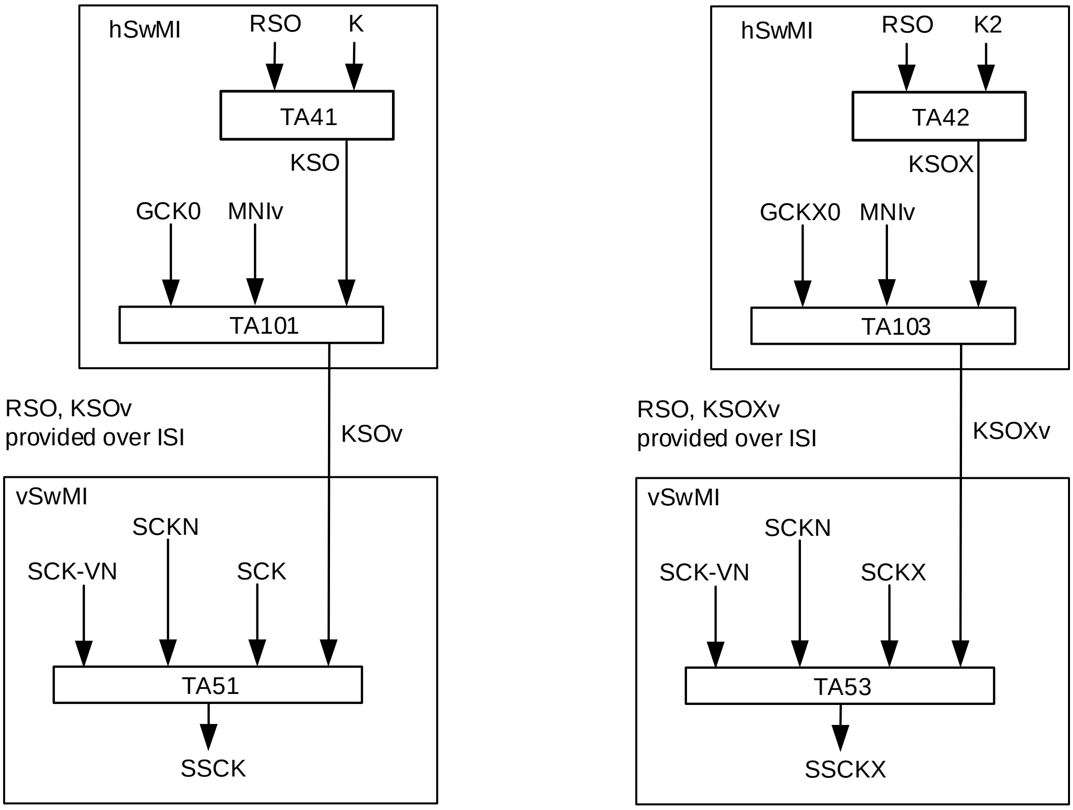


Figure 4.49: Use of KSOv and KSOXv as input to sealing algorithms TA51 and TA53 in vSwMI

Where GSKO is sealed on the vSwMI algorithm TA91 shall be used by the vSwMI with input KSO replaced by KSOv. Where GSKOX is sealed on the vSwMI algorithm TA93 shall be used by the vSwMI with input KSOX replaced by KSOXv. The OTAR protocol between vSwMI and migrating MS follows that specified in clause 4.5.13. The key sealing mechanisms are shown in Figure 4.50.

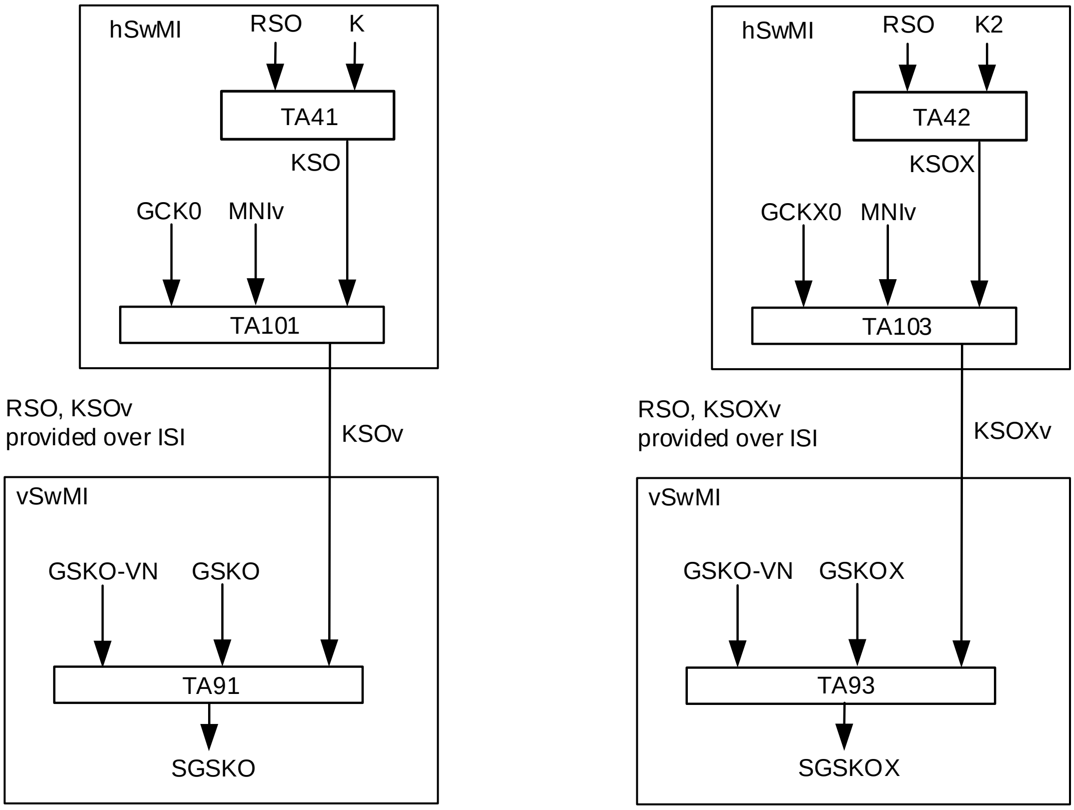


Figure 4.50: Use of KSOv and KSOXv as input to sealing algorithms TA91 and TA93 in vSwMI

4.5.15.3 Home and visited SwMI use air interface encryption algorithms from different algorithm sets

If an MS last negotiated an air interface encryption algorithm from TEA set A with the home SwMI, and migrates to a visited SwMI where TEA set B is negotiated, the home SwMI provides the visited SwMI with a KSOv derived from KSO using TA101 as shown in Figure 4.47. The visited SwMI shall then derive a KSOXv from the KSOv using algorithm TA105, as described in clause 4.2.5a.4, and shall use this KSOXv to seal GCKX, SCKX or GSKOX when providing these keys by OTAR to the migrated MS. The OTAR protocol between vSwMI and migrating MS follows that specified in clauses 4.5.2 (SCKX), 4.5.3 (GCKX) or 4.5.13 (GSKOX).

An illustration of the composite process to seal an SCKX in the visited SwMI is shown in Figure 4.51.

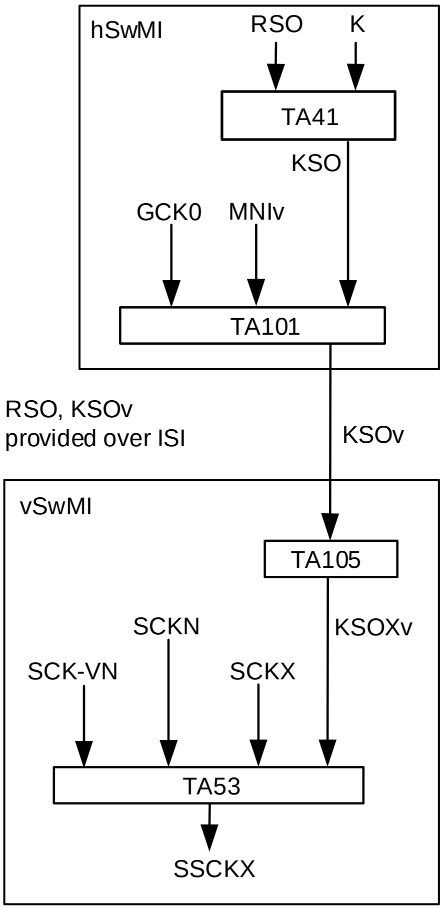


Figure 4.51: Use of KSOv and KSOXv to seal SCKX in vSwMI

NOTE: The CKX is sealed with a key derived from a shorter root key (KSOv) than the CKX. The security policy of the vSwMI should take this into account.

If an MS last negotiated an air interface encryption algorithm from TEA set B with the home SwMI, and migrates to a visited SwMI where TEA set A is negotiated, the home SwMI provides the visited SwMI with a KSOv. This KSOv is derived by first generating a KSOXv from KSOX using TA103 as shown in Figure 4.47a, and then deriving the KSOv from the KSOXv using algorithm TA104, as described in clause 4.2.5a.5, and shall use this KSOv to seal GCK, SCK or GSKO when providing these keys by OTAR to the migrated MS. The OTAR protocol between vSwMI and migrating MS follows that specified in clauses 4.5.2 (SCK), 4.5.3 (GCK) or 4.5.13 (GSKO).

An illustration of the composite process to seal a GCK in the visited SwMI is shown in Figure 4.52.

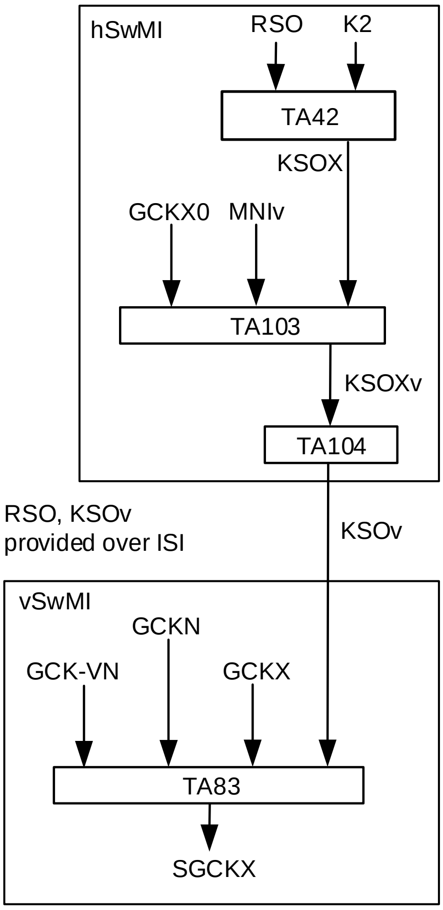


Figure 4.52: Use of KSOXv and KSOv to seal GCK in vSwMI

4.5.16 Transfer of AI cipher keys across the ISI

The mechanisms defined in ETSI EN 300 392-3-5 [8], clauses 13 (stage 1 definition), 26 (stage 2 definition) and 35.11 shall apply for transfer of SCK or SCKX across the ISI.

5 Enable and disable mechanism

5.0 General

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

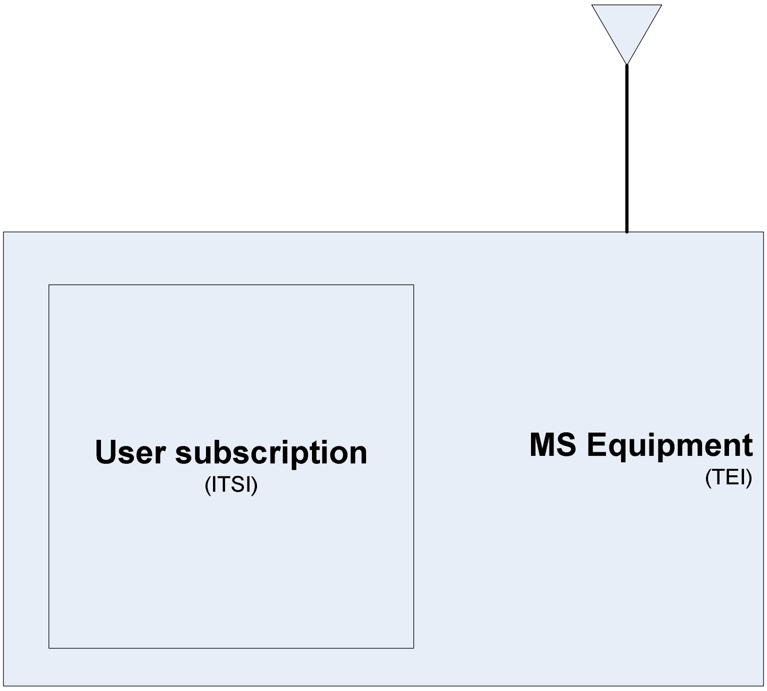
An MS moving from DMO to TMO, or from TMO to DMO, shall retain its disabled state. Thus if an MS is disabled in TMO it shall remain disabled even if the user attempts to switch to DMO.

5.1 General relationships

Figure 5.1 shows the relationship of 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 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 ETSI EN 300 812-3 [4], clause 11.4.4 shall be applied in addition to the protocols described in this clause. If a TSIM application on a UICC is used to store the ITSI the procedures described in ETSI ES 200 812-2 [10], clause 11.5.5 shall be applied in addition to the protocols described in clauses 5 to 5.4.7.2.

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

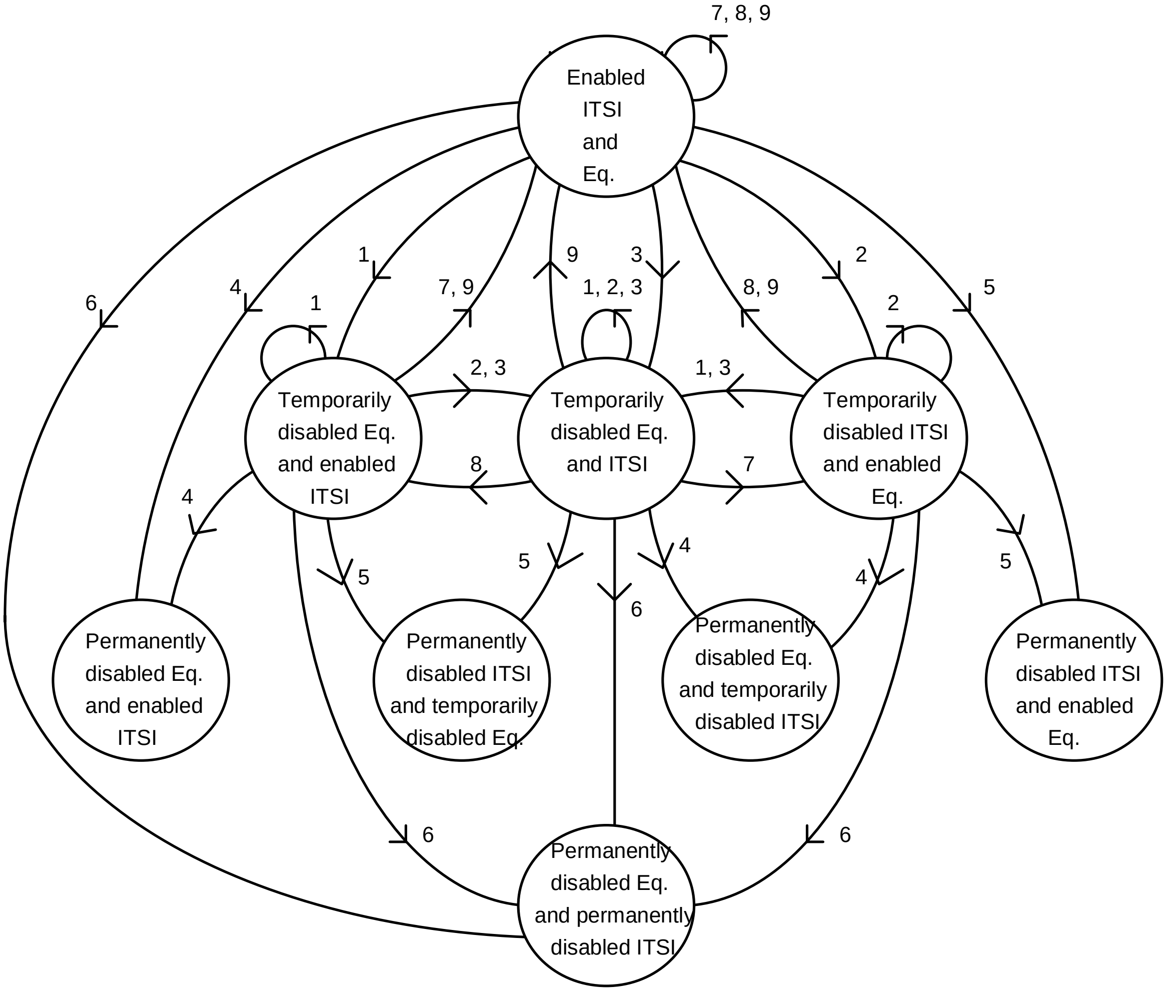


NOTE: The ITSI may be held in a removable user information module, e.g. SIM or UICC.

Figure 5.1: Relationship of TEI and ITSI in MS

5.2 Enable/disable state transitions

Figure 5.2 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.


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

KEY:

1) temporary disabling of equipment;
2) temporary disabling of ITSI;
3) temporary disabling of equipment and ITSI;
4) permanent disabling of equipment;
5) permanent disabling of ITSI;
6) permanent disabling of equipment and ITSI;
7) enabling of equipment;
8) enabling of ITSI;
9) enabling of equipment and ITSI.

Figure 5.2: State transitions of enable/disable mechanism

5.3 Mechanisms

5.3.0 General

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

The rules for when the MS may reject an enable/disable command are described in clause 5.4.6.

In cases where authentication has been initiated by the SwMI it may be made mutual by the MS.

There are nine possible transactions necessary for the enable/disable procedures which allow disable and enable of the MS equipment, the subscription, or both. These are detailed in clauses 5.3.1 to 5.3.6 in which the temporary and permanent distinctions are amalgamated.

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

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

5.3.1 Disable of MS equipment

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

5.3.2 Disable of an subscription

The 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 of subscription and equipment

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

5.3.4 Enable an MS equipment

The MS shall be capable of receiving enable commands addressed individually with a valid L2 address for the MS, i.e. ISSI/ASSI in the home network and ITSI/(V)ASSI in a visited network (during migration). The PDU shall include the TEI of the MS equipment. Only MS equipment that has been temporarily disabled may be enabled by this method: if the MS subscription has also been disabled, whether the ITSI is contained in a separable module or not, it shall not be enabled by this mechanism.

5.3.5 Enable an MS subscription

The MS shall be capable of receiving enable commands addressed individually with a valid L2 address for the MS, i.e. ISSI/ASSI in the home network and ITSI/(V)ASSI in a visited network (during migration). The PDU shall not include the TEI of the MS equipment. Only an MS subscription that has been temporarily disabled may be enabled by this method: If the MS equipment has also been disabled, whether the ITSI is contained in a separable module or not, the composite MS shall not be enabled solely by this mechanism.

5.3.6 Enable an MS equipment and subscription

The MS equipment and subscription shall be enabled using commands addressed to a valid L2 individual address for the MS, i.e. ISSI/ASSI in the home network and ITSI/(V)ASSI in a visited network (during migration), whether the subscription or equipment has previously been disabled, or both. Equipment, or subscriptions, or both, that have been temporarily disabled may be enabled by this mechanism. The PDU shall include the TEI of the MS equipment.

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

5.4 Enable/disable protocol

5.4.1 General case

NOTE 1: An MS operating in transmission inhibit mode (for example operating in radio transmission free environments such as hospitals) may be unable to transmit the protocol responses required below. In such cases the behaviour of the MS is determined by system policy (e.g. to be permitted to act on the received command without response).

All signalling should be individually addressed. The SwMI may need to know the ITSI/TEI binding, where necessary this may be obtained using the ITSI-TEI mapping at registration. Confirmation of the target for disabling and enabling is then provided by including the ITSI and/or TEI of the MS in the PDUs. If the SwMI supports authentication, it should authenticate the MS to ensure that it is obtaining a response from the correct MS. The MS should also authenticate the SwMI when possible to validate the instruction. The authentication protocol and PDUs are contained in clause 4.

The protocol shall be required to complete before the MS changes its state. If the protocol transaction does not complete (unless the failure was due to authentication failure), the MS shall indicate its unchanged state to the SwMI.

The TEI when included in PDUs is not protected by any specific cryptographic sealing mechanism. It should therefore only be provided when the security information has been established, and air interface encryption is operating on a cell of class 2 or 3 as described in clause 6.

NOTE 2: It is recommended that the TEI is not transferred across the air interface in class 1 cells.

The enabling and disabling is enacted by the primitives MLE-DISABLE request, MLE-DEACTIVATE request and MLE-ENABLE request. The MLE-DISABLE request primitive is sent from MM to MLE to indicate to the MLE entity that access to the communication resources has been closed to the other higher layer entities: SNDCP and CMCE. If the disabling is temporary the MS shall remain disabled in the sense that access to the communication resources shall remain closed for the CMCE and SNDCP entities. MM should remain active so that any roaming (or associated security) functions continue to operate, in order to allow the MS to receive an enable instruction. Should the MS be powered down the MS shall retain the information that it is temporarily disabled.

In the temporarily disabled state the MS shall disable the MMI and PEI in order to prevent the user making any change to the state of the MS and also to prevent the user being able to derive any knowledge of the operation of the MS.

The MLE-ENABLE request primitive is sent from MM to MLE to recover the MS from the temporarily disabled state.

In the temporarily disabled state the MS shall not be able to invoke any function of the CMCE and SNDCP entities.

EXCEPTION 1: For the purpose of supporting the Supplementary Service Ambience Listening according to ETSI EN 300 392-10-21 [i.7] the MS and SwMI may be able to invoke the relevant CMCE entities. The disabled MS may ignore any request from the SwMI to invoke this service.

EXCEPTION 2: For the purposes of the location information protocol according to ETSI TS 100 392-18-1 [i.6], the MS and SwMI may be able to invoke the CMCE entity. The disabled MS may ignore any request from the SwMI to invoke this service.

The MS shall not invoke any OTAR function for SCK/SCKX, GCK/GCKX or GSKO/GSKOX by any method in the temporarily disabled state. In a permanently disabled state the disabling 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.

A migrated MS shall accept temporary disable and enable commands from a visited SwMI provided the request is valid. It shall not accept permanent disable commands from the visited SwMI.

5.4.2 Status of cipher key material

5.4.2.1 Permanently disabled state

In the event of permanent disable of an ITSI all key material for use on all networks including K or K2 shall be permanently deleted such that it cannot be recovered.

In the event of permanent disable of an equipment (TEI) all key material for use on all networks maintained on the equipment (including K or K2 if present) shall be permanently deleted such that it cannot be recovered. If a SIM is fitted, entry to the permanently disabled state should not delete key material on the SIM.

NOTE: A SIM is intended to store material directly related only to an ITSI.

It is advised that where possible as a result of permanent disable the algorithms belonging to the algorithm sets TAA1 and TAA2, and any TETRA encryption algorithms (TEAx) should be permanently deleted.

Table 5.1 summarizes the state of key material after permanent disable.

Table 5.1: Summary of Permanent Disable

Identity module	Disable target	Normal operating security class	Post disable key state
Non-detachable	TEI/ITSI	All	permanently delete all
		2	
		1	
Detachable	TEI	All	permanently delete all material residing in the equipment
		2	
		1	
Detachable	ITSI	All	permanently delete all material residing in the SIM
		2	
		1	

5.4.2.2 Temporarily disabled state

In the event of temporary disable of an ITSI in class 3 networks all shared long lifetime key material relating to all networks (GCK/GCKX, SCK/SCKX where 1 ≤ SCKN ≤ 30, GSKO/GSKOX) and CMG GTSIs relating to all networks should be permanently deleted. The fallback SCK or SCKX for TMO (SCKN = 31 or SCKN = 32) should not be deleted for any network, and K or K2 should not be deleted. For class 2 networks SCKs/SCKXs used in TMO shall be retained to allow the enable protocol to work.

In the event of temporary disable of an equipment (TEI) in class 3 networks all shared long lifetime key material relating to all networks (GCK/GCKX, SCK/SCKX where 1 ≤ SCKN ≤ 30, GSKO/GSKOX) and CMG GTSIs relating to all networks should be permanently deleted. The fallback SCK or SCKX for TMO (SCKN = 31 or SCKN = 32) should not be deleted for any network, and K or K2 should not be deleted. For class 2 networks SCKs/SCKXs used in TMO shall be retained to allow the enable protocol to work. In a class 3 network in order to maintain MM functionality (required for the enable protocol to work and to allow the location update protocol to work) the following keys shall be retained for the serving network only: DCK/DCKX; CCK/CCKX. Any DCK/DCKX or CCK/CCKX stored for use on a network other than the serving network shall be deleted.

Table 5.2 summarizes the state of key material after temporary disable.

Table 5.2: Summary of Temporary Disable

Identity module	Disable target	Normal operating security class	Post disable key state
Non-detachable	TEI/ITSI	3	Retain DCK/DCKX, CCKs/CCKXs, K/K2, SCK31, SCK32
		2	Retain TMO SCKs/SCKXs, K/K2
		1	Retain K/K2
Detachable	TEI	3	Retain DCK/DCKX, CCKs/CCKXs, K/K2, SCK31, SCK32
		2	Retain TMO SCKs/SCKXs, K/K2
		1	Retain K/K2
Detachable	ITSI	3	Retain DCK/DCKX, CCKs/CCKXs, K/K2, SCK31, SCK32
		2	Retain TMO SCKs/SCKXs, K/K2
		1	Retain K/K2

5.4.3 Specific protocol exchanges

5.4.3.0 General

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

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

5.4.3.1 Disabling an MS with mutual authentication

The scenario in Figure 5.3 shall apply for MS and SwMI where the SwMI enforces authentication and the MS and SwMI supports mutual authentication. The authentication mechanisms and PDUs are described in clause 4 of the present document. The MSC shows as optional the key change procedure described in clause 4.5.5.1 which shall be considered mandatory for class 3 cells. The use of MLE-DEACTIVATE is shown as optional and shall apply when the disabling type is permanent.

Figure 5.3 shows the message sequence for this case.

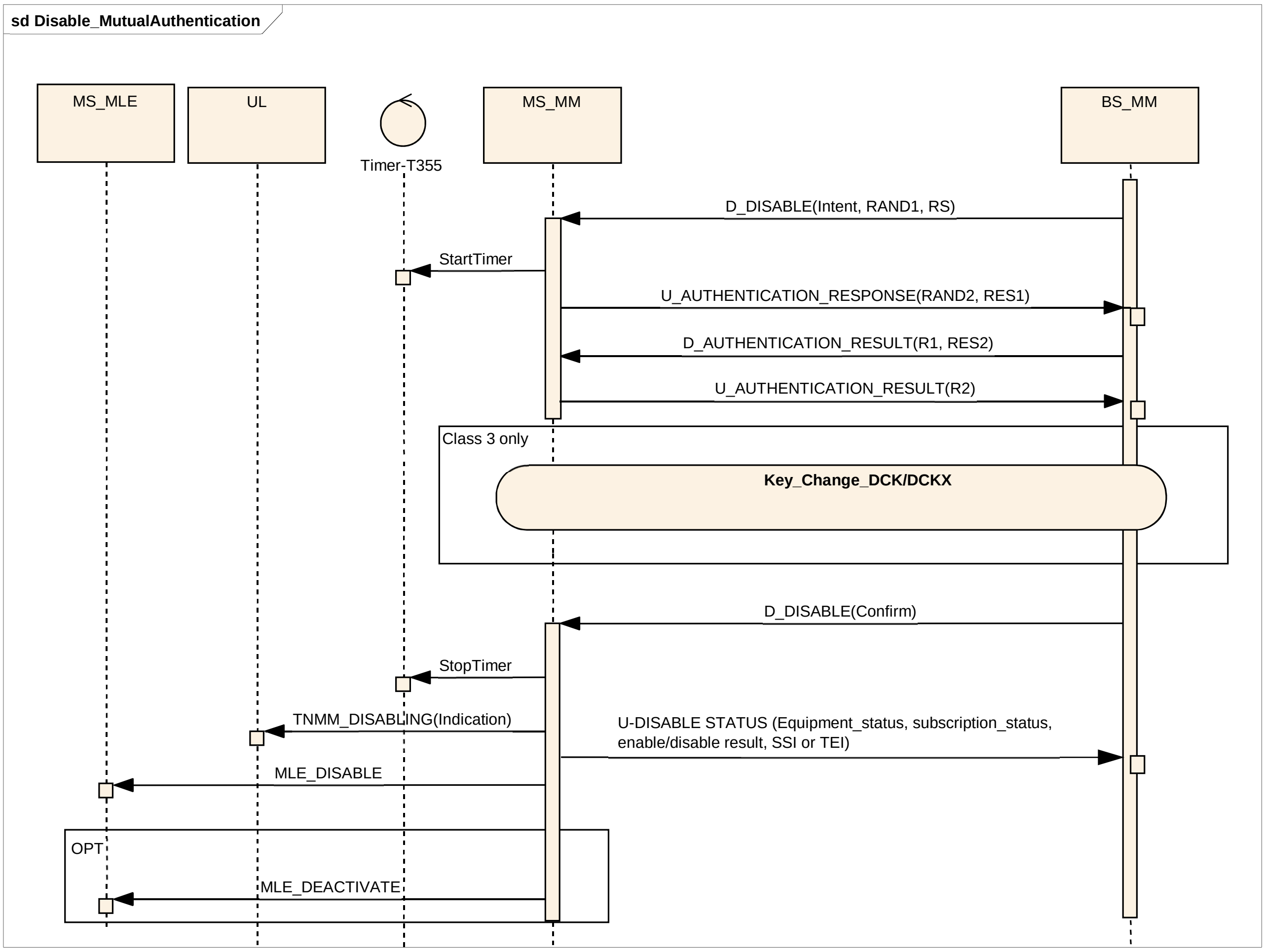

sd Disable_MutualAuthentication
MS_MLE
UL
Timer-T355
MS_MM
BS_MM
D_DISABLE(Intent, RAND1, RS)
StartTimer
U_AUTHENTICATION_RESPONSE(RAND2, RES1)
D_AUTHENTICATION_RESULT(R1, RES2)
U_AUTHENTICATION_RESULT(R2)
Class 3 only
Key_Change_DCK/DCKX
D_DISABLE(Confirm)
StopTimer
TNMM_DISABLING(Indication)
U-DISABLE STATUS (Equipment_status, subscription_status, enable/disable result, SSI or TEI)
MLE_DISABLE
OPT
MLE_DEACTIVATE

Figure 5.3: Disabling an MS with mutual authentication

5.4.3.2 Enabling an MS with mutual authentication

The scenario in Figure 5.4 shall apply for MS and SwMI where the SwMI enforces authentication and the MS and SwMI supports mutual authentication. This scenario shall only apply following temporary disabling of the MS. The authentication mechanisms and PDUs are described in clause 4 of the present document. The MSC shows as optional the key change procedure described in clause 4.5.5 which shall be considered mandatory for class 3 cells.

Figure 5.4 shows the message sequence for this case.

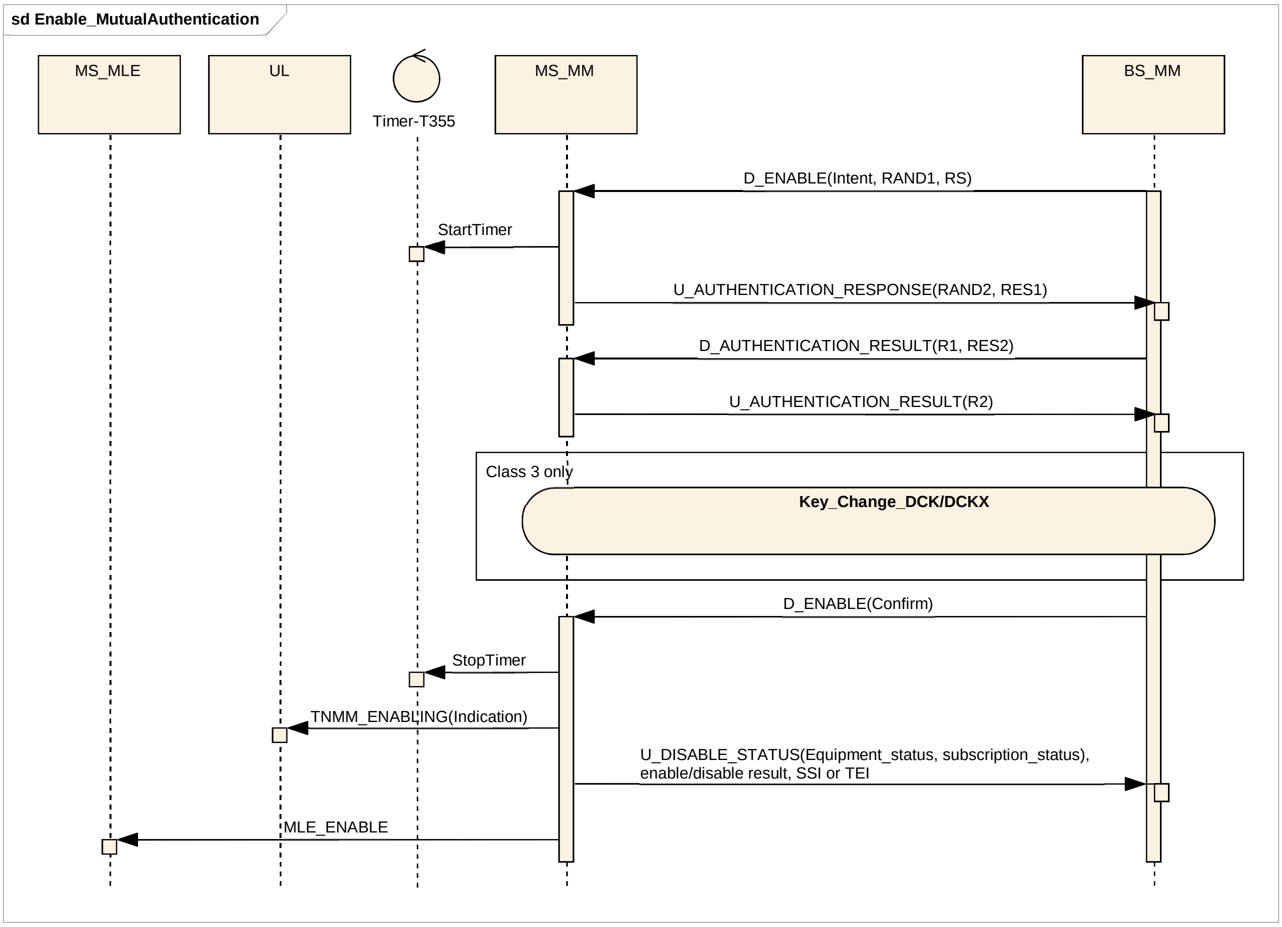

sd Enable_MutualAuthentication
MS_MLE
UL
Timer-T355
MS_MM
BS_MM
D_ENABLE(Intent, RAND1, RS)
StartTimer
U_AUTHENTICATION_RESPONSE(RAND2, RES1)
D_AUTHENTICATION_RESULT(R1, RES2)
U_AUTHENTICATION_RESULT(R2)
Class 3 only
Key_Change_DCK/DCKX
D_ENABLE(Confirm)
StopTimer
TNMM_ENABLING(Indication)
U_DISABLE_STATUS(Equipment_status, subscription_status), enable/disable result, SSI or TEI
MLE_ENABLE

Figure 5.4: Enabling an MS with mutual authentication

5.4.3.3 Enabling an MS with non-mutual authentication

The scenario in Figure 5.5 shall apply for MS and SwMI where the SwMI enforces authentication but the MS does not support mutual authentication. This scenario shall only apply following temporary disabling of the MS. The authentication mechanisms and PDUs are described in clause 4 of the present document. The MSC shows as optional the key change procedure described in clause 4.5.5.1 which shall be considered mandatory for class 3 cells.

Figure 5.5 shows the message sequence for this case.

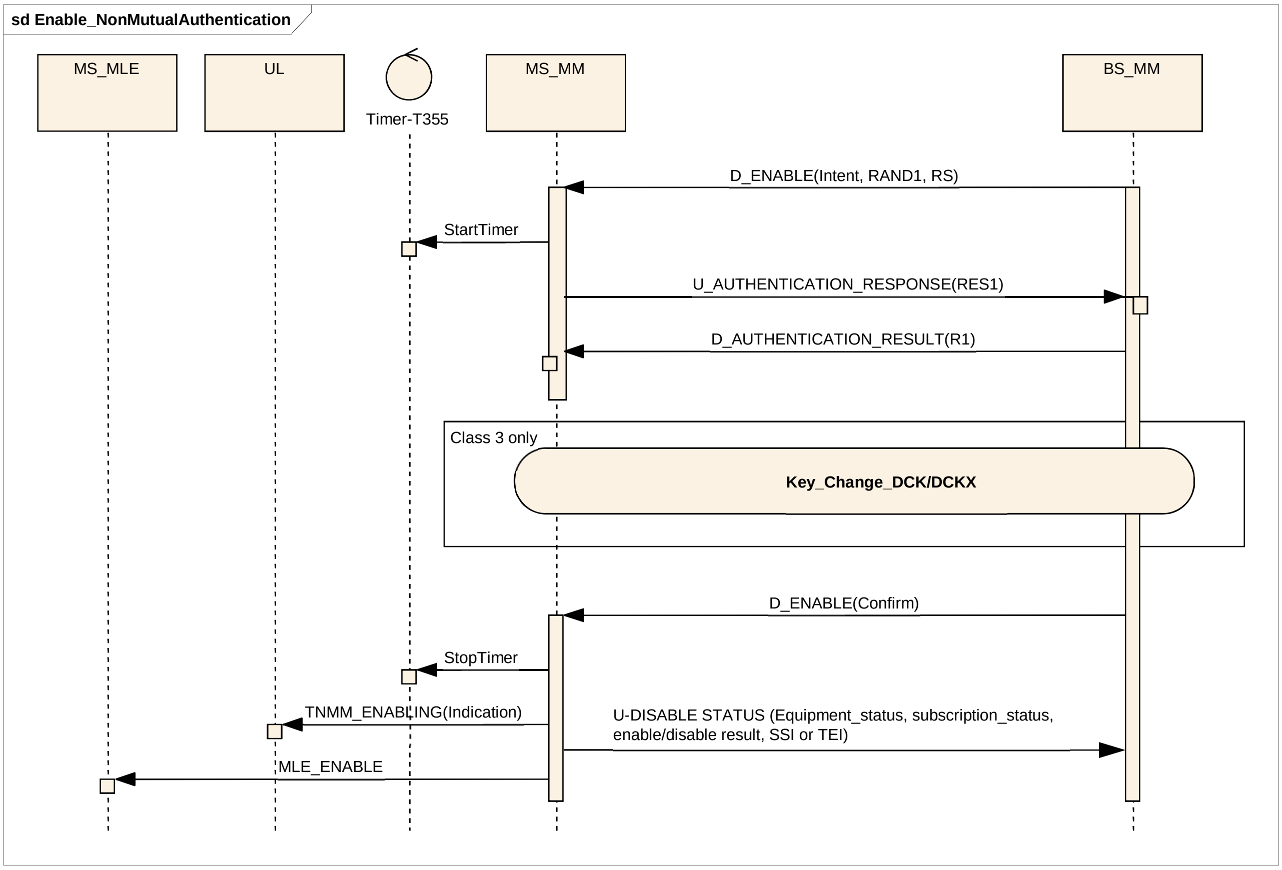

sd Enable_NonMutualAuthentication
MS_MLE
UL
Timer-T355
MS_MM
BS_MM
D_ENABLE(Intent, RAND1, RS)
StartTimer
U_AUTHENTICATION_RESPONSE(RES1)
D_AUTHENTICATION_RESULT(R1)
Class 3 only
Key_Change_DCK/DCKX
D_ENABLE(Confirm)
StopTimer
TNMM_ENABLING(Indication)
U-DISABLE STATUS (Equipment_status, subscription_status, enable/disable result, SSI or TEI)
MLE_ENABLE

Figure 5.5: Enabling an MS with non-mutual authentication

5.4.3.4 Disabling an MS with non-mutual authentication

The scenario in Figure 5.6 shall apply for MS and SwMI where the SwMI enforces authentication but the MS does not support mutual authentication. The authentication mechanisms and PDUs are described in clause 4 of the present document. The MSC shows as optional the key change procedure described in clause 4.5.5 which shall be considered mandatory for class 3 cells. The use of MLE-DEACTIVATE is shown as optional but shall apply when the disabling type is permanent.

Figure 5.6 shows the message sequence for this case.

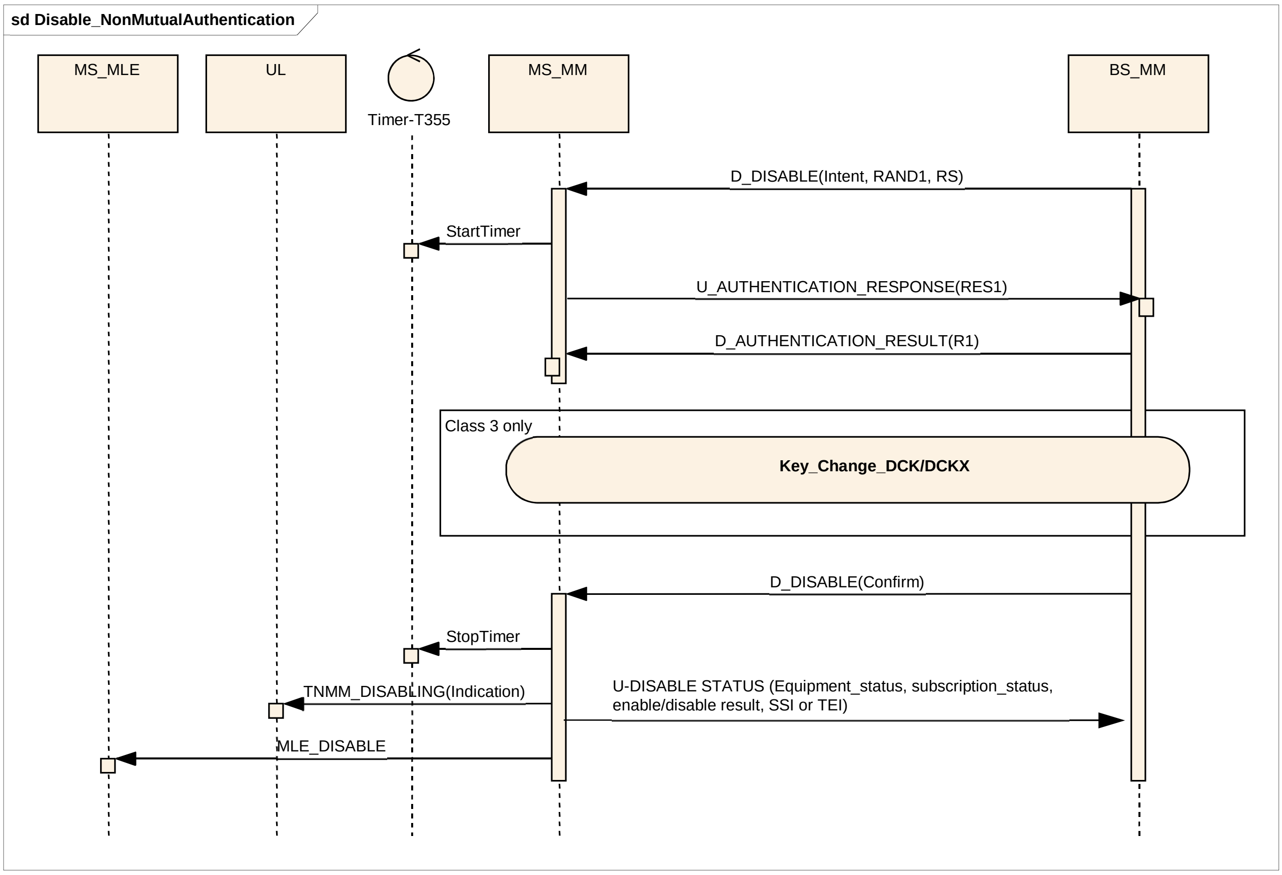

sd Disable_NonMutualAuthentication
MS_MLE
UL
Timer-T355
MS_MM
BS_MM
D_DISABLE(Intent, RAND1, RS)
StartTimer
U_AUTHENTICATION_RESPONSE(RES1)
D_AUTHENTICATION_RESULT(R1)
Class 3 only
Key_Change_DCK/DCKX
D_DISABLE(Confirm)
StopTimer
TNMM_DISABLING(Indication)
U-DISABLE STATUS (Equipment_status, subscription_status, enable/disable result, SSI or TEI)
MLE_DISABLE

Figure 5.6: Disabling an MS with non-mutual authentication

5.4.4 Enabling an MS without authentication

The scenario in Figure 5.7 shall apply for MS and SwMI where the SwMI does not enforce authentication. This scenario shall only apply following temporary disabling of the MS.

