3GPP TSG-SA3
Washington, D.C.
12-14 September 2000

Tdoc 3GPP S3-000504

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102 CR XXX Current Version: 3.5.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	SA #9	for approval	□	strategic	□	*(for SMG use only)*
list expected approval meeting # here ↑		for information	□	non-strategic	□	

Form: CR cover sheet, version 2 for 3GPP and SMG The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM □ ME □ UTRAN / Radio □ Core Network ☒
(at least one should be marked with an X)

Source:	T-Mobil	**Date:**	21.08.00
Subject:	Re-introduction of MAP application layer security		
Work item:	CNSS: Protection of MAP Application Layer		

Category:	F	Correction	□	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	☒		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	□
					Release 00	☒

Reason for change:	Introduction of MAP application layer security
Clauses affected:	Ch. 2.1, ch.3.3, ch. 7

Other specs affected:	Other 3G core specifications	□	→ List of CRs:	TS 33.103
	Other GSM core specifications	□	→ List of CRs:	
	MS test specifications	□	→ List of CRs:	
	BSS test specifications	□	→ List of CRs:	
	O&M specifications	□	→ List of CRs:	

Other comments:	The algorithms to be used and the structure of the security header remain to be specified.

help.doc

<--------- Double-click here for help and instructions on how to create a CR.

2 References

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

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

2.1 Normative references

[1] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2] 3G TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[3] UMTS 33.21, version 2.0.0: "Security requirements".

[4] UMTS 33.22, version 1.0.0: "Security features".

[5] UMTS 33.23, version 0.2.0: "Security architecture".

[6] Proposed UMTS Authentication Mechanism based on a Temporary Authentication Key.

[7] TTC Work Items for IMT-2000 – System Aspects.

[8] Annex 8 of "Requirements and Objectives for 3G Mobile Services and systems" – "Security Design Principles".

[9] ETSI GSM 09.02 Version 4.18.0: Mobile Application Part (MAP) Specification.

[10] ISO/IEC 11770-3: *Key Management – Mechanisms using Asymmetric Techniques*.

[11] ETSI SAGE: Specification of the BEANO encryption algorithm, Dec. 1995 (confidential).

[12] ETSI SMG10 WPB: SS7 Signalling Protocols Threat Analysis , Input Document AP 99-28 to SMG10 Meeting#28, Stockholm, Sweden.

[13] 3G TS 33.105: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Cryptographic Algorithm Requirements".

[13a] 3G TS 23.003: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) Core Network (CN); Numbering, addressing and identification".

[13b] 3G TS 23.060: "3rd Generation Partnership Project; Technical Specification Group and System Aspects; Digital cellular telecomunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[13c] 3G TS 29.002: “ 3rd Generation Partnership Project;Technical Specification Group Core Network; Mobile Application Part (MAP) specification”.

2.2 Informative references

GSM documents:

[14] GSM 02.09 version 5.1.1: "Security Aspects".

[15] GSM 02.22 version 6.0.0: "Personalisation of GSM Mobile Equipment (ME); Mobile functionality specification".

[16] GSM 02.48, version 6.0.0: "Security Mechanisms for the SIM Application Toolkit; Stage 1".

[17] GSM 02.60, version 7.0.0: "GPRS; Service Description; Stage 1".

[18] GSM 03.20, version 6.0.1: "Security related network functions".

[19] GSM 03.48, version 6.1.0; "Security Mechanisms for the SIM application toolkit; Stage 2".

[20] GSM 03.60, version 7.0.0: "GPRS; Service Description; Stage 2".

[21] GSM 11.11, version 7.1.0: "Specification of SIM-terminal interface".

[22] GSM 11.14, version 7.1.0: "Specification of SIM Application Toolkit for SIM-terminal interface".

UMTS documents:

[23] UMTS 21.11, version 0.4.0: "IC-card aspects".

[24] UMTS 23.01, version 1.0.0: "UMTS Network architecture".

[25] UMTS 23.20, version 1.4.0: "Evolution of the GSM platform towards UMTS".