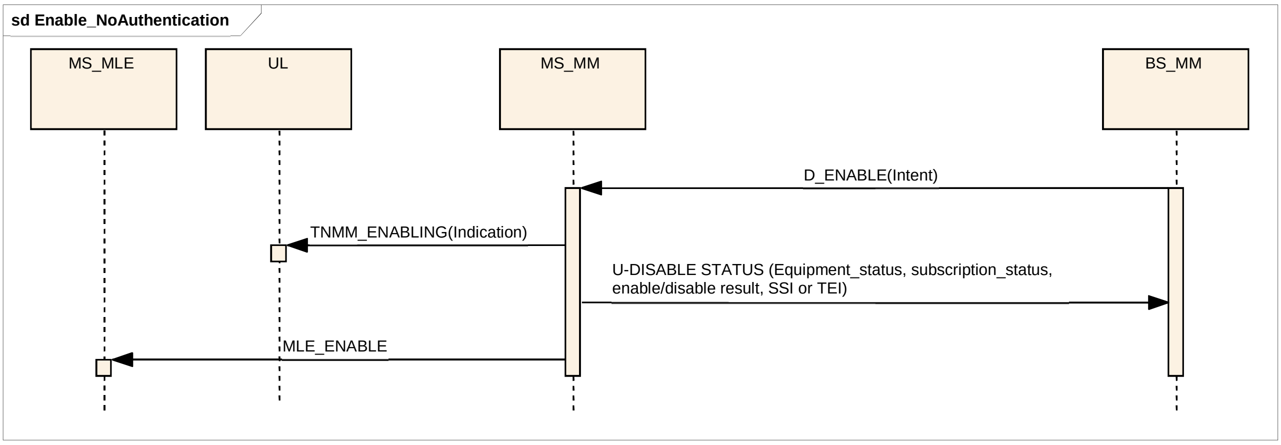

sd Enable_NoAuthentication
MS_MLE
UL
MS_MM
BS_MM
D_ENABLE(Intent)
TNMM_ENABLING(Indication)
U-DISABLE STATUS (Equipment_status, subscription_status, enable/disable result, SSI or TEI)
MLE_ENABLE

Figure 5.7: Enabling an MS without authentication

5.4.5 Disabling an MS without authentication

The scenario in Figure 5.8 shall apply for MS and SwMI where the SwMI does not enforce authentication.

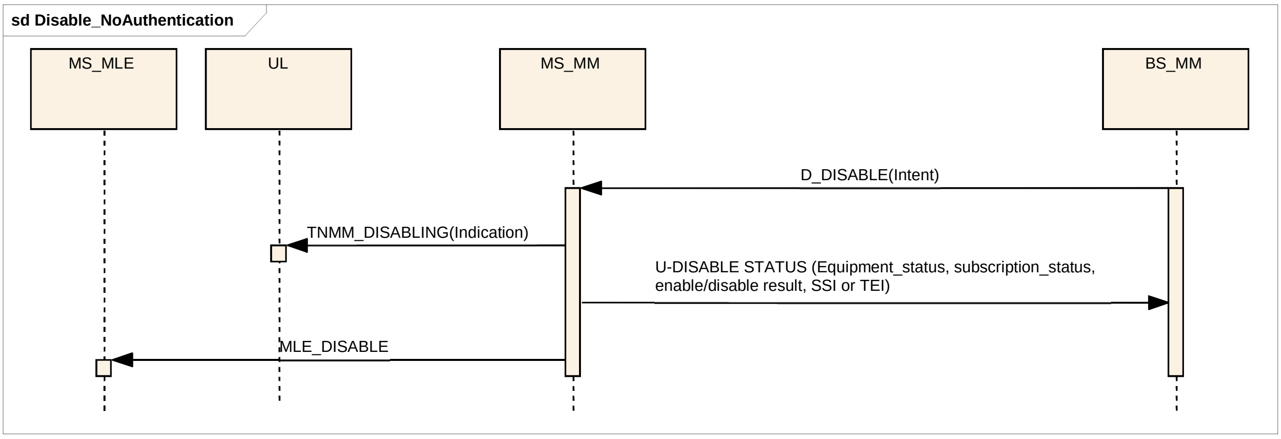

sd Disable_NoAuthentication
MS_MLE
UL
MS_MM
BS_MM
D_DISABLE(Intent)
TNMM_DISABLING(Indication)
U-DISABLE STATUS (Equipment_status, subscription_status, enable/disable result, SSI or TEI)
MLE_DISABLE

Figure 5.8: Disabling an MS without authentication

5.4.6 Rejection of enable or disable command

NOTE: Local security policy determines the behaviour required from the system.

An MS which receives an enable or disable command for a function which it does not support should reject the enable or disable command with the message "MM PDU NOT SUPPORTED".

An MS which supports enable/disable and encryption should reject an unencrypted enable/disable command with the reason "encryption is required" in the U-DISABLE STATUS PDU.

An MS which supports enable/disable, but does not support authentication, should reject an enable/disable command which includes authentication with the reason "authentication not supported" in the U-DISABLE STATUS PDU.

An MS which supports enable/disable and enforces mutual authentication should reject an enable/disable command which does not include authentication with the reason "authentication required" or "authentication and encryption are required" in the U-DISABLE STATUS PDU.

An MS which supports enable/disable should reject an enable/disable command directed at a TEI which does not match the TEI of the MS with the reason "TEI mismatch" in the U-DISABLE STATUS PDU.

An MS which receives a permanent disable command from a network other than the home network should reject an enable/disable command with the reason "address mismatch" in the U-DISABLE STATUS PDU.

An MS which receives a permanent disable command directed to TEI from a network other than the home network should reject an enable/disable command with the reason "TEI and address mismatch" in the U-DISABLE STATUS PDU.

If authentication of either party fails, the transaction shall terminate following transmission of the appropriate AUTHENTICATION RESULT PDU, and the MS shall remain in its previous state (enabled or disabled).

Figure 5.9 shows the message sequence for this case.

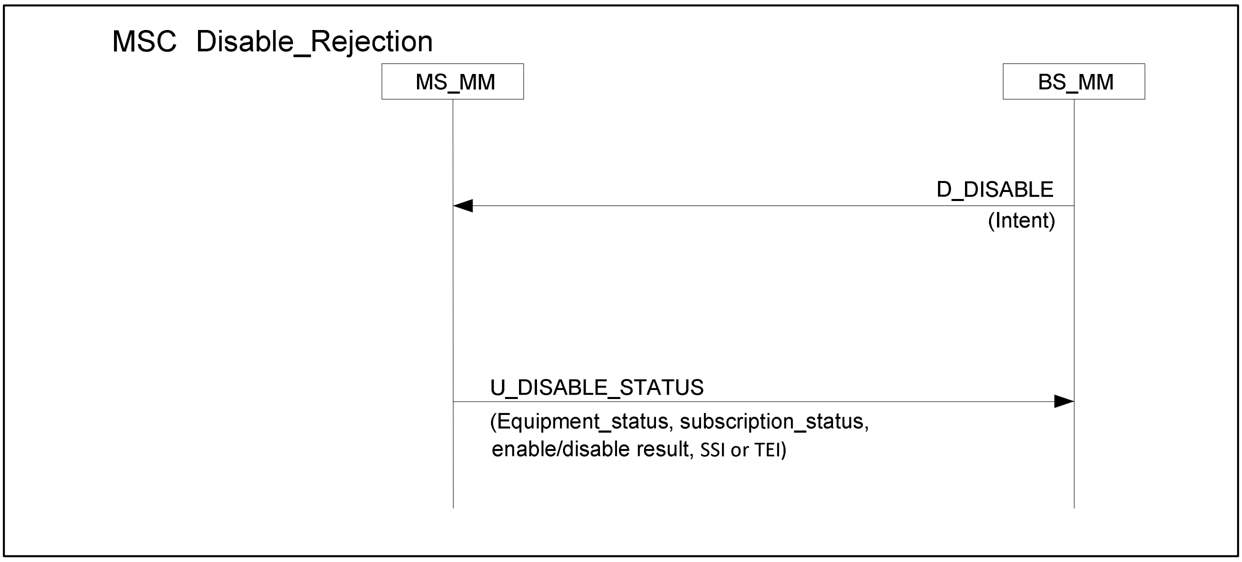

MSC Disable_Rejection
MS_MM
BS_MM
D_DISABLE
(Intent)
U_DISABLE_STATUS
(Equipment_status, subscription_status, enable/disable result, SSI or TEI)

Figure 5.9: Rejection of permanent disabling by an MS without authentication

5.4.6a Expiry of Enable/Disable protocol timer

If authentication is used in the transaction, and timer T355 expires before the receipt of D-DISABLE Confirm or D-ENABLE Confirm by the MS, the MS shall revert to its previous state. The U-DISABLE STATUS PDU shall be sent to the SwMI with the Enable/Disable result element set to "Enable/disable failure, authentication is required". The SwMI may use this reason to deduce that the transaction has failed due to timer expiry, as the transaction did make use of authentication.

If the authentication transaction has completed before expiry of the timer, the established DCK/DCKX shall follow the rules according to clause 4.5.5.1. If authentication has failed to complete, the encryption state and established DCK/DCKX shall follow the rules according to clause 4.4.2.

Timer T355 is started before the authentication timer T354, and stopped after T354, and therefore shall be greater or equal in value to T354.

5.4.7 MM service primitives

5.4.7.0 General

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

5.4.7.1 TNMM-DISABLING primitive

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

Table 5.3 defines the parameters for TNMM-DISABLING indication.

Table 5.3: 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 5.4 defines the parameters for TNMM-ENABLING indication.

Table 5.4: Parameters for the primitive TNMM-ENABLING indication

Parameter	Indication
Enable/disable status	M

The parameters in the primitives may take the values identified in Table 5.5.

Table 5.5: Enable/disable status values

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

6 Air Interface (AI) encryption

6.1 General principles

AI encryption shall provide confidentiality on the radio link between MS and BS and be resident in the upper part of the MAC layer of the TETRA protocol stack, which itself is the lower part of layer 2. Situating the encryption process at this point, prior to channel coding at the transmitting end and after channel decoding at the receiving end, enables the MAC headers to be left unencrypted. This allows the appropriate channel coding to be used, enables receiving parties to determine the applicability of a message received over air for them, and enables application of the correct key for the decryption process. Figure 6.1 illustrates this placement.

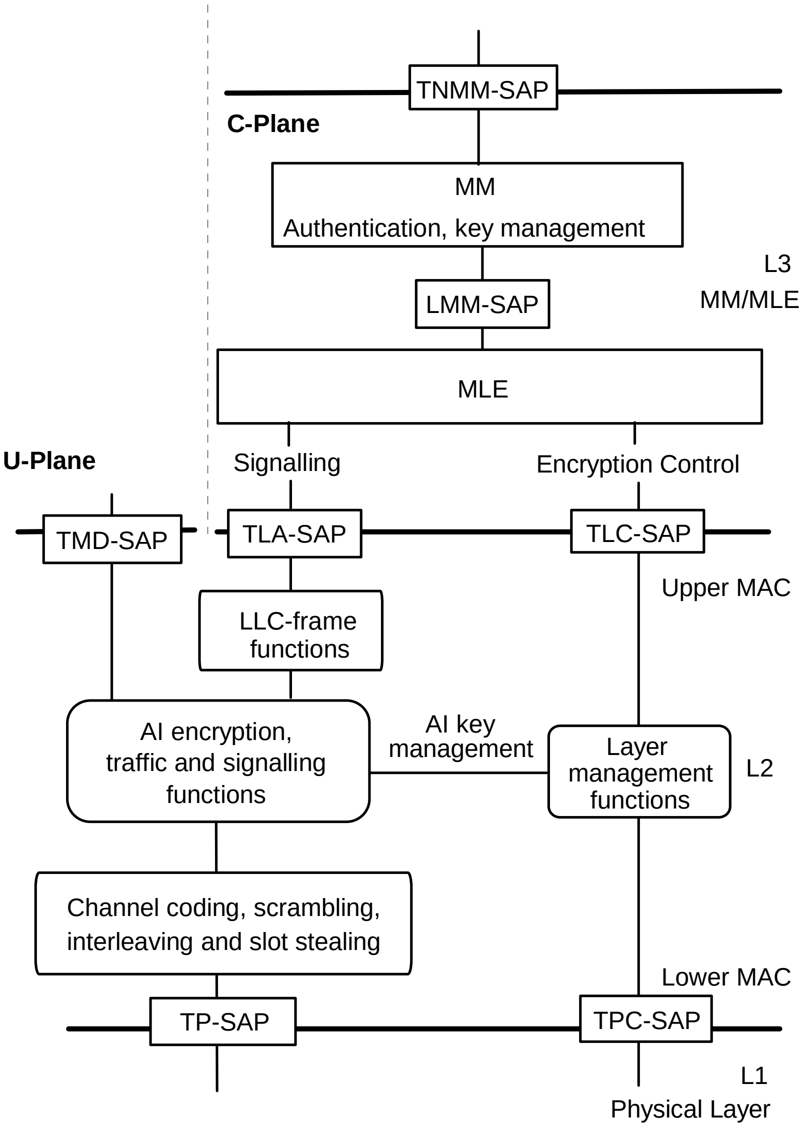


Figure 6.1: Relationship of security functions to layers functions in MS

The MS and SwMI shall use the same AI encryption algorithm. An air interface encryption algorithm may be negotiated between MS and SwMI from two sets of algorithms, TEA set A and TEA set B. These are described in clause 6.3.1.

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

Air interface encryption shall be a separate function to the end-to-end encryption service described in ETSI EN 302 109 [6]. 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 ETSI EN 300 392-1 [1], these shall be independent of air interface encryption; thus a circuit mode service invoked without end-to-end encryption may still be encrypted over the air interface.

6.2 Security class

6.2.a General

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

- Security class 2: For AI encryption without enforced authentication. This mode shall use SCK or SCKX for signalling and traffic encryption, and for address encryption.

- Security class 3: For AI encryption where authentication is mandatory. This mode shall use DCK or DCKX for individually addressed signalling and traffic encryption. This mode shall use CCK or CCKX for address encryption, and shall also use CCK or CCKX to encrypt group addressed signalling (including broadcast) and traffic alone or in combination with GCK or GCKX.

Table 6.1 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 6.1: Security classes

Class 1:	Shall not use encryption.
	May use authentication.
Class 2: SCK Mode	Shall use SCK/SCKX encryption.
	Shall use ESI with SCK/SCKX or MAE with SCKX.
	May use authentication.
Class 3: DCK Mode	Shall use authentication.
	Shall use DCK/DCKX, CCK/CCKX and may use MGCK/MGCKX encryption (GCK/GCKX in combination with CCK/CCKX).
	Shall use ESI with CCK/CCKX or MAE with CCKX.

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

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

- class 1 only;
- class 2 only;
- class 2 and class 1;
- class 3 only; or
- class 3 and class 1.

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

In class 3 systems post authentication all individually addressed signalling exchanges on the downlink, and all signalling exchanges on the uplink, are also implicitly authenticated by use of DCK/DCKX as the encryption key. In group addressed signalling exchanges protected by MGCK/MGCKX implicit authentication is also provided in class 3 systems as the CCK/CCKX can only be received if the MS is in possession of DCK/DCKX.

6.2.0 Notification of security class

6.2.0.0 General

The security class and other parameters shall be broadcast by each cell in the SYSINFO, SYSINFO-DA or SYSINFO-Q PDUs (see ETSI EN 300 392-2 [2], clause 21). When sent using SYSINFO the broadcast shall use the "Extended Service Broadcast" information element defined in ETSI EN 300 392-2 [2] and signalled by setting the "Optional Field flag" element of SYSINFO to 11_2. It should be noted that SYSINFO may not always contain security information as the "Extended Service Broadcast" element can be alternated with one or more of the following information fields:

- "Even multiframe definition for TS mode";
- "Odd multiframe definition for TS mode"; or
- "Default definition for access code A".

Systems employing the security provisions described in the present document should ensure regular broadcast of the security information.

NOTE: SYSINFO-DA PDUs always contain the "Extended DA Services" element and SYSINFO-Q PDUs always contain the "Extended Services" element, and therefore the "Security Information" Element is always present on a QAM channel. Security class is also broadcast in the "Security Parameters" element in the SYNC-DA PDU on DA cells.

6.2.0.1 Security class of neighbouring Cells

The serving cell may indicate the security class capabilities of neighbouring cells through the "Timeshare cell or security parameters" information element in the D-NWRK BROADCAST and "Security parameters" information element in D-NWRK BROADCAST-DA PDUs. The MS should assume that the neighbour cells have the same security class as that of the serving cell (i.e. the network is homogenous), unless the MS is given information to the contrary through this information element. Note that security class of neighbouring cells shall be identical to that of the serving cell if the neighbour cell shares channels with the serving cell, see clause 6.6.3.

6.2.0.2 Identification of MS security capabilities

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 MS, and the MS also supports class 3 and class 1, the MS shall register at class 3).

The MS shall use the fields present in the "class of MS" element (see ETSI EN 300 392-2 [2]) to indicate at registration the authentication, DCK/DCKX encryption and SCK/SCKX encryption capabilities of the MS for security. Furthermore, when registering for SC3 operation, the MS shall use the additional fields available in the "ciphering parameters" information element to indicate the MS's support for TM-SCK OTAR, SDMO and DM-SCK OTAR, GCK encryption/OTAR, SCK OTAR (for an SCK used with an algorithm in TEA set A) if the MS proposes an algorithm in TEA set B, and also support for the information request protocol.

If the MS proposes a KSG which uses an algorithm from TEA set A (see clause 6.3), "class of MS" shall be used to indicate support for encryption using DCK (and CCK) and support for encryption using SCK, and "ciphering parameters" shall be used when registering for security class 3 operation to indicate support for encryption using GCK and for OTAR of SCK and GCK. If the MS proposes a KSG which uses an algorithm from TEA set B (see clause 6.3), "class of MS" shall be used to indicate support for encryption using DCKX (and CCKX) and support for encryption using SCKX, and "ciphering parameters" shall be used when registering for security class 3 operation to indicate support for encryption using GCKX and for OTAR of SCKX and GCKX. An MS that proposes a KSG which uses an algorithm from TEA set B and supports OTAR of SCKX may also support OTAR of SCK and shall indicate this support in "ciphering parameters" when registering for security class 3 operation.

NOTE: When registering for SC2 operation, the MS is unable to indicate its support for TM-SCK/SCKX OTAR, SDMO and DM-SCK/SCKX OTAR, GCK/GCKX encryption/OTAR and OTAR of SCK when proposing an algorithm in TEA set B.

The TETRA Air Interface standard version number given in ETSI EN 300 392-2 [2], applies for value 000_2 to ETSI ETS 300 392-2 edition 1 only [i.1]. Value 001_2 shall apply to ETSI ETS 300 392-2 edition 1 [i.1], plus ETSI EN 300 392-7 (V2.2.1) [i.4]. Value 010_2 shall apply to ETSI EN 300 392-2 (V2.3.2) to (V2.6.1) [2] plus ETSI EN 300 392-7 (V2.1.1) [i.5] to ETSI TS 100 392-7 (V2.4.1) [i.8]. Value 011_2 shall apply to ETSI EN 300 392-2 [2] (V3.1.1) onwards, and ETSI EN 300 392-7 (V3.1.1) [i.9] onwards. There shall be no signalling to indicate that an MS complies with ETSI ETS 300 392-7 [i.2], implying that ETSI ETS 300 392-7 [i.2] is not accepted as a valid implementation.

This edition of the present document is compatible with ETSI EN 300 392-7 (V2.1.1) [i.5].

6.2.1 Constraints on LA arising from cell class

In a fully operational LA, all cells should be of the same security class (see also clause 6.5.1.3 and constraints defined for periods of class change in clause 4.5.6).

6.3 Key Stream Generator (KSG)

6.3.0 General

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

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

The KSG shall have two inputs, an Initial Value (IV) and a cipher key. These parameters shall be as specified in clause 6.3.2. The KSG shall produce one output as a sequence of key stream bits referred to as a Key Stream Segment (KSS).

A separate KSS shall be produced to encrypt every timeslot for each different key to be used to encrypt PDUs in that timeslot. Sufficient length of each KSS shall be produced to encrypt those PDUs using that KSS, taking into account the rules for allocation of KSS to logical channels specified in clause 6.4.1. The bits of each KSS are labelled KSS(0), … KSS(n-1), where KSS(0) is the first bit output from the generator and n is the number of bits output from the generator for that KSS. The bits in the appropriate KSS shall be used to encrypt or decrypt the data of the control or traffic field. On a phase modulation channel the maximum value of n shall be 432, which enables encryption of a TCH/7,2 unprotected traffic channel, and on a 150 kHz QAM channel, the maximum value of n shall be 8 288. Where a KSG from TEA set B is in use (see clause 6.3.1) and where CCKX or SCKX is the key in use, the first 34 bits of KSS, KSS(0) to KSS(33), shall be reserved to allow the encryption of a MAC address.

6.3.1 KSG numbering and selection

TETRA supports both standard and proprietary algorithms for air interface encryption. However requirements for interoperability should be taken into account when considering use of proprietary algorithms. Location update signalling shall identify which algorithm is in use. Migration should only be possible if there is agreement between operators on the algorithm used.

There are two sets of standard algorithms, identified as TEA set A and TEA set B. TEA set A comprises algorithms TEA1, TEA2, TEA3 and TEA4. These algorithms have a Cipher Key (CK) length of 80 bits. TEA set B comprises algorithms TEA5, TEA6 and TEA7. These algorithms have an Extended Cipher Key (CKX) length of 192 bits.

NOTE 1: A KSG that implements an algorithm from TEA set A is referred to as a KSG from TEA set A, and a KSG that implements an algorithm from TEA set B is referred to as a KSG from TEA set B in the present document.

The SwMI should only have one encryption algorithm from TEA set A. The SwMI should only have one encryption algorithm from TEA set B. A SwMI may support one encryption algorithm from TEA set A and one algorithm from TEA set B at the same time. An MS may support more than one algorithm but shall use the algorithm negotiated with the SwMI.

NOTE 2: Support for more than one algorithm at a time by the SwMI may allow MSs to transition from use of one algorithm to use of another algorithm, without the MSs all needing to transition at the same time. Support of more than one algorithm at a time outside a transition period is not recommended.

Table 6.2 shows that the values 0000_2 to 0111_2 of KSG number used in signalling are reserved for the TETRA standard algorithms (see also ETSI EN 300 392-2 [2], clause 16.10.29).

Table 6.2: KSG Number element contents

Information element	Length	Value	Remark
KSG Number	4	0000_2	TETRA Standard Algorithm, TEA1
		0001_2	TETRA Standard Algorithm, TEA2
		0010_2	TETRA Standard Algorithm, TEA3
		0011_2	TETRA Standard Algorithm, TEA4
		0100_2	TETRA Standard Algorithm, TEA5
		0101_2	TETRA Standard Algorithm, TEA6
		0110_2	TETRA Standard Algorithm, TEA7
		0111_2	Reserved for future expansion
		1000_2 to 1011_2	Proprietary TETRA Algorithms See note 1
		1100_2 to 1111_2	Reserved for future expansion See note 2
NOTE 1: Refer to clause 4.1.1a. NOTE 2: Prior to V4.1.1 of the present document, values from 1100_2 to 1111_2 were allocated to proprietary algorithms.			

The TETRA standard algorithms are only available on a restricted basis. The rules for the management and use of these algorithms are specified in ETSI TS 101 053-1 [i.10], ETSI TS 101 053-2 [i.11], ETSI TS 101 053-3 [i.12], and ETSI TS 101 053-4 [i.13] for TEA1, 2, 3 and 4 respectively, and in ETSI TS 101 053-5 [i.15], ETSI TS 101 053-6 [i.16] and ETSI TS 101 053-7 [i.17] for TEA5, 6 and 7 respectively. The Confidentiality and Restricted Use Undertakings for TEA1, 3 and 4 can be found at the ETSI Web Portal (http://www.etsi.org/algorithms). The Confidentiality and Restricted Use Undertaking for TEA2 is available on request from the TEA2 custodian. Details of the TEA2 custodian are also provided on the ETSI Web Portal as referenced above.

Where a SwMI supports more than one encryption algorithm in security class 3 systems the CCK has to be common to users of all TEA algorithms (where the SwMI may derive the CCK from a CCKX), and in security class 2 systems the SCK has to be common to users of all TEA algorithms (where the SwMI may derive the SCK from an SCKX), in order for commonality of the ESI address encryption mechanism (see clause 4.2.6).

NOTE 3: The MAE mechanism is only able to be used where all MSs negotiate the same KSG from TEA set B.

Groups of users should be differentiated by GCK or GCKX in class 3 systems. Terminals shall support only one active encryption algorithm. There shall be no dynamic change of registered algorithm for MSs in a session. If there is more than one KSG in use in the SwMI, then broadcast messages should not be encrypted.

6.3.2 Interface parameters

6.3.2.0 General

The two inputs to the KSG, Initial Value (IV) and cipher key described in clause 6.3.0 are composed differently for encryption algorithms from TEA set A and TEA set B. For algorithms in TEA set A, a 29 bit IV is derived from the slot and frame numbering system together with a TX/RX bit, and the cipher key is modified by parameters relating to the BS. For algorithms in TEA set B, the IV is 80 bits long, and consists of the 29 bit slot and frame numbering system and the uplink/downlink bit, plus further parameters relating to the BS. The cipher key used in algorithms in TEA set B is unmodified.

6.3.2.0a IV validity

In this clause, 'IV' refers to the value of the slot and frame numbering part of the IV, which is the entire IV for a KSG from TEA set A, or part of the IV for a KSG from TEA set B.

The value of the IV shall be maintained by the SwMI and broadcast on the SYNC and SYSINFO PDUs, or SYNC-DA and SYSINFO-DA PDUs (layer 2). The value of hyper-frame (IV(13) to IV(27) for a KSG in TEA set A, or IV(13) to IV(28) for a KSG in TEA set B) shall be broadcast to a schedule determined by the SwMI with the value of CCK-id on cells of security class 3, and with the value of SCK-VN in cells of security class 2, in the SYSINFO broadcast.

The MS may assume that the value of the IV provided by the SwMI is valid following a successful authentication of the SwMI, or following a successful procedure that includes mutual authentication with the SwMI. The MS should keep track of successive SwMI broadcasts of this IV information, and if the value of IV provided by the SwMI deviates from the expected value, the MS should consider:

a) if neighbour cells are synchronized to the serving cell, scan one or more neighbour cells and if the value of IV on a scanned neighbour cell matches the value expected by the MS, perform cell reselection to that neighbour cell; or

b) initiate authentication of the SwMI using the IV provided by the SwMI to ensure that the newly provided value of IV is valid. If the MS initiates authentication of the SwMI in this case, it shall maintain its previously established encryption state and shall apply the IV received from the SwMI.

NOTE: Use of the latest IV received from the SwMI ensures that the authentication challenge can be decrypted by the SwMI in case the unexpected IV is a result of an error in the MS or a change in timing of the BS.

If the MS does not receive an encrypted response to the authentication challenge, the MS may decide to perform cell reselection without attempting a clear authentication on the serving cell.

When an MS performs cell reselection, the IV on the neighbour cell can be considered valid if the cells are synchronized as indicated in the "Neighbour cell information for CA" or "Neighbour cell information for DA" elements in the D-NWRK-BROADCAST or D-NWRK-BROACAST-DA PDUs, and the IV matches that provided by the serving cell. If the neighbour cell is not synchronized with the serving cell, or if the IV deviates from the expected value based on the IV provided by the serving cell, the MS should consider authenticating the neighbour cell following cell reselection to validate the IV provided by the neighbour cell.

In case of authentication failure either on the serving cell or the newly selected neighbour cell, the MS shall perform the actions for authentication failure cases specified in clause 4.4.2.0.

6.3.2.1 Initial Value (IV) for algorithms in TEA set A

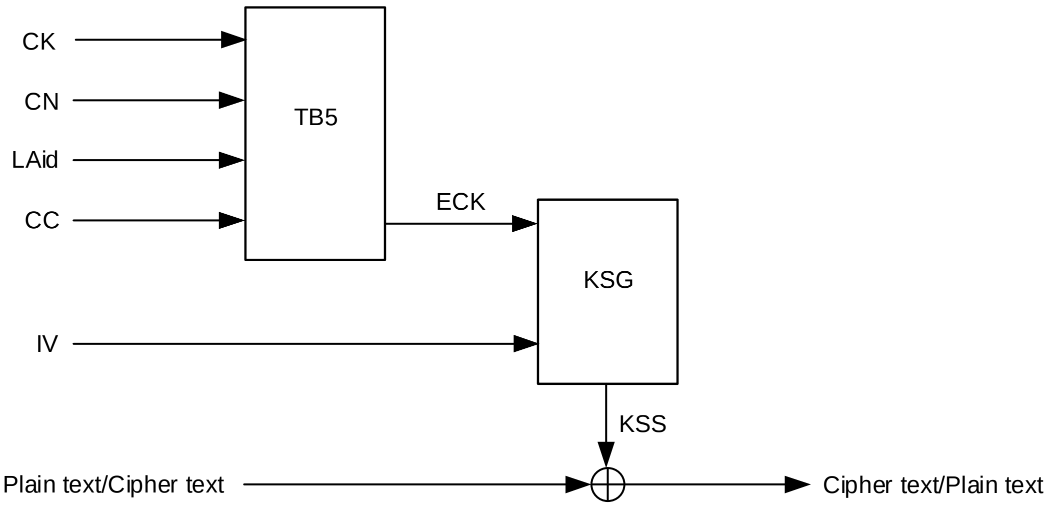
The composition of the slot and frame numbering input to IV shall be as follows:

- the first two bits IV(0) and IV(1) shall correspond to the slot number, and shall take values from 0 to 3, where value 0 corresponds to slot 1, and value 3 corresponds to slot 4. IV(0) shall be the least significant bit of the slot number (ETSI EN 300 392-2 [2], clause 9.3.5);
- the next five bits IV(2) to IV(6) shall correspond to the frame number, and shall take values from 1 (00001 binary) to 18 (10010 binary). IV(2) shall correspond to the least significant bit of the frame number (ETSI EN 300 392-2 [2], clause 9.3.4);
- 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 (ETSI EN 300 392-2 [2], clause 9.3.7);
- the next 15 bits IV(13) to IV(27) shall correspond to the 15 least significant bits of an extension that numbers the hyper-frames. These can take all values from 0 to 32 767. IV(13) shall correspond to the least significant bit of the hyper-frame numbering extension (ETSI EN 300 392-2 [2], clause 9.3.8); and
- the final bit, IV(28), shall be used to indicate the direction of transmission and shall be given the value 0 for downlink transmissions, and shall be given the value 1 for uplink transmissions.

6.3.2.2 Cipher Key for algorithms in TEA set A

The CK shall not be used directly at the air interface for encryption but shall be modified by the Colour Code (CC), LA-id and Carrier Number (CN) using algorithm TB5 (see Figure 6.2). This shall randomize the input to the encryption algorithm amongst the carriers of a single cell and between cells in a location area.

The ciphering process shall be as shown in Figure 6.2. A cipher key shall be used in conjunction with a KSG to generate a key stream for encryption and decryption of information at the MAC layer. It can be considered a binary vector of 80 bits, labelled ECK(0) … ECK(79). The cipher key used for encryption and decryption of the uplink may be different from the cipher key used for encryption and decryption of the downlink, as described in clause 6.5.



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

Figure 6.2: Speech and control information encryption using a KSG from TEA set A

6.3.2.3 Initial Value (IV) for algorithms in TEA set B

The 80 bit 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 (ETSI EN 300 392-2 [2], clause 9.3.5);

- the next five bits IV(2) to IV(6) shall correspond to the frame number, and shall take values from 1 (00001 binary) to 18 (10010 binary). IV(2) shall correspond to the least significant bit of the frame number (ETSI EN 300 392-2 [2], clause 9.3.4);

- 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 (ETSI EN 300 392-2 [2], clause 9.3.7);

- the next 16 bits IV(13) to IV(28) shall correspond to the 16 bits of an extension that numbers the hyper-frames. These can take all values from 0 to 65 535. IV(13) shall correspond to the least significant bit of the hyper-frame numbering extension (ETSI EN 300 392-2 [2], clause 9.3.8);

- IV(29) shall be used to indicate the direction of transmission and shall be given the value 0 for downlink transmissions, and shall be given the value 1 for uplink transmissions;

- IV(30) shall be used to indicate the subslot used for transmission on the uplink, and shall take the value of 0 for the first half slot in a timeslot and 1 for the second half slot in a timeslot; and shall take the value of 0 on the downlink;

- IV(31) to IV(42) shall correspond to the value of the Carrier Number (CN) relating to the carrier of the BS that is providing service to the MS, where IV(31) shall correspond to the least significant bit of CN (ETSI EN 300 392-2 [2], clause 18.5.2c);

- IV(43) to IV(56) shall correspond to the value of the Location Area containing the BS that is providing service to the MS, where IV(43) shall correspond to the least significant bit of LA (ETSI EN 300 392-2 [2], clause 18.5.9);

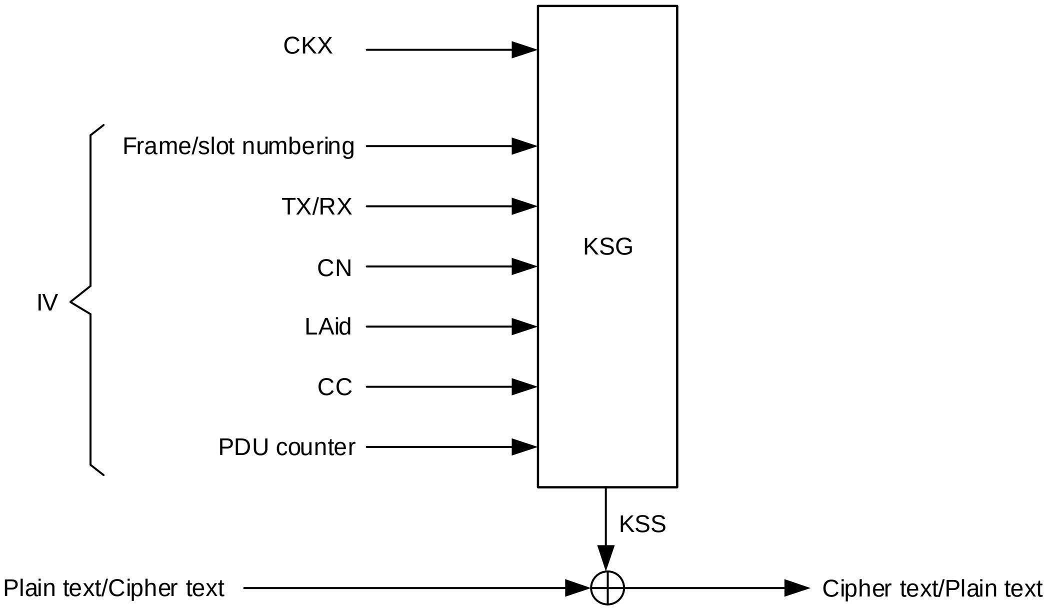
- IV(57) to IV(62) shall correspond to the colour code (CC) utilized by the BS, where IV(57) shall correspond to the least significant bit of CC. Colour code is broadcast in SYNC PDU (ETSI EN 300 392-2 [2], clause 21.4.4.2) or SYNC-DA PDU (ETSI EN 300 392-2 [2], clause 21.4.4.2a);

- IV(63) to IV(70) shall correspond to the value of a PDU counter that is implemented on control channels when PDU association takes place as described in clause 6.4.2, where IV(63) shall correspond to the least significant bit of the PDU counter, and shall be set to zero for all cases where PDU association does not take place on control channels; and shall be set to zero on all Traffic CHannels (TCH);
- IV(71) to IV(79) shall be set to zero for this version of the present document.

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

6.3.2.4 Cipher Key for algorithms in TEA set B

The cipher key shall be input directly to the KSG without modification, as shown in Figure 6.2a below.



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

Figure 6.2a: Speech and control information encryption using a KSG from TEA set B

6.4 Encryption mechanism

6.4.0 General

The KSS bits shall be modulo 2 added (XORed) with plain text bits in data, speech and control channels to obtain encrypted cipher text bits, with the exception of the MAC header bits and fill bits. KSS(0) shall be XORed with the first transmitted bit of the first TM-SDU, and so on. The exceptions to this procedure occur when the address in the MAC header is encrypted, as described in clause 6.7.1.2a, and/or where the MAC header includes channel allocation element data, as described in clause 6.7.1.2. In these cases, KSS(0) shall be XORed with the first bit of the MAC address or the first bit of the channel allocation element.

6.4.1 Allocation of KSS to logical channels

The set of logical channels in TETRA is defined by the modulation applied. TETRA supports 3 modulation schemes each with a specific set of logical channels as shown in Table 6.3.

Table 6.3: Logical Channels per modulation type

Modulation	Logical channel
π/4-DQPSK	TCH/2.4
	TCH/4.8
	TCH/7.2
	STCH
	TCH/S (full)
	SCH/F
	SCH/HU
	SCH/HD
	BSCH
	BNCH
π/8-D8PSK	SCH-P8/HU
	SCH-P8/HD
	SCH-P8/F
QAM	SCH-Q/RA
	SCH-Q/HU25
	SCH-Q/HU50
	SCH-Q/HU100
	SCH-Q/HU150
	SCH-Q/U25
	SCH-Q/U50
	SCH-Q/U100
	SCH-Q/U150
	SCH-Q/D25
	SCH-Q/D50
	SCH-Q/D100
	SCH-Q/D150
NOTE 1: TETRA speech is only supported by π/4-DQPSK modulated channels. NOTE 2: QAM and π/8-D8PSK modulations are only used for packet data and control (no circuit mode data or speech).	

KSS shall be allocated to TETRA logical channels as shown in Table 6.4. Any unused bits shall be discarded. The same KSS allocation shall apply to KSGs from TEA set A and to KSGs from TEA set B.

Table 6.4: KSS allocation to logical channels

Logical channel	Maximum number of bits in logical channel	KSS allocation
TCH/2.4	144	KSS(124 to 267)
TCH/4.8	288	KSS(124 to 411)
TCH/7.2	432	KSS(0 to 431)
STCH+TCH/2.4	124 + 144	KSS(0 to 123) + KSS(124 to 267)
STCH+TCH/4.8	124 + 288	KSS(0 to 123) + KSS(124 to 411)
STCH+TCH/7.2	124 + 432	KSS(0 to 123) + KSS(0 to 431) (see note 1)
TCH/S (full)	274	KSS(0 to 273)
STCH+TCH/S	124 + 137	KSS(0 to 123) + KSS(216 to 352)
SCH/F	268	KSS(0 to 267)
SCH/HU (see note 2)	92	KSS(0 to 91)
SCH/HD+SCH/HD	124 + 124	KSS(0 to 123) + KSS(216 to 339)
STCH+STCH	124 + 124	KSS(0 to 123) + KSS(216 to 339)
BSCH+SCH/HD	60 + 124	clear +KSS(216 to 339)
SCH/HD+BNCH	124 + 124	KSS(0 to 123) + clear
SCH-P8/HU (see note 2)	148	KSS(0 to 147)
SCH-P8/HD+SCH-P8/HD	196 + 196	KSS(0 to 195) + KSS(216 to 411)
SCH-P8/F	412	KSS(0 to 411)
SCH-Q/RA (first half slot)	65	KSS(0 to 64)
SCH-Q/RA (second half slot)	65	KSS(65 to 129)
SCH-Q/HU25 (see note 2)	440	KSS(0 to 439)
SCH-Q/HU50 (see note 2)	944	KSS(0 to 943)
SCH-Q/HU100 (see note 2)	1 952	KSS(0 to 1 951)
SCH-Q/HU150 (see note 2)	2 960	KSS(0 to 2 959)
SCH-Q/U25	1 184	KSS(0 to 1 183)
SCH-Q/U50	2 432	KSS(0 to 2 431)
SCH-Q/U100	4 928	KSS(0 to 4 927)
SCH-Q/U150	7 424	KSS(0 to 7 423)
SCH-Q/D25	1 208	KSS(0 to 1 207)
SCH-Q/D50	2 624	KSS(0 to 2 623)
SCH-Q/D100	5 456	KSS(0 to 5 455)
SCH-Q/D150	8 288	KSS(0 to 8 287)
NOTE 1: Where TCH/7.2 is stolen the first 216 encrypted bits of TCH/7.2 are not transmitted. NOTE 2: The same KSS allocation applies whether the first or second half slot is selected for transmission.		

NOTE 1: KSS repeat is possible only for multi-slot interleaved circuit mode data when both half slots in a single slot are stolen.

NOTE 2: The AACH, BSCH, BNCH, SICH-Q/U, SICH-Q/D, AACH-Q/D and BNCH-Q/D logical channels are not encrypted.

NOTE 3: The numbers of bits and the KSS allocations indicated in Table 6.4 for QAM channels are those required for uncoded logical channels using 64-QAM (except for SCH-Q/RA which always uses 4-QAM). ETSI EN 300 392-2 [2], clause 23.2.1 lists the sizes of all SCH-Q logical channels. The starting points indicated in Table 6.4 for the KSS allocations apply to uncoded and coded logical channels. Coded logical channels require fewer KSS bits than uncoded logical channels. Also, 4-QAM and 16-QAM logical channels require fewer KSS bits than 64-QAM logical channels using the same coding rate.

6.4.2 Allocation of KSS to logical channels

6.4.2.1 General

This clause describes the allocation of KSS to logical channels, including where PDU association takes place. On the control channel, the MAC may perform PDU association, where more than one PDU may be transmitted within one slot. These PDUs may be addressed to different identities and may use different cipher keys. The MAC headers themselves may be of varying lengths.

6.4.2.2 KSS allocation on phase modulation channels

This clause applies whether an algorithm from TEA set A or an algorithm from TEA set B is in use.

On phase modulation channels the KSS shall be restarted at the commencement of each SDU (see Figure 6.3, Figure 6.4 and Figure 6.5).

Where a KSG from TEA set B is in use and PDU association takes place, the PDU counter of the IV shall be set to zero for the first transmitted MAC PDU in a timeslot or subslot, and shall increment for each subsequent MAC PDU in the same timeslot or subslot.

Where a KSG from TEA set B is in use with a cipher key of CCKX or SCKX, the first 34 bits of KSS, KSS(0) to KSS(33), shall be reserved to encrypt the address contained in the MAC header, which may be one of event label, SSI, USSI, SMI, SSI+Usage Marker or SSI/SMI+Event Label. KSS(0) to KSS(33) shall be reserved for this purpose whether or not an address is present in the MAC header, and whether or not the MAE mechanism is in use. See Figures 6.3a, 6.4a and 6.5a and clause 6.7.1.2a.

NOTE 1: KSS(0) to KSS(33) are reserved when a KSG from TEA set B is in use with CCKX or SCKX, even if the ESI mechanism using the TA61 algorithm are in use (see clause 4.2.6).

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

Figure 6.3 shows the allocation of KSS bits to MAC PDUs where there is one PDU sent in a full slot for all cases except where a KSG from TEA set B is used for encryption with CCKX or SCKX.

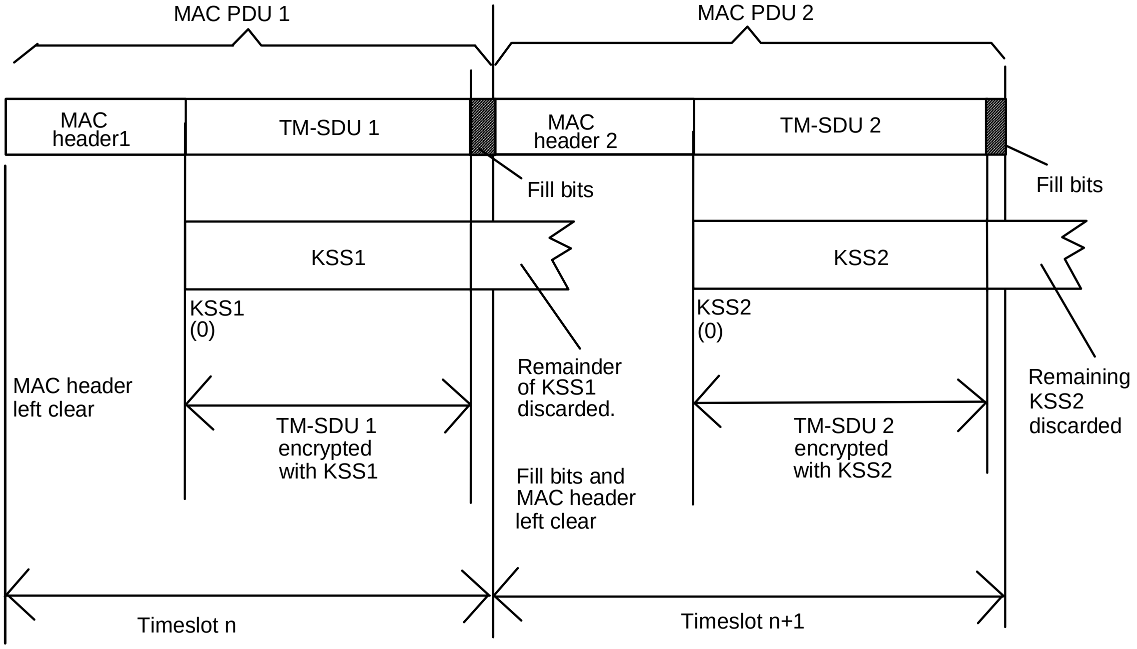
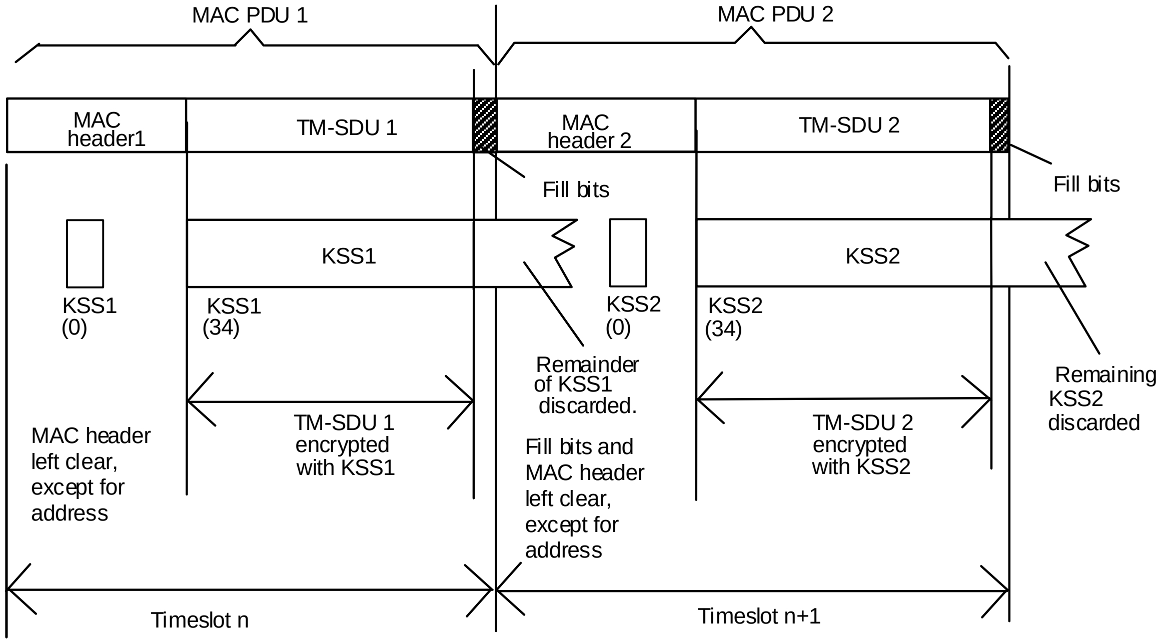


Figure 6.3: Allocation of KSS to encrypt MAC PDUs (general case)

Figure 6.3a shows the allocation of KSS bits to MAC PDUs where there is one PDU sent in a full slot where a KSG from TEA set B is in use, and the cipher key in use is CCKX or SCKX.

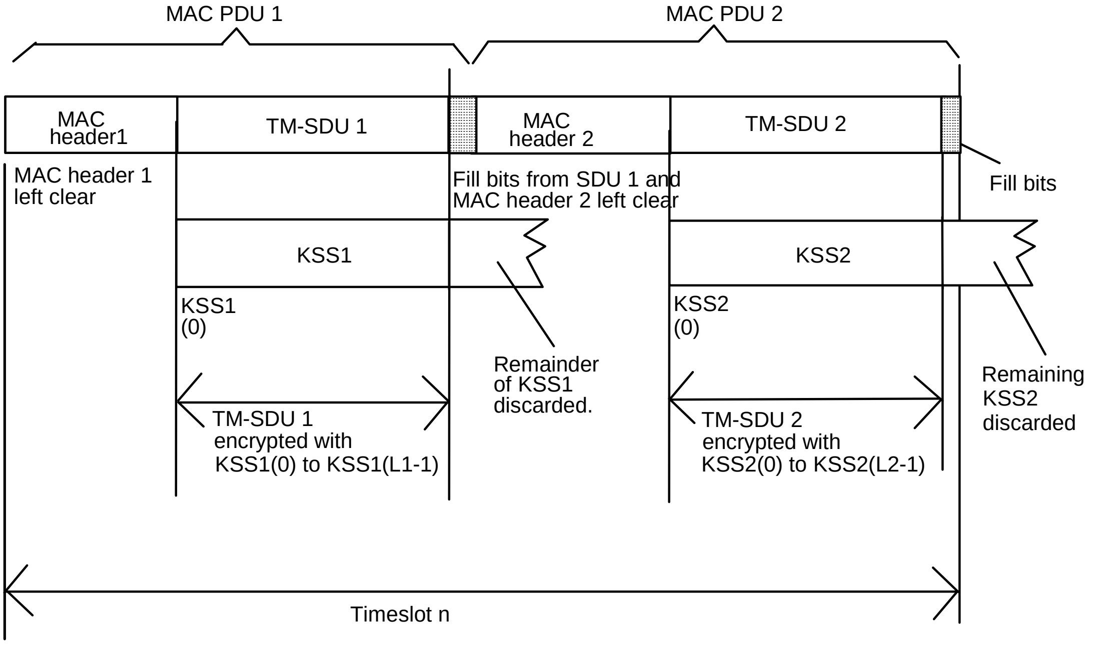

MAC PDU 1
MAC PDU 2
MAC header1
TM-SDU 1
MAC header 2
TM-SDU 2
Fill bits
Fill bits
KSS1
KSS2
KSS1 (0)
KSS1 (34)
KSS2 (0)
KSS2 (34)
Remainder of KSS1 discarded.
Remaining KSS2 discarded
MAC header left clear, except for address
TM-SDU 1 encrypted with KSS1
Fill bits and MAC header left clear, except for address
TM-SDU 2 encrypted with KSS2
Timeslot n
Timeslot n+1

NOTE 1: KSS1(0) to KSS1(33) and KSS2(0) to KSS2(33) are reserved to encrypt the address (if any) contained in the MAC header, irrespective of the length of the address or whether an address is sent at all.

NOTE 2: KSS1(0) to KSS1(33) and KSS2(0) to KSS2(33) are discarded if the MAE mechanism is not applied, e.g. if the ESI mechanism is in use.

Figure 6.3a: Allocation of KSS to encrypt MAC PDUs where a KSG from TEA set B is in use with CCKX or SCKX

Figure 6.4 shows the allocation of KSS bits where PDU association takes place in a full slot, except where a KSG from TEA set B, and the cipher key in use is CCKX or SCKX.

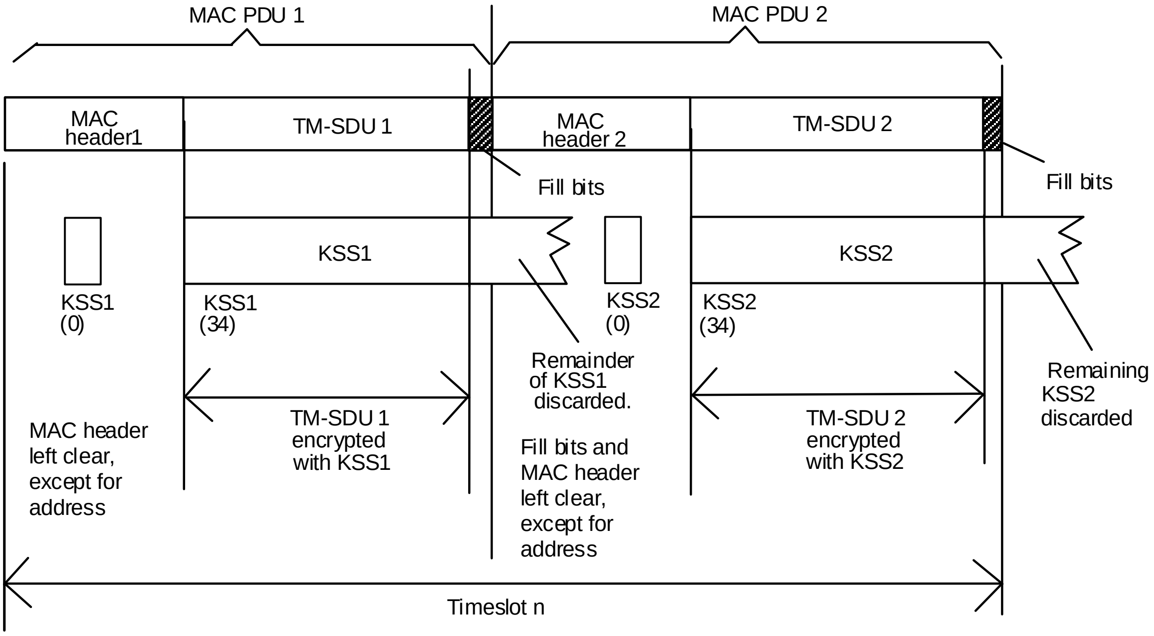

MAC PDU 1
MAC PDU 2
MAC header1
TM-SDU 1
MAC header 2
TM-SDU 2
MAC header 1 left clear
Fill bits from SDU 1 and MAC header 2 left clear
Fill bits
KSS1
KSS2
KSS1 (0)
KSS2 (0)
Remainder of KSS1 discarded.
Remaining KSS2 discarded
TM-SDU 1 encrypted with KSS1(0) to KSS1(L1-1)
TM-SDU 2 encrypted with KSS2(0)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

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

NOTE 2: Where a KSG from TEA set B is in use, the PDU counter of the IV is set to zero when generating KSS1, and incremented when generating KSS2.

Figure 6.4: Allocation of KSS to encrypt MAC PDUs with PDU Association for full slot logical channels (general case)

Figure 6.4a shows the allocation of KSS bits where PDU association takes place in a full slot where a KSG from TEA set B is used for encryption, and the cipher key in use is CCKX or SCKX.


MAC PDU 1
MAC PDU 2
MAC header1
TM-SDU 1
MAC header 2
TM-SDU 2
Fill bits
Fill bits
KSS1
KSS2
KSS1 (0)
KSS1 (34)
KSS2 (0)
KSS2 (34)
Remainder of KSS1 discarded.
Remaining KSS2 discarded
MAC header left clear, except for address
TM-SDU 1 encrypted with KSS1
Fill bits and MAC header left clear, except for address
TM-SDU 2 encrypted with KSS2
Timeslot n

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

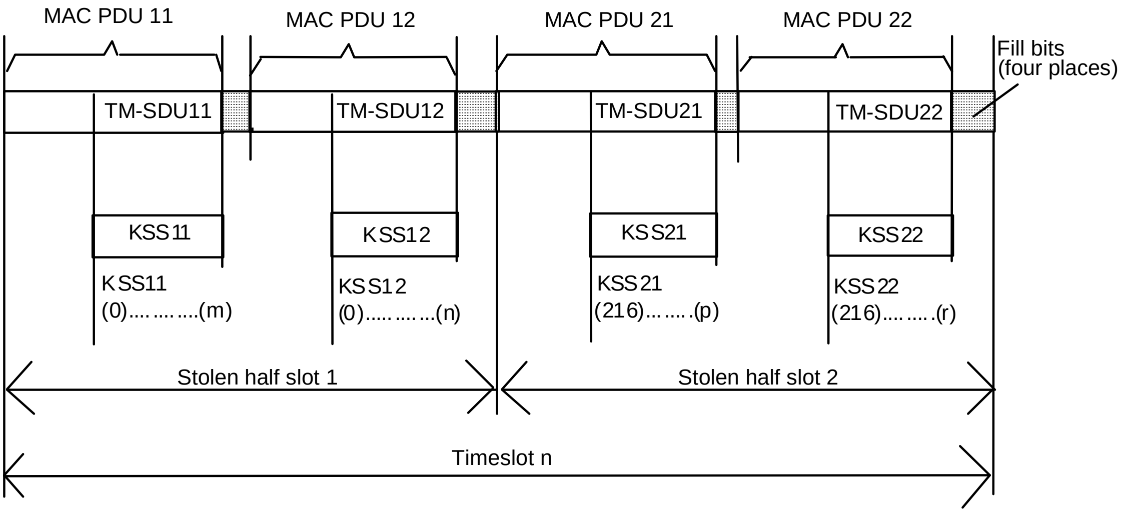
NOTE 2: The PDU counter of the IV is set to zero when generating KSS1, and incremented when generating KSS2.

NOTE 3: KSS1(0) to KSS1(33) and KSS2(0) to KSS2(33) are reserved to encrypt the address (if any) contained in the MAC header, irrespective of the length of the address or whether an address is sent at all.

NOTE 4: KSS1(0) to KSS1(33) and KSS2(0) to KSS2(33) are discarded if the MAE mechanism is not applied, e.g. if the ESI mechanism is in use.

Figure 6.4a: Allocation of KSS to encrypt MAC PDUs with PDU Association for full slot logical channels for encryption where a KSG from TEA set B is in use with CCKX or SCKX

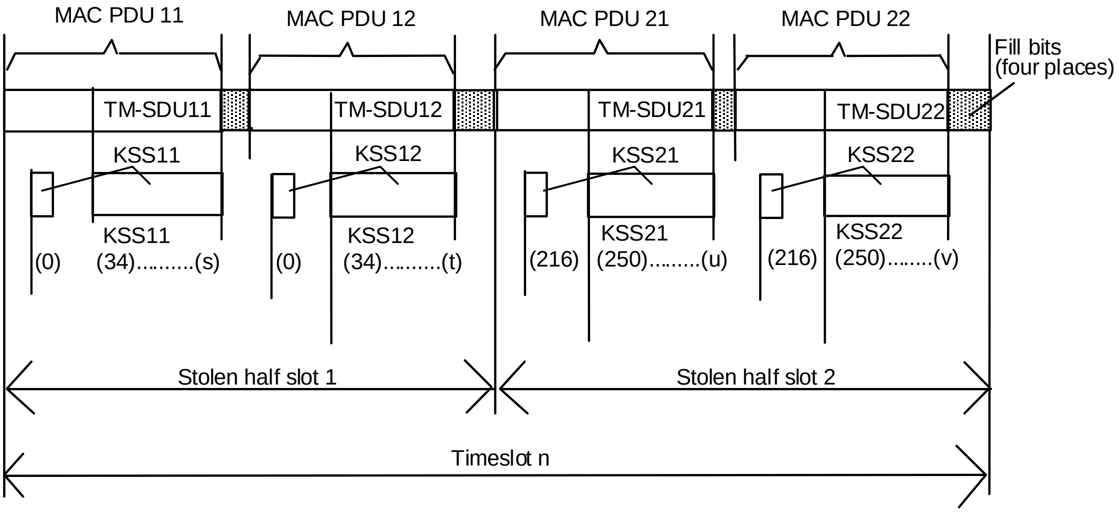
Figure 6.5 shows the allocation of KSS bits where PDU association is used in half slot logical channels, except where a KSG from TEA set B is used for encryption, and the cipher key in use is CCKX or SCKX.



NOTE 1: KSS11(m+1) onwards discarded.
NOTE 2: KSS12(n+1) onwards discarded.
NOTE 3: KSS21(0) to KSS21(215) and KSS21(p+1) onwards discarded.
NOTE 4: KSS22(0) to KSS22(215) and KSS22(r+1) onwards discarded.
NOTE 5: Where a KSG from TEA set B is in use, the PDU counter of the IV is set to zero when generating KSS11 and KSS21 and incremented when generating KSS12 and KSS22.

Figure 6.5: Allocation of KSS to encrypt MAC PDUs with PDU Association for half slot logical channels (general case)

Figure 6.5a shows the allocation of KSS bits where PDU association is used in half slot logical channels where a KSG from TEA set B is used for encryption, and the cipher key in use is CCKX or SCKX.



NOTE 1: KSS(0) to KSS(33) of KSS11 and KSS12, and KSS(216) to KSS(249) of KSS21 and KSS22 are reserved to encrypt the address (if any) sent in the MAC header, irrespective of the length of the address or whether an address is sent at all.

NOTE 2: KSS(0) to KSS(33) of KSS11 and KSS12, and KSS(216) to KSS(249) of KSS21 and KSS22 are discarded if the MAE mechanism is not applied, e.g. if the ESI mechanism is in use.

NOTE 3: KSS11(s+1) onwards discarded.

NOTE 4: KSS12(t+1) onwards discarded.

NOTE 5: KSS21(0) to KSS21(215) and KSS21(u+1) onwards discarded.

NOTE 6: KSS22(0) to KSS22(215) and KSS22(v+1) onwards discarded.

NOTE 7: The PDU counter of the IV is set to zero when generating KSS11 and KSS21 and incremented when generating KSS12 and KSS22.

Figure 6.5a: Allocation of KSS to encrypt MAC PDUs with PDU Association for half slot logical channels where a KSG from TEA set B is in use with CCKX or SCKX

NOTE 2: In Figures 6.3, 6.3a, 6.4, 6.4a, 6.5 and 6.5a, KSS bits shown for SDU encryption may also be used to encrypt the channel allocation element in the MAC header, if the "channel allocation flag" = 1. If the length of the channel allocation is N bits, the first bit of the MAC SDU is encrypted with KSS(34+N).

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

- sending more than one SDU encrypted with the same encryption key within one logical channel where a KSG from TEA set A is in use.

NOTE 3: For the sake of clarity Figures 6.4, 6.4a, 6.5 and 6.5a show only two MAC PDUs being associated within a full or half slot, but there may be more if the MAC PDUs are sufficiently small.

6.4.2.3 KSS allocation on QAM channels for algorithms in TEA set A

6.4.2.3.0 General

On QAM channels where a KSG from TEA set A is in use, two different KSS allocation schemes exist. The fixed-mapping KSS allocation scheme applies to all class 2 encryption (using the SCK), to class 3 encryption using the CCK and to class 3 encryption using a GCK. The offset-mapping KSS allocation scheme applies to all class 3 encryption using a DCK.

6.4.2.3.1 Fixed mapping

This method of allocating KSS to QAM channels shall apply to all encryption using an SCK, a CCK or a GCK. Each fixed-mapped KSS used in a logical channel shall be mapped so that a defined starting bit from the KSS corresponds to the first bit of the timeslot or subslot (e.g. KSS(0) or KSS(65) may be mapped to the first bit of the first MAC header), and successive KSS bits shall be mapped to successive bits of the logical channel, encrypted or not. Where a PDU bit does not require encryption, the corresponding KSS bit shall be discarded. Where a PDU bit does require encryption, the corresponding KSS bit shall be XORed with the PDU bit. Where different PDUs use different cipher keys, the KSS for each different cipher key shall be mapped to the logical channel in the same way. This is illustrated in Figure 6.6 and Figure 6.7 (Figure 6.7 shows three MAC PDUs being associated within a timeslot, but there may be more, depending on the sizes of the PDUs and the capacity of the timeslot). The starting bit numbers for the mapping to each type of QAM logical channel are defined in Table 6.4.

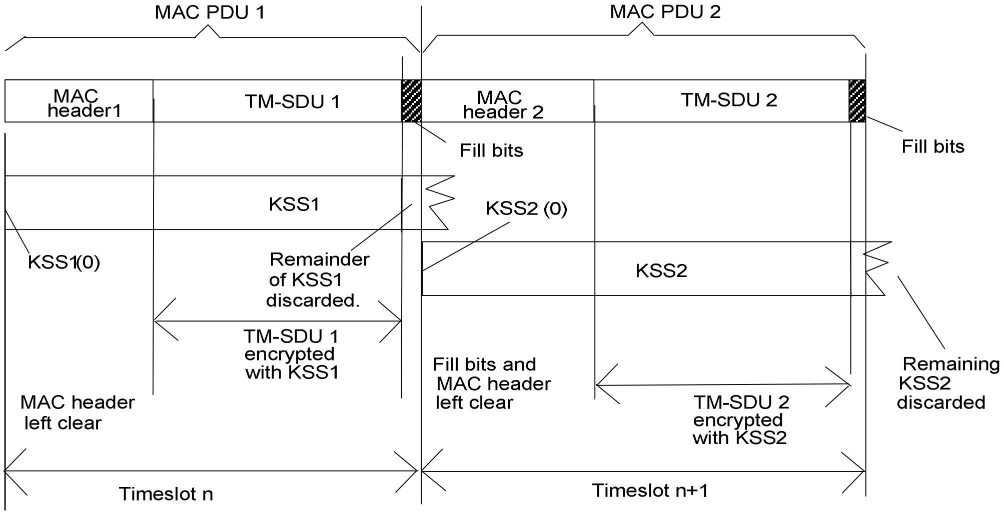
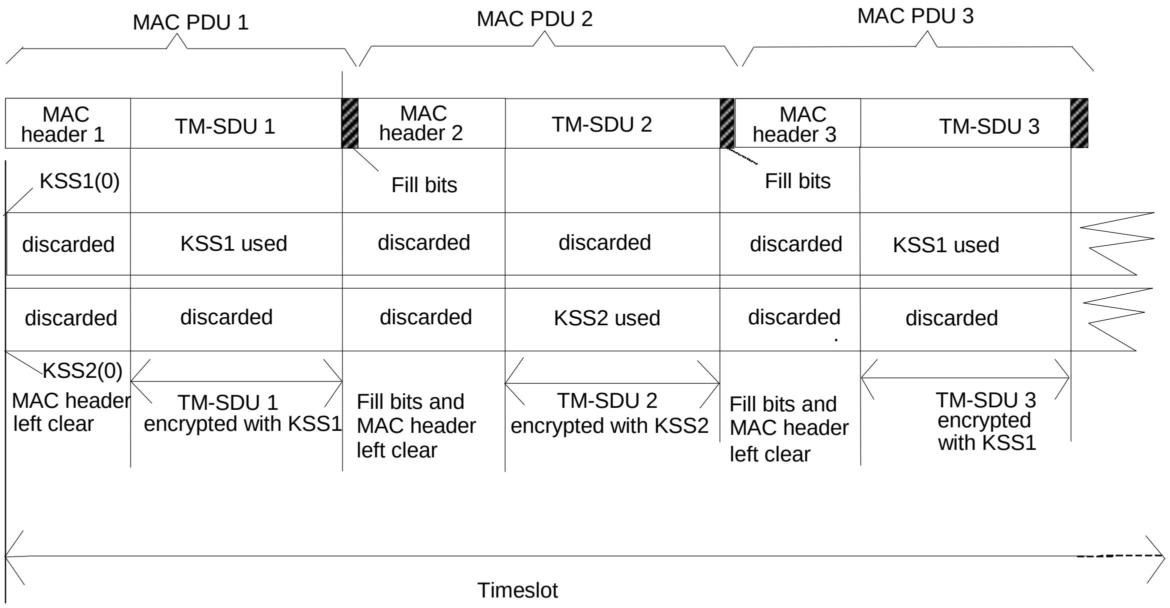


Figure 6.6: Fixed-mapped allocation of KSS to encrypt QAM MAC PDUs



NOTE: In this example, TM-SDU 1 and TM-SDU 3 use the same cipher key but TM-SDU 2 uses a different cipher key.

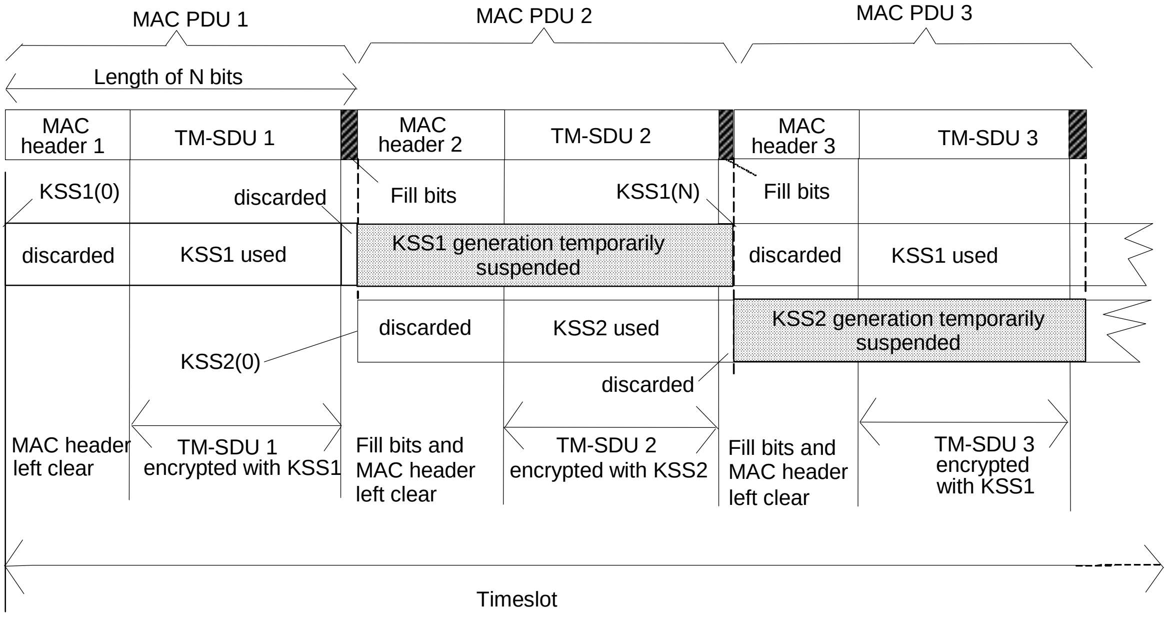
Figure 6.7: Fixed-mapped allocation of KSS to encrypt QAM MAC PDUs with PDU association for full slot logical channels

6.4.2.3.2 Offset mapping

This method of allocating KSS to QAM channels shall apply to all encryption using a DCK. Each offset-mapped KSS used in a logical channel shall be mapped so that a defined starting bit from the KSS corresponds to the first bit of the first MAC-PDU to be encrypted with that KSS (e.g. KSS(0) or KSS(65) may be mapped to the first bit of the first MAC header), and successive KSS bits shall be mapped to successive bits of PDUs encrypted using the same DCK in the current timeslot or subslot.

Where a PDU bit does not require encryption, the corresponding KSS bit shall be discarded. Where a PDU bit does require encryption, the corresponding KSS bit shall be XORed with the PDU bit. Where further PDUs using the same DCK (i.e. using the same address) are associated in the same timeslot or subslot, the KSS shall be temporarily suspended following the last bit of the previous PDU (including any fill bits) encrypted with the same DCK but continued from the first bit of the next PDU encrypted with the same DCK. Where associated PDUs use different DCKs (i.e. using different addresses), the KSS for each different DCK shall be mapped to the logical channel in the same way (starting from the first bit of the first MAC header using that address). This is illustrated in Figure 6.8 (Figure 6.8 shows three MAC PDUs being associated within a timeslot, but there may be more, depending on the sizes of the PDUs and the capacity of the timeslot).

Fill bits shall not be encrypted.



NOTE: In this example, TM-SDU 1 and TM-SDU 3 use the same DCK but TM-SDU 2 uses a different DCK.

Figure 6.8: Offset-mapped allocation of DCK-derived KSS to encrypt QAM MAC PDUs with PDU association for full slot logical channels

6.4.2.4 KSS allocation on QAM channels for algorithms in TEA set B

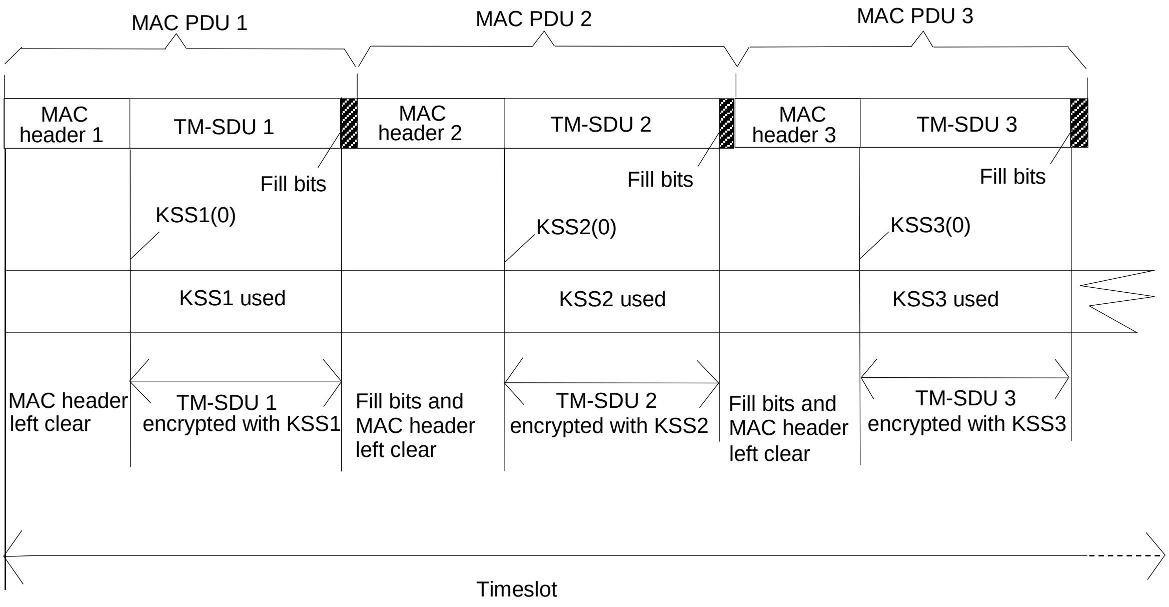
On QAM channels where a KSG from TEA set B is in use, the KSG shall be restarted for each MAC PDU transmitted in the same full slot or subslot. This applies for any cipher key: DCKX, CCKX, GCKX or SCKX, and applies whether the destination addresses of the MAC PDUs are the same as or different to each other.

The KSS for the first transmitted MAC PDU in a timeslot or subslot shall be generated with the PDU counter of the IV set to zero. The PDU counter shall be incremented for each subsequent transmitted MAC PDU, i.e. the the PDU counter value shall be set to 1 for the second transmitted MAC PDU, to 2 for the third transmitted MAC PDU and so on.

Where the cipher key in use is DCKX or MGCKX, KSS(0) shall be allocated to the first transmitted bit of the TM-SDU, unless a channel allocation element is included in the MAC header, in which case KSS(0) is used to encrypt the first transmitted bit of the channel allocation element.

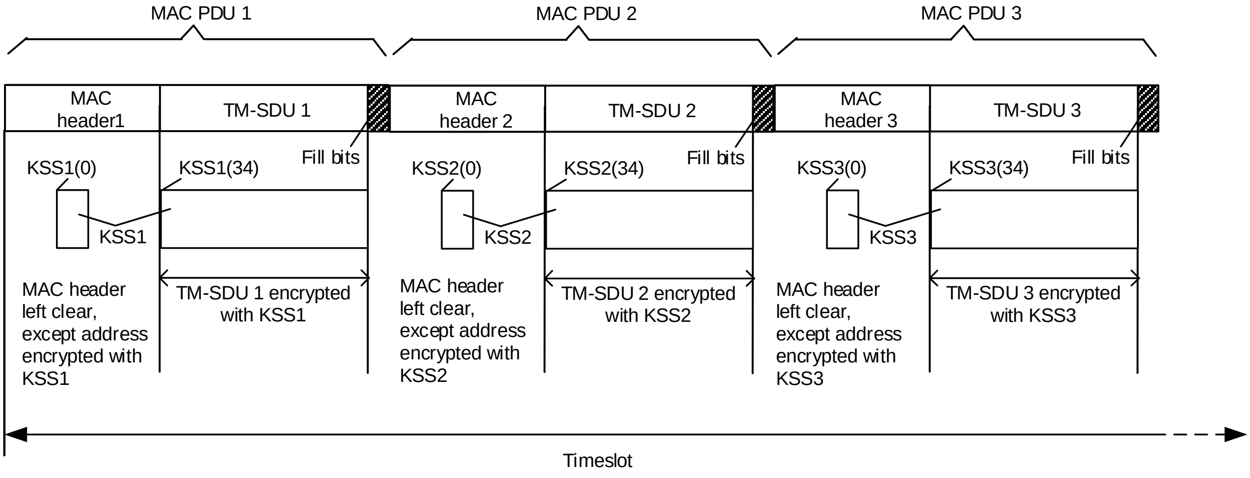
Where the cipher key in use is CCKX or SCKX, KSS(0) to KSS(33) shall be reserved to encrypt the address sent in the MAC header. The reservation of KSS(0) to KSS(33) shall occur whether the MAE mechanism is in use or not (e.g. if the ESI mechanism specified in clause 4.2.6 is in use), and whether there is an address present in the MAC header or not. KSS(34) shall be used to encrypt the first transmitted bit of the TM-SDU, or the first transmitted bit of the channel allocation element if a channel allocation element is sent in the PDU.

This is illustrated in Figures 6.8a and 6.8b below.



NOTE: PDU counter set to zero to generate KSS1, set to 1 to generate KSS2 and set to 2 to generate KSS3.

Figure 6.8a: Allocation of KSS to MAC PDUs for KSGs in TEA set B where DCKX or MGCKX is in use


MAC PDU 1
MAC PDU 2
MAC PDU 3
MAC header1
TM-SDU 1
MAC header 2
TM-SDU 2
MAC header 3
TM-SDU 3
Fill bits
KSS1(0)
KSS1(34)
KSS1
KSS2(0)
KSS2(34)
KSS2
KSS3(0)
KSS3(34)
KSS3
MAC header left clear, except address encrypted with KSS1
TM-SDU 1 encrypted with KSS1
MAC header left clear, except address encrypted with KSS2
TM-SDU 2 encrypted with KSS2
MAC header left clear, except address encrypted with KSS3
TM-SDU 3 encrypted with KSS3
Timeslot

NOTE 1: PDU counter set to zero to generate KSS1, set to 1 to generate KSS2 and set to 2 to generate KSS3.

NOTE 2: KSS1(0) to KSS1(33), KSS2(0) to KSS2(33) and KSS3(0) to KSS3(33) are reserved to encrypt the address (if any) contained in the MAC header, irrespective of the length of the address or whether an address is sent at all.

NOTE 3: KSS1(0) to KSS1(33), KSS2(0) to KSS2(33) and KSS3(0) to KSS3(33) are discarded if the MAE mechanism is not applied, e.g. if the ESI mechanism is in use.

Figure 6.8b: Allocation of KSS to MAC PDUs for KSGs in TEA set B for downlink encryption where CCKX or SCKX is in use

NOTE: In Figures 6.8a and 6.8b, KSS bits shown for SDU encryption (KSS(34) onwards) may be used to encrypt the channel allocation element in the MAC header, if the "channel allocation flag" = 1. If the length of the channel allocation is N bits, the first bit of the MAC SDU is encrypted with KSS(34+N).

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

This clause applies where an algorithm from TEA set A or an algorithm from TEA set B is in use.

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. Figure 6.9 shows the allocation of IV for an interleaving depth of 4.

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

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

Figure 6.9: 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 6.10.

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

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

6.4.4 Recovery of stolen frames from interleaved data

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

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

6.5 Use of cipher keys

6.5.0 General

The cipher keys and their allocation are described in clauses 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 (MAC address and channel allocation elements) are encrypted or not. In addition the header of MAC downlink PDUs includes one bit that shall indicate the least significant bit of the version of CCK/CCKX or SCK/SCKX that is in use. This indication is used to assist the MS to detect if the CCK/CCKX or SCK/SCKX has been changed if the D-CK CHANGE DEMAND PDU has been missed. It can only provide this assistance when the least significant bits of the old and new keys are different.

In cells of security class 2 the SCK/SCKX shall be used to encrypt individual addressed signalling and traffic. SCK/SCKX shall also be used with the identity encryption mechanism to conceal identities in use at the air interface within a SwMI. Only one SCK or one SCKX shall be in use within a SwMI at any one time except during key change period.

NOTE 1: A SwMI may support one SCK and one SCKX at the same time in security class 2 cells if the SwMI supports MSs that negotiate a KSG from TEA set A and MSs that support a KSG from TEA set B at the same time. In this case, the SwMI derives SCK from SCKX to enable correct operation of the ESI mechanism; see clause 4.2.6. The SCKN and SCK-VN of the SCK and the SCKX are the same, see clause 4.2.4.0b.

In cells of security class 3 the DCK or DCKX 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.

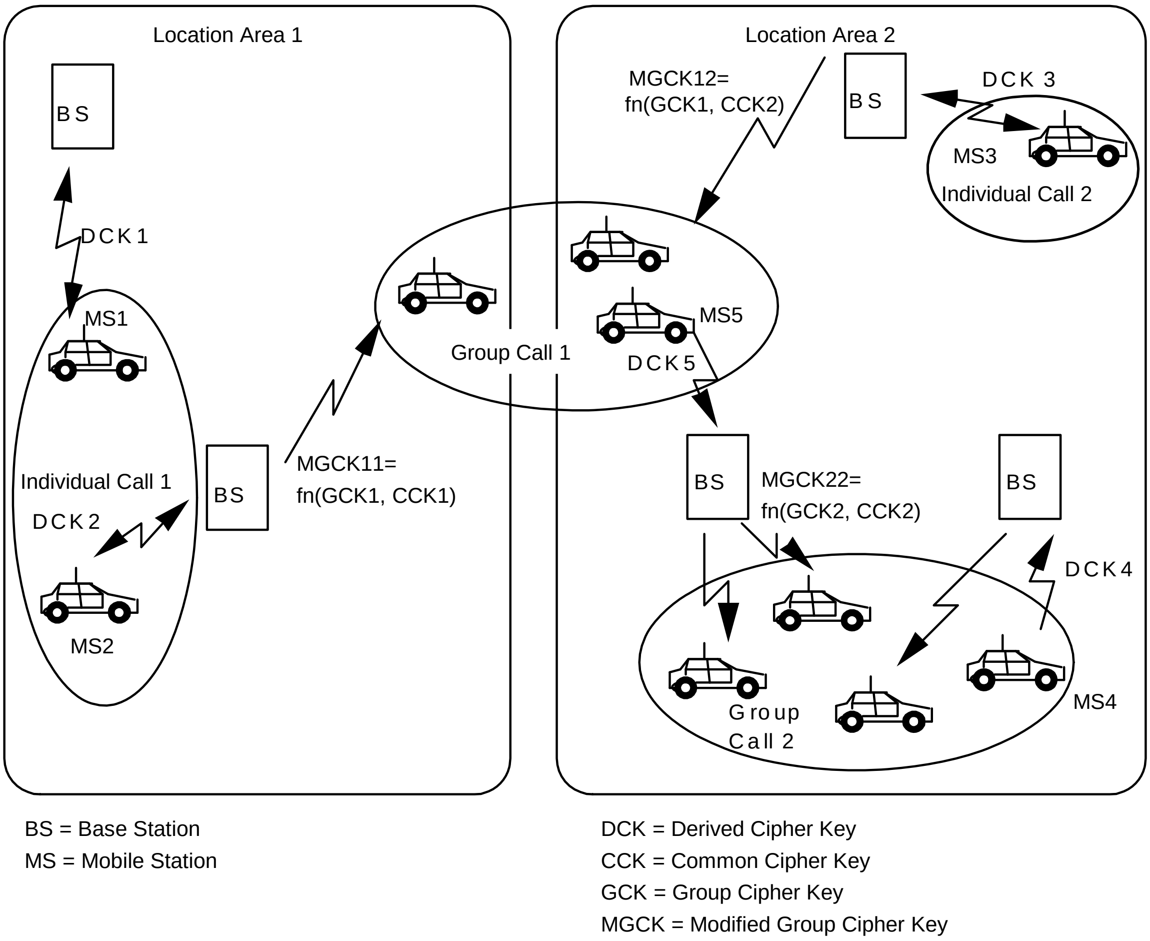
In cells of security class 3 that support group calls a GCK or GCKX may be associated with a single or multiple group addresses at any time. A group shall not be associated with more than one group cipher key (which may be either a GCK or a GCKX) identified by a GCKN, although different versions of the same GCKN, identified by GCK-VN, may be associated to one or more groups to enable key change over. The CCK shall be used as a key modifier to produce the MGCK, or the CCKX shall be used as a key modifier to GCKX, and the modified key shall be used to encrypt group addressed signalling and traffic (see clause 4.2.2). If no GCK/GCKX is assigned to a group then the CCK/CCKX shall be used to encrypt all signalling and traffic addressed to that group. Only one CCK shall be in use within a cell at any one time. Only one CCKX shall be in use within a cell at any one time.

NOTE 2: A SwMI may support one CCK and one CCKX at the same time in security class 3 cells if the SwMI supports MSs that negotiate a KSG from TEA set A and MSs that support a KSG from TEA set B at the same time. In this case, the SwMI derives CCK from CCKX to enable correct operation of the ESI mechanism; see clause 4.2.6.

NOTE 3: This rule for choice of GCK/GCKX or CCK/CCKX applies also when the SwMI is addressing signalling and traffic to a temporary address (see ETSI EN 300 392-2 [2], clause 14.5.2.2.6). The temporary address is used within a group-addressed call. The temporary address should be chosen such that all MSs to be included in the call possess the correct key (GCK/GCKX or CCK/CCKX) and have key associations that enable those MSs to use it to decrypt the signalling and traffic.

CCK or CCKX shall also be used in conjunction with the identity encryption mechanism to protect addresses used with encryption within an LA. An MS may store the CCKs or CCKXs 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 6.11.



NOTE: This figure illustrates the cipher keys in use with an encryption algorithm from TEA set A. Where the extended cipher keys are in use with algorithms from TEA set B, DCKX applies instead of DCK, CCKX applies instead of CCK, GCKX applies instead of GCK and MGCKX applies instead of MGCK.

Figure 6.11: Illustration of cipher key use in class 3 system

6.5.1 Identification of encryption state of downlink MAC PDUs

6.5.1.0 General

The encryption mode element (two bits) in the header of the downlink MAC-RESOURCE PDU shall be used for air interface encryption management and shall indicate the encryption state of each TM-SDU for each cell security class as shown in clauses 6.5.1.1 to 6.5.1.3. These bits also indicate the use of the address encryption mechanism.