3.3 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
KAC	Key Administration Center
KSI	Key Set Identifier
KSS	Key Stream Segment
KS_{XY}(con)	Confidentiality Session Key
KS_{XY}(int)	Integrity Session Key
LAI	Location Area Identity
MAC	Message Authentication Code
MAC-A	The message authentication code included in AUTN, computed using f1
ME	Mobile Equipment
MS	Mobile Station
MSC	Mobile Services Switching Centre
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector

RAI	Routing Area Identifier
RAND	Random challenge
SA	Security Association
SQN	Sequence number
SQN_{HE}	Sequence number counter maintained in the HLR/AuC
SQN_{MS}	Sequence number counter maintained in the USIM
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TMSI	Temporary Mobile Subscriber Identity
TVP	Time Variant Parameter
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
USIM	User Services Identity Module
VLR	Visitor Location Register
XRES	Expected Response

NEXT MODIFIED SECTION

7 Network domain security mechanisms

This subclause describes mechanisms for establishing secure signalling links between network nodes, in particular between SN/VLRs and HE/AuCs, communicating with the protocols MAP and CAP. Such procedures may be incorporated into the roaming agreement establishment process.

7.1 Overview of Mechanism

The proposed mechanism consists of three layers.

7.1.1 Layer I

Negotiations take place in Layer I between the KACs (Key Administration Centers) of two different network operators in order to establish one or several SAs (Security Associations), to be used for the communication between the network elements themselves in Layer III. An SA consists of paramters needed for (integrity and/or confidentiality) protected exchanges, such as cryptographic keys or (an indicator of) the cryptographic algorithm used.

7.1.2 Layer II

In Layer II the agreed Security Associations for sending and receiving data are distributed by the KACs in each network to the relevant network elements. For example, an AuC will normally send sensitive authentication data to VLRs belonging to other networks and will therefore get an SA from its KAC. Layer II is carried out entirely inside one operator's network.

7.1.3 Layer III

Layer III uses the distributed SAs for securely exchanging sensitive data between the network elements of one operator (internal use) or different operators (external use) by means of a symmetric encryption algorithm. A block cipher shall be used for this purpose [13]. The encrypted (resp. authenticity/integrity-protected) messages will be transported via the MAP protocol [13c].

7.1.4 General Overview

Figure 20 provides an overview of the whole mechanism. Note that the messages are not fully specified in this figure. Rather, only the "essential" parts of the messages are given. More details on the format of the messages in the single layers will be provided in subsequent chapters.

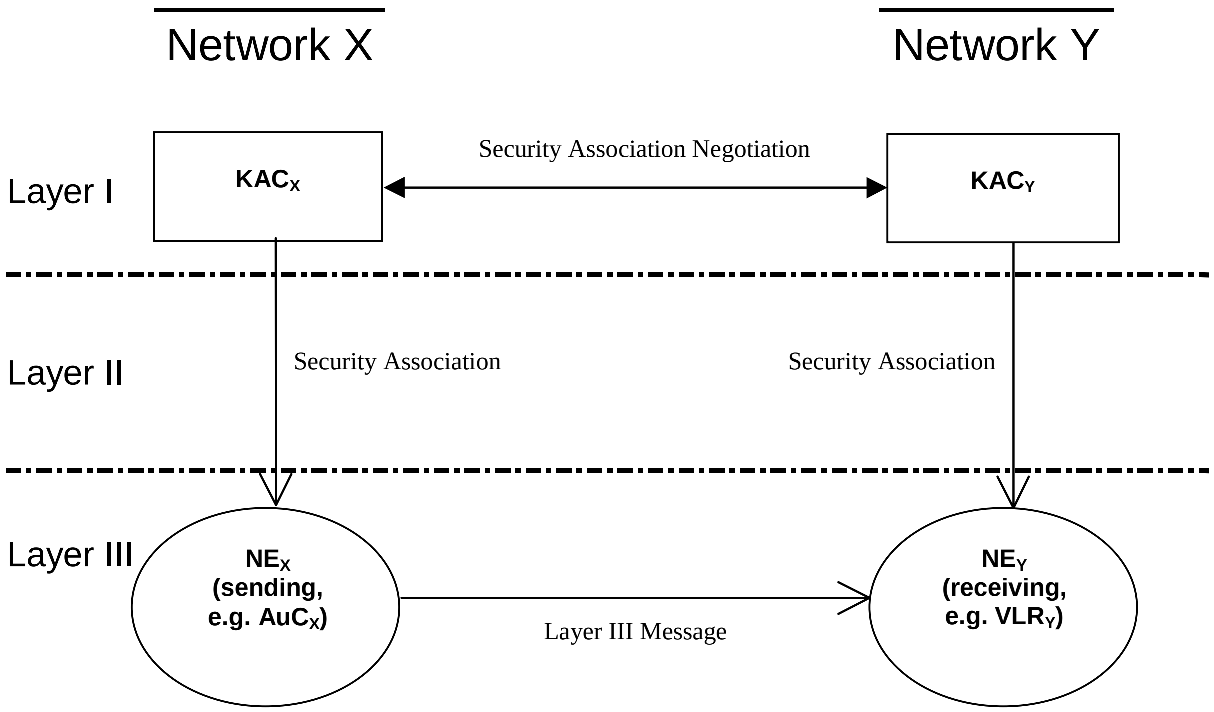


Figure 20: Overview of Proposed Mechanism

7.2 Layer I Message Format

Layer I describes the communication between two newly defined network entities of different networks, the so-called Key Administration Centres (KACs). This communication is to negotiate the SAs to be distributed in Layer II and used in Layer III.

7.3 Layer II Message Format

In Layer II, a KAC distributes a negotiated SA within its own network to those elements that have a need for such.

7.4 Layer III Message Format

7.4.1 General Structure of Layer III Messages

Layer III messages are transported via the MAP protocol, that means, they form the payload of a MAP message after the original MAP message header. For Layer III Messages, three levels of protection (or protection modes) are defined providing the following security features:

Protection Mode 0: No Protection

Protection Mode 1: Integrity, Authenticity

Protection Mode 2: Confidentiality, Integrity, Authenticity

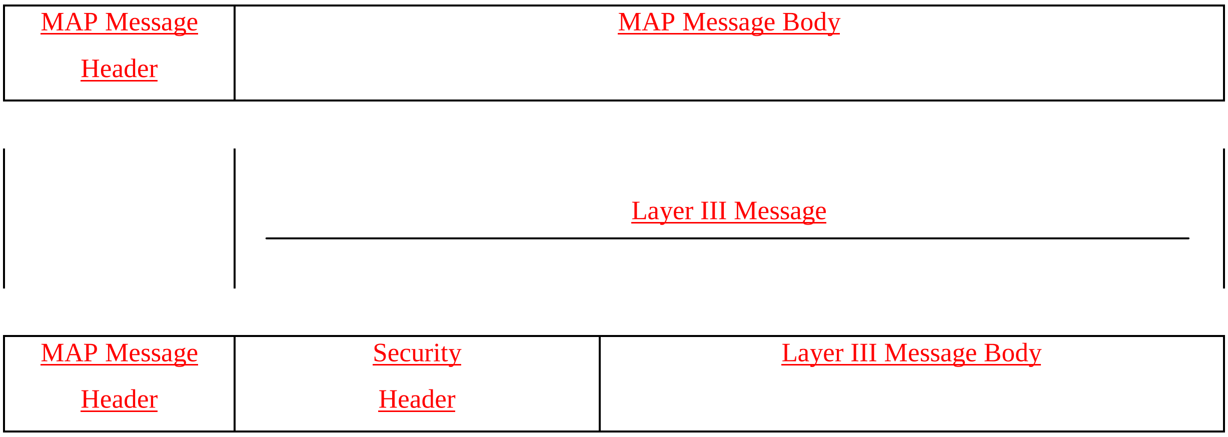
Layer III messages consists of a Security Header and the Layer III Message Body that is protected by the symmetric encryption algorithm, using the symmetric session keys that were distributed as part of the SA in layer II. Layer III Messages have the following structure:

Security Header	Layer III Message Body

In all three protection modes, the security header is transmitted in cleartext.