6.5.1.1 Class 1 cells

In a cell supporting only class 1only the values and interpretations given in Table 6.5 shall apply.

Table 6.5: Encryption mode element in class 1 cell contents

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

6.5.1.2 Class 2 cells

In a class 2 cell only the values and interpretations given in Table 6.6 shall apply.

Table 6.6: Encryption mode element in class 2 cell contents

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

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

If the cell supports an algorithm from TEA set A and an algorithm from TEA set B at the same time, the SCKN and SCK-VN of the SCK and the SCKX in use shall be the same.

NOTE: During a key changeover there may be a period when keys are different on different cells.

6.5.1.3 Class 3 cells

In a class 3 cell only the values and interpretations given in Table 6.7 shall apply.

Table 6.7: Encryption mode element in class 3 cell contents

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

In class 3 cells every cell in an LA shall use the same CCK/CCKX and it shall be identified by a common CCK-id in all the cells of the LA. The SwMI may also provide a CCK/CCKX that it is applicable in more than one LA. If so the CCK and/or CCKX shall be identified by a common CCK-id in all these applicable LAs. CCK/CCKX change shall therefore be synchronized across all cells in an LA, and across all LAs in which SwMI tells that the same CCK is applicable. The CCK/CCKX shall be identified by a CCK-id which shall be sent to an MS together with the CCK/CCKX. The CCK-id can be selected independently for each location area by the SwMI. When a PDU is encrypted, the least significant bit of the encryption mode element in the MAC header shall be equal to the least significant bit of the CCK-id for the CCK/CCKX in use.

If the cell supports an algorithm from TEA set A and an algorithm from TEA set B at the same time, the CCK-id of the CCK and the CCKX in use shall be the same.

NOTE 1: During a key changeover there may be a period when keys are different on different cells of applicable LAs.

NOTE 2: When CCK/CCKX is changed the SwMI has to ensure that the MS can recognize a CCK/CCKX change in the encryption mode element.

6.5.2 Identification of encryption state of uplink MAC PDUs

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

This bit shall take one of the following values:

- 0 = Encryption off;
- 1 = Encryption on.

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

The encryption mode element shall also indicate the use of the encrypted short identity mechanism described in clause 4.2.6 for cells of class 2 and class 3.

6.6 Mobility procedures

6.6.1 General requirements

6.6.1.0 Common requirements

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

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

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

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

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

6.6.1.1 Additional requirements for class 3 systems

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

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

6.6.2 Protocol description

6.6.2.0 General

If the SwMI supports GCK/GCKX operation the SwMI shall indicate this using the "GCK Supported" field, described in clause A.8.29a, in the Extended Service Broadcast information element, described in ETSI EN 300 392-2 [2]. This field shall be used to indicate to the MS when GCKs/GCKXs are in use or not in use by the cell.

6.6.2.1 Negotiation of ciphering parameters

6.6.2.1.0 General

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 ciphering parameters negotiation to allow the MS to establish the security information advised in the cell broadcast.

ETSI EN 300 392-2 [2] defines the presence of the "ciphering parameters" information element in the D-LOCATION UPDATE COMMAND, D-LOCATION UPDATE REJECT and U-LOCATION UPDATE DEMAND PDUs. The use of the parameters contained in this information element is described in the present document.

The "ciphering parameters" information element shall be used to negotiate SCKN and KSG in class 2 cells, and KSG in class 3 cells using the "ciphering parameters" information element defined in Table A.46.

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

NOTE: When registering for SC3 operation, the "ciphering parameters" information element is also used by the MS to indicate its support for TM-SCK/SCKX OTAR, SDMO and DM-SCK/SCKX OTAR, and GCK/GCKX encryption/OTAR (see clause 6.2.0.2).

6.6.2.1.1 Class 1 cells

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

6.6.2.1.2 Class 2 cells

"Cipher control" shall always be set to true and the "ciphering parameters" information element shall be provided.

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 ETSI EN 300 392-2 [2], clause 16. If the parameters are unacceptable the SwMI shall reject the registration and shall indicate the preferred parameters in the D-LOCATION UPDATE REJECT PDU.

The MS should store the KSG number that it successfully negotiates with the SwMI, and should propose that same KSG first in future registrations with that SwMI. If the SwMI requires a different KSG to be used to that proposed by the MS, the MS shall delete any stored DCK/DCKX, CCK/CCKX, TM-SCK/SCKX and GSKO/GSKOX that were previously used with that SwMI. If the MS last negotiated a KSG in TEA set B with the SwMI, the MS should also store an indication of which identity encryption mechanism, ESI or MAE, was negotiated to enable encrypted registration to take place.

6.6.2.1.3 Class 3 cells

"Cipher control" shall always be set to true and the "ciphering parameters" information element shall be provided.

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 ETSI EN 300 392-2 [2], clause 16. If the parameters are unacceptable the SwMI shall reject the registration and shall indicate the preferred parameters in the D-LOCATION UPDATE REJECT PDU.

The MS should store the KSG number that it successfully negotiates with the SwMI, and should propose that same KSG first in future registrations with that SwMI. If the SwMI requires a different KSG to be used to that proposed by the MS, the MS shall delete any stored DCK/DCKX, CCK/CCKX, TM-SCK/SCKX and GSKO/GSKOX that were previously used with that SwMI. If the MS last negotiated a KSG in TEA set B with the SwMI, the MS should also store an indication of which identity encryption mechanism, ESI or MAE, was negotiated to enable encrypted registration to take place.

6.6.2.2 Initial and undeclared cell re-selection

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

In cells of security class 2 the MS may, if required, register and authenticate to the new cell. For initial cell selection in the home network (ITSI-attach at power on or on returning home following migration to a visited network), the MS may only apply AI encryption if it possesses the SCK or SCKX with the SCKN broadcast by the SwMI. In this case, it shall use the same KSG that was last negotiated with the SwMI, and if a KSG from TEA set B was in use, the same identity encryption mechanism (ESI or MAE) that was last negotiated with the SwMI.

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

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

For initial cell selection in the home network (ITSI-attach at power on or on returning home following migration to a visited network), the MS may only apply AI encryption if the SwMI indicates it supports "DCK retrieval during initial cell selection" (DCK retrieval), shown in Table A.104, and the MS possesses a valid DCK or DCKX and a valid CCK or CCKX for the LA of the cell. A valid DCK or DCKX is defined as the DCK or DCKX that was last derived between the MS and the home SwMI. If the MS applies AI encryption to the ITSI-attach, it shall use the same KSG that was last negotiated with the SwMI, and if a KSG from TEA set B was in use, the same identity encryption mechanism (ESI or MAE) that was last negotiated with the SwMI.

For initial cell selection (power on or migration) in a visited network, the MS shall assume that the DCK or DCKX generated in the previous network is no longer valid. Therefore, the MS shall not apply AI encryption regardless of the indication by the SwMI to support "DCK retrieval during initial cell selection" (DCK retrieval), shown in Table A.104.

When the MS has successfully invoked initial cell selection with the SwMI but suffers radio link failure, the MS may use "roaming location updating" when the radio link is re-established, in which case the MS may only apply AI encryption if the SwMI indicates it supports "DCK retrieval during cell re-selection" (DCK retrieval), shown in Table A.104, and the MS possesses a valid DCK or DCKX and a valid CCK or CCKX for the LA of the cell. A valid DCK or DCKX is defined as the DCK or DCKX that was last derived between the MS and the SwMI.

When the SwMI supports DCK retrieval during cell re-selection, if the MS possesses a valid CCK or CCKX for the LA of the new cell the MS shall not use U-OTAR PREPARE and may apply AI encryption to location update signalling on the new cell.

When the SwMI supports DCK retrieval during cell re-selection and the MS does not possess a valid CCK or CCKX for the LA of the new cell, the MS shall request the CCK or CCKX of the new cell using U-OTAR PREPARE before selection of the new cell, and may apply AI encryption to location update signalling on the new cell.

If the SwMI does not support DCK retrieval during cell re-selection, and if the MS knows the preferred neighbour cell, the MS may use the U-OTAR PREPARE PDU indicating the LA of the new cell where the PDU is sent on the MCCH and shall start timer T372. On receipt of U-OTAR PREPARE, the SwMI shall forward the DCK or DCKX belonging to the MS to the cells belonging to the LA (DCK forwarding), if possible. The MS shall reset timer T372 on receipt of D-OTAR NEWCELL or D-OTAR NEWCELL-X. Following this, the MS may apply AI encryption to location update signalling on the new cell if the DCK forwarding was successful and if the MS possesses a valid CCK or CCKX for the LA of the new cell. This procedure is shown in Figure 6.12 where the LA-id of the new cell is known to the MS. The MS may request the CCK or CCKX of the new cell using U-OTAR PREPARE if it does not already have it.

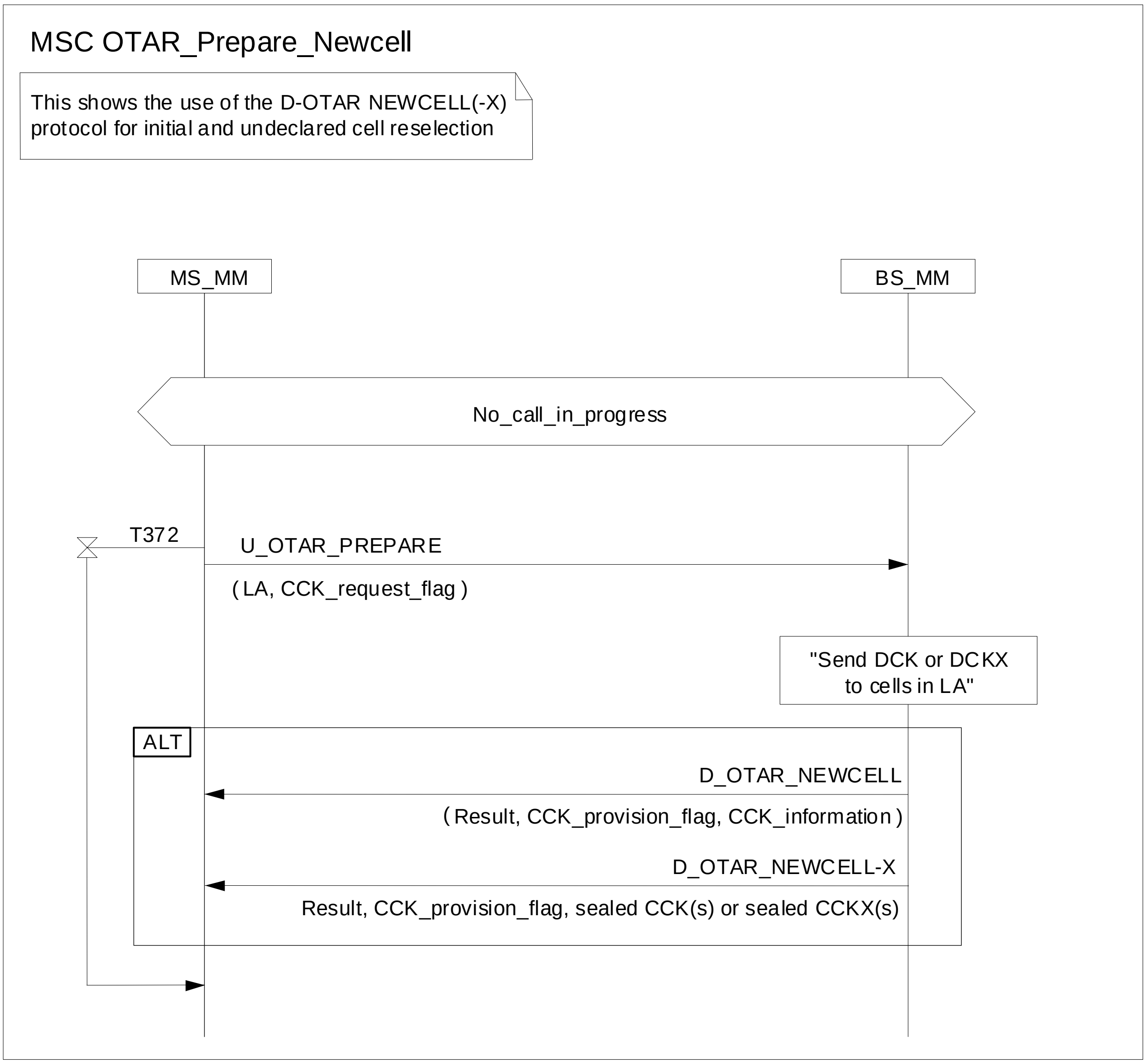

MSC OTAR_Prepare_Newcell
This shows the use of the D-OTAR NEWCELL(-X) protocol for initial and undeclared cell reselection
MS_MM
BS_MM
No_call_in_progress
T372
U_OTAR_PREPARE
(LA, CCK_request_flag)
"Send DCK or DCKX to cells in LA"
ALT
D_OTAR_NEWCELL
(Result, CCK_provision_flag, CCK_information)
D_OTAR_NEWCELL-X
Result, CCK_provision_flag, sealed CCK(s) or sealed CCKX(s)

Figure 6.12: Use of U-OTAR PREPARE and D-OTAR NEWCELL(-X) protocol

If the MS does not know a preferred neighbour cell, it cannot indicate the preferred neighbour cell to the SwMI and therefore the SwMI cannot forward the DCK or DCKX to the new cell. On successful completion of cell re-selection, and if forwarding of the DCK or DCKX failed or was not possible (due to radio link failure), the MS may only apply AI encryption to location updating if the SwMI indicates it supports "DCK retrieval during cell re-selection" (referred to herein as DCK retrieval), shown in Table A.104, and the MS possesses a valid CCK or CCKX for the LA of the new cell.

6.6.2.3 Unannounced cell re-selection

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

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

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

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

When the SwMI supports DCK retrieval during cell re-selection, the MS shall not use U-OTAR PREPARE and may apply AI encryption to location update signalling on the new cell if it possesses a valid CCK or CCKX for the LA of the new cell. However, if the SwMI does not support DCK retrieval during cell re-selection, and if the MS knows the preferred neighbour cell it should indicate the LA of the new cell using the U-OTAR PREPARE PDU (which should be sent on the MCCH to avoid any potential overloading of the SACCH) and shall start timer T372. When the SwMI receives this signalling it shall forward the DCK or DCKX belonging to the MS to the cells belonging to the LA (DCK forwarding) if possible. The MS shall reset timer T372 on receipt of D-OTAR NEWCELL or D-OTAR NEWCELL-X. Following this, the MS may apply AI encryption to location update signalling on the new cell if the DCK forwarding was successful and it possesses a valid CCK or CCKX for the LA of the new cell.

If the MS does not know a preferred neighbour cell it cannot indicate the preferred neighbour cell to the SwMI and therefore the SwMI cannot forward the DCK or DCKX to the new cell. On successful completion of cell re-selection, the MS may only apply AI encryption if the SwMI indicates it supports "DCK retrieval during cell re-selection" (DCK retrieval), shown in Table A.104, and the MS possesses a valid CCK or CCKX for the LA of the new cell.

6.6.2.4 Announced cell re-selection type-3

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

When the SwMI supports DCK retrieval during cell re-selection, the MS shall not use U-OTAR PREPARE and may apply AI encryption to location update signalling on the new cell if it possesses a valid CCK or CCKX for the LA of the new cell. However, if the SwMI does not support DCK retrieval during cell re-selection, and if the MS knows the preferred neighbour cell it should indicate the LA of the new cell using the U-OTAR PREPARE PDU and shall start timer T372. When the SwMI receives this signalling it shall forward the DCK or DCKX belonging to the MS to the cells belonging to the LA (DCK forwarding) if possible. The MS shall reset timer T372 on receipt of D-OTAR NEWCELL or D-OTAR NEWCELL-X. Following this, the MS may apply AI encryption to location update signalling on the new cell if the DCK forwarding was successful and it possesses a valid CCK or CCKX for the LA of the new cell.

6.6.2.5 Announced cell re-selection type-2

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

The SwMI shall use the cell identifier in the U-PREPARE to forward the DCK or DCKX to the new cell (DCK forwarding). On successful completion of cell re-selection, the MS may apply AI encryption on the new cell if it possesses a valid CCK or CCKX for the location area of the new cell. If the MS does not possess a valid CCK or CCKX for the new cell it should request it before selection of the new cell.

6.6.2.6 Announced cell re-selection type-1

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

The SwMI shall use the cell identifier in the U-PREPARE to forward the DCK or DCKX to the new cell (DCK forwarding). On successful completion of cell re-selection, the MS may apply AI encryption on the new cell if it possesses a valid CCK or CCKX for the location area of the new cell. If the MS does not possess a valid CCK or CCKX for the new cell it shall request it before selection of the new cell.

6.6.2.7 Key forwarding

When the SwMI does not support DCK retrieval during cell re-selection, the U-OTAR PREPARE/D-OTAR NEWCELL or D-OTAR NEWCELL-X signalling is used for forwarding the DCK or DCKX to the new LA and requesting the associated CCK or CCKX. No other mobility management or call restoration functionality shall be assumed by the SwMI or the MS.

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

T372 shall indicate the maximum time the MM shall wait for a response to U-OTAR PREPARE. If timer T372 expires, or radio link failure occurs, the MS shall abandon signalling and initiate the cell change procedure immediately (see Figure 6.13).

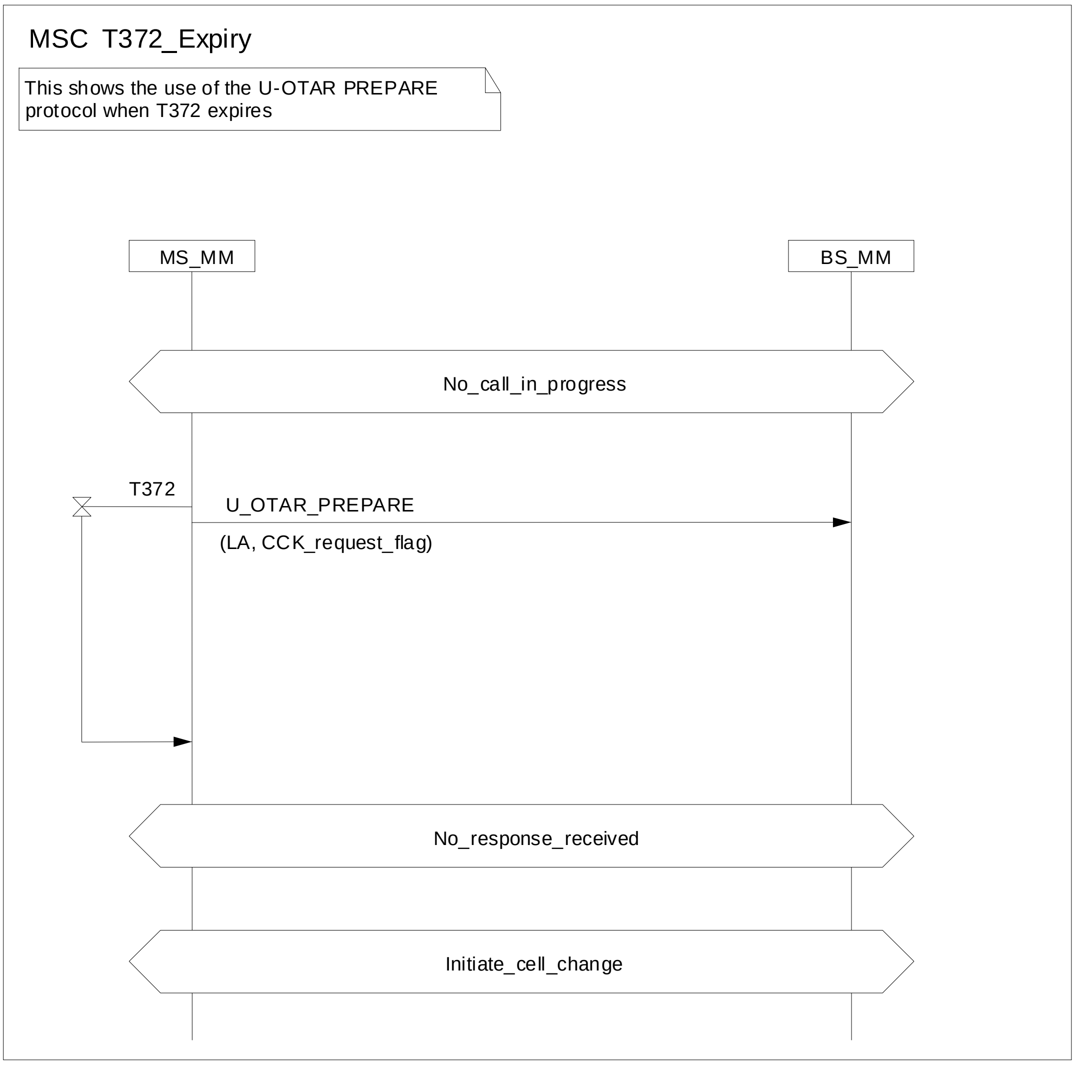


Figure 6.13: Use of U-OTAR PREPARE protocol with T372 expiry

6.6.3 Shared channels

Channels may be shared between two or more cells, where at least one of those cells is a Direct Access cell, and where one cell may be a Conventional Access cell. Refer to ETSI EN 300 392-2 [2], clause 18 for more information. Where channels are shared between cells, all cells which share those channels shall utilize the same security class. Class 2 cells shall use the same SCK/SCKX (with same SCKN and SCK-VN), and security class 3 cells shall use the same CCK/CCKX (with same CCK-id). Where GCK/GCKX encryption is enabled on a security class 3 cell that shares channels with other cells, GCK/GCKX encryption shall be enabled on all cells which share channels with that cell, and each GCK/GCKX used shall be the same (with same GCKN and GCK-VN) on all of these cells. The "Security information" element contained in SYSINFO, SYSINFO-Q and SYSINFO-DA shall contain identical parameters on all cells which share channels with each other, and the security class related elements of this element shall be identical to those contained in the "Security parameters" information element in SYNC-DA sent on any Direct Access cells which share these same channels. Where information about cells that share channels is provided in D-NWRK-BROADCAST and D-NWRK-BROADCAST-DA PDUs sent on other cells, the "Security parameters" element shall be identical for each of a set of neighbour cells that share channels with each other.

NOTE: The SwMI will be responsible for ensuring that security class and keys in use are identical between cells that share channels.

6.7 Encryption control

6.7.0 General

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

6.7.1 Data to be encrypted

6.7.1.1 Downlink control channel requirements

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

- cell synchronization messages sent to the MAC via the TMB-SAP (SYNC, SYNC-DA, SYSINFO, SYSINFO-DA or SYSINFO-Q); and the ACCESS DEFINE PDU is not encrypted as it has no associated TM-SDU.

6.7.1.2 Encryption of MAC header elements

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

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

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

The encryption process shall be accomplished in the same manner as is used to encrypt TM-SDUs, i.e. the modulo 2 addition of a key stream, where the key stream shall be generated as a function of frame numbering and cipher key relevant to the addressed party or parties.

The KSG shall be initialized as described in clause 6.3.2.1 or clause 6.3.2.3.

The address contained in the header of a MAC PDU may be encrypted as follows:

- Where a KSG from TEA set A is in use, if the MAC header indicates that encryption is in use and that MAC header contains an address that is an SSI, the SSI shall be encrypted using the ESI mechanism and algorithm TA61, as described in clause 4.2.6.

- Where an MS negotiates a KSG from TEA set B and the SwMI indicates that the ESI identity encryption is in use by setting the "Identity encryption" element in the "Security downlink" element provided in a D-LOCATION UPDATE ACCEPT PDU to "1", the ESI mechanism and TA61 shall be used to encrypt the SSI as described in clause 4.2.6.

- Where the MS negotiates a KSG from TEA set B and the SwMI sets the "Identity encryption" element in the "Security downlink" element provided in a D-LOCATION UPDATE ACCEPT PDU to "0", or omits the "Identity encryption" element from the D-LOCATION UPDATE ACCEPT PDU, modulo 2 encryption using the MAE mechanism shall be applied to the MAC address as described in clause 6.7.1.2a.

6.7.1.2a MAC Address Encryption mechanism for KSGs in TEA set B

6.7.1.2a.1 Usage of MAC Address Encryption mechanism

The MAC Address Encryption (MAE) mechanism may be used in security class 2 or security class 3 cells where all MSs have negotiated the same KSG from TEA set B. It is used instead of the ESI mechanism described in clause 4.2.6. Use of the MAE mechanism is indicated to an MS that has negotiated a KSG from TEA set B by the SwMI setting the "Identity encryption" element in the "Security downlink" element provided in a D-LOCATION UPDATE ACCEPT PDU to "0", or omitting the "Identity encryption" element from the D-LOCATION UPDATE ACCEPT PDU, see clause 4.2.6.

The MAE mechanism shall not be used if more than one KSG from TEA set B is in use in the same LA, as there could be conflicts in encrypted identities produced by the mechanism with different KSGs. Where more than one KSG from TEA set B is in use in the same LA, the ESI mechanism specified in clause 4.2.6 shall be used, and the CCK input to TA61 shall be derived by the SwMI from the CCKX, or the SCK input to TA61 shall be derived by the SwMI from SCKX.

6.7.1.2a.2 MAE operation

To encrypt the address sent in an uplink or downlink MAC header, 34 bits of keystream KSS(0) to KSS(33) shall be generated using the KSG with the CCKX as cipher key on security class 3 cells, or with SCKX as the cipher key on security class 2 cells. These KSS bits shall be modulo 2 added (XORed) with the address (if any) contained in the MAC header of MAC PDUs whenever the "Encryption control" information element in the MAC header indicates that encryption is to be applied.

If the cipher key used to encrypt the address is the same cipher key that is used to encrypt the remainder of the MAC PDU (i.e. the cipher key is CCKX or SCKX), the 34 bits of keystream shall be the first 34 bits of the same KSS that is generated to encrypt the remainder of the MAC PDU. In this case, 34 bits of KSS shall be generated and reserved whether there is an address present in the MAC header or not. Therefore, the 34 bits KSS(0) to KSS(33) shall be generated and reserved for address encryption when any of MAC-RESOURCE, MAC-FRAG, MAC-END, MAC-D-BLCK, MAC-ACCESS, MAC-END-HU, MAC-DATA, or MAC-U-BLCK is sent and CCKX or SCKX is the cipher key used to encrypt the remainder of the MAC PDU. In this case, KSS(34) onwards are used to encrypt the remainder of the MAC PDU (channel allocation element, if any, and TM-SDU).

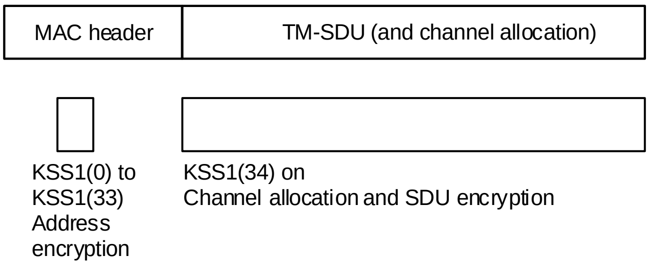
NOTE 1: Where the timeslot does not contain a MAC PDU, e.g. on a TCH used for speech or circuit mode data, these 34 KSS bits are not reserved.

If the cipher key used to encrypt the address is different to the cipher key that is used to encrypt the remainder of the MAC PDU (i.e. the remainder of the PDU is encrypted with DCKX or MGCKX), the KSS bits used to encrypt the address shall be generated separately from the KSS used to encrypt the remainder of the PDU. In this case, the KSG shall be initialized and operated twice: once with CCKX to generate 34 bits of KSS that are used to encrypt the MAC address, and a second time with DCKX or MGCKX. In this case, the remainder of the MAC PDU (channel allocation if any, and TM-SDU) shall be encrypted using KSS(0) onwards from the second KSS.

NOTE 2: Use of a different cipher key to encrypt the address from that used to encrypt the remainder of the MAC PDU only occurs on security class 3 cells.

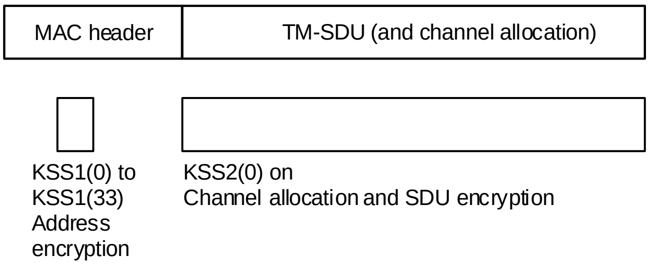
The IV used to initialize the KSG to generate each KSS shall be as specified in clause 6.3.2.3.

The mechanism is shown in Figures 6.13a and 6.13b below.


MAC header
TM-SDU (and channel allocation)
KSS1(0) to
KSS1(33)
Address
encryption
KSS1(34) on
Channel allocation and SDU encryption

NOTE: KSS1 is generated with CCKX or SCKX.

Figure 6.13a: Allocation of KSS to address and SDU encryption where CCKX or SCKX is used for MAC PDU encryption


MAC header
TM-SDU (and channel allocation)
KSS1(0) to
KSS1(33)
Address
encryption
KSS2(0) on
Channel allocation and SDU encryption

NOTE: KSS1 is generated with CCKX, KSS2 is generated with DCKX or MGCKX

Figure 6.13b: Allocation of KSS to address and SDU encryption where DCKX or MGCKX is used for MAC PDU encryption

The generation and allocation of KSS bits to the MAE mechanism and to the remainder of the MAC PDU are summarized in Table 6.7a.

Table 6.7a: Cipher key and KSS allocation for address and MAC PDU encryption

Cipher key used for channel allocation and TM-SDU encryption	Cipher key used and allocation of KSS bits	
	Address encryption	**Channel allocation and TM-SDU encryption**
Uplink		
SCKX	SCKX KSS(0) to KSS(33)	SCKX KSS(34) onwards
DCKX	CCKX KSS(0) to KSS(33)	DCKX KSS(0) onwards
Downlink		
SCKX	SCKX KSS(0) to KSS(33)	SCKX KSS(34) onwards
DCKX	CCKX KSS(0) to KSS(33)	DCKX KSS(0) onwards
CCKX	CCKX KSS(0) to KSS(33)	CCKX KSS(34) onwards
MGCKX	CCKX KSS(0) to KSS(33)	MGCK KSS(0) onwards

6.7.1.2a.3 Addresses to be encrypted

Table 6.7b shows the addresses that shall be encrypted with the MAE mechanism, and the allocation of KSS bits to those addresses.

Table 6.7b: KSS allocation to MAC address type for MAE mechanism

MAC address type	Address length (bits)	KSS allocation
Null PDU	0	None
SSI	24	KSS(0) to KSS(23)
Event label	10	KSS(0) to KSS(9)
USSI (see note 3)	24	N/A
SMI	24	KSS(0) to KSS(23)
SSI + Event label	34	KSS(0) to KSS(33)
SSI + Usage Marker	30	KSS(0) to KSS(29)
SMI + Event label	34	KSS(0) to KSS(33)
NOTE 1: Any remaining KSS (i.e. from the last KSS bit used to KSS(33) shall be discarded. NOTE 2: SSI is any of the short addresses valid for the MS: ISSI, GSSI, ASSI, V-ASSI, V-GSSI. NOTE 3: USSI shall not be encrypted by this mechanism.		

6.7.1.3 Traffic channel encryption control

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

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

The initial use of encryption on the U-PLANE shall maintain the use of encryption of the C-PLANE signalling message which contains the channel allocation element.

The MAC-RESOURCE PDU indicates the encryption state of the PDU and when the PDU contains a channel allocation element the encryption state of the assigned channel shall follow the state of MAC RESOURCE PDU (see ETSI EN 300 392-2 [2], clause 21.4.3.1) and the "Encryption mode element" as defined in clause 6.5.1. Encryption of control and traffic (speech/data) channels shall be switched on and off only by the SwMI. For the duration of the channel allocation the encryption state shall not change, however change of parameters within the encryption state may be allowed.

In the case that U-PLANE mode is "encrypted" the MS shall send all signalling encrypted (sent with one of stealing, Fast Associated Control Channel (FACCH), Slow Associated Control Channel (SACCH)). In the case where U-PLANE mode of an assigned channel for a call is "clear" the MS shall send all signalling related to that call in clear (sent with one of stealing, FACCH, SACCH) and other signalling may be encrypted.

U-PLANE signalling (using STCH) is encrypted starting from the first bit of TM-SDU (see ETSI EN 300 392-2 [2], clause 21.4.5). In this case the MAC header does not contain the encryption flag, hence security information shall be the same as for the traffic.

6.7.1.4 Handling of PDUs that do not conform to negotiated ciphering mode

The SwMI is not required to send a layer 2 or layer 3 response to PDUs received from an MS with a ciphering mode differing from the ciphering mode negotiated with that MS.

The MS is not required to send a layer 2 or layer 3 response to PDUs received from the SwMI with a ciphering mode differing from the ciphering mode negotiated with that SwMI.

6.7.2 Service description and primitives

6.7.2.0 General

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

The primitives required to control encryption are summarized in Figure 6.14.

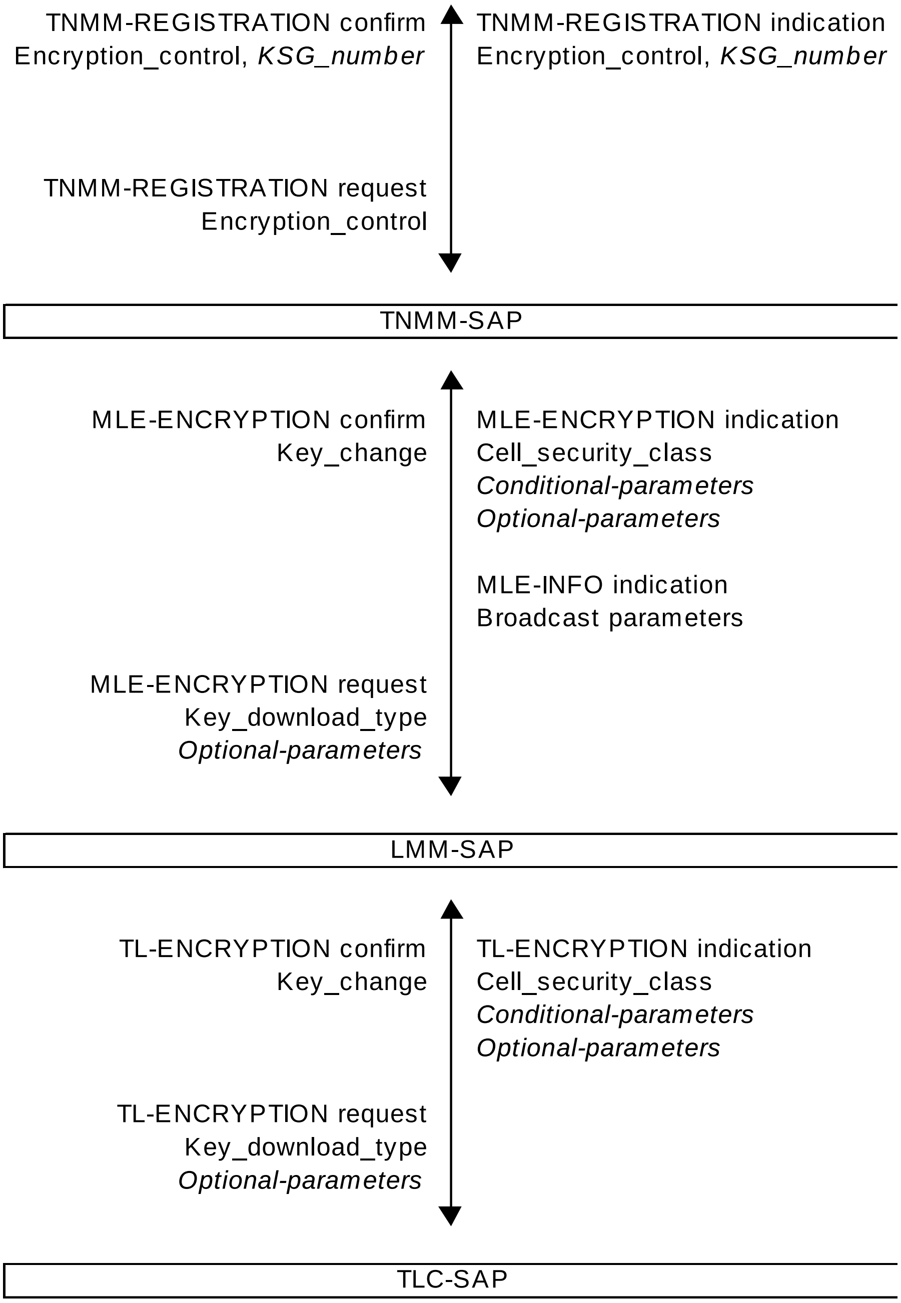


Figure 6.14: Protocol stack and primitives for encryption control

6.7.2.1 Mobility Management (MM)

TNMM SAP: the encryption control procedure shall only be invoked by the SwMI using the registration procedure. The MS-MM may indicate its current state, or a change of state, to the MS application.

The primitive TNMM-REGISTRATION shall contain the parameter "Encryption control" to enable/disable the encryption process, and the parameter "KSG number" (see Table 6.8).

Table 6.8: TNMM-REGISTRATION parameters (see ETSI EN 300 392-2 [2], clause 15.3.3.7)

Parameter	Request	Indication	Confirm
Registration Status	-	M	M
Registration Reject Cause (see note 1)	-	C	-
Registration Type	M	-	-
Location Area (see note 2)	C	-	-
MCC (see note 3)	C	-	-
MNC (see note 3)	C	-	-
ISSI or ASSI or USSI (see 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 (see Table 6.9). The MAC shall indicate to MM the current CCK-id that is received in the broadcast SYSINFO, SYSINFO-DA or SYSINFO-Q PDU.

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

NOTE: The short CCK-id is equal to the least significant bit of CCK-id, and indicates whether the value of CCK-id is odd or even. Similarly, the short SCK-VN is equal to the least significant bit of SCK-VN, and indicates whether the value of SCK-VN is odd or even.

Table 6.9: MLE-ENCRYPTION parameters

Parameter	Request	Confirm	Indication
Key download type	M		-
KSG Number (see note 1)	O		-
SCK/SCKX (see note 2)	C		-
DCK/DCKX (see note 2)	C		-
CCK/CCKX (see note 2)	C		-
CCK-id (see notes 2, 4)	C		C
SCK-VN	C		C
SCKN	C		C
MGCK/MGCKX (see note 2)	C		-
GTSI (see note 3)	C		-
xSSI (see note 5)	C		-
GSKO/GSKOX	C		
Cipher usage (see note 1)	O		-
Time (see note 6)	O		
Key change (see 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 or MGCKX downloaded.

NOTE 4: CCK-id supplied in indication.

NOTE 5: This is the SSI associated with the DCK or DCKX when DCK or DCKX 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/DCKX, SCKN, SCK-VN;
  - DCK/DCKX, xSSI pair;
  - CCK/CCKX, CCK-id, LA-id;
  - MGCK/MGCKX, GTSI;
  - GSKO/GSKOX.

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 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 ETSI EN 300 392-2 [2], clause 21.

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

In security class 3 the MAC shall indicate to MLE/MM the CCK-id of the current CCK/CCKX in use in the cell. In security class 2, the MAC shall indicate the SCK-VN in use.

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

6.7.3 Protocol functions

6.7.3.0 General

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 present clause.

6.7.3.1 MM

The protocol functions for air interface security shall be the following:

- "ciphering parameter" information elements shall be contained in the U- and D- LOCATION UPDATE PDUs. A negotiation for ciphering parameters shall be performed in a re-registration if the parameters are not acceptable;

- MM may have to perform a re-registration if the SwMI requires a change in the ciphering 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 security information to the MAC (including those to be used in the ciphering parameters information element) and to receive an indication of a change in the short SCK-VN (class 2) or CCK-id (class 3) from the MAC.

6.7.3.3 LLC

The LLC is used to control the encryption mode of BL-ACK/BL-ADATA/BL-ACK+DATA, etc.

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 encryption parameters to the MAC (including those negotiated in the "ciphering parameters" information element) and to receive an indication of a change in the short SCK-VN (class 2) or CCK-id (class 3) from the MAC.

6.7.3.4 MAC

The MAC shall indicate to MM a change in the SCK-VN (Class 2) or CCK-id (Class 3) broadcast in MAC SYSINFO, SYSINFO-DA or SYSINFO-Q using the MLE-INFO primitive.

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

6.7.4 PDUs for cipher negotiation

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

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

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

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

If the proposed security information is rejected by the SwMI the MS-MM shall use MLE-ENCRYPTION to inform the MAC to modify the parameters in accordance with the D-LOCATION UPDATE REJECT cause.

If the reject cause is "ciphering required" the MS may choose a set of parameters and send a new U-LOCATION UPDATE DEMAND or it may initiate the authentication process using the U-AUTHENTICATE DEMAND exchange described in clause 4.4.2.

NOTE: If the MS cannot negotiate compatible security parameters it should consider rejection, with one of these causes, to be rejection from the cell and not rejection from the complete SwMI. The MS may attempt cell reselection to find a cell where acceptable security information can be negotiated.

Annex A (normative): PDU and element definitions

A.0 General

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

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

A.1 Authentication PDUs

A.1.1 D-AUTHENTICATION DEMAND

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

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

Table A.1: D-AUTHENTICATION DEMAND PDU contents

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

A.1.2 D-AUTHENTICATION REJECT

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

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-AUTHENTICATION DEMAND or U-LOCATION UPDATE DEMAND containing RAND2;
- Response expected: none.

Table A.2: D-AUTHENTICATION REJECT PDU contents

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

A.1.3 D-AUTHENTICATION RESPONSE

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

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

Table A.3: D-AUTHENTICATION RESPONSE PDU contents

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

A.1.4 D-AUTHENTICATION RESULT

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

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

Table A.4: D-AUTHENTICATION RESULT PDU contents

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

A.1.5 U-AUTHENTICATION DEMAND

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

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

Table A.5: U-AUTHENTICATION DEMAND PDU contents

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

A.1.6 U-AUTHENTICATION REJECT

Shall be used by the MS to report to the infrastructure rejection of an authentication demand which does not occur within the ENABLE/DISABLE protocol.

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

Table A.6: U-AUTHENTICATION REJECT PDU contents

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

A.1.7 U-AUTHENTICATION RESPONSE

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

- Direction: MS to SwMI;
- Service used: MM;
- Response to: D-AUTHENTICATION DEMAND or D-ENABLE or D-DISABLE;
- Response expected: D-AUTHENTICATION RESULT.

Table A.7: U-AUTHENTICATION RESPONSE PDU contents

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

A.1.8 U-AUTHENTICATION RESULT

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

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

Table A.8: U-AUTHENTICATION RESULT PDU contents

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

A.2 OTAR PDUs

A.2.1 D-OTAR CCK PROVIDE

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

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR CCK DEMAND or none;
- Response expected: U-OTAR CCK RESULT or none.

Table A.9: D-OTAR CCK PROVIDE PDU contents

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

A.2.1a D-OTAR CCKX PROVIDE

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

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR CCK DEMAND or none;
- Response expected: U-OTAR CCK RESULT or none.

Table A.9a: D-OTAR CCKX PROVIDE PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	OTAR extension
OTAR extension	4	1	M	CCKX provide
CCK provision flag	1	1	M	
KSG number	4		C	Provided if CCK provision flag = 1
CCK identifier (CCK-id)	16		C	Provided if CCK provision flag = 1
Key type flag	1		C	Provided if CCK provision flag = 1 0 = Current, 1 = Future
Sealed CCK (SCCK)	120		C	Provided if KSG number element has value 0000_2 - 0011_2
Sealed CCKX (SCCKX)	224		C	Provided if KSG number element has value 0100_2 - 0110_2
CCK location area information	2-216		C	Provided if CCK provision flag = 1 Applies to both current and future key (if provided)
Future key flag	1		C	Provided if CCK provision flag = 1 Always 0 if Key type flag = 1
Sealed CCK (SCCK)	120		C	Provided if Future key flag = 1 and KSG number element has value 0000_2 - 0011_2
Sealed CCKX (SCCKX)	224		C	Provided if Future key flag = 1 and KSG number element has value 0100_2 - 0110_2
Proprietary element		3	O	

A.2.2 U-OTAR CCK DEMAND

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

- Direction: MS to SwMI;
- Service used: MM;
- Response to: none;
- Response expected: D-OTAR CCK PROVIDE or D-OTAR CCKX PROVIDE.

Table A.10: U-OTAR CCK DEMAND PDU contents

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

A.2.3 U-OTAR CCK RESULT

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

- Direction: MS to SwMI;
- Service used: MM;
- Response to: D-OTAR CCK PROVIDE, D-OTAR CCKX PROVIDE or D-LOCATION UPDATE ACCEPT containing "CCK Information";
- Response expected: none.

Table A.11: U-OTAR CCK RESULT PDU contents

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

A.2.4 D-OTAR GCK PROVIDE

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

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR GCK DEMAND or none;
- Response expected: U-OTAR GCK RESULT.

Table A.12: D-OTAR GCK PROVIDE PDU contents

Information element	Length	Type	C/O/M	Remark
PDU type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	GCK Provide
Acknowledgement flag	1	1	M	If "0" No acknowledgement required If "1" Acknowledgement required
Reserved	1		C	Provided if Acknowledgement flag set to "0"
Explicit response (see note 1)	1		C	Provided if Acknowledgement flag set to "1"
Max response timer value	16	1	M	Identifies the maximum period of timer T371 over which the MS will randomly choose to respond
Session key	1	1	M	Identifies if encrypted with group or individual encryption session key
Random Seed for OTAR	80		C	Provided if session key for individual
GSKO-VN	16		C	Provided if session key for group
Number of GCKs provided	3	1	M	See note 2
GCK key and identifier	152		C	See note 3
KSG number	4	1	M	Associates GCK to a particular encryption algorithm
Group association	1	1	M	See note 4
GSSI	24		C	If Group association = GSSI
OTAR retry interval	3	1	M	
Reserved	24	2	O	See note 5
Proprietary element		3	O	
NOTE 1: The "explicit response" element is only valid if "Acknowledgment field" is set to "1". If the "explicit response" element = 1, the MS shall respond whether the key provide changes the MS state or not; if "explicit response" = 0, the MS shall only respond if the SwMI provides a key or key version that the MS did not previously have. NOTE 2: The number of GCKs/GCKXs provided may not be the same as the number of GCKs/GCKXs originally requested. NOTE 3: This element is repeated according to "Number of GCKs provided" value. If "Number of GCKs provided" = 0, there shall be no "GCK key and identifier" elements in the PDU. NOTE 4: Where group association indicates GSSI the provided GCKs/GCKXs shall all have the GCKN associated with the indicated GSSI and shall have different GCK-VNs. NOTE 5: Optional element not used in this version of the present document and shall not be present in the PDU.				

A.2.4a D-OTAR GCKX PROVIDE

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

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR GCK DEMAND or none;
- Response expected: U-OTAR GCK RESULT.

Table A.12a: D-OTAR GCKX PROVIDE PDU contents

Information element	Length	Type	C/O/M	Remark
PDU type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	OTAR extension
OTAR extension	4	1	M	GCKX provide
Acknowledgement flag	1	1	M	If "0" No acknowledgement required
				If "1" Acknowledgement required
Reserved	1		C	Provided if Acknowledgement flag set to "0"
Explicit response (see note 1)	1		C	Provided if Acknowledgement flag set to "1"
Max response timer value	16	1	M	Identifies the maximum period of timer T371 over which the MS will randomly choose to respond
Session key	1	1	M	Identifies if encrypted with group or individual encryption session key
Random Seed for OTAR	80		C	Provided if session key for individual
GSKO-VN	16		C	Provided if session key for group
KSG number	4	1	M	Associates GCK/GCKX to a particular encryption algorithm
Number of GCKs provided	3	1	M	See note 2
GCK key and identifier	152		C	See note 3 Provided if KSG number = 0000_2 to 0011_2
GCKX key and identifier	256		C	See note 3 Provided if KSG number = 0100_2 to 0101_2
Group association	1	1	M	See note 4
GSSI	24		C	If Group association = GSSI
OTAR retry interval	3	1	M	
Reserved	24	2	O	See note 5
Proprietary element		3	O	

NOTE 1: The "explicit response" element is only valid if "Acknowledgment field" is set to "1". If the "explicit response" element = 1, the MS shall respond whether the key provide changes the MS state or not; if "explicit response" = 0, the MS shall only respond if the SwMI provides a key or key version that the MS did not previously have.

NOTE 2: The number of GCKs/GCKXs provided may not be the same as the number of GCKs/GCKXs originally requested.

NOTE 3: This element is repeated according to "Number of GCKs provided" value. If "Number of GCKs provided" = 0, there shall be no "GCK key and identifier" elements in the PDU.

NOTE 4: Where group association indicates GSSI the provided GCKs/GCKXs shall all have the GCKN associated with the indicated GSSI and shall have different GCK-VNs.

NOTE 5: Optional element not used in this version of the present document and shall not be present in the PDU.

A.2.5 U-OTAR GCK DEMAND

Shall be used by the MS to request GCKs or GCKXs from the SwMI.

- Direction: MS to SwMI;
- Service used: MM;
- Response to: none;

- Response expected: D-OTAR GCK PROVIDE or D-OTAR GCKX PROVIDE.

Table A.13: U-OTAR GCK DEMAND PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	GCK Demand
KSG number	4	1	M	Associates GCK/GCKX with a particular encryption algorithm
Number of GCKs requested by GCKN	3	1	M	See note 1
GCKN	16		C	Shall be repeated the number of times indicated by the "Number of GCKs requested by GCKN" information element
Number of GCKs requested by GSSI	3	1	M	See note 1
GSSI	24		C	Shall be repeated the number of times indicated by the "Number of GCKs requested by GSSI" information element
Reserved	24	2	O	See note 2
Proprietary element		3	O	
NOTE 1: The total number of GCKs or GCKXs requested in this PDU (i.e. the sum of these elements) shall not be zero and shall not exceed seven. NOTE 2: Optional element not used in this version of the present document and shall not be present in the PDU.				

A.2.6 U-OTAR GCK RESULT

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

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

Table A.14: U-OTAR GCK RESULT PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	GCK Result
Number of GCKs provided	3	1	M	
GCK provision result	Varies		C	Repeated according to Number of GCKs provided value
Reserved	24	2	O	See note
Proprietary element		3	O	
NOTE: Optional element not used in this version of the present document and shall not be present in the PDU.				

A.2.6a D-OTAR GCK REJECT

Shall be used by the infrastructure to explicitly reject GCK or GCKX requests from an MS.

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR GCK DEMAND.

Table A.15: D-OTAR GCK REJECT PDU contents

Information element	Length	Type	C/O/M	Remark
PDU type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	GCK Reject
Number of GCKs rejected	3	1	M	
GCK rejected	Varies		C	See note 1
OTAR Retry Interval	3	1	M	
Reserved	24	2	O	See note 2
Proprietary element		3	O	
NOTE 1: This element is repeated according to the "Number of GCKs rejected" value. NOTE 2: Optional element not used in this version of the present document and shall not be present in the PDU.				

A.2.7 D-OTAR SCK PROVIDE

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

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR SCK DEMAND or none;
- Response expected: U-OTAR SCK RESULT.

Table A.16: D-OTAR SCK PROVIDE PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	SCK Provide
Acknowledgement flag	1	1	M	If "0" No acknowledgement required If "1" Acknowledgement required
Reserved	1		C	Provided if Acknowledgement flag set to "0"
Explicit response (see note 1)	1		C	Provided if Acknowledgement flag set to "1"
Max response timer value	16	1	M	Identifies the maximum period over which the MS will randomly choose to respond
Session key	1	1	M	Identifies if encrypted with group or individual encryption session key
Random seed for OTAR	80		C	Provided if session key for individual
GSKO-VN	16		C	Provided if session key for group
Number of SCKs provided	3	1	M	See note 2
SCK key and identifier	143		C	See note 3
KSG number	4	1	M	Associates SCK with a particular encryption algorithm
OTAR Retry Interval	3	1	M	
Address Extension	24	2	O	See note 4
Proprietary element		3	O	
NOTE 1: If the "explicit response" element = 1, the MS shall respond whether the key provide changes the MS state or not; if "explicit response" = 0, the MS shall only respond if the SwMI provides a key or key version that the MS did not previously have. NOTE 2: The number of SCKs provided may be different to the number of SCKs originally requested. NOTE 3: This element is repeated according to "Number of SCKs provided" value. If "Number of SCKs provided" = 0, there shall be no "SCK key and identifier" elements in the PDU. NOTE 4: The Address extension element shall be present only if the network code for which the provided SCK relates is different to the serving network.				

A.2.7a D-OTAR SCKX PROVIDE

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

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR SCK DEMAND or none;
- Response expected: U-OTAR SCK RESULT.

Table A.16a: D-OTAR SCKX PROVIDE PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	OTAR extension
OTAR extension type	4	1	M	SCKX Provide
Acknowledgement flag	1	1	M	If "0" No acknowledgement required If "1" Acknowledgement required
Reserved	1		C	Provided if Acknowledgement flag set to "0"
Explicit response (see note 1)	1		C	Provided if Acknowledgement flag set to "1"
Max response timer value	16	1	M	Identifies the maximum period over which the MS will randomly choose to respond
Session key	1	1	M	Identifies if encrypted with group or individual encryption session key
Random seed for OTAR	80		C	Provided if session key for individual
GSKO-VN	16		C	Provided if session key for group
KSG number	4	1	M	Associates SCK/SCKX with a particular encryption algorithm
Number of SCKs provided	3	1	M	See note 2
SCK key and identifier	143		C	See note 3 Provided if KSG number = 0000_2 to 0011_2
SCKX key and identifier	247		C	See note 3 Provided if KSG number = 0100_2 to 0101_2
OTAR Retry Interval	3	1	M	
Address Extension	24	2	O	See note 4
Proprietary element		3	O	
NOTE 1: If the "explicit response" element = 1, the MS shall respond whether the key provide changes the MS state or not; if "explicit response" = 0, the MS shall only respond if the SwMI provides a key or key version that the MS did not previously have. NOTE 2: The number of SCKs/SCKXs provided may be different to the number of SCKs/SCKXs originally requested. NOTE 3: This element is repeated according to "Number of SCKs provided" value. If "Number of SCKs provided" = 0, there shall be no "SCK key and identifier" elements in the PDU. NOTE 4: The Address extension element shall be present only if the network code for which the provided SCK/SCKX(s) relates is different to the serving network.				

A.2.8 U-OTAR SCK DEMAND

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

- Direction: MS to SwMI;
- Service used: MM;
- Response to: none;
- Response expected: D-OTAR SCK PROVIDE or D-OTAR SCKX PROVIDE.

Table A.17: U-OTAR SCK DEMAND PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	SCK Demand
KSG number	4	1	M	Associates SCK/SCKX with a particular encryption algorithm
Number of SCKs requested	3	1	M	
SCK Number (SCKN)	5		C	See note 1
Address Extension	24	2	O	See note 2
Proprietary element		3	O	
NOTE 1: This element is repeated according to the "Number of SCKs element. Requested" value. NOTE 2: The Address extension element shall be present only if the network code for which the requested SCK relates is different to the serving network.				

A.2.9 U-OTAR SCK RESULT

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

- Direction: MS to SwMI;
- Service used: MM;
- Response to: D-OTAR SCK PROVIDE, D-OTAR SCKX PROVIDE or D-LOCATION UPDATE ACCEPT containing "SCK Information";
- Response expected: none.

Table A.18: U-OTAR SCK RESULT PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	SCK Result
Number of SCKs provided	3	1	M	
SCK number and result	Varies		C	See note 1
Address Extension	24	2	O	See note 2
Proprietary element		3	O	
NOTE 1: This element is repeated according to the "Number of SCKs provided" value. NOTE 2: The Address extension element shall be present only if the network code for which the requested SCK/SCKX relates is different to the serving network.				

A.2.9a D-OTAR SCK REJECT

Shall be used by the infrastructure to reject provision of SCK or SCKX to an MS.

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR SCK DEMAND;
- Response expected: none.

Table A.19: D-OTAR SCK REJECT PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	SCK Reject
Number of SCKs rejected	3	1	M	
SCK rejected	8		C	See note 1
OTAR Retry Interval	3	1	M	
Address Extension	24	2	O	See note 2
Proprietary element		3	O	
NOTE 1: This element is repeated according to the "Number of SCKs rejected" value. Each rejected SCK/SCKX shall be associated with its own OTAR reject reason. NOTE 2: The Address extension element shall be present only if the network code for which the requested SCK/SCKX relates is different to the serving network.				

A.2.10 D-OTAR GSKO PROVIDE

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

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR GSKO DEMAND or none;
- Response expected: U-OTAR GSKO RESULT.

Table A.20: D-OTAR GSKO PROVIDE PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	GSKO Provide
Random seed for OTAR	80	1	M	
GSKO-VN	16	1	M	
Sealed GSKO	120	1	M	
GSSI	24	1	M	
Reserved (see note)	24	2	O	
Proprietary element		3	O	
NOTE: Optional element not used in this version of the present document and shall not be present in the PDU.				

A.2.10a D-OTAR GSKOX PROVIDE

Shall be used by the infrastructure to provide GSKO or GSKOX and CMG GSSI to an MS.

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR GSKO DEMAND or none;
- Response expected: U-OTAR GSKO RESULT.

Table A.20a: D-OTAR GSKOX PROVIDE PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	OTAR extension
OTAR extension	4	1	M	GSKOX Provide
Random seed for OTAR	80	1	M	
KSG number	4	1	M	
GSKO-VN	16	1	M	
Sealed GSKO	120		C	Provided if KSG number is 0000_2 to 0011_2
Sealed GSKOX	288		C	Provided if KSG number is 0100_2 to 0110_2
GSSI	24	1	M	
Reserved (see note)	24	2	O	
Proprietary element		3	O	
NOTE: Optional element not used in this version of the present document and shall not be present in the PDU.				

A.2.11 U-OTAR GSKO DEMAND

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

- Direction: MS to SwMI;
- Service used: MM;
- Response to: none;
- Response expected: D-OTAR GSKO PROVIDE or D-OTAR GSKOX PROVIDE.

Table A.21: U-OTAR GSKO DEMAND PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	GSKO Demand
Reserved (see note)	24	2	O	
Proprietary element		3	O	
NOTE: Optional element not used in this version of the present document and shall not be present in the PDU.				

A.2.12 U-OTAR GSKO RESULT

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

- Direction: MS to SwMI;
- Service used: MM;
- Response to: D-OTAR GSKO PROVIDE or D-OTAR GSKOX PROVIDE;
- Response expected: none.

Table A.22: U-OTAR GSKO RESULT PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	GSKO Result
GSKO-VN	16	1	M	
Provision result	3	1	M	
GSSI	24	1	M	
Reserved (see note)	24	2	O	
Proprietary element		3	O	
NOTE: Optional element not used in this version of the present document and shall not be present in the PDU.				

A.2.12a D-OTAR GSKO REJECT

Shall be used by the infrastructure to reject provision of GSKO or GSKOX to an MS.

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR GSKO DEMAND;
- Response expected: none.

Table A.23: D-OTAR GSKO REJECT PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	GSKO Reject
OTAR reject reason	3	1	M	
GSSI	24	1	M	
OTAR Retry Interval	3	1	M	
Reserved (see note)	24	2	O	
Proprietary element		3	O	
NOTE: Optional element not used in this version of the present document and shall not be present in the PDU.				

A.3 PDUs for key association to GTSI

A.3.1 D-OTAR KEY ASSOCIATE DEMAND

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

- Direction: SwMI to MS;
- Service used: MM;
- Response to: none;
- Response expected: U-OTAR KEY ASSOCIATE STATUS or none.

Table A.24: D-OTAR KEY ASSOCIATE DEMAND contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub type	4	1	M	Key associate demand
Acknowledgement flag	1	1	M	If "0" No acknowledgement required If "1" Acknowledgement required
Explicit response (see note 3)	1	1	M	If "0" MS shall respond if state changes If "1" MS shall always respond
Max response timer value	16	1	M	Identifies the maximum period over which the MS will randomly choose to respond
Key association type	1	1	M	SCK/SCKX (0), GCK/GCKX (1)
SCK select number	6		C	Provided if key type = SCK/SCKX
SCK subset grouping type	4		C	Provided if key type = SCK/SCKX
GCK select number	17		C	Provided if key type = GCK/GCKX
Number of groups	5	1	M	(0) reserved, (1 to 30) number of groups, (31) range of groups
GSSI (see note 1)	24		C	Repeated element
Address extension (see note 2)	24	2	O	
NOTE 1: The GSSI element is repeated; total number GSSI elements = value of "Number groups" element. For 0 < Number of Groups < 31; = 2 for Number of Groups = 31, and GSSI elements shall contain the lowest followed by the highest value GSSI in the range. GSSI can only be provided for a single network within the same PDU. NOTE 2: The Address extension element is only present if the network code for which the provided GSSIs relate is different to the serving network. NOTE 3: The "explicit response" element is only valid if "Acknowledgment field" is set to "1".				

A.3.2 U-OTAR KEY ASSOCIATE STATUS

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

- Direction: MS to SwMI;
- Service used: MM;
- Response to: D-OTAR KEY ASSOCIATE DEMAND;
- Response expected: none.

Table A.25: U-OTAR KEY ASSOCIATE STATUS contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub type	4	1	M	Key associate status
Key association type	1	1	M	SCK/SCKX (0), GCK/GCKX (1)
SCK subset grouping type	4		C	Provided if "Key association type" = SCK/SCKX
Key association status	3	1	M	
Number of groups	5		C	Provided if "Key association status" = "Address not valid", and indicates the number of GSSI fields that follow. Valid range = 1 to 30
GSSI	24		C	Provided if "Key association status" = "Address not valid". Element is repeated the number of times indicated by the value of the "Number of groups" element and contains each unknown address
Address extension (see note)	24	2	O	
NOTE: The Address extension element is only present if the network code for which the provided GSSIs relate is different to the serving network.				

A.4 PDUs to synchronize key or security class change

A.4.1 D-CK CHANGE DEMAND

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

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

Table A.26: D-CK CHANGE DEMAND contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-CK CHANGE DEMAND
Acknowledgement flag	1	1	M	If "0" No acknowledgement required
				If "1" Acknowledgement required
Change of security class	2	1	M	
Key change type	3	1	M	
SCK use	1		C	Provided if key change type = SCK/SCKX; "0" = TMO, "1" = DMO
Number of SCKs changed	4		C	Provided if key change type = SCK/SCKX; (0000) indicates subset of SCKs/SCKXs; (1) to (1111) indicate number of single SCKs/SCKXs to follow
SCK subset grouping type	4		C	Provided if SCK use = DMO and Number of SCKs changed = 0
SCK subset number	5		C	Provided if SCK use = DMO and Number of SCKs changed = 0
SCK-VN	16		C	Provided if SCK use = DMO and Number of SCKs changed = 0
SCK data (see note 1)	21		C	Provided if key change type = SCK/SCKX; and Number of SCKs = 1 to 1111; repeated element
CCK-id	16		C	Provided if key change type = CCK/CCKX, or if key change type = "Class 3 CCK(X) and GCK(X) activation"
Number of GCKs changed	4		C	Provided if key change type = GCK/GCKX; Reserved (0000_2)
GCK data (see note 1)	32		C	Provided if key change type = GCK/GCKX; repeated element
GCK-VN	16		C	Provided if key change type = All GCK/GCKX, or if key change type = "Class 3 CCK(X) and GCK(X) activation"
Time type	2	1	M	
Slot number	2		C	Provided if time type = Absolute IV
Frame number	5		C	Provided if time type = Absolute IV
Multiframe number	6		C	Provided if time type = Absolute IV
Hyperframe number	16		C	Provided if time type = Absolute IV
Network time (see note 2)	48		C	Provided if time type = network time
NOTE 1: The SCK data or GCK data elements are repeated; total number of SCK data or GCK data elements = value of "Number of SCKs changed" or value of "Number of GCKs changed" element. NOTE 2: As specified in ETSI EN 300 392-2 [2], clause 18.5.24.				

A.4.2 U-CK CHANGE RESULT

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

- Direction: MS to SwMI;
- Service used: MM;
- Response to: D-CK CHANGE DEMAND;
- Response expected: none.

Table A.27: U-CK CHANGE RESULT contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-CK CHANGE RESULT
Change of security class	2	1	M	
Key change type	3	1	M	If "change of security class" is "transition to security class 1" then this element is set to "no cipher key"
SCK use	1		C	Provided if key change type = SCK/SCKX; "0" = TMO, "1" = DMO
Number of SCKs changed	4		C	Provided if key change type = SCK/SCKX; indicates the number of SCK data elements to follow
SCK subset grouping type	4		C	Provided if SCK use = DMO; and Number of SCKs = 0
SCK subset number	5		C	Provided if SCK use = DMO; and Number of SCKs = 0
SCK-VN	16		C	Provided If SCK use = DMO; and Number of SCKs = 0
SCK data (see note)	21		C	Provided if key change type = SCK/SCKX; repeated element
CCK-id	16		C	Provided if key change type = CCK/CCKX
Number of GCKs changed	4		C	Provided if key change type = GCK/GCKX
GCK data (see note)	32		C	Provided if key change type = GCK/GCKX; repeated element
GCK-VN	16		C	Provided if key change type = All GCKs/GCKXs
NOTE: The SCK data or GCK data elements are repeated to inform the SwMI of all keys that have been successfully selected. This may be different to the number demanded by the SwMI.				

A.4.2a Void

NOTE: The U-OTAR KEY DELETE RESULT PDU is specified in clause A.4a.2.

A.4.2b Void

NOTE: The U-OTAR KEY STATUS RESPONSE PDU is specified in clause A.4b.2.

A.4.3 D-DM-SCK ACTIVATE DEMAND

Shall be used by SwMI to indicate a change of active DMO SCK for use with a different MNI than the serving SwMI either in the future or immediately.

- Direction: SwMI to MS;
- Service used: MM;
- Response to: none;
- Response expected: U-DM-SCK ACTIVATE RESULT or none.

Table A.27a: D-DM-SCK ACTIVATE DEMAND contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	DM SCK ACTIVATE DEMAND
Acknowledgement flag	1	1	M	If "0" No acknowledgement required
				If "1" Acknowledgement required
Number of SCKs changed	4		C	(0000) indicates subset of SCKs/SCKXs; (1) to (1111) indicate number of single SCKs/SCKXs to follow
SCK subset grouping type	4		C	Provided if Number of SCKs changed = 0
SCK subset number	5		C	Provided if Number of SCKs changed = 0
SCK-VN	16		C	Provided if Number of SCKs changed = 0
SCK data (see note 1)	21		C	Provided if Number of SCKs = 1 to 1111; repeated element
Time type	2	1	M	
Slot number	2		C	Provided if time type = Absolute IV
Frame number	5		C	Provided if time type = Absolute IV
Multiframe number	6		C	Provided if time type = Absolute IV
Hyperframe number	16		C	Provided if time type = Absolute IV
Network time (see note 2)	48		C	Provided if time type = network time
Address extension	24	1	M	MNI of DMO network where SCKs are to be used
NOTE 1: The SCK data elements are repeated; total number of SCK data elements = value of "Number of SCKs changed". NOTE 2: As specified in ETSI EN 300 392-2 [2], clause 18.5.24.				

A.4.4 U-DM-SCK ACTIVATE RESULT

Shall be used by MS-MM to inform the SwMI that it has registered the required DMO SCK activation.

- Direction: MS to SwMI;
- Service used: MM;
- Response to: D-DM-SCK ACTIVATE DEMAND;
- Response expected: none.

Table A.27b: U-DM-SCK ACTIVATE RESULT contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	DM SCK ACTIVATE RESULT
Number of SCKs changed	4		C	Indicates the number of SCK data elements to follow
SCK subset grouping type	4		C	Provided if Number of SCKs = 0
SCK subset number	5		C	Provided if Number of SCKs = 0
SCK-VN	16		C	Provided If Number of SCKs = 0
SCK data (see note)	21		C	Repeated element
Address extension	24	1	M	MNI of DMO network where SCKs are to be used
NOTE: The SCK data elements are repeated to inform the SwMI of all keys that have been successfully selected. This may be different to the number demanded by the SwMI.				

A.4a PDUs to delete air interface keys in MS

A.4a.1 D-OTAR KEY DELETE DEMAND

Shall be used by the SwMI to delete air interface key material from the MS.

- Direction: SwMI to MS;
- Service used: MM;
- Response to: none;
- Response expected: U-OTAR KEY DELETE RESULT or none.

Table A.27c: D-OTAR KEY DELETE DEMAND contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	Key Delete Demand
Key delete type	3	1	M	
Number of SCKs deleted	5		C	Provided if key delete type = (000) or (001), individual SCK(s)/SCKX(s) or members of a KAG; indicates number of SCKN elements to follow
SCKN	5		C	Provided if key delete type = (000) or (001), individual SCK(s)/SCKX(s) or members of a KAG; Repeated element, number of elements corresponds to value of Number of SCKs deleted element
SCK subset grouping type	4		C	Provided if key delete type = (010), SCK subset
SCK subset number	5		C	Provided if key delete type = (010), SCK subset; Value corresponds to subset number to be deleted
Number of GCKs deleted	4		C	Provided if key delete type = (100) individual GCK(s)/GCKX(s)
GCKN	16		C	Provided if key delete type = (100), individual GCK(s)/GCKX(s); Repeated element, number of elements corresponds to value of Number of GCKs deleted element
Address extension (see note 1)	24	2	O	
NOTE 1: The address extension element shall be present only if the network code for which the deleted key relates is different to the serving network. NOTE 2: If key delete type = 001, members of a KAG, the MS shall delete all other SCKNs in other subsets that correspond with the SCKN listed for deletion by the SwMI in this PDU.				

A.4a.2 U-OTAR KEY DELETE RESULT

Shall be used by MS-MM to inform the SwMI that it has deleted the required cipher keys.

- Direction: MS to SwMI;
- Service used: MM;
- Response to: D-OTAR KEY DELETE DEMAND;
- Response expected: none.

Table A.27d: U-OTAR KEY DELETE RESULT contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	Key Delete Result
Key delete type	3	1	M	
Number of SCKs deleted	5		C	Provided if key delete type = (000) or (001), individual SCK(s)/SCKX(s) or members of a KAG; (00000) to (11111) indicate number of individual SCKs/SCKXs to follow
SCKN	5		C	Provided if key delete type = (000) or (001), individual SCK(s)/SCKX(s) or members of a KAG; Repeated element, number of elements corresponds to value of Number of SCKs deleted element
SCK subset grouping type	4		C	Provided if key delete type = (010) or (001), SCK subset or members of a KAG
SCK subset number	5		C	Provided if key delete type = (010), SCK subset; Value corresponds to subset number to be deleted
Number of GCKs deleted	4		C	Provided if key delete type = (100) individual GCK(s)/GCKX(s)
GCKN	16		C	Provided if key delete type = (100), individual GCK(s)/GCKX(s); Repeated element, number of elements corresponds to value of Number of GCKs deleted element
GSKO-VN	16		C	Provided if key delete type = (110), GSKO/GSKOX
Key delete extension type	8		C	Provided if key delete type = (111), Key delete extension
Reject reason	8		C	Provided if key delete extension type = (00000000), reject
Address extension (see note 2)	24	2	O	
NOTE 1: The address extension element shall be present only if the network code for which the deleted key relates is different to the serving network. NOTE 2: If the MS sets key delete type = 001, members of a KAG, the MS shall indicate that all other SCKNs in other subsets that correspond with the SCKN listed in this PDU have been deleted.				

A.4b PDUs to obtain Air Interface Key Status

A.4b.1 D-OTAR KEY STATUS DEMAND

Shall be used by the SwMI to discover the current numbers and versions of air interface keys held by an MS by means of a status enquiry. May be used to allow a SwMI to maintain a record of the MS keying state without needing to explicitly update the MS with new key material to force a response.

- Direction: SwMI to MS;
- Service used: MM;
- Response to: none;
- Response expected: U-OTAR KEY STATUS RESPONSE or none.

Table A.27e: D-OTAR KEY STATUS DEMAND contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	Key Status Demand
Acknowledgement flag	1	1	M	If "0" No acknowledgement required
				If "1" Acknowledgement required
Explicit response (see note 1)	1	1	M	If "0" MS shall respond if state changes If "1" MS shall always respond
Max response timer value	16	1	M	Identifies the maximum period over which the MS will randomly choose to respond
Key status type	3	1	M	
SCKN	5		C	If Key status type = (000), SCK/SCKX
SCK subset grouping type	4		C	If Key status type = (001), SCK subset
SCK subset number	5		C	If Key status type = (001), SCK subset
GCKN	16		C	If Key status type = (011), GCK/GCKX
Address extension (see note 2)	24	2	O	

NOTE 1: The "explicit response" element is only valid if "Acknowledgment flag" is set to "1".

NOTE 2: The address extension element shall be present only if the network code for which the requested key relates is different to the serving network.

A.4b.2 U-OTAR KEY STATUS RESPONSE

Shall be used by the MS to respond to the SwMI's request to report the current numbers and versions of air interface keys held by the MS.

- Direction: MS to SwMI;
- Service used: MM;
- Response to: D-OTAR KEY STATUS DEMAND;
- Response expected: none.

Table A.27f: U-OTAR KEY STATUS RESPONSE contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub-type	4	1	M	Key Status Response
Key status type	3	1	M	
SCK subset grouping type	4		C	Provided if key status type = (001), SCK subset
SCK subset number	5		C	Provided if key status type = (001), SCK subset
Number of SCK status	6		C	Provided if key status type = (000, 001 or 010), SCK/SCKX, SCK subset or all SCKs/SCKXs
SCK data	21		C	Provided if key status type = (000, 001 or 010), SCK/SCKX, SCK subset or all SCKs/SCKXs; repeated element
Number of GCK status	5		C	Provided if key status type = (011 or 100), GCK/GCKX or all GCKs/GCKXs
GCK data	32		C	Provided if key status type = (011 or 100), GCK/GCKX or all GCKs/GCKXs; repeated element
Number of GSKO status	2		C	Provided if key status type = (101), GSKO/GSKOX
GSKO-VN	16		C	Provided if key status type = (101), GSKO/GSKOX, repeated element
Reject reason	8		C	Provided if key status type = (110), Reject
Address extension (see note 4)	24	2	O	
NOTE 1: The number of "SCK data" elements following the "Number of SCK status" element shall be the same as the value of the "Number of SCK status" element. If MS has no SCKs/SCKXs, or does not have the requested SCK/SCKX, no "SCK data" elements shall be sent. NOTE 2: The number of "GCK data" elements following the "Number of GCK status" element shall be the same as the value of the "Number of GCK status" element. If the MS has no GCKs/GCKXs, or does not have the requested GCK/GCKX, no "GCK data" elements shall be sent. NOTE 3: The number of "GSKO-VN" elements following the "Number of GSKO status" element shall be the same as the value of the "Number of GSKO status" element. If the MS has no GSKOs/GSKOXs, no "GSKO-VN" elements shall be sent. NOTE 4: The address extension element shall be present only if the network code for which the requested key relates is different to the serving network.				

A.5 Other security domain PDUs

A.5.1 U-TEI PROVIDE

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

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

Table A.28: U-TEI PROVIDE PDU contents

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

A.5.2 U-OTAR PREPARE

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

- Direction: MS to SwMI;
- Service used: MM;
- Response to: none;
- Response expected: D-OTAR NEWCELL or D-OTAR NEWCELL-X.

Table A.29: U-OTAR PREPARE

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

A.5.3 D-OTAR NEWCELL

Shall be used by SwMI to inform the MS of the result of the U-OTAR PREPARE exchange and may provide one or more sealed CCKs.

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR PREPARE;
- Response expected: none.

Table A.30: D-OTAR NEWCELL

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

A.5.3a D-OTAR NEWCELL-X

Shall be used by SwMI to inform the MS of the result of the U-OTAR PREPARE exchange, and may provide one or more sealed CCKs or CCKXs.

- Direction: SwMI to MS;
- Service used: MM;
- Response to: U-OTAR PREPARE;
- Response expected: none.

Table A.30a: D-OTAR NEWCELL-X

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub-type	4	1	M	OTAR extension
OTAR extension	4	1	M	OTAR NEWCELL-X
DCK Forwarding Result	1	1	M	
CCK provision flag	1	1	M	
KSG number	4		C	If CCK provision flag is true
CCK identifier (CCK-id)	16		C	Provided if CCK provision flag = 1
Key type flag	1		C	Provided if CCK provision flag = 1 0 = Current, 1 = Future
Sealed CCK (SCCK)	120		C	Provided if KSG number element has value 0000_2 - 0011_2
Sealed CCKX (SCCKX)	224		C	Provided if KSG number element has value 0100_2 - 0110_2
CCK location area information	2-216		C	Provided if CCK provision flag = 1 Applies to both current and future key (if provided)
Future key flag	1		C	Provided if CCK provision flag = 1 Always 0 if Key type flag = 1
Sealed CCK (SCCK)	120		C	Provided if Future key flag = 1 and KSG number element has value 0000_2 - 0011_2
Sealed CCKX (SCCKX)	224		C	Provided if Future key flag = 1 and KSG number element has value 0100_2 - 0110_2
Proprietary element		3	O	

A.5.4 D-OTAR CMG GTSI PROVIDE

Shall be used by SwMI to provide a GSSI or GTSI to be used for group addressed OTAR functions.

- Direction: SwMI to MS;
- Service used: MM;
- Response to: none;
- Response expected: U-OTAR CMG GTSI RESULT or none.

Table A.30b: D-OTAR CMG GTSI PROVIDE contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	D-OTAR
OTAR sub type	4	1	M	CMG GTSI PROVIDE
GSSI	24	1	M	
Address extension (see note)	24	2	O	
NOTE: The address extension element is only present if the network code for which the provided GSSI relates is different to the serving network.				

A.5.5 U-OTAR CMG GTSI RESULT

Shall be used by MS to indicate successful reception of a GSSI or GTSI to be used to receive group addressed OTAR functions.

- Direction: MS to SwMI;
- Service used: MM;
- Response to: D-OTAR CMG GTSI PROVIDE;
- Response expected: none.

Table A.30c: U-OTAR CMG GTSI RESULT contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U-OTAR
OTAR sub type	4	1	M	CMG GTSI RESULT
GSSI	24	1	M	
Address extension (see note)	24	2	O	
NOTE: The address extension element is only present if the network code for which the provided GSSI relates is different to the serving network.				

A.5.6 U-INFORMATION PROVIDE

Shall be used by MS-MM to inform the SwMI of version number and other information.

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

Table A.30d: U-INFORMATION PROVIDE PDU contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	U- Information Provide
Information Provide PDU sub-type	4	1	M	0000_2 = Version information provision
SSI	24	1	M	
Address extension present	1	1	M	
Address extension	24		C	Present if "Address extension" = 1
TEI present	1	1	M	
TEI	60		C	Present if "TEI present" = 1
Model number information present	1	1	M	
Model number information length	8		C	Length of "Model number information" element in bytes Note 1, note 2
Model number information	Varies		C	Note 1, note 3
HW version information present	1	1	M	
HW version information length	8		C	Length of "HW version information" element in bytes Note 4, note 2
HW version information	Varies		C	Note 4, note 3
SW version information present	1	1	M	
SW version length	8		C	Length of "SW version information" element in bytes Note 5, note 2
SW version information	Varies		C	Note 5, note 3
AI algorithm information present	1	1	M	
Number of KSGs present	4		C	Note 6
KSG Number	4		C	This element is repeated according to the " Number of KSGs present " value. Note 6
Additional information present	1	1	M	
Additional information length	8		C	Length of "Additional information" element in bytes Note 7, note 2
Additional information	Varies		C	Note 7, note 3
Further information follows	1	1	M	Set to 0 if the only PDU, or last PDU sent. Set to 1 if further Information Provide PDUs follow
Future information present	1	1	M	The value of "Future Information" shall be zero in the present document. A BS receiving a value of 1 shall discard the remainder of the PDU
Proprietary element		3	O	The proprietary element can only be present in the present document if the 'Future information present' element is set to zero

NOTE 1: Present if "Model number information present" = 1.
NOTE 2: Valid element values 1-63; value of 0 is reserved.
NOTE 3: Format of information shall be 8 bit ASCII text. The content is outside the scope of the present document.
NOTE 4: Present if "HW version information present" = 1.
NOTE 5: Present if "SW version information present" = 1.
NOTE 6: Present if "AI algorithm information present" = 1.
NOTE 7: Present if "Additional information present" = 1.

A.6 PDUs for Enable and Disable

A.6.1 D-DISABLE

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

- Direction: SwMI to MS;
- Service used: MM;
- Response to: -;
- Response expected: U-DISABLE STATUS or U-AUTHENTICATION RESPONSE.

Table A.31: D-DISABLE contents

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

A.6.2 D-ENABLE

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

- Direction: SwMI to MS;
- Service used: MM;
- Response to: -;
- Response expected: U-DISABLE STATUS or U-AUTHENTICATION RESPONSE.

Table A.32: D-ENABLE contents

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

A.6.3 U-DISABLE STATUS

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

- Direction: MS to SwMI;
- Service used: MM;
- Response to: D-DISABLE or D-ENABLE;
- Response expected: none.

Table A.33: U-DISABLE STATUS contents

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

A.7 MM PDU type 3 information elements coding

A.7.0 General

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

A.7.1 Authentication downlink

This type 3 element shall be appended to D-LOCATION UPDATE ACCEPT to inform the MS about the result of an authentication procedure which has been combined with registration and/or to request that an MS supplies its TEI and/or to supply the MS with CCK information (class 3) or SCK information (class 2) for the cell to which it is registering.

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

Table A.34: Authentication downlink element contents

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

A.7.2 Authentication uplink

This type 3 element shall be appended to U-LOCATION UPDATE DEMAND when the MS combines a registration request with a request to authenticate the SwMI or when the MS requests the CCK (class 3) or SCK (class 2) information for the cell to which it is registering.

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

Table A.35: Authentication uplink element contents

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

A.7.3 Security 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 version numbering and/or other information related to the MS. This element may also supply the MS with one or more sealed CCKs or CCKXs (class 3 operation), and may supply the MS with one or more sealed SCKs or SCKXs (class 2 operation).

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

Table A.35a: Security downlink element contents

Information element	Length	Type	C/O/M	Remark
Authentication result [R1]	1	1	M	Only valid for authentication exchanges
TEI request flag	1	1	M	
Model number information request flag	1	1	M	
HW SW version request flag	1	1	M	
AI algorithm information request flag	1	1	M	
Additional security	1	1	M	See note 1
CK provision flag	1		C	Provided if Additional security=1
KSG number	4		C	Provided if CK provision flag = 1
SCK provision flag	1		C	Provided if CK provision flag = 1
Session key	1		C	Provided if SCK provision flag = 1 Identifies if encrypted with group or individual encryption session key
Random seed for OTAR	80		C	Provided if session key for individual
GSKO-VN	16		C	Provided if session key for group
SCK Number (SCKN)	5		C	Provided if SCK provision flag = 1
SCK version number (SCK-VN)	16		C	Provided if SCK provision flag = 1
Sealed SCK (SSCK)	120		C	Provided if SCK provision flag = 1 and KSG number element has value 0000_2 - 0011_2
Sealed SCKX (SSCKX)	224		C	Provided if SCK provision flag = 1 and KSG number element has value 0100_2 - 0110_2
Future key flag for SCK	1		C	Provided if SCK provision flag = 1
SCK Number (SCKN)	5		C	Provided if future key flag for SCK = 1
SCK version number (SCK-VN)	16		C	Provided if future key flag for SCK = 1
Sealed SCK (SSCK)	120		C	Provided if future key flag for SCK = 1 and KSG number element has value 0000_2 - 0011_2
Sealed SCKX (SSCKX)	224		C	Provided if future key flag for SCK = 1 and KSG number element has value 0100_2 - 0110_2
CCK provision flag	1		C	Provided if CK provision flag = 1
CCK identifier (CCK-id)	16		C	Provided if CCK provision flag = 1
Key type flag	1		C	Provided if CCK provision flag = 1 0 = Current, 1 = Future
Sealed CCK (SCCK)	120		C	Provided if CCK provision flag = 1 and KSG number element has value 0000_2 - 0011_2
Sealed CCKX (SCCKX)	224		C	Provided if CCK provision flag = 1 and KSG number element has value 0100_2 - 0110_2
CCK location area information	2-216		C	Provided if CCK provision flag = 1 Applies to both current and future key (if provided)
Future key flag for CCK	1		C	Provided if CCK provision flag = 1 Always false if Key type flag = 1
Sealed CCK (SCCK)	120		C	Provided if Future key flag for CCK =1 and KSG number element has value 0000_2 - 0011_2
Sealed CCKX (SCCKX)	224		C	Provided if Future key flag for CCK =1 and KSG number element has value 0100_2 - 0110_2
Identity encryption	1		C	Provided if Additional security=1
Reserved	1		C	Provided if Additional security=1 See note 2
NOTE 1: An MS compliant to a version earlier than V4.1.1 of the present document is expected to discard any elements following this element. The SwMI should not send the any elements following this element to an MS that is not known to be compliant to V4.1.1 or later of the present document. NOTE 2: Intended for future expansion. Shall be set to zero in the present document. An MS receiving a non zero value shall discard the remainder of this element.				

A.8 PDU Information elements coding

A.8.0 General

The encoding of the information elements and sub-elements for the PDUs described in clauses A.1 to A.7 are given in the following clauses. The most significant bit of the values shown in the tables is transmitted first.

A.8.1 Acknowledgement flag

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

Table A.36: Acknowledgement flag element contents

Information element	Length	Value	Remark
Acknowledgement flag	1	0_2	No acknowledgement required
		1_2	Acknowledgement required

A.8.1a Additional information present

The Additional information present element is used to indicate whether or not additional information is included in the PDU.

Table A.36a: Additional information present element contents

Information element	Length	Value	Remark
Additional information present	1	0_2	Additional information is not included
		1_2	Additional information is included

A.8.1b Additional security

The Additional security element is used to indicate whether or not additional security related information is included in the Security downlink element.

Table A.36b: Additional information present element contents

Information element	Length	Value	Remark
Additional security	1	0_2	Additional security related information is not included
		1_2	Additional security related information is included

A.8.2 Address extension

The Address Extension Element is defined in ETSI EN 300 392-2 [2], clause 16.10.1.

A.8.2a AI algorithm information present

The AI algorithm information present element is used to indicate whether or not AI algorithm information is included in the PDU.

Table A.36c: AI algorithm information present element contents

Information element	Length	Value	Remark
AI algorithm information present	1	0	AI algorithm information is not included
		1	AI algorithm information is included

A.8.2b AI algorithm information request flag

The AI algorithm information request flag element is used to request the list of AI algorithms contained in the MS.

Table A.36d: AI algorithm information request flag element contents

Information element	Length	Value	Remark
AI algorithm information request flag	1	0	AI algorithm information is not requested
		1	AI algorithm information is requested

A.8.3 Authentication challenge

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

Table A.37: Authentication challenge element contents

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

A.8.4 Authentication reject reason

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

Table A.38: Authentication reject reason element contents

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

A.8.5 Authentication result

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

Table A.39: Authentication result element contents

Information element	Length	Value	Remark
Authentication Result [R1 or R2]	1	0_2	Authentication failed
		1_2	Authentication successful or no authentication currently in progress

A.8.6 Authentication sub-type

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

Table A.40: Authentication sub-type element contents

Information element	Length	Value	Remark
Authentication sub-type (uplink)	2	00_2	U-AUTHENTICATION DEMAND
		01_2	U-AUTHENTICATION RESPONSE
		10_2	U-AUTHENTICATION RESULT
		11_2	U-AUTHENTICATION REJECT
Authentication sub-type (downlink)	2	00_2	D-AUTHENTICATION DEMAND
		01_2	D-AUTHENTICATION RESPONSE
		10_2	D-AUTHENTICATION RESULT
		11_2	D-AUTHENTICATION REJECT

A.8.7 CCK identifier

The CCK identifier (CCK-id) is the numerical value associated with a version number of a Common Cipher Key (CCK or CCKX).