NOTE: The content of the security header has yet to be finalised. Probably it will be just a pointer to the applicable SA; only in the event of message dependent security parameters (e.g. counters) or something similar would these also be included.

Both parts of the Layer III messages, security header and message body, will become part of the "new" MAP message body. Therefore, the complete "new" MAP messages take the following form in this proposal:



MAP Message Header

MAP Message Body

Layer III Message

MAP Message Header

Security Header

Layer III Message Body

Like the security header, the MAP message header is transmitted in cleartext. In protection mode 2 providing confidentiality, the Layer III Message Body is essentially the encrypted "old" MAP message body. For integrity and authenticity, an encrypted hash calculated on the MAP message header, security header and the "old" MAP message body in cleartext is included in the Layer III Message Body in protection modes 1 and 2. In protection mode 0 no protection is offered, therefore the Layer III Message Body is identical to the "old" MAP message body in cleartext in this case.

Summing up, the Protected MAP Message (i.e. the Layer III Message) is a sequence of data elements consisting of the MAP Message Header, the Security Header and the Layer III Message Body. In the following subchapters, the contents of the Layer III Message Body for the different protection modes and the security header will be specified in greater detail.

7.4.2 Format of Layer III Message Body

7.4.2.1 Protection Mode 0

Protection Mode 0 offers no protection at all. Therefore, the Layer III message body in protection mode 0 is identical to the original MAP message body in cleartext.

7.4.2.2 Protection Mode 1

The message body of Layer III messages in protection mode 1 takes the following form:

TVP||Cleartext|| $H_{KSXY(int)}$(TVP|| MAP Header||Security Header||Cleartext)

where "Cleartext" is the message body of the original MAP message in clear text. Therefore, in Protection Mode 1 the Layer III Message Body is a concatenation of the following information elements:

- Time Variant Parameter TVP
- Cleartext
- Integrity Check Value

Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function H with the integrity session key KS_{XY}(int) to the concatenation of Time Variant Parameter TVP, MAP Header, Security Header and Cleartext.

The TVP used for replay protection of Layer III messages is a 32 bit time-stamp. The receiving network entity will accept a message only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

7.4.2.3 Protection Mode 2

The Layer III Message Body in protection mode 2 takes the following form:

$$\boxed{\text{TVP}\|\ E_{KSXY(con)}(\text{ Cleartext})\ \|\ H_{KSXY(int)}(\text{TVP}\|\text{ MAP Header}\|\text{Security Header}\|\ E_{KSXY(con)}(\text{ Cleartext}))}$$

where "Cleartext" is the original MAP message in clear text. Message confidentiality is achieved by encrypting Cleartext with the confidentiality session key KS_{XY}(con). Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function H with the integrity session key KS_{XY}(int) to the concatenation of Time Variant Parameter TVP, MAP Header, Security Header and $E_{KSXY(con)}$(Cleartext).

The TVP used for replay protection of Layer III messages is a 32 bit time-stamp. The receiving network entity will accept a message only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

7.4.3 Structure of Security Header

NOTE: The content of the security header has yet to be finalised. Probably it will be just a pointer to the applicable SA; only in the event of message dependent security parameters (e.g. counters) or something similar would these also be included.

7.5 Mapping of MAP Messages and Modes of Protection

The network operator should be able to assign the mode of protection to each MAP message in order to adapt the level of protection according to its own security policy. Guidance may be obtained from the SS7 Signalling Protocols Threat Analysis [12].

7.6 Distribution of security parameters to UTRAN

Confidentiality and integrity between the user and the network is handled by the UE/USIM and the RNC.

The security parameters for the confidentiality and integrity algorithms must be distributed from the core network to the RNC over the Iu-interface in a secure manner. The actual mechanism for securing these parameters has not yet been identified.