Table A.41: CCK Identifier element contents

Information element	Length	Value	Remark
CCK Identifier	16	Any	

A.8.8 CCK information

The CCK information element is defined as below.

Table A.42: CCK information element contents

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

A.8.9 CCK Location area information

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

Table A.43: CCK Location area information element contents

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

A.8.10 CCK request flag

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

Table A.44: CCK request flag element contents

Information element	Length	Value	Remark
CCK request flag	1	0_2	No CCK/CCKX requested
		1_2	CCK/CCKX requested

A.8.11 Change of security class

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

Table A.45: Change of security class element contents

Information element	Length	Value	Remark
Change of security class	2	00_2	No change of security class
		01_2	Transition to security class 1
		10_2	Transition to security class 2
		11_2	Transition to security class 3

A.8.12 Ciphering parameters

The ciphering parameters information element is used to negotiate SCKN and KSG in class 2 cells, and KSG in class 3 cells. In addition, when registering for SC3 operation, the MS shall indicate its support for TM-SCK OTAR, SDMO and DM-SCK OTAR, and GCK/GCKX encryption/OTAR.

Table A.46: Ciphering parameters information element contents

Information sub-element	Length	Type	C/O/M	Remark
KSG number	4	1	M	

Security class	1	1	M	Value = 0 for class 2
				Value = 1 for class 3

SCK number	5		C	Provided if class 2

TM-SCK/SCKX OTAR
(see note 1, note 2)
	1		C	Provided if class 3:
				Value = 0 if not supported
				Value = 1 if supported

SDMO and DM-SCK/SCKX OTAR
(see note 1, note 2)
	1		C	Provided if class 3:
				Value = 0 if not supported
				Value = 1 if supported

GCK/GCKX encryption/OTAR
(see note 1, note 2)
	1		C	Provided if class 3:
				Value = 0 if not supported
				Value = 1 if supported

Security information protocol support (see note 1)	1		C	Provided if class 3: Value 0 if not supported Value 1 if supported
SCK OTAR while using TEA set B (see note 2)	1		C	Provided if class 3: Value 0 if MS registers with a KSG in TEA set A Value 0 if MS registers with a KSG in TEA set B, and OTAR of SCK is not supported Value 1 if MS registers with a KSG in TEA set B, and OTAR of SCK is supported
NOTE 1: These elements only have meaning on the uplink. On the downlink these fields shall be set to value "0". NOTE 2: These elements indicate support for the described function using the negotiated algorithm only.				

A.8.13 CK provision flag

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

Table A.47: CK provision flag element contents

Information element	Length	Value	Remark
CK provision flag	1	0_2	No CK information provided (FALSE)
		1_2	CK information provided (TRUE)

A.8.14 CK provision information

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

Table A.48: CK provision information element contents

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

A.8.15 CK request flag

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

Table A.49: CK request flag element contents

Information element	Length	Value	Remark
CK request flag	1	0_2	No CK/CKX requested
		1_2	CK/CKX requested

A.8.16 Class Change flag

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

Table A.50: Class Change flag element contents

Information element	Length	Value	Remark
Class Change flag	1	0_2	No Class change
		1_2	Class change

A.8.17 DCK forwarding result

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

Table A.51: DCK forwarding result element contents

Information element	Length	Value	Remark
DCK Forwarding Result	1	0_2	DCK/DCKX forwarding failure
		1_2	DCK/DCKX forwarding successful

A.8.18 Disabling type

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

Table A.52: Disabling Type element contents

Information element	Length	Value	Remark
Disabling Type	1	0_2	Temporary
		1_2	Permanent

A.8.19 Enable/Disable result

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

Table A.53: 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 mismatch
		010_2	Enable/disable failure, TEI mismatch
		011_2	Enable/disable failure, TEI and address mismatch
		100_2	Enable/disable failure, authentication is required
		101_2	Enable/disable failure, encryption is required
		110_2	Enable/disable failure, encryption and authentication are required
		111_2	Enable/disable failure, authentication not supported

A.8.20 Encryption mode

A.8.20.1 Class 1 cells

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

Table A.54: Encryption mode element in class 1 cell contents

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

A.8.20.2 Class 2 cells

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

Table A.55: Encryption mode element in class 2 cell contents

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

A.8.20.3 Class 3 cells

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

Table A.56: Encryption mode element in class 3 cell contents

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

A.8.21 Equipment disable

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

Table A.57: Equipment disable element contents

Information element	Length	Value	Remark
Equipment disable	1	0_2	Equipment not to be disabled
		1_2	Equipment to be disabled

A.8.22 Equipment enable

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

Table A.58: Equipment enable element contents

Information element	Length	Value	Remark
Equipment enable	1	0_2	Equipment not to be enabled
		1_2	Equipment to be enabled

A.8.23 Equipment status

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

Table A.59: 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

A.8.23a Explicit response

The purpose of the explicit response element is to indicate whether the MS is required to acknowledge a key provision or key association explicitly, or conditionally on whether the transaction changes the MS state and provides a key, key version or key association that it did not already have.

Table A.59a: Explicit response element contents

Information element	Length	Value	Remark
Explicit response	1	0_2	Response to be sent only if state of MS is changed
		1_2	Response to be sent whether state changed or not

A.8.24 Frame number

Refer to ETSI EN 300 392-2 [2], clause 16.10.11.

A.8.24a Future information present

The Future information present element is used to indicate whether or not Future information is included in the PDU.

Table A.59b: Future information present element contents

Information element	Length	Value	Remark
Future information present	1	0_2	Future information is not included
		1_2	Reserved

A.8.25 Future key flag

The future key flag information element is defined in Table A.60.

Table A.60: Future key flag information element contents

Information element	Length	Value	Remark
Future key flag	1	0_2	Indicates that no future key data is provided
		1_2	Indicates that future key data is provided

A.8.26 GCK data

The GCK data information element is defined in Table A.61. It may apply to GCK or GCKX.

Table A.61: GCK data information element contents

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

A.8.27 GCK key and identifier

The GCK key and identifier element is defined as in Table A.62.

Table A.62: GCK key and identifier element contents

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

A.8.27a GCKX key and identifier

The GCKX key and identifier element is defined as in Table A.62a.

Table A.62a: GCKX key and identifier element contents

Information element	Length	Type	C/O/M	Remark
GCKN	16	1	M	
GCK version number	16	1	M	
Sealed GCKX (SGCKX)	224	1	M	

A.8.28 GCK Number (GCKN)

The GCKN is the identifier for a GCK used to associate it to one or more groups. It also identifies the session key modifier for migration (GCK0 or GCKX0).

Table A.63: GCKN element contents

Information element	Length	Value	Remark
GCKN	16	0	GCK0/GCKX0, session key modifier for migration
		00000001_2 to 11111111_2	GCK number

A.8.28a GCK Provision result

The GCK provision result indicates the result when provisioning a GCK or GCKX using OTAR.

Table A.63a: GCK Provision Result

Information element	Length	Type	C/O/M	Remark
GCK data	32	1	M	
Provision result (GCK)	3	1	M	
Current GCK Version number	16		C	Defined as GCK-VN and sent when provision result has value incorrect key-VN

A.8.28b GCK rejected

The GCK rejected element is defined in Table A.63b, and indicates the reason for rejection to supply a requested GCK or GCKX.

Table A.63b: GCK rejected element contents

Information element	Length	Type	C/O/M	Remark
OTAR reject reason	3	1	M	
Group association	1	1	M	
GCKN	16		C	If Group association = GCKN
GSSI	24		C	If Group association = GSSI

A.8.29 GCK select number

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

Table A.64: GCK select number element contents

Information element	Length	Value	Remark
GCK select number	17	0 to (2^{16}- 1)	GCK number (GCKN) selected
		2^{16}	No GCKN selected (see note)
		(2^{16} + 1) to (2^{17} - 1)	Reserved
NOTE: The value of "No GCKN selected" shall be used to disassociate a GCK/GCKX from an address and return the association for that address to CCK/CCKX, as described in clause 4.5.4.2.			

A.8.29a GCK Supported

The GCK Supported information element is found in the SYSINFO, SYSINFO-DA or SYSINFO-Q broadcast message and indicates to the MS whether or not GCKs or GCKXs are supported on the current cell.

Table A.64a: GCK Supported information element in SYSINFO, SYSINFO-DA or SYSINFO-Q

Information element	Length	Value	Remark
GCK Supported	1	0	GCK/GCKX not supported on this cell
(see note)		1	GCK/GCKX supported on this cell
NOTE: If the "Air interface encryption service" element in the BS service details element contained in the D-MLE SYSINFO, D-MLE SYSINFO-Q and D-NWRK-BROADCAST PDUs, and in the "BS service details DA" element in the D-MLE SYSINFO-DA and D-NWRK-BROADCAST-DA PDUs is set to value 0, "Service is not available on this cell", then the value of this element has no meaning. This element is only valid if the security information element in the SYSINFO, SYSINFO-DA or SYSINFO-Q PDUs, sub-element "Security class 2 or 3" is set to "Security class 3 is supported on this cell".			

A.8.30 GCK Version Number (GCK-VN)

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

Table A.65: GCK-VN element contents

Information element	Length	Value	Remark
GCK-VN	16	any	

A.8.31 Group association

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

Table A.66: Group association element contents

Information element	Length	Value	Remark
Group association	1	0_2	Associated with GCKN
		1_2	Associated with specific GSSI

A.8.31a Group Identity Security Related Information

The group identity security related information indicates the association of cipher keys to group identity.

Table A.66a: Group Identity Security Related Information Element

Information element	Length	Type	C/O/M	Value	Remark
Number of groups	5	1	M		Indicates the number of GSSI corresponding to the given key association that follows.
GSSI	24		C		Shall be present as many times as indicated in the "Number of groups" value.
GCK Association	1	1	M	0_2 1_2	GCK association information not provided. GCK association information provided.
GCK Select Number	17		C		Provided if GCK Association indicates "GCK Association Information Provided"
SCK Association	1	1	M	0_2 1_2	SCK association information not provided. SCK association information provided.
SCK Subset Grouping Type	4		C		Provided if SCK Association indicates "SCK Association Information Provided".
SCK Subset Number	5		C		Provided if SCK Association indicates "SCK Association Information Provided".

A.8.32 GSKO Version Number (GSKO-VN)

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

Table A.67: GSKO Version Number (GSKO-VN) element contents

Information element	Length	Value	Remark
GSKO-VN	16	any	

A.8.33 GSSI

See ETSI EN 300 392-1 [1], clause 7.

A.8.33a HW SW version request flag

This bit indicates whether the MS should supply hardware or software version or other security related information.

Table A.67a: HW SW version request flag contents

Information element	Length	Value	Remark
HW SW version request flag	1	0_2	HW SW version number information is not requested
		1_2	HW SW version number information is requested

A.8.33b HW version number present

The HW version number present element is used to indicate whether or not the HW version number is included in the PDU.

Table A.67b: HW version number present element contents

Information element	Length	Value	Remark
HW version number present	1	0_2	HW version number is not included
		1_2	HW version number is included

A.8.34 Hyperframe number

Refer to ETSI EN 300 392-2 [2].

A.8.34a Identity encryption

The purpose of the Identity encryption element is to indicate to an MS negotiating a KSG from TEA set B whether to use ESI identity encryption or MAE address encryption.

Table A.67c: Identity encryption element contents

Information element	Length	Value	Remark
Identity encryption	1	0_2	If KSG from TEA set B is in use, shall use MAE address encryption
		1_2	If KSG from TEA set B is in use, shall use ESI identity encryption
NOTE: If a KSG from TEA set A is in use, this element shall be set to 0 and ESI identity encryption shall be used.			

A.8.35 Intent/confirm

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

Table A.68: Intent/confirm element contents

Information element	Length	Value	Remark
Intent/confirm	1	0_2	Intent
		1_2	Confirm

A.8.36 Void

A.8.37 Key association status

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

Table A.69: Key association result element contents

Information element	Length	Value	Remark
Key association status	3	000_2	Association carried out as requested
		001_2	Key not valid
		010_2	Address not valid
		011_2	Association rejected
		Others	Reserved

A.8.38 Key association type

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

Table A.70: Key association type information element contents

Information element	Length	Value	Remark
Key association type	1	0_2	SCK/SCKX
		1_2	GCK/GCKX

A.8.39 Key change type

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

Table A.71: Key change type information element contents

Information element	Length	Value	Remark
Key change type	3	000_2	SCK/SCKX
		001_2	CCK/CCKX
		010_2	GCK/GCKX
		011_2	Class 3 CCK(X) and GCK(X) activation
		100_2	All GCKs/GCKXs
		101_2	No cipher key
		110_2	Reserved
		111_2	Reserved

A.8.39a Key delete type

Key delete type identifies the type of key and organization of keys, where applicable, to be deleted by the D-OTAR KEY DELETE DEMAND PDU.

Table A.71a: Key delete type information element contents

Information element	Length	Value	Remark
Key delete type	3	000_2	Individual SCK(s)/SCKX(s)
		001_2	Members of a KAG
		010_2	SCK subset
		011_2	All SCKs/SCKXs
		100_2	Individual GCK(s)/GCKX(s)
		101_2	All GCKs/GCKXs
		110_2	GSKO/GSKOX
		111_2	Key delete extension

A.8.39b Key status type

Key status type identifies the type of key and organization of keys, where applicable, of which the SwMI is requesting status, or of which the MS is providing the status.

Table A.71b: Key status type information element contents

Information element	Length	Value	Remark
Key status type	3	000_2	Individual SCK(s)/SCKX(s)
		001_2	SCK subset
		010_2	All SCKs/SCKXs
		011_2	Individual GCK(s)/GCKX(s)
		100_2	All GCKs/GCKX(s)
		101_2	GSKO/GSKOX
		110_2	Reject
		111_2	Reserved

A.8.39c Key delete extension

Key delete extension identifies an extended function contained in the Key delete result PDU.

Table A.71c: Key delete extension information element contents

Information element	Length	Value	Remark
Key delete extension	8	00000000_2	Reject
		00000001_2 to 11111111_2	Reserved

A.8.40 Key type flag

Table A.72: Key type flag information element contents

Information element	Length	Value	Remark
Key type flag	1	0_2	Current
		1_2	Future

A.8.41 KSG-number

KSG number identifies the encryption algorithm in use.

Table A.73: KSG Number element contents

Information element	Length	Value	Remark
KSG Number	4	0000_2	TETRA Standard Algorithm, TEA1
		0001_2	TETRA Standard Algorithm, TEA2
		0010_2	TETRA Standard Algorithm, TEA3
		0011_2	TETRA Standard Algorithm, TEA4
		0100_2	TETRA Standard Algorithm, TEA5
		0101_2	TETRA Standard Algorithm, TEA6
		0110_2	TETRA Standard Algorithm, TEA7
		0111_2	Reserved for future expansion
		1000_2 to 1011_2	Proprietary TETRA Algorithms
		1100_2 to 1111_2	Reserved for future expansion See note
NOTE: Prior to V4.1.1 of the present document, values from 1100_2 to 1111_2 were allocated to proprietary algorithms.			

A.8.42 Location area

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

A.8.43 Location area bit mask

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

Table A.74: Location area bit mask element contents

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

A.8.44 Location area selector

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

Table A.75: Location area selector element contents

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

A.8.45 Location area list

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

Table A.76: Location area list element contents

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

A.8.46 Location area range

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

Table A.77: Location area range element contents

Information element	Length	Value	Remark
Low Location Area Value (LLAV)	14	0 to 2^{14}-1	Lowest value of LA-id for which CCK/CCKX is valid
High Location Area Value (HLAV)	14	1 to 2^{14}-1	Highest value of LA-id for which CCK/CCKX is valid
NOTE: HLAV shall always be greater than LLAV.			

A.8.46a Max response timer value

The max response timer value element is used to set the maximum period over which an MS shall randomly choose a response time to a group addressed OTAR, key status or key association command.

Table A.77a: Max response timer value element contents

Information element	Length	Value	Remark
Max response timer value	16	0	Immediate response, for individually addressed transactions
		1 to 2^{16}-1	Value in seconds from 1 to 65 535

A.8.47 Mobile country code

See ETSI EN 300 392-1 [1], clause 7.

A.8.48 Mobile network code

See ETSI EN 300 392-1 [1], clause 7.

A.8.48a Model number information present

The Model number information present element is used to indicate whether or not model number information is included in the PDU.

Table A.77b: Model number information present element contents

Information element	Length	Value	Remark
Model number information present	1	0_2	Model number information is not included
		1_2	Model number information is included

A.8.48b Model number request flag

This bit indicates whether the MS should supply model number version information.

Table A.77c: Model number request flag contents

Information element	Length	Value	Remark
Model number request flag	1	0_2	Model number information is not requested
		1_2	Model number information is requested

A.8.49 Multiframe number

See ETSI EN 300 392-2 [2].

A.8.50 Mutual authentication flag

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

Table A.78: Mutual authentication flag element contents

Information element	Length	Value	Remark
Mutual authentication flag	1	0_2	Mutual authentication elements included = FALSE
		1_2	Mutual authentication elements included = TRUE

A.8.51 Network time

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

A.8.52 Number of GCKs changed

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

Table A.79: Number of GCKs changed element contents

Information element	Length	Value	Remark
Number of GCKs changed	4	0000_2	No GCK/GCKXs changed
		0001_2	1 GCK/GCKX changed
		0010_2	2 GCK/GCKXs changed
		0011_2	3 GCK/GCKXs changed
		0100_2	4 GCK/GCKXs changed
		Others	Etc. up to 15 GCKs/GCKXs changed

A.8.52a Number of GCKs deleted

The Number of GCKs deleted element indicates how many Group Cipher Keys (GCKs or GCKXs) are to be or were deleted by the MS in the OTAR Key Delete protocol.

Table A.79a: Number of GCKs deleted element contents

Information element	Length	Value	Remark
Number of GCKs deleted	5	00000_2	No GCK/GCKXs deleted
		00001_2 to 11111_2	1 to 31 GCK/GCKXs deleted

A.8.52b Number of GCK status

The Number of GCK status element indicates how many group cipher keys' (GCKs or GCKXs) status information are being provided by the MS.

Table A.79b: Number of GCK status element contents

Information element	Length	Value	Remark
Number of GCK status	5	00000_2	MS has no GCK/GCKXs, no GCK data element follows
		00001_2 to 11111_2	1 to 31 GCKs/GCKXs' data is provided

A.8.52c Number of GCKs provided

The Number of GCKs provided element indicates how many group cipher keys (GCKs or GCKXs) there are to follow in the PDU.

Table A.79c: Number of GCKs provided element contents

Information element	Length	Value	Remark
Number of GCKs provided	3	000_2	No GCK/GCKXs provided
		001_2	1 GCK/GCKX provided
		010_2	2 GCK/GCKXs provided
		011_2	3 GCK/GCKXs provided
		100_2	4 GCK/GCKXs provided
		101_2	5 GCK/GCKXs provided
		110_2	6 GCK/GCKXs provided
		111_2	7 GCK/GCKXs provided

A.8.52d Number of GCKs rejected

The Number of GCKs rejected element indicates how many Group Cipher Keys (GCKs or GCKXs) are rejected by the MS.

Table A.79d: Number of GCKs rejected element contents

Information element	Length	Value	Remark
Number of GCKs rejected	3	000_2	Reserved
		001_2	1 GCK/GCKX rejected
		010_2	2 GCK/GCKXs rejected
		011_2	3 GCK/GCKXs rejected
		100_2	4 GCK/GCKXs rejected
		101_2	5 GCK/GCKXs rejected
		110_2	6 GCK/GCKXs rejected
		111_2	7 GCK/GCKXs rejected

A.8.52e Number of GCKs requested by GCKN

The Number of GCKs requested by GCKN element indicates how many Group Cipher Keys (GCKs or GCKXs) are requested by the MS referenced by GCKN.

Table A.79e: Number of GCKs requested by GCKN element contents

Information element	Length	Value	Remark
Number of GCKs requested by GCKN	3	000_2	0 GCK/GCKXs requested
		001_2	1 GCK/GCKX requested
		010_2	2 GCK/GCKXs requested
		011_2	3 GCK/GCKXs requested
		100_2	4 GCK/GCKXs requested
		101_2	5 GCK/GCKXs requested
		110_2	6 GCK/GCKXs requested
		111_2	7 GCK/GCKXs requested

A.8.52f Number of GCKs requested by GSSI

The Number of GCKs requested by GSSI element indicates how many group cipher keys (GCKs or GCKXs) are requested by the MS referenced by GSSI.

Table A.79f: Number of GCKs requested by GSSI element contents

Information element	Length	Value	Remark
Number of GCKs requested by GSSI	3	000_2	0 GCK/GCKXs requested
		001_2	1 GCK/GCKX requested
		010_2	2 GCK/GCKXs requested
		011_2	3 GCK/GCKXs requested
		100_2	4 GCK/GCKXs requested
		101_2	5 GCK/GCKXs requested
		110_2	6 GCK/GCKXs requested
		111_2	7 GCK/GCKXs requested

A.8.53 Number of groups

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

Table A.80: Number of groups element contents

Information element	Length	Value	Remark
Number of groups	5	00000_2	Reserved.
		00001_2 to 11110_2	Number of GSSIs
		11111_2	Range of GSSIs (see notes 1 and 2)
NOTE 1: Range of GSSIs will be indicated by a lower and a higher value. NOTE 2: Value 11111 is not valid when used in U-OTAR Key Associate Status PDU and when used in Group Identity Security Related Information Element.			

A.8.53a Number of GSKO status

The Number of GSKO status element indicates how many group session keys for OTARs' (GSKOs' or GSKOXs') status information are being provided by the MS.

Table A.80a: Number of GSKO status element contents

Information element	Length	Value	Remark
Number of GSKO status	2	00_2	MS has no GSKO/GSKOX, no GSKO/GSKOX data element follows
		01_2 to 11_2	1 to 3 GSKO/GSKOXs' data is provided

A.8.53b Number of KSGs present

The Number of KSGs present element indicates how many air interface encryption algorithms are present in the MS.

Table A.80b: Number of KSGs present element contents

Information element	Length	Value	Remark
Number of KSGs present	4	0000_2	Reserved
		0001_2	1 KSG present
		0010_2	2 KSGs present
		...	
		1111_2	15 KSGs present

A.8.54 Number of location areas

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

Table A.81: 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

A.8.55 Number of SCKs changed

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

Table A.82: Number of SCKs changed element contents

Information element	Length	Value	Remark
Number of SCKs changed	4	0000_2	No SCK/SCKXs changed
		0001_2	1 SCK/SCKX changed
		0010_2	2 SCK/SCKXs changed
		0011_2	3 SCK/SCKXs changed
		0100_2	4 SCK/SCKXs changed
		0101_2 to 1111_2	5 to 15 SCK/SCKXs changed

A.8.55a Number of SCKs deleted

The Number of SCKs deleted element indicates how many static cipher keys (SCKs or SCKXs) are to be or were deleted by the MS in the OTAR Key Delete protocol.

Table A.82a: Number of SCKs deleted element contents

Information element	Length	Value	Remark
Number of SCKs deleted	5	00000_2	No SCKs deleted
		00001_2 to 11111_2	1 to 31 SCK/SCKXs deleted

A.8.56 Number of SCKs provided

The Number of SCKs provided element indicates how many Static Cipher Keys (SCKs or SCKXs) there are to follow in the PDU.

Table A.83: 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/SCKX provided
		010_2	2 SCK/SCKXs provided
		011_2	3 SCK/SCKXs provided
		100_2	4 SCK/SCKXs provided
		101_2	5 SCK/SCKXs provided
		110_2	6 SCK/SCKXs provided
		111_2	7 SCK/SCKXs provided

A.8.56a Number of SCKs rejected

The Number of SCKs rejected element indicates how many Static Cipher Keys (SCKs or SCKXs) there are to follow in the PDU.

Table A.83a: Number of SCKs rejected element contents

Information element	Length	Value	Remark
Number of SCKs rejected	3	000_2	No SCK/SCKXs rejected
		001_2	1 SCK/SCKX rejected
		010_2	2 SCK/SCKXs rejected
		011_2	3 SCK/SCKXs rejected
		100_2	4 SCK/SCKXs rejected
		101_2	5 SCK/SCKXs rejected
		110_2	6 SCK/SCKXs rejected
		111_2	7 SCK/SCKXs rejected

A.8.57 Number of SCKs requested

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

Table A.84: Number of SCKs requested element contents

Information element	Length	Value	Remark
Number of SCKs requested	3	000_2	Reserved
		001_2	1 SCK/SCKX requested
		010_2	2 SCK/SCKXs requested
		011_2	3 SCK/SCKXs requested
		100_2	4 SCK/SCKXs requested
		101_2	5 SCK/SCKXs requested
		110_2	6 SCK/SCKXs requested
		111_2	7 SCK/SCKXs requested

A.8.57a Number of SCK status

The Number of SCK status element indicates how many Static Cipher Keys' (SCKs' or SCKXs') status information are being provided by the MS.

Table A.84a: Number of SCK status element contents

Information element	Length	Value	Remark
Number of SCK status	6	000000_2	MS has no SCK/SCKXs, no SCK data element follows
		000001_2 to 100000_2	1 to 32 SCK/SCKXs' data is provided
		100001_2 to 111111_2	Reserved

A.8.57b OTAR reject reason

The OTAR reject reason element indicates the reason that the SwMI does not supply the requested key.

Table A.84b: OTAR reject reason element contents

Information element	Length	Value	Remark
OTAR reject reason	3	000_2	Key not available
		001_2	Invalid key number
		010_2	Invalid address
		011_2	KSG number not supported
		Others	Reserved

A.8.57c OTAR retry interval

The OTAR retry interval information element indicates how many hyperframes the MS shall wait before retrying an OTAR Demand for SCK, GSKO or GCK.

Table A.84c: OTAR retry interval element contents

Information element	Length	Value	Remark
OTAR retry interval	3	000_2	Do not retry
		001_2	Wait 1 hyperframe
		010_2	Wait 2 hyperframes
		011_2	Wait 4 hyperframes
		100_2	Wait 8 hyperframes
		101_2	Wait 16 hyperframes
		110_2	Wait 32 hyperframes
		111_2	Wait 64 hyperframes

A.8.58 OTAR sub-type

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

Table A.85: OTAR sub-type element contents

Information element	Length	Value	Remark
OTAR sub-type	4	0000_2	CCK Demand (uplink) or CCK Provide (downlink)
		0001_2	CCK Result (uplink) or CCK Reject (downlink)
		0010_2	SCK Demand (uplink) or SCK Provide (downlink)
		0011_2	SCK Result (uplink) or SCK Reject (downlink)
		0100_2	GCK Demand (uplink) or GCK Provide (downlink)
		0101_2	GCK Result (uplink) or GCK Reject (downlink)
		0110_2	Key associate Demand (downlink) or Key associate Status (uplink)
		0111_2	OTAR Prepare (Uplink) or OTAR NEWCELL (downlink)
		1000_2	GSKO Demand (uplink) or GSKO Provide (downlink)
		1001_2	GSKO Result (uplink) or GSKO Reject (downlink)
		1010_2	Key delete demand (downlink) or Key delete result (uplink)
		1011_2	Key status demand (downlink) or Key status response (uplink)
		1100_2	CMG GTSI provide (downlink) or CMG GTSI result (uplink)
		1101_2	DM SCK Activate (downlink) or DM SCK Activate result (uplink)
		1110_2	Reserved
		1111_2	OTAR extension

A.8.58a OTAR extension

The OTAR extension element indicates whether the PDU is used to provide sealed CCKX, SCKX, GCKX or GSKOX, or to transfer a key.

Table A.85a: OTAR extension element contents

Information element	Length	Value	Remark
OTAR sub-type	4	0000_2	Reserved (uplink) or CCKX Provide (downlink)
		0001_2	Reserved (uplink) or SCKX Provide (downlink)
		0010_2	Reserved (uplink) or GCKX Provide (downlink)
		0011_2	Reserved (uplink) or GSKOX Provide (downlink)
		0100_2	Reserved (uplink) or D-OTAR NEWCELL-X (downlink)
		0101_2 to 1111_2	Reserved

A.8.59 PDU type

The PDU type indicates the MM PDU type for all the security PDUs including the authentication and OTAR PDUs. The PDU types in Table A.86 are taken from the unused or security-reserved values of PDU type in the MM protocol. For more details, see ETSI EN 300 392-2 [2], clause 16.

Table A.86: 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
		0110_2		U-INFORMATION PROVIDE
		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 ETSI EN 300 392-2 [2], clause 16.10.39.

A.8.60 Proprietary

See ETSI EN 300 392-2 [2], clause 14.8.35.

A.8.61 Provision result

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

Table A.87: 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 key number (e.g. SCKN, GCKN)
		011_2	OTAR rejected
		100_2	Incorrect Key version number (e.g. SCK-VN, GCK-VN, CCK-id)
		101_2	Identified GSKO-VN not present
		110_2	KSG number not supported
		Others	Reserved

A.8.62 Random challenge

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

Table A.88: Random challenge element contents

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

A.8.63 Random seed

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

Table A.89: Random seed element contents

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

A.8.64 Random seed for OTAR

The random seed for OTAR (RSO) is an 80-bit number used as the input to the session key for OTAR generation algorithm when sealing GCK/GCKX, GSKO/GSKOX and SCK/SCKX. Only one random seed is used per D-OTAR PDU, irrespective of the number of keys contained in the PDU. It is only provided from SwMI to MS.

Table A.90: Random seed element contents

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

A.8.65 Void

Table A.91: Void

A.8.65a Reject reason

Reject reason identifies the reason for rejection of a request.

Table A.91a: Reject reason information element contents

Information element	Length	Value	Remark
Reject reason	8	00000000_2	Invalid MNI
		00000001_2 to 11111111_2	Reserved

A.8.66 Response value

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

Table A.92: Response value element contents

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

A.8.67 SCK data

The SCK data information element is defined in Table A.93. It may apply to SCK or SCKX.

Table A.93: SCK data information element contents

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

A.8.68 SCK information

The SCK information element is defined in Table A.94.

Table A.94: SCK information element contents

Information element	Length	Type	C/O/M	Remark
Session key	1	1	M	Identifies if encrypted with group or individual encryption session key
Random seed for OTAR	80		C	Provided if session key for individual
GSKO-VN	16		C	Provided if session key for group
SCK Number (SCKN)	5	1	M	
SCK version number (SCK-VN)	16	1	M	
Sealed SCK (SSCK)	120	1	M	
Future key flag	1	1	M	
SCK Number (SCKN)	5		C	If future key flag = true
SCK version number (SCK-VN)	16		C	If future key flag = true
Sealed SCK (SSCK)	120		C	If future key flag = true

A.8.69 SCK key and identifier

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

Table A.95: SCK key and identifier element contents

Information element	Length	Type	C/O/M	Remark
SCKN	5	1	M	
SCK version number (SCK-VN)	16	1	M	
SCK use	1	1	M	If "0" Trunked Mode Operation If "1" Direct Mode Operation
Reserved	1	1	M	For future expansion
Sealed key (SSCK)	120	1	M	

A.8.69a SCKX key and identifier

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

Table A.95a: SCKX key and identifier element contents

Information element	Length	Type	C/O/M	Remark
SCKN	5	1	M	
SCK version number (SCK-VN)	16	1	M	
SCK use	1	1	M	If "0" Trunked Mode Operation If "1" Direct Mode Operation
Reserved	1	1	M	For future expansion
Sealed key (SSCKX)	224	1	M	

A.8.70 SCK Number (SCKN)

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

Table A.96: 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
		11101_2	SCK number 30
		11110_2	Class 2: SCK number 31; Class 3: fallback SCK or SCKX number 31
		11111_2	Class 2: SCK number 32; Class 3: fallback SCK or SCKX number 32

A.8.71 SCK number and result

The SCK number and result contains the result of the SCK/SCKX key transfer for the key identified by the SCK number.

Table A.97: SCK number and result element contents

Information element	Length	Type	C/O/M	Remark
SCK Number (SCKN)	5	1	M	
Provision result (SCK)	3	1	M	
Current SCK Version number	16		C	Defined as SCK-VN and sent when provision result has value incorrect key-VN

A.8.72 SCK provision flag

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

Table A.98: SCK provision flag element contents

Information element	Length	Value	Remark
SCK provision flag	1	0_2	No SCK information provided (FALSE)
		1_2	SCK information provided (TRUE)

A.8.72a Void

Table A.99: Void

A.8.72b SCK rejected

The SCK rejected element is defined as in Table A.99a, and indicates the reason for refusal to provide a requested SCK or SCKX.

Table A.99a: SCK rejected element contents

Information element	Length	Type	C/O/M	Remark
OTAR reject reason	3	1	M	
SCK Number (SCKN)	5	1	M	

A.8.73 SCK select number

The SCK select number is contained in OTAR key associate messages to indicate either which key should be associated with the signalled group(s); or whether no key should be associated and any existing key disassociated. It is also used to indicate which keys have been selected in result PDUs. Where SCKs or SCKXs have been grouped into subsets, association with a single SCK or SCKX shall automatically associate the group or groups with the other corresponding SCK/SCKX members of other subsets. The SCKN selected shall be taken from the first subset only, i.e. the subset with SCKN = 1 as its lowest value.

Table A.100: SCK select number element contents

Information element	Length	Value	Remark
SCK select	6	000000_2 to 011111_2	SCK Number (SCKN) selected
		100000_2	No SCKN selected
		100001_2	SCKN dissociated
		100010_2 to 111111_2	Reserved

A.8.73a SCK subset grouping type

The SCK subset grouping type element is contained in OTAR key associate messages where the SCK set is split into 2 or more subsets. It allows the MS to associate multiple associated SCKs or SCKXs in different SCK subsets with the same group or groups.

Table A.100a: SCK subset grouping type element contents

Information element	Length	Value	Remark
SCK subset grouping type	4	0000_2	SCKs/SCKXs grouped into 1 subset of 30 keys
		0001_2	SCKs/SCKXs grouped into 2 subsets of 15 keys
		0010_2	SCKs/SCKXs grouped into 3 subsets of 10 keys
		0011_2	SCKs/SCKXs grouped into 4 subsets of 7 keys
		0100_2	SCKs/SCKXs grouped into 5 subsets of 6 keys
		0101_2	SCKs/SCKXs grouped into 6 subsets of 5 keys
		0110_2	SCKs/SCKXs grouped into 7 subsets of 4 keys
		0111_2	SCKs/SCKXs grouped into 10 subsets of 3 keys
		1000_2	SCKs/SCKXs grouped into 15 subsets of 2 keys
		1001_2	SCKs/SCKXs grouped into 30 subsets of 1 key
		1010_2	SCK grouping not valid, used to indicate a mismatch in key deletion or subset activation conditions
		1011_2 to 1111_2	Reserved

A.8.73b SCK subset number

The SCK subset number element is contained in CK Change Demand messages where the SCK set is split into 2 or more subsets and a complete subset is to be made active. It indicates the number of the subset that is to be activated.

Table A.100b: SCK subset number element contents

Information element	Length	Value	Remark
SCK subset number	5	00000_2	Mismatched number, used to indicate a mismatch in grouping when responding to a key status or delete demand
		00001_2 to 11110_2	Subset 1 to 30, value indicates number of subset
		11111_2	Reserved
NOTE 1: SCK subset number element value shall not be greater than the highest number of subsets permitted by the grouping signified by the SCK subset group number element. NOTE 2: SCK subset number = 1 corresponds to subset where lowest SCKN = 1.			

A.8.74 SCK use

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

Table A.101: SCK version number element contents

Information element	Length	Value	Remark
SCK use	1	0_2	Trunked Mode Operation
		1_2	Direct Mode Operation

A.8.75 SCK version number

The SCK Version Number (SCK-VN) is the numerical value associated with a version number of a key being transferred in an OTAR SCK transaction. Multiple SCK-VNs shall be sent where multiple keys are transferred, one SCK-VN per key.

Table A.102: SCK version number element contents

Information element	Length	Value	Remark
SCK version number	16	Any	

A.8.76 Sealed CCK, Sealed SCK, Sealed GCK, Sealed GSKO

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

Table A.103: Sealed Key element contents

Information element	Length	Value	Remark
Sealed Key	120	Any	

A.8.76a Sealed CCKX, Sealed SCKX, Sealed GCKX

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

Table A.103a: Sealed Extended Key element contents

Information element	Length	Value	Remark
Sealed Extended Key	224	Any	

A.8.76b Sealed GSKOX

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

Table A.103b: Sealed GSKOX element contents

Information element	Length	Value	Remark
Sealed GSKOX	288	Any	

A.8.77 Security information element

The Security information element is found in the Extended services broadcast information element in SYSINFO and SYSINFO-Q PDUs and indicates to the MS the current security capabilities of a conventional access cell. The Security information element is found also in the Extended DA services broadcast information element in SYSINFO-DA PDU and indicates to the MS the current security capabilities of a direct access cell.

Table A.104: Security information element in SYSINFO, SYSINFO-Q and SYSINFO-DA

Information element	Length	C/O/M	Value	Remark
Authentication	1	M	0_2	Authentication not required on this cell
(see note 4)			1_2	Authentication required on this cell
Security class 1	1	M	0_2	Security class 1 MS not supported on this cell
(see note 1)			1_2	Security class 1 MS supported on this cell
Security class 2 or 3	1	M	0_2	Security class 2 MS supported on this cell
(see note 1)			1_2	Security class 3 MS supported on this cell
SCKN (see notes 1 and 2)	5	C		If security class 2 MS supported on this cell
DCK retrieval during initial	1	C	0_2	Service not supported
Cell selection (see notes 1 and 3)			1_2	Service supported
DCK retrieval during cell	1	C	0_2	Service not supported
Re-selection (see notes 1 and 3)			1_2	Service supported
Linked GCK crypto-periods (see notes 3 and 5)	1	C	0_2	Service not supported
			1_2	Service supported
Short GCK-VN (see notes 3 and 6)	2	C		Represents the 2 least significant bits of the GCK-VN associated with the linked GCKs

NOTE 1: The elements to which this note applies have no meaning and shall be set to zero under the following conditions:

- if the element is contained in the SYSINFO PDU, and the "Air interface encryption service" element contained in the accompanying D-MLE-SYSINFO PDU has value 0, "Service is not available on this cell";
- if the element is contained in the SYSINFO-Q PDU, and the "Air interface encryption service" element contained in the accompanying D-MLE-SYSINFO-Q PDU has value 0, "Service is not available on this cell";
- if the element is contained in the SYSINFO-DA PDU, and the "Air interface encryption service" element contained in the accompanying D-MLE-SYSINFO-DA PDU has value 0, "Service is not available on this cell".

NOTE 2: If security class 2 MS supported on this cell.

NOTE 3: If security class 3 MS supported on this cell.

NOTE 4: An MS that does not support authentication should not select a cell that broadcasts "authentication required".

NOTE 5: The elements to which this note applies have no meaning and shall be set to zero under the following conditions:

- if the element is contained in the SYSINFO PDU, and the "GCK Supported" element contained in the same SYSINFO PDU indicates "GCK/GCKX not supported on this cell";
- if the element is contained in the SYSINFO-Q PDU, and the "GCK Supported" element contained in the same SYSINFO-Q PDU indicates "GCK/GCKX not supported on this cell";
- if the element is contained in the SYSINFO-DA PDU, and the "GCK Supported" element contained in the same SYSINFO-DA PDU indicates "GCK/GCKX not supported on this cell".

NOTE 6: If the "Linked GCK crypto-periods" information element indicates "Service not supported" then the value of this element has no meaning and shall be set to zero.

A.8.77a Security parameters

The Security parameters information element is found in the SYNC-DA, D-NWRK-BROADCAST and D-NWRK-BROADCAST-DA PDUs and indicates to the MS the basic security services of a cell.

Table A.104a: Security parameters information element contents

Information element	Length	Type	Value	Remark
Authentication (see note 1)	1	M	0	Authentication not required on this cell.
			1	Authentication required on this cell.
Security class 1 (see note 2)	1	M	0	Security class 1 MS not supported on this cell.
			1	Security class 1 MS supported on this cell.
Security class 2 or 3 (see notes 2 and 3)	1	M	0	Security class 2 MS supported on this cell.
			1	Security class 3 MS supported on this cell.
NOTE 1: An MS that does not support authentication should not select a cell that broadcasts "authentication required". NOTE 2: The elements to which this note applies have no meaning and shall be set to zero under the following conditions: - if the element is contained in the SYNC-DA PDU, and the "Air interface encryption service" element contained in the accompanying D-MLE-SYNC-DA PDU has value 0, "Service is not available on this cell"; - if the element is contained in the D-NWRK BROADCAST PDU, and the "Air interface encryption service" element contained in the same D-NWRK BROADCAST PDU has value 0, "Service is not available on this cell"; - if the element is contained in the D-NWRK BROADCAST-DA PDU, and the "Air interface encryption service" element contained in the same D-NWRK BROADCAST-DA PDU has value 0, "Service is not available on this cell". NOTE 3: Security class 2 and security class 3 are mutually exclusive.				

A.8.77b Security related information element

The security related information element is included in the D-FACILITY (ASSIGN) PDU for SS-DGNA to indicate the security associations of the GSSI.

Table A.104b: Security Related Information Element

Information element	Length	Type	C/O/M	Value	Remark
GCK Association	1	1	M	0_2 1_2	GCK association information not provided GCK association information provided
GCK Select Number	17		C		Provided if *GCK Association* indicates "GCK Association Information Provided"
SCK Association	1	1	M	0_2 1_2	SCK association information not provided SCK association information provided
SCK Subset Grouping Type	4		C		Provided if SCK Association indicates "SCK Association Information Provided"
SCK Subset Number	5		C		Provided if SCK Association indicates "SCK Association Information Provided"

A.8.78 Session key

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

Table A.105: Session key element contents

Information element	Length	Value	Remark
Session key	1	0_2	Sealed key has been generated using individually generated session key KSO or KSOX for MS
		1_2	Sealed key has been generated using Group Session Key for OTAR known to group of MSs

A.8.79 Slot Number

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

A.8.80 SSI

See ETSI EN 300 392-1 [1], clause 7.

A.8.81 Subscription disable

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

Table A.106: Subscription disable element contents

Information element	Length	Value	Remark
Subscription disable	1	0_2	Subscription not to be disabled
		1_2	Subscription to be disabled

A.8.82 Subscription enable

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

Table A.107: Subscription enable element contents

Information element	Length	Value	Remark
Subscription enable	1	0_2	Subscription not to be enabled
		1_2	Subscription to be enabled

A.8.83 Subscription status

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

Table A.108: 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

A.8.83a SW version number present

The SW version number present element is used to indicate whether or not the SW version number is included in the PDU.

Table A.108a: SW version number present element contents

Information element	Length	Value	Remark
SW version number present	1	0_2	SW version number is not included
		1_2	SW version number is included

A.8.84 TEI

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

Table A.109: TEI contents

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

A.8.85 TEI request flag

This bit indicates whether the MS should supply the TEI.

Table A.110: TEI request flag contents

Information element	Length	Value	Remark
TEI request flag	1	0_2	Do not supply TEI
		1_2	Supply TEI

A.8.86 Time type

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

Table A.111: Time type information element contents

Information element	Length	Value	Remark
Time type	2	00_2	Absolute IV
		01_2	Network time
		10_2	Immediate, first slot of first frame of next multiframe
		11_2	Currently in use

A.8.87 Type 3 element identifier

The type 3-element identifier indicates the MM type 3 elements to be used in the MM PDUs for authentication and OTAR purposes. The type 3 element identifiers in Tables A.112 and A.113 are identified in the present document only and are taken from the reserved values of type 3 element identifier defined in the MM protocol.
For more details, see ETSI EN 300 392-2 [2], clause 16.

Table A.112: Type 3 element identifier element contents for downlink

Information element	Length	Value	Remarks
Type 3 element identifier	4	0011_2	Security downlink
		1010_2	Authentication downlink

Table A.113: Type 3 element identifier element contents for uplink

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

Annex B (normative): Boundary conditions for the cryptographic algorithms and procedures

B.0 General

This clause lists the input and output parameters of the algorithms specified in the TAA1 and TAA2 sets of authentication and key management algorithms. Their membership of each algorithm set is stated.

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 (TAA1 set): 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).

TA12 (TAA1 set): 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).

TA13 (TAA2 set): shall be used to compute KS and KS' from K2 and RS. The algorithm shall have the following properties:

- Input 1: Bit string of length |K2|;
- Input 2: Bit string of length |RS|;
- Output 1: Bit string of length |KS|;
- Output 2: 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, Output 1 and Output 2 (even if the details of the algorithm are known). It should also be difficult to infer any information about Output 2 from knowledge of Output 1 and RS, and also difficult to infer any information about Output 1 from knowledge of Output 2 and RS if Input 1 is unknown.

TA14 (TAA2 set): shall be used to compute DCKX from KS, KS', RAND1 and RAND2. The algorithm shall have the following properties:

- Input 1: Bit string of length |KS|;
- Input 2: Bit string of length |KS'|;
- Input 3: Bit string of length |RAND1|;

- Input 4: Bit string of length |RAND2|;
- Output: Bit string of length |DCKX|.

The algorithm should be designed such that it is difficult to infer any information about Input 1, Input 2 or the Output from the knowledge of Inputs 3 or 4 (even if the details of the algorithm are known). This should remain true if one of Input 3 or Input 4 is set to a fixed constant, or if Input 3 and Input 4 are equal to each other.

The algorithm should be designed such that every bit of output 1 depends on every bit of all inputs.

TA15 (TAA2 set): shall be used to compute (X)RES1 from KS, KS' and RAND1. The algorithm shall have the following properties:

- Input 1: Bit string of length |KS|;
- Input 2: Bit string of length |KS'|;
- Input 3: Bit string of length |RAND1|;
- Output: Bit string of length |(X)RES1|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 or Input 2 from knowledge of one or more sets of Input 3 and the corresponding Output (even if the details of the algorithm are known).

It should also be difficult to infer any knowledge about Input 1 and Input 2 by observations of the values of Input 3 and the Output in conjunction with observations of the values of Input 3 and the Output of TA23 when Input 1 to TA15 = Input 1 to TA23 at the same time as Input 2 to TA15 = Input 2 to TA23.

The probability of (X)RES1 output from TA15 having the same value as (X)RES2 output from TA23 shall be low when Input 1 to TA15 = Input 1 to TA23 at the same time as Input 2 to TA15 = Input 2 to TA23 at the same time as Input 3 to TA15 = Input 3 to TA23.

TA21 (TAA1 set): 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).

TA22 (TAA1 set): 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).

TA23 (TAA2 set): shall be used to compute (X)RES2 from KS, KS' and RAND2. The algorithm shall have the following properties:

- Input 1: Bit string of length |KS|;
- Input 2: Bit string of length |KS'|;
- Input 3: Bit string of length |RAND2|;

- Output: Bit string of length |(X)RES2|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 or Input 2 from knowledge of one or more sets of Input 3 and the corresponding Output (even if the details of the algorithm are known).

It should also be difficult to infer any knowledge about Input 1 and Input 2 by observations of the values of Input 3 and the Output in conjunction with observations of the values of Input 3 and the Output of TA15 when Input 1 to TA15 = Input 1 to TA23 at the same time as Input 2 to TA15 = Input 2 to TA23.

The probability of (X)RES2 output from TA23 having the same value as (X)RES1 output from TA15 shall be low when Input 1to TA15 = Input 1 to TA23 at the same time as Input 2 to TA15 = Input 2 to TA23 at the same time as Input 3 to TA15 = Input 3 to TA23.

TA31 (TAA1 set): 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 (TAA1 set): 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).

TA33 (TAA2 set): shall be used to compute SCCKX from CCKX, CCK-id and DCKX. The algorithm shall have the following properties:

- Input 1: Bit string of length |CCKX|;
- Input 2: Bit string of length |CCK-id|;
- Input 3: Bit string of length |DCKX|;
- Output: Bit string of length |SCCKX|.

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). It should also be difficult to infer any knowledge about Input 3 from observation of various corresponding values of Input 1, Input 2 and the Output.

TA34 (TAA2 set): shall be used to compute CCKX from SCCKX, CCK-id and DCKX. The algorithm shall have the following properties:

- Input 1: Bit string of length |SCCKX|;
- Input 2: Bit string of length |DCKX|;

- Input 3: Bit string of length |CCK-id|;
- Output 1: Bit string of length |CCKX|;
- 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 will be difficult to derive (parts of) Input 2 from the observation of various matching values of other inputs and outputs (known plain text attack).

If Output 2 assumes the value of "TRUE" then Output 1 shall be set to zero.

TA41 (TAA1 set): 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).

TA42 (TAA1 set): shall be used to compute KSOX from K2 and RSO. The algorithm shall have the following properties:

- Input 1: Bit string of length |K2|;
- Input 2: Bit string of length |RSO|;
- Output: Bit string of length |KSOX|.

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). It should also be difficult to infer any information about Input 1 from observation of various corresponding values of Input 2 and the Output.

TA51 (TAA1 set): 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 (TAA1 set): 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).

TA53 (TAA2 set): shall be used to compute SSCKX from SCKX, SCKN, SCK-VN, and one of either KSOX or GSKOX. The algorithm shall have the following properties:

- Input 1: Bit string of length |SCKX|;
- Input 2: Bit string of length |SCK-VN|;
- Input 3: Bit string of length |KSOX|;
- Input 4: Bit string of length |SCKN|;
- Output: Bit string of length |SSCKX|.

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). It should also be difficult to infer any knowledge about Input 3 from observations of various corresponding values of Input 1, Input 2, Input 4 and the Output.

NOTE 1: Length |GSKOX| = length |KSOX|.

TA54 (TAA2 set): shall be used to compute SCKX and SCKN from SSCKX, SCK-VN and one of either KSOX or GSKOX. The algorithm shall have the following properties:

- Input 1: Bit string of length |SSCKX|;
- Input 2: Bit string of length |KSOX|;
- Input 3: Bit string of length |SCK-VN|;
- Output 1: Bit string of length |SCKX|;
- 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 will be difficult to derive (parts of) Input 2 from the observation of various matching values of other inputs and outputs (known plain text attack).

If Output 2 assumes the value of "TRUE" then Output 1 and Output 3 shall be set to zero.

NOTE 2: Length |GSKOX| = length |KSOX|.

TA61 (TAA1 set): 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 input 2s and outputs. Further it should be difficult to infer any knowledge of Input 2 from observation of various matching values of other input 2s and outputs. Moreover, for a fixed input 1 different values of Input 2 shall always give different values of the output.

TA71 (TAA1 set): 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).

TA72 (TAA2 set): shall be used to compute MGCKX from GCKX and CCKX. The algorithm shall have the following properties:

- Input 1: Bit string of length |GCKX|;
- Input 2: Bit string of length |CCKX|;
- Output: Bit string of length |MGCKX|.

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). Moreover, it will also be difficult to infer any information about Input 2 from knowledge of Input 1 and the Output (even if details of the algorithm are known). It will also be difficult to infer any information about the Output if one of Input 1 or Input 2 is known but the other Input is unknown.

TA81 (TAA1 set): shall be used to compute SGCK from GCK, GCKN**,** GCK-VN and KSO. The algorithm shall have the following properties:

- Input 1: Bit string of length |GCK|;
- Input 2: Bit string of length |GCK-VN|;
- Input 3: Bit string of length |KSO|;
- Input 4: Bit string of length |GCKN|;
- Output: Bit string of length |SGCK|.

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

TA82 (TAA1 set): shall be used to compute GCK and GCKN from SGCK, GCK-VN, and KSO. The algorithm shall have the following properties:

- Input 1: Bit string of length |SGCK|;
- Input 2: Bit string of length |KSO|;
- Input 3: Bit string of length |GCK-VN|;
- Output 1: Bit string of length |GCK|;
- Output 2: Boolean;
- Output 3: Bit string of length |GCKN|.

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

TA83 (TAA2 set): shall be used to compute SGCKX from GCKX, GCKN**,** GCK-VN and one of either KSOX or GSKOX. The algorithm shall have the following properties:

- Input 1: Bit string of length |GCKX|;
- Input 2: Bit string of length |GCK-VN|;
- Input 3: Bit string of length |KSOX|;

- Input 4: Bit string of length |GCKN|;
- Output: Bit string of length |SGCKX|.

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). It should also be difficult to infer any knowledge about Input 3 from observations of various corresponding values of Input 1, Input 2, Input 4 and the Output.

NOTE 3: Length |GSKOX| = length |KSOX|.

TA84 (TAA2 set): shall be used to compute GCKX and GCKN from SGCKX, GCK-VN, and one of either KSOX or GSKOX. The algorithm shall have the following properties:

- Input 1: Bit string of length |SGCKX|;
- Input 2: Bit string of length |KSOX|;
- Input 3: Bit string of length |GCK-VN|;
- Output 1: Bit string of length |GCKX|;
- Output 2: Boolean;
- Output 3: Bit string of length |GCKN|.

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

If Output 2 assumes the value of "TRUE" then Output 1 and Output 3 shall be set to zero.

NOTE 4: Length |GSKOX| has the same length as a bit string of length |KSOX|.

TA91 (TAA1 set): shall be used to compute SGSKO from GSKO, GSKO-VN and KSO. The algorithm shall have the following properties:

- Input 1: Bit string of length |GSKO|;
- Input 2: Bit string of length |GSKO-VN|;
- Input 3: Bit string of length |KSO|;
- Output: Bit string of length |SGSKO|.

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

TA92 (TAA1 set): shall be used to compute GSKO from SGSKO, GSKO-VN, and KSO. The algorithm shall have the following properties:

- Input 1: Bit string of length |SGSKO|;
- Input 2: Bit string of length |KSO|;
- Input 3: Bit string of length |GSKO-VN|;
- Output 1: Bit string of length |GSKO|;
- Output 2: Boolean.

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

TA93 (TAA2 set): shall be used to compute SGSKOX from GSKOX, GSKO-VN and KSOX. The algorithm shall have the following properties:

- Input 1: Bit string of length |GSKOX|;
- Input 2: Bit string of length |GSKO-VN|;
- Input 3: Bit string of length |KSOX|;
- Output: Bit string of length |SGSKOX|.

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).

TA94 (TAA2 set): shall be used to compute GSKOX from SGSKOX, GSKO-VN, and KSOX. The algorithm shall have the following properties:

- Input 1: Bit string of length |SGSKOX|;
- Input 2: Bit string of length |KSOX|;
- Input 3: Bit string of length |GSKO-VN|;
- Output 1: Bit string of length |GSKOX|;
- Output 2: Boolean.

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

If Output 2 assumes the value of "TRUE" then Output 1 shall be set to zero.

TA101 (TAA1 set): shall be used to compute KSv from KS, GCK0 and MNI, or to compute KSOv from KSO, GCK0 and MNI.

- Input 1: Bit string of length |KS|;
- Input 2: Bit string of length |GCK0|;
- Input 3: Bit string of length |MNI|;
- Output: Bit string of length |KSv|.

NOTE 5: Length |KS| = length |KSO|.

The algorithm should be designed so that the Output is dependent on every bit of all Inputs. The algorithm shall be designed such that Inputs 1 and 2 shall be difficult to infer from knowledge of Input 3 and the Output.

TA102 (TAA2 set): shall be used to compute KSv from KS, GCKX0 and MNI.

- Input 1: Bit string of length |KS|;
- Input 2: Bit string of length |GCKX0|;
- Input 3: Bit string of length |MNI|;
- Output: Bit string of length |KSv|.

The algorithm should be designed so that the Output is dependent on every bit of all Inputs. The algorithm shall be designed such that Inputs 1 and 2 shall be difficult to infer from knowledge of Input 3 and the Output.

TA103 (TAA2 set): shall be used to compute KSOXv from KSO, GCKX0 and MNI.

- Input 1: Bit string of length |KSOX|;
- Input 2: Bit string of length |GCKX0|;

- Input 3: Bit string of length |MNI|;
- Output: Bit string of length |KSOXv|.

The algorithm should be designed so that the Output is dependent on every bit of all Inputs. The algorithm will be designed such that Inputs 1 and 2 will be difficult to infer from knowledge of Input 3 and the Output.

TA104 (TAA2 set): shall be used to compute KSOv from KSOXv or KSO from KSOX.

- Input: Bit string of length |KSOXv|;
- Output: Bit string of length |KSOv|.

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

TA105 (TAA2 set): shall be used to compute KSOXv from KSOv.

- Input: Bit string of length |KSOv|;
- Output: Bit string of length |KSOXv|.

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

TA106 (TAA2 set): shall be used to compute CK from CKX.

- Input: Bit string of length |CKX|;
- Output: Bit string of length |CK|.

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

The following algorithms, TB1, TB2 and TB3 may be used to generate K locally to an MS but do not directly alter the air interface.

TB1 (TAA1 set): 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 (TAA1 set): 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 (TAA1 set): shall be used to compute K from UAK and AC. The algorithm shall have the following properties:

- Input 1: Bit string of length |AC|;
- Input 2: Bit string of length |UAK|;
- Output: Bit string of length |K|.

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

TB4 (TAA1 set): shall be used to compute DCK from DCK1 and DCK2. The algorithm shall have the following properties:

- Input 1: Bit string of length |DCK1|;
- Input 2: Bit string of length |DCK2|;
- Output: Bit string of length |DCK|.

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

TB5 (TAA1 set): shall be used to compute ECK from CK, CC, CN (see ETSI EN 300 392-2 [2], clause 21.5) and LA. The algorithm shall have the following properties:

- Input 1: Bit string of length |CK|;
- Input 2: Bit string of length |LA|;
- Input 3: Bit string of length |CN|;
- Input 4: Bit string of length |CC|;
- Output: Bit string of length |ECK|.

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

TB6 (TAA1 set): reserved for DMO Security (ETSI EN 300 396-6 [5]).

TB7 (TAA1 set): shall be used to compute EGSKO from GSKO. The algorithm shall have the following properties:

- Input: Bit string of length |GSKO|;
- Output: Bit string of length |EGSKO|.

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

B.1 Dimensioning of the cryptographic parameters

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

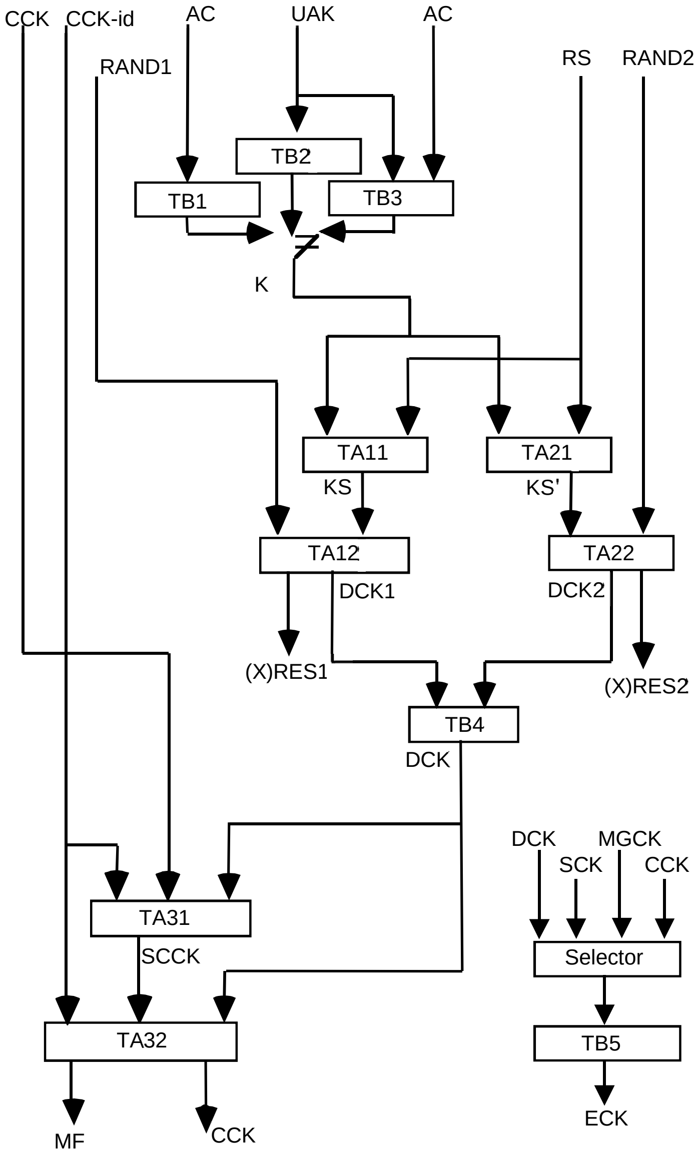
Table B.1: Dimensioning of cryptographic parameters

Abbreviation	No. of bits
AC	16 to 32
CC	6
CCK	80
CCKX	192
CCK-id	16
CK	80
CKX	192
CN	12
DCK	80
DCK1	80
DCK2	80
DCKX	192
ECK	80
EGSKO	128
ESI	24
GCK	80
GCKX	192
GCK0	80
GCKX0	192
GCKN	16
GCK-VN	16
GSKO	96
GSKOX	256
GSKO-VN	16
K	128
K2	256
KS	128
KS'	128
KSO	128

Abbreviation	No. of bits
KSOX	256
KSv	128
KSv'	128
KSOv	128
KSOXv	256
LAid	14
MF	1
MGCK	80
MGCKX	192
MNI	24
PIN	16 to 32
RAND1	80
RAND2	80
RES1	32
RES2	32
RS	80
RSO	80
SCCK	120
SCCKX	224
SCK	80
SCKX	192
SCKN	5
SCK-VN	16
SGCK	120
SGCKX	224
SGSKO	120
SGSKOX	288
SSCK	120
SSCKX	224
SSI	24
UAK	128
XRES1	32
XRES2	32

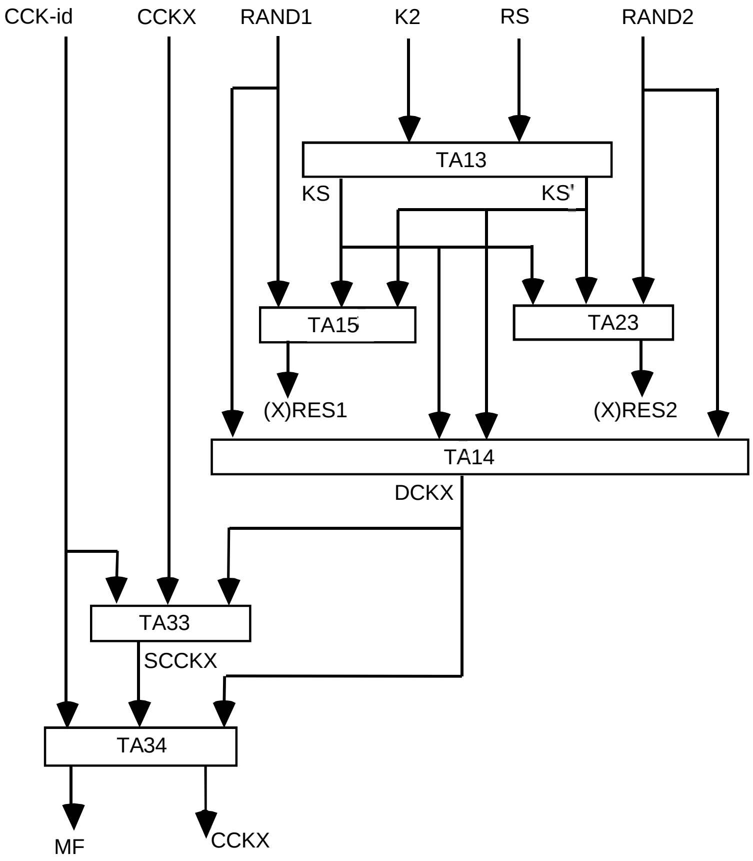
B.2 Summary of the cryptographic processes

A summary of the authentication and air interface key management mechanisms when operating in the home SwMI explained in the previous clauses is given in Figures B.1 to B.2a. Only the paths where keys are generated by an algorithm are shown.



NOTE: Algorithms TB1, TB2 and TB3 are shown for information and may be used in deriving K within an MS.

Figure B.1: Overview of air interface authentication and key management in home SwMI: authentication and dynamic keys where an air interface encryption algorithm from TEA set A is in use



NOTE: K2 may be derived in the MS from an AC and/or UAK, in a similar manner to the optional derivation of K from AC and/or UAK shown in Figure B.1. Any such derivation is outside the scope of the present document.

Figure B.1a: Overview of air interface authentication and key management in home SwMI: authentication and dynamic keys where an air interface encryption algorithm from TEA set B is in use

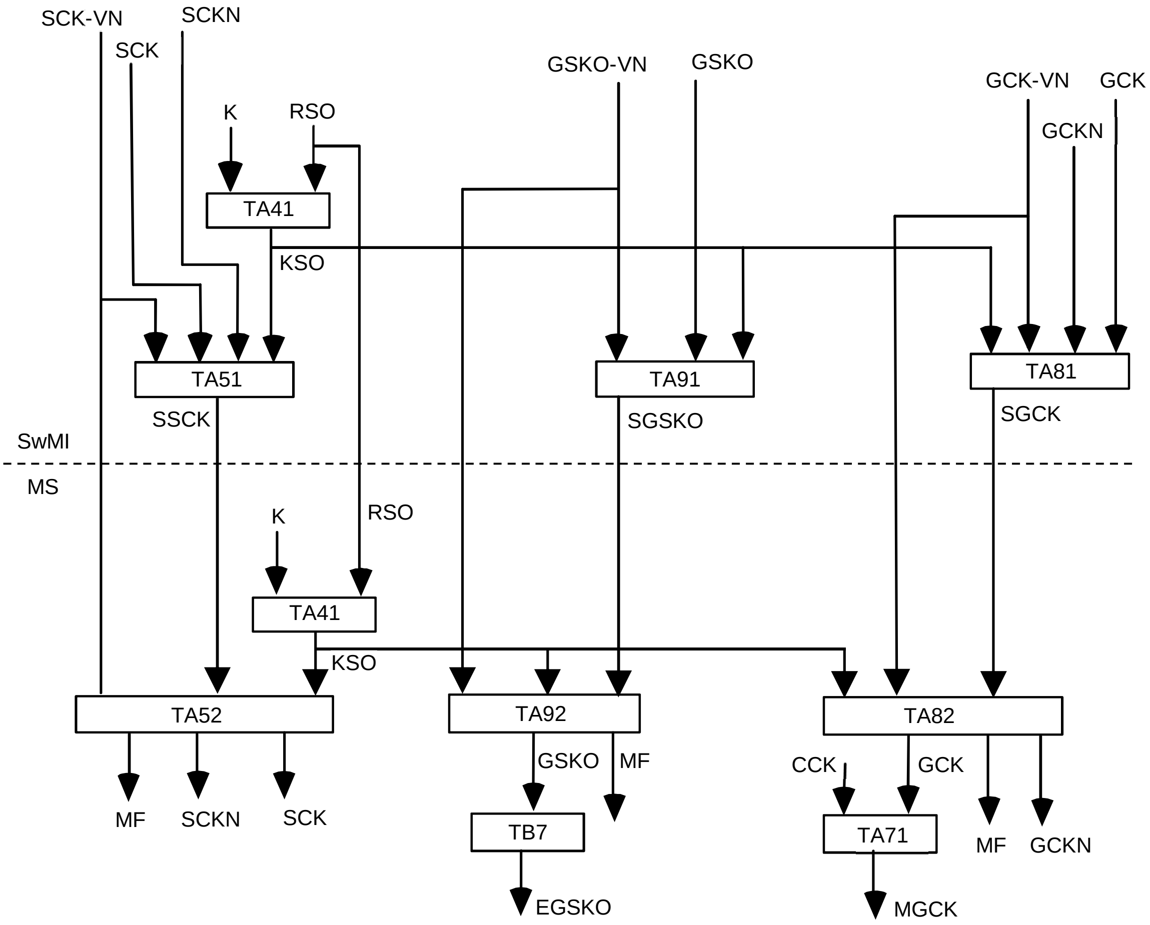


Figure B.2: Overview of air interface authentication and key management in home SwMI: key management for SCK, GCK and GSKO where an air interface encryption algorithm from TEA set A is in use

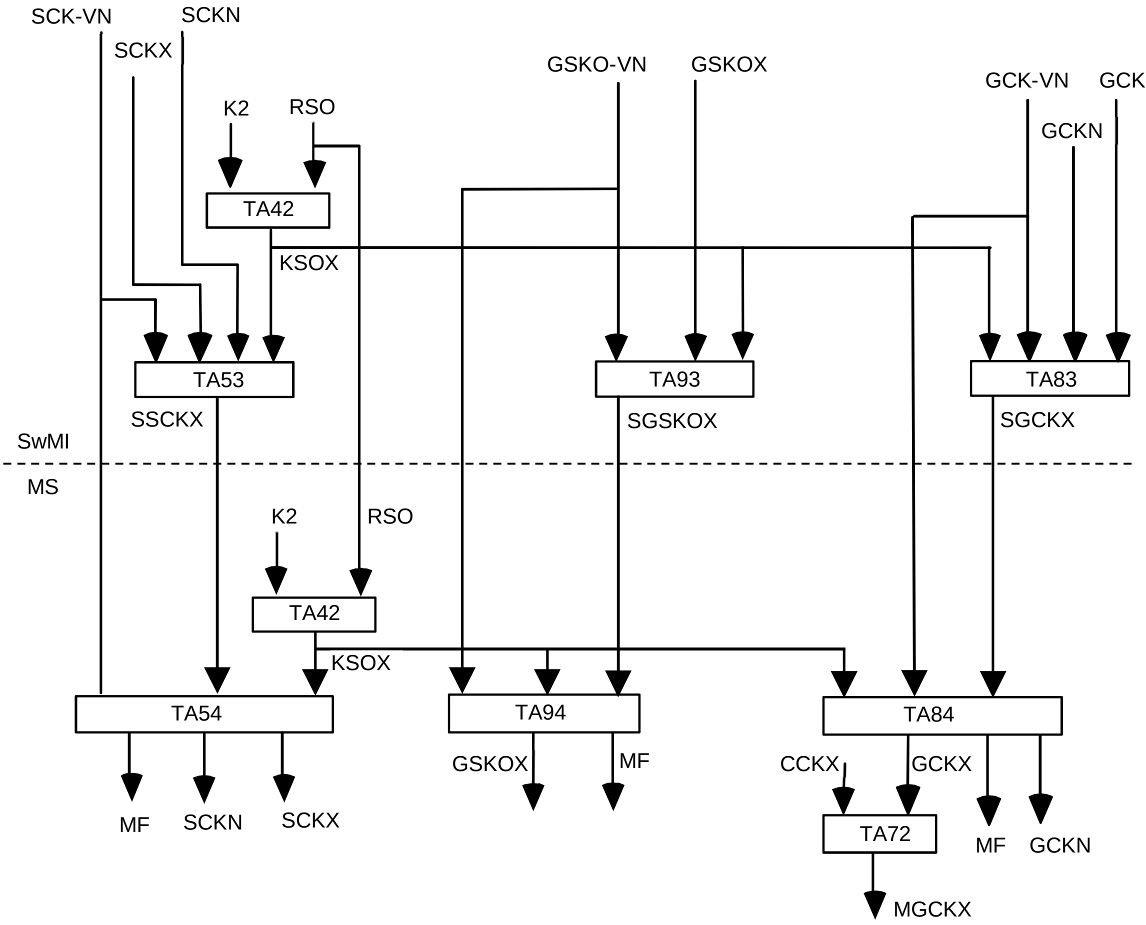
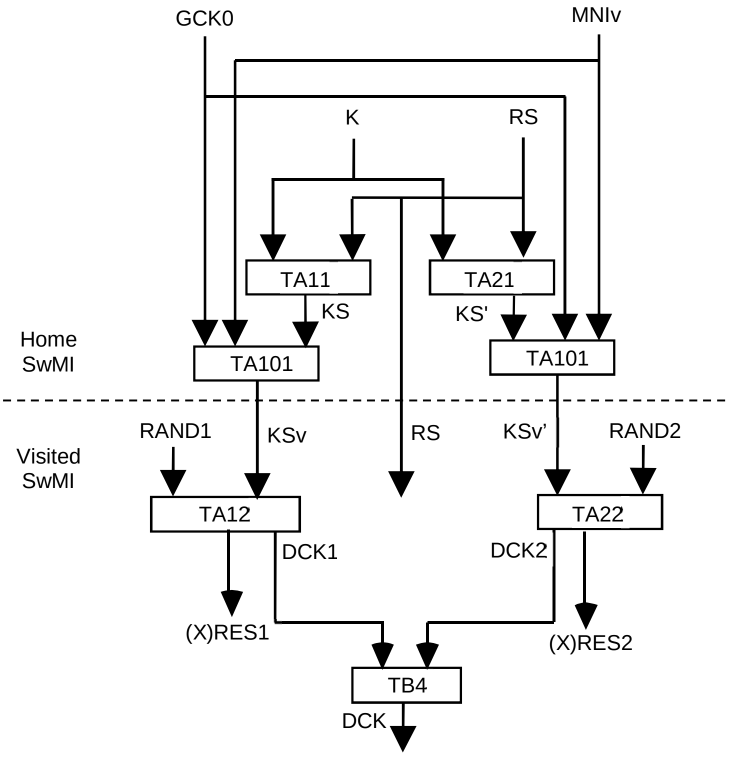


Figure B.2a: Overview of air interface authentication and key management in home SwMI: key management for SCKX, GCKX and GSKOX where an air interface encryption algorithm from TEA set B is in use

Figure B.3 to Figure B.8 show the differences in the authentication and air interface key distribution mechanisms that apply when the MS is migrated. Figures B.3 and B.3a show the operation of authentication with the visited session key where air interface encryption algorithms from the same set are in use in home and visited SwMIs, and Figures B.3b and B.3c show authentication with the visited session key where air interface encryption algorithms from different sets are in use in the home and the visited SwMIs. Figures B.4 and B.4a show the provision of SCK or SCKX where the keys are sealed by the home SwMI, and Figures B.5 and B.6 show the same case when SCK or SCKX, GCK or GCKX and GSKO or GSKOX are sealed by the visited SwMI. Figures B.7 and B.8 show the case where the keys are sealed by the visited SwMI, but where air interface encryption algorithms from different sets are used in the home SwMI and the visited SwMI. Mechanisms are not shown where these are the same as those shown in the previous figures.



NOTE: If the MS is provisioned with K2 but last negotiated TEA set A with the home SwMI, KS and KS' are derived from K2 using algorithm TA13 as shown in Figure B.1a.

Figure B.3: Overview of authentication key management for migrated MS where an air interface encryption algorithm from TEA set A is in use in both home and visited SwMIs

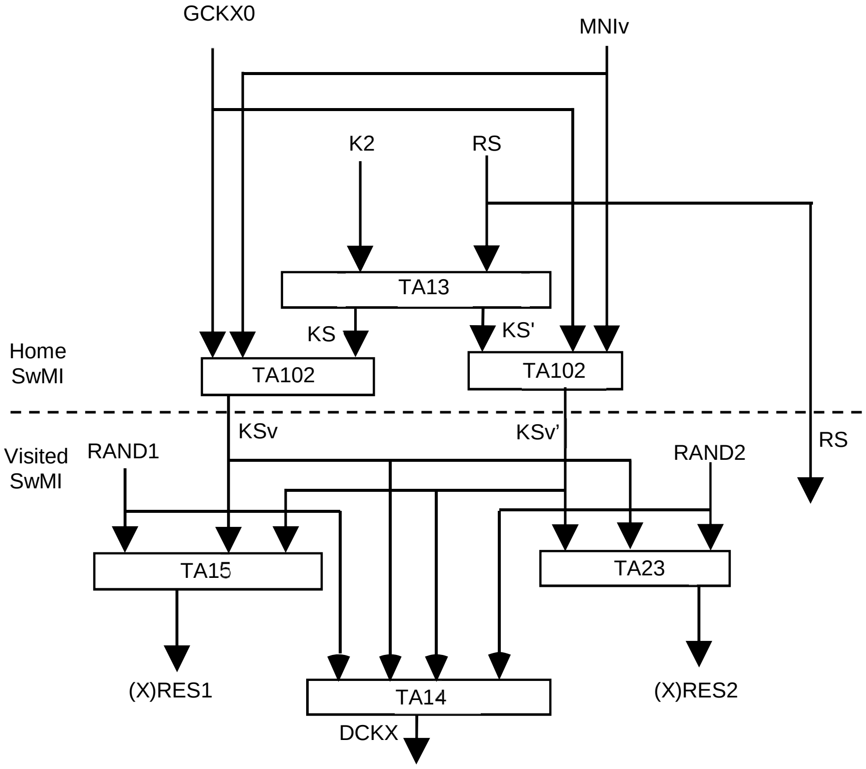
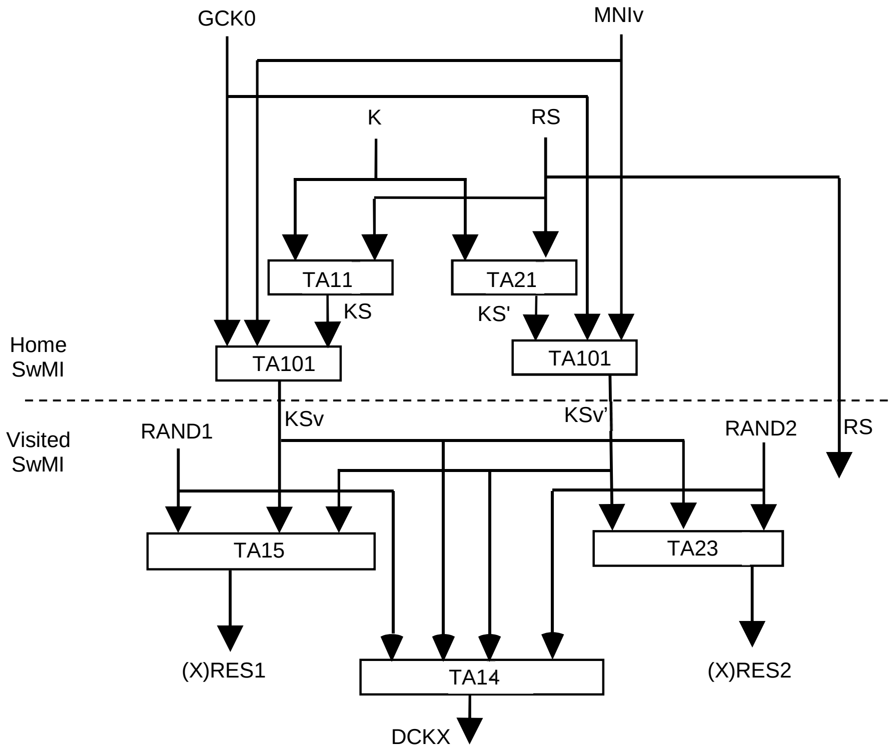


Figure B.3a: Overview of authentication key management for migrated MS where an air interface encryption algorithm from TEA set B is in use in both home and visited SwMIs



NOTE: If the MS is provisioned with K2 but last negotiated TEA set A with the home SwMI, KS and KS' are derived from K2 using algorithm TA13 as shown in Figure B.1a.

Figure B.3b: Overview of authentication key management for migrated MS where an air interface encryption algorithm from TEA set A is in use in the home SwMI, and from TEA set B in the visited SwMI

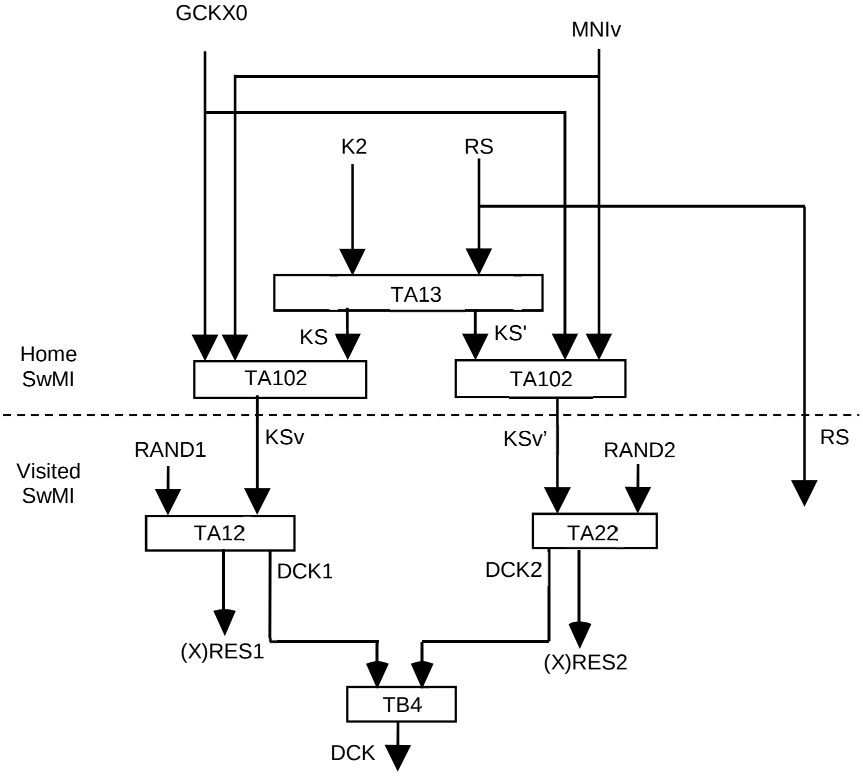


Figure B.3c: Overview of authentication key management for migrated MS where an air interface encryption algorithm from TEA set B is in use in the home SwMI, and from TEA set A in the visited SwMI

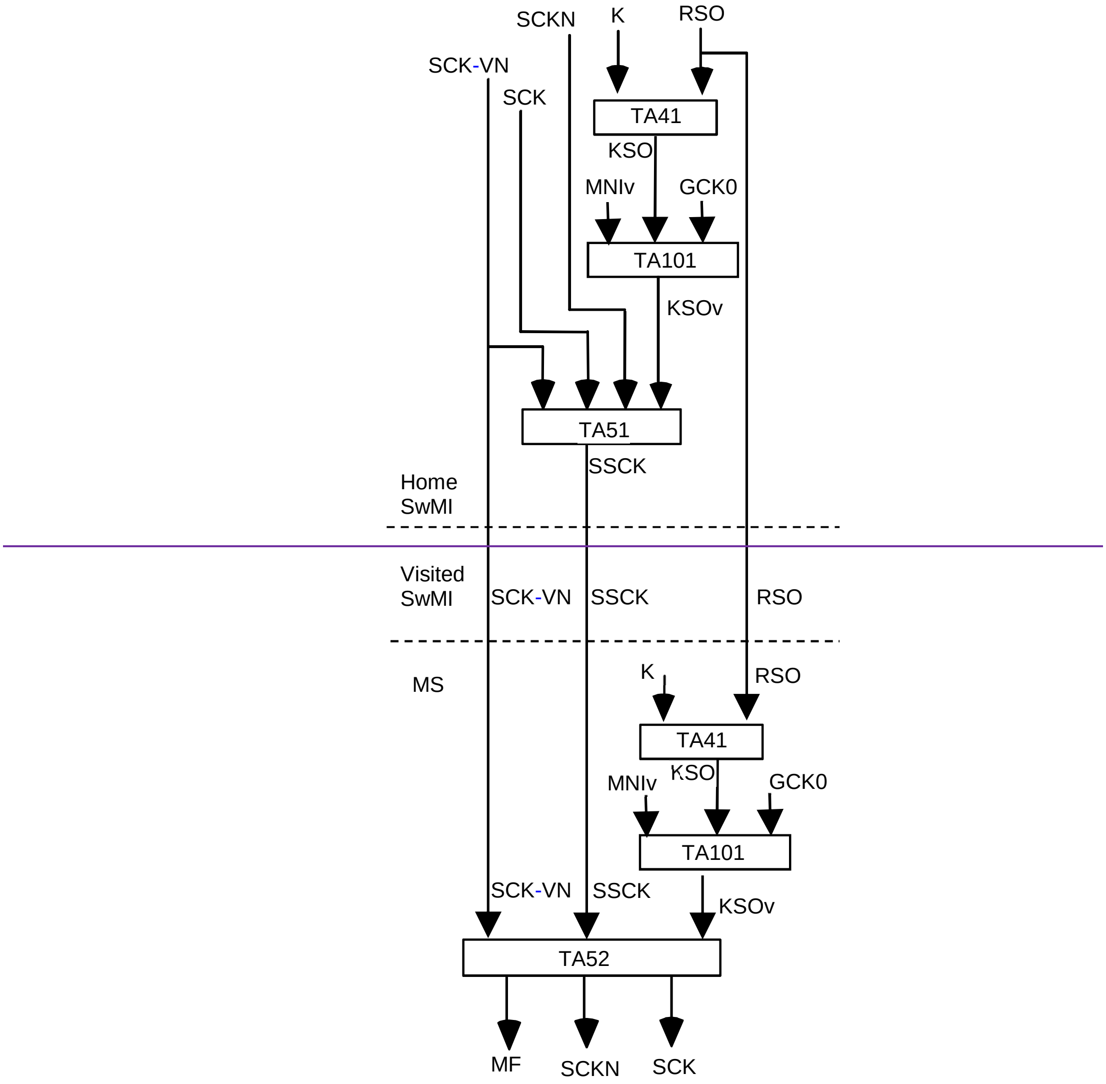


Figure B.4: Overview of provision of SCK to migrated MS where keys are sourced from the home SwMI, and where an air interface encryption algorithm from TEA set A is in use in both home and visited SwMIs

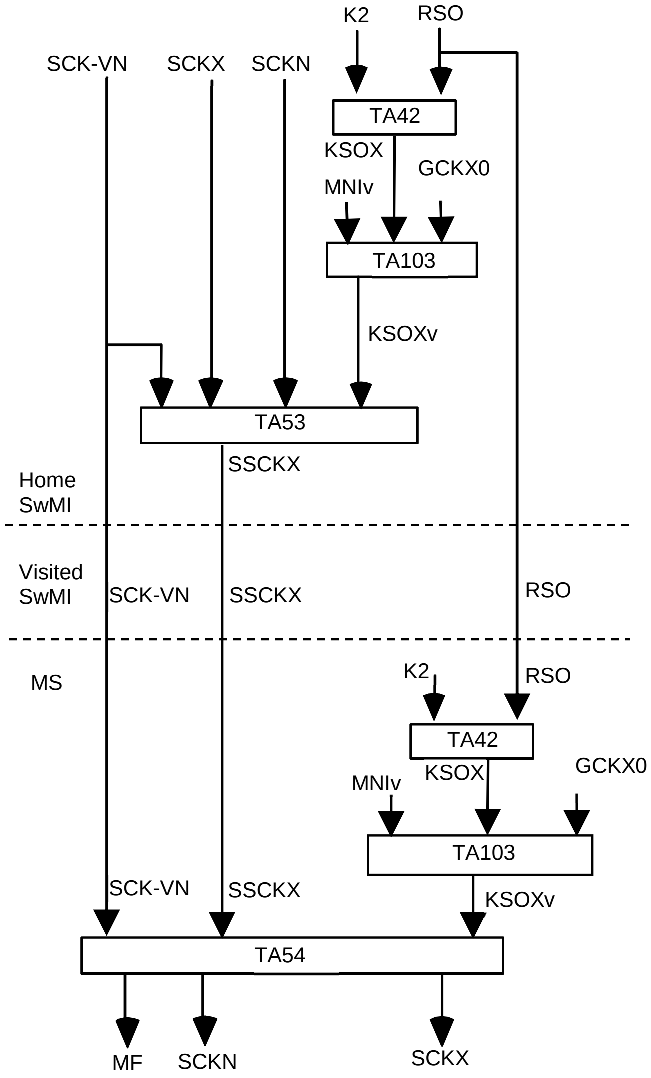


Figure B.4a: Overview of provision of SCKX to migrated MS where keys are sourced from the home SwMI, and where an air interface encryption algorithm from TEA set B is in use in both home and visited SwMIs

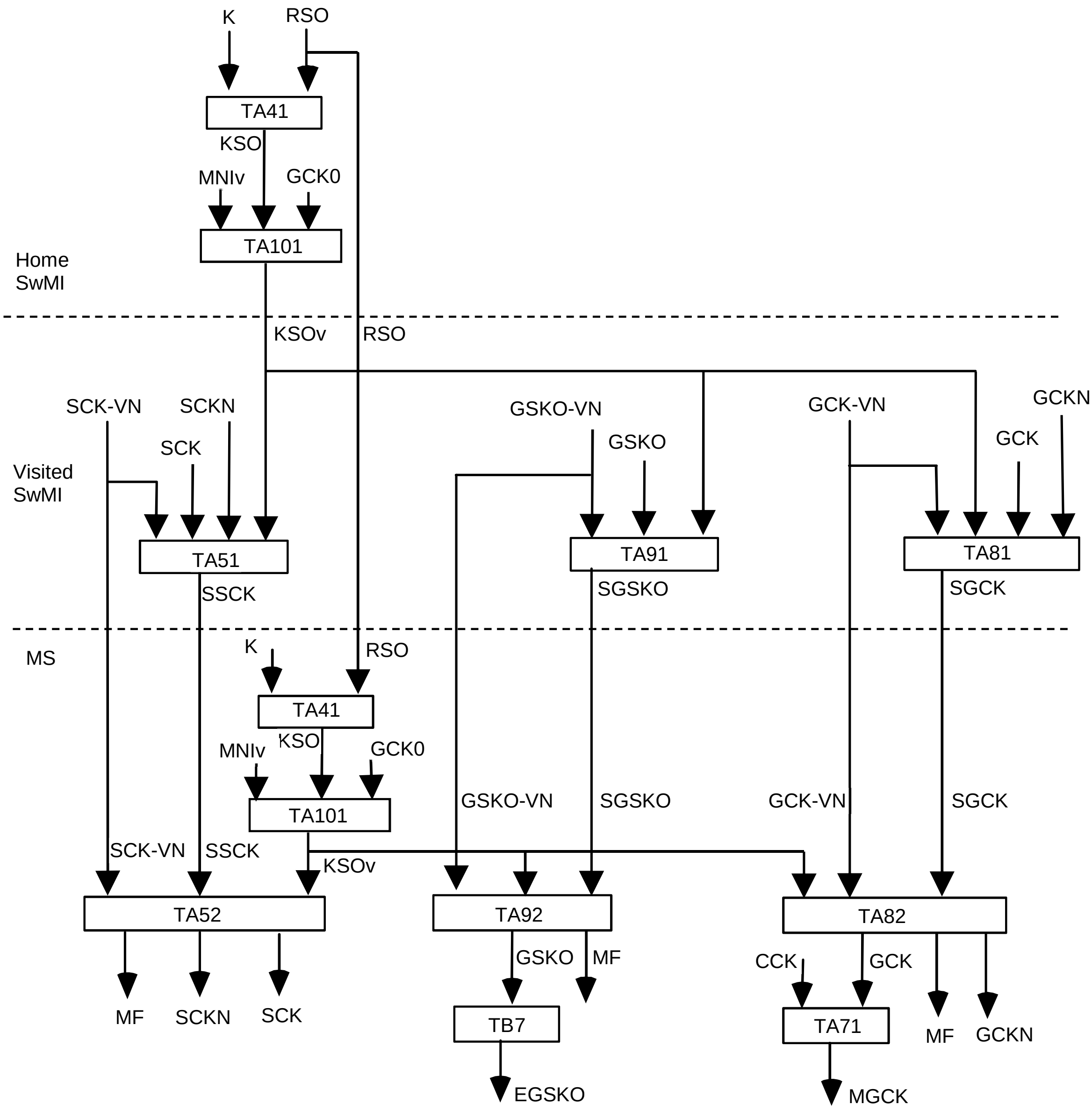


Figure B.5: Overview of provision of SCK, GCK and GSKO to migrated MS where keys are sourced from the visited SwMI, and where an air interface encryption algorithm from TEA set A is in use in both home and visited SwMIs

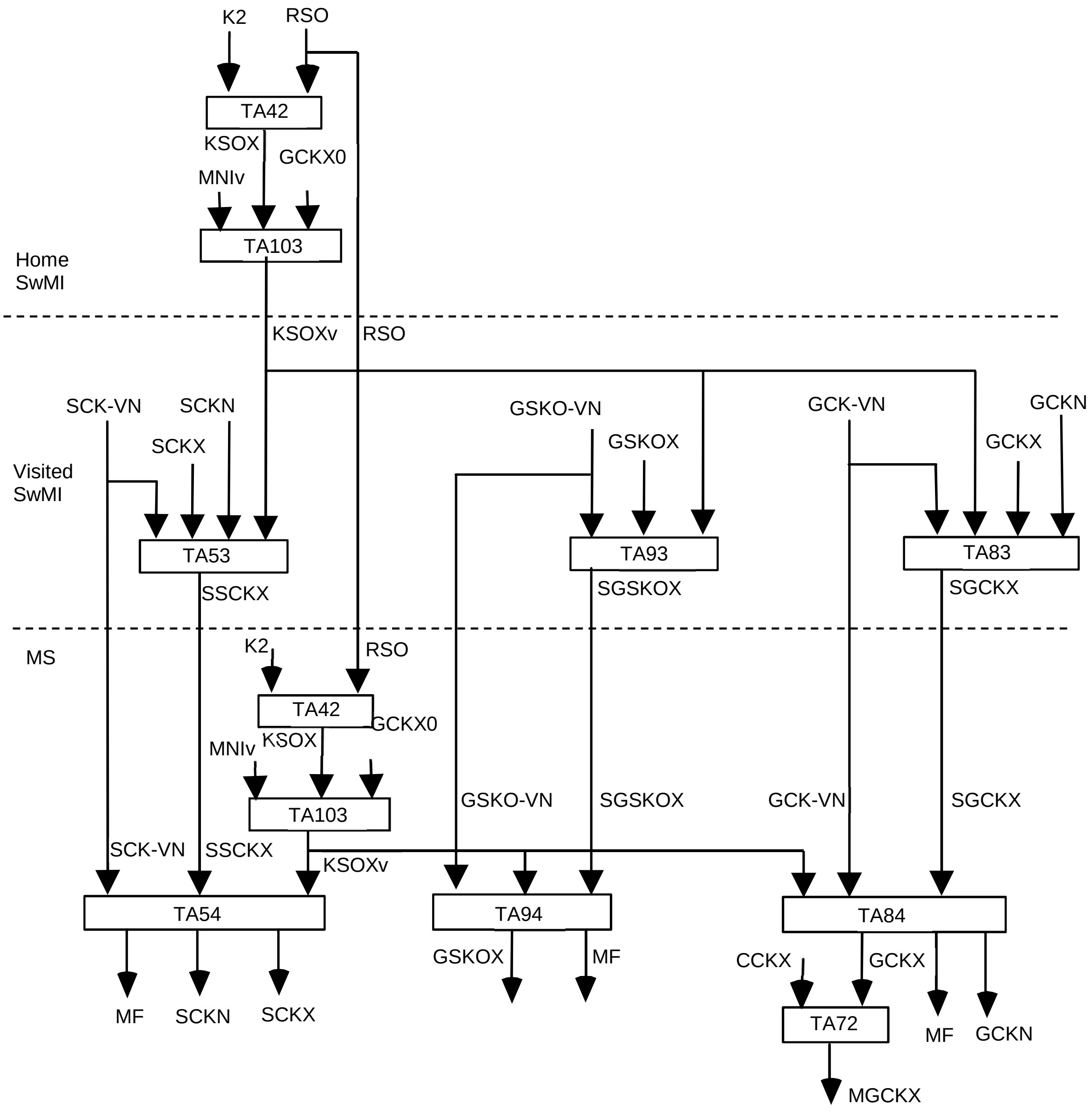


Figure B.6: Overview of provision of SCKX, GCKX and GSKOX to migrated MS where keys are sourced from the visited SwMI, and where an air interface encryption algorithm from TEA set B is in use in both home and visited SwMIs

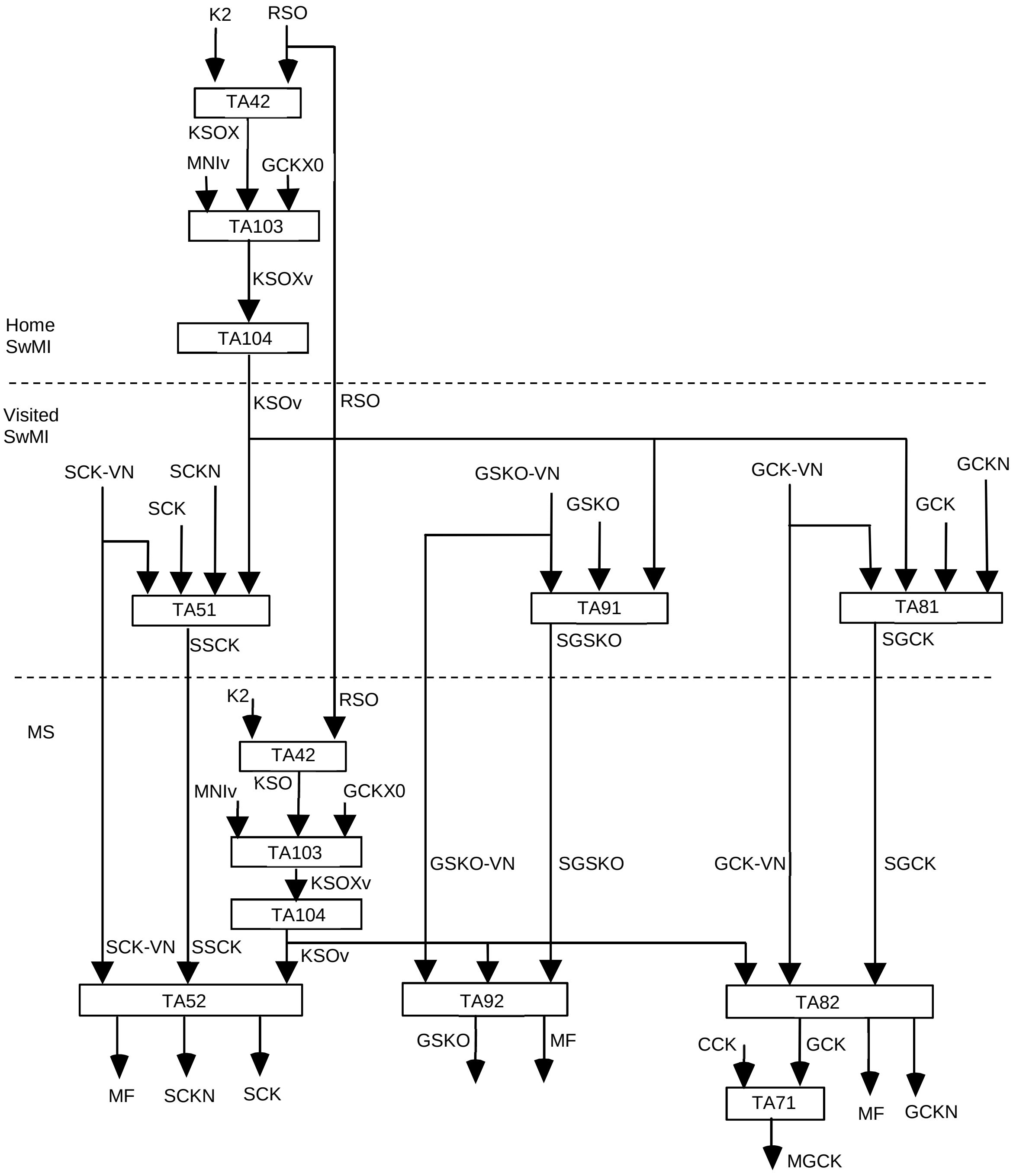


Figure B.7: Overview of provision of SCK, GCK and GSKO to migrated MS where keys are sourced from the visited SwMI, and where an air interface encryption algorithm from TEA set B is in use in the home SwMI

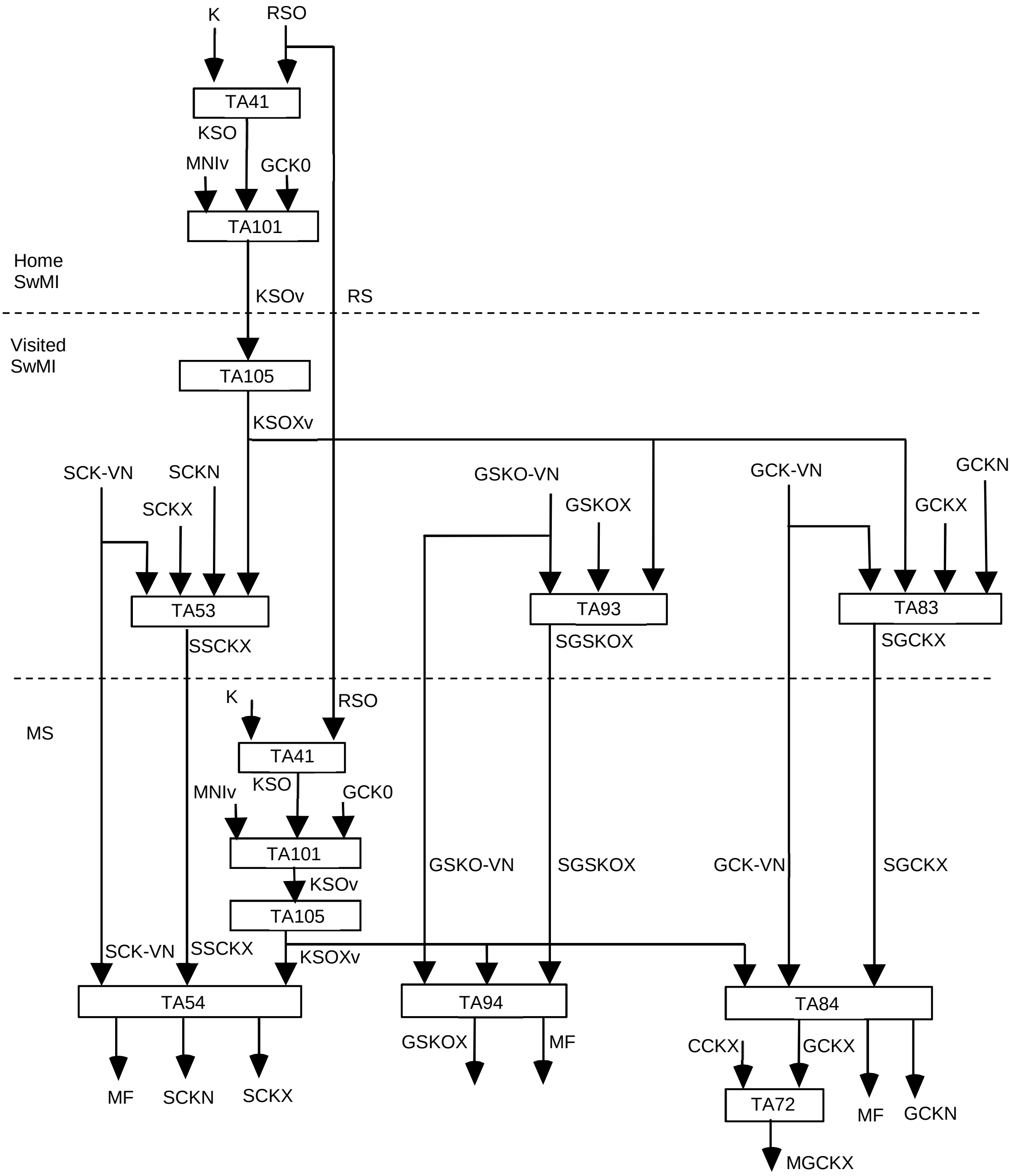


Figure B.8: Overview of provision of SCKX, GCKX and GSKOX to migrated MS where keys are sourced from the visited SwMI, and where an air interface encryption algorithm from TEA set A is in use in the home SwMI

Annex C (normative): Timers

C.1 T354, authentication protocol timer

The value of T354 shall be 30 seconds.

C.2 T371, delay timer for group addressed delivery of SCK/SCKX and GCK/GCKX

T371 is a timer with a value in seconds randomized to fall within the range 1 and the SwMI-supplied "max response timer value" (which can be given a value from 1 to 65 535, i.e. 18,2 hours).

C.3 T372, key forwarding timer

The value of T372 shall be 5 seconds.

C.4 T355, disable control timer

The value of T355 shall be at least 30 seconds.

Annex D (informative): Transition between air interface encryption algorithms in TEA set A and TEA set B

D.1 Overview

This annex provides considerations for transition of a TETRA system (SwMI and MSs) from use of an Air Interface Encryption (AIE) algorithm from TEA set A to an algorithm from TEA set B, accompanied with authentication and key management algorithms from the TAA2 algorithm set. The underlying principles that such a transition may need to follow include:

- Any loss in TETRA service for transitioning MSs (or other MSs) should be minimized
- Any loss in security class 2 or security class 3 encrypted service resulting in a period of security class 1 (clear) operation should be minimized.
- Not all MSs may be required or able to transition within the same time period.
- It is preferable for a SwMI to only support a single AIE algorithm at any one time (see clause 6.3.1), however the SwMI may be able to support two algorithms during a process of transition.
- All MSs that need to communicate in the same group using the same GSSI need to have the same algorithm and cipher key associated with the group in order to receive downlink transmissions.

The process of transition to a new AIE algorithm can be considered to have two phases. The first phase takes place while the MS population is being upgraded to install the new algorithm. The second phase takes place once the MS population has been upgraded, and the actual transition (switch over) to the new algorithm is carried out. The first phase can take a long time (e.g. months), depending on the size of the MS population. The second phase should be much faster (e.g. minutes or hours).

This annex considers cases where a SwMI can support a single AIE algorithm, and where a SwMI can support two AIE algorithms for different MS populations at the same time. It also considers cases where an MS can support more than one algorithm, and can negotiate the algorithm to be used with the SwMI at registration, and where the MS can only support a single algorithm.

A SwMI that can support more than one AIE algorithm may be able to support separate MS populations, where each population is using a different AIE algorithm. Individual calls will be possible between MSs in different populations, but encrypted downlink group communication to a GSSI can only be sent using a single AIE algorithm and cipher key, and so can only be sent to one population of MSs.

If the SwMI and MSs support the information request protocol (see clause 4.4a), the SwMI can keep track of the algorithms supported by individual MSs, and use this information to determine when the actual transition phase can take place.

D.2 Algorithm support

D.2.1 General

An MS is only permitted to negotiate and use a single Air Interface Encryption (AIE) algorithm during a period of registration with the SwMI. However, an MS may support more than one AIE algorithm to allow negotiations of different algorithms at different registrations with the SwMI. This may ease the process of transition.

The following clauses describe the implications for the use of AIE during the phases of MS population upgrade and the transition itself, depending on the capabilities of the SwMI and MS to support one or more authentication and AIE algorithm sets. The resulting AIE capabilities are summarized in Table D.1 in clause D.4.2.

Some of the transition scenarios described in these following clauses will require a period of operation using security class 1 (clear operation). This will expose signalling and user traffic at the air interface. To avoid exposure of user traffic, the use of end-to-end encryption could be considered.

D.2.2 SwMI dependencies

It is preferable for a SwMI to only support a single AIE algorithm at any one time (see clause 6.3.1), however the SwMI may be able to support two algorithms during a transition process.

It is only possible to support a single identity encryption/decryption mechanism (ESI or MAE) in a Location Area to avoid conflicts between encrypted identities generated with two different algorithms. Thus ESI using TA61 needs to be used for identity encryption if any MSs within an LA negotiate use of a KSG from TEA set A. As an MS does not renegotiate KSGs when roaming from one LA to another, in practice a region and probably an entire SwMI will need to maintain use of ESI with TA61 unless all MSs that are served by the SwMI negotiate a KSG from TEA set B.

A secure transition process should be possible if the SwMI can support MSs that are provisioned with K2 negotiating a KSG from TEA set A at the same time as supporting other MSs that also negotiate use of the same KSG from TEA set A that are provisioned with K. An MS provisioned with K2 uses the TA13 algorithm from the TAA2 algorithm set to generate session keys used for authentication, as described in clause 4.1. Support of both session key mechanisms at the same time will permit MS by MS upgrade while maintaining the use of AIE.

If the SwMI requires all MSs to either support authentication using K or authentication using K2, but not a mixture of the two, the SwMI will need to be configured to operate in security class 2 during the transition, if the MSs can support more than one algorithm (see clause D.2.3 below). If the SwMI cannot support both authentication mechanisms at the same time and the MS can only support a single algorithm (see clause D.2.4 below), or if the SwMI does not support security class 2 operation, the SwMI will need to be configured to operate in security class 1 during the transition process, and in this case all communications will be carried in clear until transition is complete. The SwMI changes the security class on a BS by sending a D-CK CHANGE Demand PDU, with the "Change of security class" element identifying the new security class. A security class of security class 1 applies to all communications on the BS. A security class of security class 2 or security class 3 applies to all encrypted communications on the BS, while still allowing communications in security class 1 where so configured.

D.2.3 MSs able to support more than one algorithm

An MS that is able to support more than one algorithm and initially only supports the TEA set A algorithm can be upgraded to add the TEA set B algorithm together with the required algorithms from the TAA2 algorithm set. At the same time, the MS can be loaded with the K2 authentication key, and the same K2 loaded to the Authentication Centre (AuC) in the SwMI. This requires the SwMI to support authentication of MSs using K and the TAA1 algorithm set at the same time as supporting authentication of MSs using K2 and the TAA2 algorithm set as described in clause D.2.2 above.

NOTE: The method for upgrading the MS is outside the scope of the present document, but may include reprogramming, or changing some form of hardware such as a SIM card or module.

D.2.4 MSs only able to support one algorithm

An MS that can only support a single AIE algorithm is assumed to have the TEA set A algorithm deleted when the TEA set B algorithm is loaded. In this case, the SwMI needs to switch those MSs and the groups that they use to security class 1 operation while the MSs are upgraded. AIE can only be restored in the SwMI for those MSs after all MSs have been loaded with the TEA set B algorithm. In practice, this may mean that the entire SwMI operates in security class 1 while the MSs are upgraded.

As each MS is upgraded, the K2 authentication key can be loaded to the MS, and the same K2 loaded to the AuC in the SwMI. This requires the SwMI to support authentication for MSs using K and the TAA1 algorithm set at the same time as MSs using K2 and the TAA2 algorithm set. If the SwMI only supports a single authentication session key generation process, authentication will need to be switched off during the upgrade and transition process, which means that no security is possible while the upgrade takes place (unless end-to-end encryption is used between MSs).

D.3 Group and broadcast communication during transition

D.3.1 Group communication

A downlink group communication can only be encrypted with a single algorithm and single key. This requires that all MSs that use a particular group transition to the new algorithm at the same time unless some loss of group communications is accepted. The SwMI needs to ensure that the correct algorithm is used for transmission to each group. To avoid loss of group communications, the downlink group transmissions could be switched to clear operation during the transition process. Alternatively, the SwMI will need to support the group of MSs with two separate GSSIs, where one GSSI is used to support MSs using the TEA set A algorithm, and another GSSI is used to support MSs using the TEA set B algorithm, and the same content is sent to both groups. This will increase the downlink capacity demanded of the SwMI, which needs to be taken into account in the traffic planning of affected BSs on the SwMI.

A group that uses CCK or CCKX in security class 3 can support encrypted downlink communications as soon as its MSs have been registered using the relevant AIE algorithm, have authenticated to establish a DCK(X) and have received the CCK(X).

If a group uses GCK or GCKX in security class 3G to encrypt group communications with an MGCK(X), the MSs will also need to receive OTAR of the relevant GCK(X). This may necessitate receiving individually addressed OTAR of GCK(X), or receiving individually addressed OTAR of GSKO(X) followed by group addressed OTAR of GCK(X). There may be service interruption to downlink group transmissions during transition while MSs are waiting to receive OTAR of GCK(X), and also there may be an additional capacity demand on the SwMI to send the OTAR. It may be preferable to switch operation to ecurity class 3 from security class 3G for those groups during the transition process (using the D-CK CHANGE Demand PDU), to allow OTAR of GCK(X) to be performed gradually, and to return to security class 3G operation only after all MSs have received the relevant GCK(X)s. Thus, to avoid any loss in communication in a group that normally uses security class 3G, it may be necessary to use security class 1 operation while all MSs that are group members re-register with a new KSG, and then switch to security class 3 once the re-registration has completed, and finally to switch to security class 3G once OTAR of GCKX has been completed.

D.3.2 Broadcast communications

Broadcast communications intended for all MSs are sent to a single broadcast address. If MSs using different algorithms are receiving service from the same BS, broadcast transmissions need to be sent in clear. An MS will not be able to decrypt a broadcast transmission encrypted with a different algorithm to that negotiated by the MS, and a failed decryption may cause erroneous operation.

D.4 Transition scenarios for TMO

D.4.1 Transition overview

As described in clause D.1, there are two phases leading to a transition: a first phase during which the new algorithm is loaded to the MS population, and a second phase during which the actual transition takes place. The possible states of AIE in MS and SwMI during the first phase are summarized in Table D.1 below.

At the time of the actual transition, to support security class 3 operation MSs need to re-register and negotiate the new KSG, derive a DCK(X) from the authentication process and be provided with CCK(X) by OTAR. As described in previous clauses, this may cause a short loss of service (especially for group calls) as the process takes place across the MS population, and an increased capacity demand on the SwMI due to the registration and OTAR signalling.

In security class 2 operation, there is a similar issue as the MS will need to re-register with the SwMI and to be provided with the TMO SCK(X) by OTAR, unless the SCKX can be provided in advance by an out of band method.

NOTE 1: The possibility of using one of SCKNs 31 or 32 for the TMO SCK pre-transition, and the other SCKN of 31 or 32 post transition may allow correct selection of TMO SCK(X) before and after transition.

NOTE 2: An MS cannot receive OTAR of an SCKX when it has negotiated a KSG from TEA set A, hence an out of band method to provision SCKX in advance would be needed.

The loss of service due to the time taken for OTAR of cipher keys (in security class 2 or security class 3 operation) can be mitigated by temporarily operating the SwMI in security class 1.

Where GCK is used for group calls, capacity loading on the SwMI or temporary interruption to service for MS requiring OTAR of GCK(X) for group communication may be mitigated by operating in security class 3 instead of security class 3G as described in clause D.3, allowing the OTAR load to be spread out in time.

The following clauses describe the possible encryption classes that can be used by SwMI and MS during the process of loading the new set B algorithm to the MS, and then the means for transition once all MSs are capable of operation with the new algorithm.

D.4.2 Encryption class while loading set B algorithm to MSs

If the SwMI supports use of two algorithms at the same time, and if group communications are not required, each MS can negotiate use of the TEA set B algorithm at the first registration following its upgrade, and MSs can be upgraded one by one and maintain use of their normal encryption class with the SwMI. Identity encryption using ESI with TA61 needs to be used for all MSs. If group communications are needed, and loss of group communications is not acceptable, the TEA set B algorithm cannot be used until all members of each group have been upgraded with the TEA set B algorithm. In practice, as MSs generally use many groups, this means delaying the activation of the TEA set B algorithm until an MS fleet has been upgraded.

Table D.1 below shows the possible classes of operation of the SwMI and MSs while an MS fleet is being upgraded to add the TEA set B algorithms, where group communications cannot be lost.

Table D.1: Encryption class while MS fleet is being loaded with new algorithms

Constraints			Encryption class during transition	Scenario
1	2	3		
MS can only be loaded with one algorithm at a time			Switch to security class 1 until all MSs have been upgraded See note 1	1
MS can be loaded with two algorithms at the same time SwMI supports session key generation using K and TA11/TA21 only	SwMI does not support security class 2		Switch to security class 1 until all MSs have been upgraded See note 1	2a
	SwMI supports security class 2	MS does not support security class 2	Switch to security class 1 until all MSs have been upgraded See note 1	2b
		MS supports security class 2	Switch to security class 2 using TEA set A algorithm until all MSs have been upgraded See note 2	2c
MS can be loaded with two algorithms at the same time SwMI supports session key generation using K and TA11/TA21 as well as using K2 and TA13			Maintain security class 3 (or security class 2 if SwMI normally uses security class 2) with TEA set A algorithm until all MSs have been upgraded.	3

NOTE 1: If the SwMI supports use of KSGs from both TEA set A and TEA set B at the same time, only those MSs that are to transition need to be switched to security class 1 during transition (by negotiating the use of security class 1 at registration). All groups used for communication by the transitioning MSs also need to be switched to security class 1.

NOTE 2: If the SwMI supports use of KSGs from both TEA set A and TEA set B at the same time, all of the BSs that provide service to the transitioning MSs need to switch to security class 2 during transition. A BS can either support security class 2 or security class 3, but not both together.

The security class of a cell can be changed by ensuring that support for the new security class is broadcast in the SYSINFO PDU, and changing the security class using the D-CK CHANGE Demand PDU. If the MS has a security policy that does not permit the use of security class 1, the security policy may need to be temporarily changed to permit security class 1 during the upgrade phase.

D.4.3 Encryption during transition

Once the TEA set B algorithm has been loaded to the MS population, MSs need to be re-registered with the SwMI and to negotiate the TEA set B algorithm. In general, to minimize the time taken for transition and to minimize the time spent using a different encryption class to the normal encryption class, the transition should take place at a time of low system load (e.g. during the night). An MS can be re-registered by the SwMI if the BS sends a D-LOCATION UPDATE COMMAND PDU to initiate the re-registration process. Alternatively, the user could perform an action on the MS to initiate the re-registration (e.g. switching the MS off and on again).

An MS may attempt to re-register with encryption applied using its last encryption parameters if DCK retrieval is supported, and the DCK and CCK have been stored, and the CCK-id broadcast by the BS has not changed. To avoid such an attempted encrypted registration using the previous KSG, the CCK-id broadcast by the SwMI should be advanced to a CCK-id that does not have an associated CCK stored by the MS when transition commences. If the MS attempted an encrypted registration using the TEA set A algorithm and keys once the SwMI has activated the TEA set B algorithm, the encrypted registration would fail and the MS would revert to a clear location update. This is due to conflicts in identity encryption and due to the failure to decrypt signalling encrypted with an incorrect key or algorithm. However, a failed encrypted registration and reversion to clear would lead to unnecessary loading on the control channel, hence it is preferable to ensure that the registration is carried out in clear.

If the SwMI had been configured to use security class 1 while MSs are loaded with the TEA set B algorithm, i.e. scenarios 1, 2a and 2b in Table D.1, then the SwMI can broadcast support for security class 1 and security class 2 or security class 1 and security class 3, and re-register each MS in turn negotiating the TEA set B algorithm. The SwMI can maintain the use of security class 1 in the cell until the MS population has been re-registered, and then revert to security class 2 or security class 3 to avoid any loss of group communications.

If the SwMI had been configured to use security class 2 or security class 3 while MSs are loaded with the TEA set B algorithm, i.e. scenarios 2c and 3 in Table D.1, to avoid the loss of group communications the SwMI can be configured for security class 1 operation during the transition process. The cell is switched to security class 1 by use of the D-CK CHANGE Demand PDU. Each MS can be re-registered in turn negotiating the TEA set B algorithm. Once the MS population has negotiated the TEA set B algorithm, security class 2 or security class 3 operation can be restored.

NOTE: It would be possible for the SwMI to simply send downlink group communications in clear to avoid loss of group communications, while MSs are registering for encrypted operations, and using encrypted communications on the uplink. However if the uplink communications are sent encrypted, this would lead to a known plaintext attack on MSs' DCKXs and so is not advisable.

If the SwMI normally uses security class 3G, it is recommended to change to security class 3 operation until after the transition is complete, so that GCKXs for use with the TEA set B algorithm can be sent by OTAR later. This will reduce the system load during transition (by reducing the amount of OTAR signalling that is necessary).

For security class 3 operation, every MS needs to authenticate to generate a DCKX for use with the TEA set B algorithm, and needs to receive OTAR of CCKX before encrypted communications are possible. For security class 2 operations, every MS needs to receive OTAR of SCKX (or to be manually provisioned with the SCKX) before encrypted communications are possible. Any security class 1 operation should therefore remain in place until all MSs have authenticated and received the CCKX (or SCKX). Note that an MS may roam between BSs, and so the same encryption algorithm(s) need to be in use on all BSs where an MS may request service. This may mean that the switch to security class 1 and renegotiation of algorithm needs to occur at the same time on all BSs.

If the SwMI only supports a single algorithm at a time,MAE address encryption can be used immediately when encryption in security class 2 or security class 3 is resumed using the KSG from TEA set B. If the SwMI supports both a TEA set A and a TEA set B algorithm for different MS populations when security class 2 or security class 3 is resumed, ESI identity encryption needs to be used.

If different organizations sharing the same SwMI transition to a TEA set B algorithm at different times, and if the SwMI supports two algorithms at the same time, ESI identity encryption will be used for all MSs while both algorithms are active on the SwMI. Once all MSs have transitioned to a TEA set B algorithm, the SwMI can negotiate the use of MAE address encryption with the MSs. However, to avoid conflicts in encrypted identities, the SwMI will again need to be switched to security class 1 operation while the re-registration and algorithm negotiation takes place for all MSs.

D.5 Transition scenarios for DMO

D.5.1 General

DMO security is specified in ETSI EN 300 396-6 [5]. Transition scenarios are provided in this annex for completeness.

D.5.2 MS to MS DMO operation

DMO operation normally associates a KAG of SCKs/SCKXs to the GSSI of a group, as described in clause 4.2.4.1 of the present document. A KAG should only contain either SCKs or SCKXs but not both, and all keys within a KAG should be associated with the same KSG. Exceptionally for transition purposes, a KAG may contain both SCK(s) associated with a KSG from TEA set A and SCKX(s) associated with a KSG from TEA set B. Use of both SCKs and SCKXs within a KAG is likely to require the MS to be able to dynamically load a KSG on reception of the SCKN and KSG number in the DMAC-SYNC PDU at the start of a transmission.

If the MS to be able to dynamically load a KSG on reception of the SCKN and KSG number in the DMAC-SYNC PDU at the start of a transmission and a KAG is able to contain both SCKs and SCKXs, DMO groups can be transitioned from use of a TEA set A algorithm to a TEA set B algorithm by maintaining the association of the KAG to the group with an SCK active until the MSs have transitioned to the TEA set B algorithm in TMO. Once MSs are operating in TMO with the TEA set B algorithm, an SCKX can be provided by OTAR to the KAG associated with the GSSI of the group, overwriting an SCK with an inactive SCKN. Once all MSs have been provided with the SCKX, MSs are then instructed to start using the SCKX for transmissions to the group by the SwMI sending a D-CK CHANGE Demand PDU activating the SCK subset that contains the SCKX. If MSs receive the changeover command at different times to each other, some may transmit using SCK and some may transmit using SCKX, hence the need to dynamically load the algorithm when the SCKN is received at the start of a transmission.

If the MS can support two algorithms, but not dynamically switch between algorithms when receiving a DMO transmission, the simplest means of transition is to use different DMO groups for pre-transition and post-transition. A pre-transition group can be associated with a KAG containing only SCKs that are for use with the TEA set A KSG, and the post-transition group associated with a KAG containing only SCKX s that are for use with the TEA set B KSG. Once all MSs using the group have been provisioned with SCKX, they can use the post-transition group (and the pre-transition group can be rekeyed with SCKX if needed). In order to support this approach, the MS will need to have additional groups provisioned. The organization will need to decide when to start using the groups provisioned with SCKX and the TEA set B KSG, and the end users need to be informed in advance of the time to avoid losing any communications.

If MSs can only support one algorithm, it is likely that DMO groups will need to use security class 1 while those MSs are being upgraded to the TEA set B algorithm. These DMO groups could either be groups that are normally used by the transitioning MSs, which are set to clear operation for the duration of transition, or could be additional groups used for the transition process. In this case, the 'normal' groups could be provisioned with SCKX by OTAR once the MSs have transitioned, ready for post-transition use when all MSs have been upgraded. As in the previous case, end users need to be informed when to start using the alternative groups.

If loss of user traffic protection due to the use of security class 1 is not acceptable, the use of end-to-end encryption could be considered.

Where an MS supports both KSGs from TEA set A and TEA set B, irrespective of whether dynamic switching between KSGs is possible, the SCKs do not need to be deleted until after transition is complete. This may allow reversion to the original set A KSG and use of SCK in case there are problems with the transition.

D.5.3 DMO repeater operation

A repeater operating in security class DM-2-A does not need to have the capability to encrypt or decrypt messages, and passes the encrypted Layer 2 MAC elements without change. Thus there should not be any dependencies on the repeater when transitioning to TEA set B algorithms.

A repeater operating in security class DM-2-B may not need the capability to decrypt signalling unless the destination address of a transmission is checked. If destination address checking is needed, then the repeater needs to support the KSGs and SCKs/SCKXs allocated to MSs and groups that make use of the repeater.

A repeater operating in security class DM-2-C is required to decrypt signalling and identities sent to the repeater by a transmitting DM-MS, and to encrypt signalling as necessary when sent to a slave DM-MS. Thus the repeater needs to support the KSGs and SCKs/SCKXs allocated to MSs and groups that make use of the repeater.

If the repeater can dynamically switch between two KSGs, the groups can be provisioned with different SCKs and SCKXs for different crypto periods, and transition can be made in the same way that is possible for DM-MSs.

If the repeater cannot dynamically switch between two KSGs, separate groups will be needed for use with TEA set A and TEA set B algorithms, as has been described in clause D.5.1. If the repeater has this constraint, separate groups will be needed even if the DM-MSs are capable of dynamically switching between KSGs.

If the repeater can only support a single KSG, different repeaters need to be used for pre-transition and post-transition operation with a DMO group.

D.5.4 DMO gateway operation

A gateway carries out encryption independently on the TMO and DMO links. Thus transition in DMO needs to follow that required by the DM-MSs and DMO groups, and transition in TMO needs to follow that required by the SwMI.

If the gateway can only support one KSG, or can only support one KSG on both the DMO and TMO links in the same call, transition in DMO needs to be synchronized to transition in TMO.

If the gateway can support more than one KSG and can support separate KSGs on each link, DMO and TMO transition can remain independent.

Annex E (informative): Bibliography

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

- ETSI ES 202 109: "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption".

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

- ETSI Drafting Rules contained in the ETSI Directives.

NOTE: Available at https://portal.etsi.org/Resources/ETSI-Directives.

Annex F (informative): Change request history

The following CRs have been incorporated in the present document.

CR	Date	Version	Short description	Status
103	17-3-05	V2.2.1	Definition of security related information and group identity security related information element	**WG6 approved (updated)**
113	9-3-06	V3.0.0	Encryption of π/8 D8PSK and QAM logical channels	**WG6 approved**
124	11-1-07	V3.0.0	Inclusion of timer between disable intent and disable confirm PDUs	**WG6 approved**
125	4-10-06	V3.0.0	ETSI TS 100 392-7 v2.4.0 incorporates PDU elements whose use is not described in protocol section: this CR provides text to correct this	**WG6 approved**
126	29-10-06	V2.4.1	Editorial changes recommended by ETSI editHelp on review of ETSI TS 100 392-7v2.4.1	**WG6 approved**
128	12-12-06	V2.4.1	Definitions for DCK Forwarding and DCK Retrieval	**WG6 approved**
129	14-12-06	V2.4.1	Clarification on behaviour on deletion of CMG GSSI	**WG6 approved**
131	1-3-07	V3.0.0	Boundary conditions for TA101	**WG6 approved**
132	12-4-07	V3.0.0	Removal of spurious value for GCK Select Number	**WG6 approved**
133	14-5-07	V3.0.0	Clarification of status of CK after disable	**WG6 approved**
134	5-6-07	V3.0.0	Correction of Figure 39 in clause 5.1	**WG6 approved**
137	22-6-07	V3.0.0	Removal of mandates from scope clause	**WG6 approved**
138	20-7-07	V3.0.0	Explicit mention of pi/8-D8PSK modulation	**WG6 approved**
139	26-11-07	V3.0.2	Correction of the D-OTAR and U-OTAR PDUs	**WG6 approved**
130	1-3-07	V3.1.1	Extension of scope to explicitly cover ISI security	**WG6 approved**
135	6-6-07	V3.1.1	Authentication of MS when migrated (use of KSv)	**WG6 approved**
136	6-6-07	V3.1.1	Authentication of SwMI when migrated (use of KSv')	**WG6 approved**
201	15-4-08	V3.1.1	Multiple OTAR keys request and change to OTAR retry mechanism	**WG6 approved**
202		V3.1.1	ISI support for CK transfer to, and for use in, vSwMI	**WG6 approved**
203		V3.1.1	Addition of multiple AIE key sets and mutual authentication for ISI operation	**WG6 approved**
205	8-7-09	V3.1.1	Correction of editorial errors concerning ciphering parameters	**Not fully implemented**
206	8-7-09	V3.1.1	Key associations for temporary group addresses	**WG6 approved**
120	26-6-06	V2.3.1	Use of LIP during temporary disable	**WG6 approved**
205	8-7-09	V3.2.1	Correction of editorial errors concerning ciphering parameters	**WG6 approved**
301	12-11-10	V3.2.2	New security services IE	**WG6 approved**
302	12-11-10	V3.2.2	Definition of GCK0	**WG6 approved**
303	14-09-11	V3.2.3	Direct Access changes	**WG6 approved**
304	06-09-15	V3.3.2	Definitions of session keys for visited networks	**WG6 approved**
306	06-09-15	V3.3.2	Clarification on the usage of authentication method on migration	**WG6 approved**
307	06-09-15	V3.3.2	Missing U-DISABLE STATUS in diagrams	**WG6 approved**
308	06-09-15	V3.3.2	Correction of references to SIM standards	**WG6 approved**
309	06-09-15	V3.3.2	Reference error in proprietary element	**WG6 approved**
310	06-09-15	V3.3.2	Addition of Hardware/Software version number reporting	**WG6 approved**
311	06-09-15	V3.3.2	Use of timer T354	**WG6 approved**
312	06-09-15	V3.3.2	Algorithm rules	**WG6 approved**
313	06-09-15	V3.3.2	DCK and CCK storage in visited SwMI	**WG6 approved**
314	24-12-15	V3.3.4	T354 stop during location update	**WG6 approved**
315	30-08-18	V3.4.1	Authentication failure cases	**WG6 approved**
316	23-09-22	V3.5.1	Inclusion of additional authentication, air interface key management and air interface encryption algorithms	

History

Document history		
Edition 1	December 1996	Publication as ETSI ETS 300 392-7 (Historical)
V2.1.1	December 2000	Publication
V2.1.1	February 2001	Publication as ETSI EN 300 392-7
V2.2.1	September 2004	Publication as ETSI EN 300 392-7
V2.3.1	June 2006	Publication as ETSI EN 300 392-7 (Withdrawn)
V2.4.1	October 2006	Publication
V3.1.1	June 2008	Publication as ETSI EN 300 392-7
V3.2.1	June 2010	Publication as ETSI EN 300 392-7
V3.3.1	July 2012	Publication as ETSI EN 300 392-7
V3.4.1	January 2017	Publication as ETSI EN 300 392-7
V3.5.1	July 2019	Publication as ETSI EN 300 392-7
V4.1.1	October 2022	Publication