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

Tdoc 3GPP S3-000505

CHANGE REQUEST

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

33.103	**CR**	**XXX**	Current Version:	3.3.0

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

For submission to: *list expected approval meeting # here ↑*

for approval [ ]
for information [ ]

strategic [ ]
non-strategic [ ]
(for SMG use only)

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: *(at least one should be marked with an X)* (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]

Source: T-Mobil **Date:** 21.08.00

Subject: Re-introduction of MAP application level security

Work item: CNSS: Protection of MAP Application Layer

Category: *(only one category shall be marked with an X)*

F	Correction	[ ]
A	Corresponds to a correction in an earlier release	[ ]
B	Addition of feature	[X]
C	Functional modification of feature	[ ]
D	Editorial modification	[ ]

Release:

Phase 2	[ ]
Release 96	[ ]
Release 97	[ ]
Release 98	[ ]
Release 99	[ ]
Release 00	[X]

Reason for change: Introduction of MAP application level security.

Clauses affected: Ch. 3.3, ch. 5

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs: TS 33.102
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:


help.doc

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

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
~~$D_{SK(X)}$(data)~~	~~Decryption of "data" with Secret Key of X used for signing~~
~~$E_{KSXY(i)}$(data)~~	~~Encryption of "data" with Symmetric Session Key #i for sending data from X to Y~~
~~$E_{PK(X)}$(data)~~	~~Encryption of "data" with Public Key of X used for encryption~~
EMSI	Encrypted Mobile Subscriber Identity
EMSIN	Encrypted MSIN
Hash(data)	The result of applying a collision-resistant one-way hash-function to "data"
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
IV	Initialisation Vector
KAC_X	Key Administration Centre of Network X
KS_{XY}(int)	~~Symmetric~~ Integrity Session Key ~~#i for sending data from X to Y~~
KS_{XY}(con)	Confidentiality Session Key
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAP	Mobile Application Part
MAC	Message Authentication Code
MAC-A	The message authentication code included in AUTN, computed using f1
MS	Mobile Station
MSC	Mobile Services Switching Centre
MSIN	Mobile Station Identity Number
MT	Mobile Termination
NE_X	Network Element of Network X
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
~~RND_X~~	~~Unpredictable Random Value generated by X~~
SQN	Sequence number
SQN_{UIC}	Sequence number user for enhanced user identity confidentiality
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
TE	Terminal Equipment
TEMSI	Temporary Encrypted Mobile Subscriber Identity used for paging instead of IMSI
Text1	Optional Data Field
Text2	Optional Data Field
Text3	Public Key algorithm identifier and Public Key Version Number (eventually included in Public Key Certificate)
TMSI	Temporary Mobile Subscriber Identity
TTP	Trusted Third Party
TVP	Time Variant Parameter (time stamp)
UE	User equipment

UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UIDN	User Identity Decryption Node
USIM	User Services Identity Module
VLR	Visitor Location Register
X	Network Identifier
XEMSI	Extended Encrypted Mobile Subscriber Identity
XRES	Expected Response
Y	Network Identifier

NEXT MODIFIED SECTION

5 Provider domain security

5.1 Functional security architecture

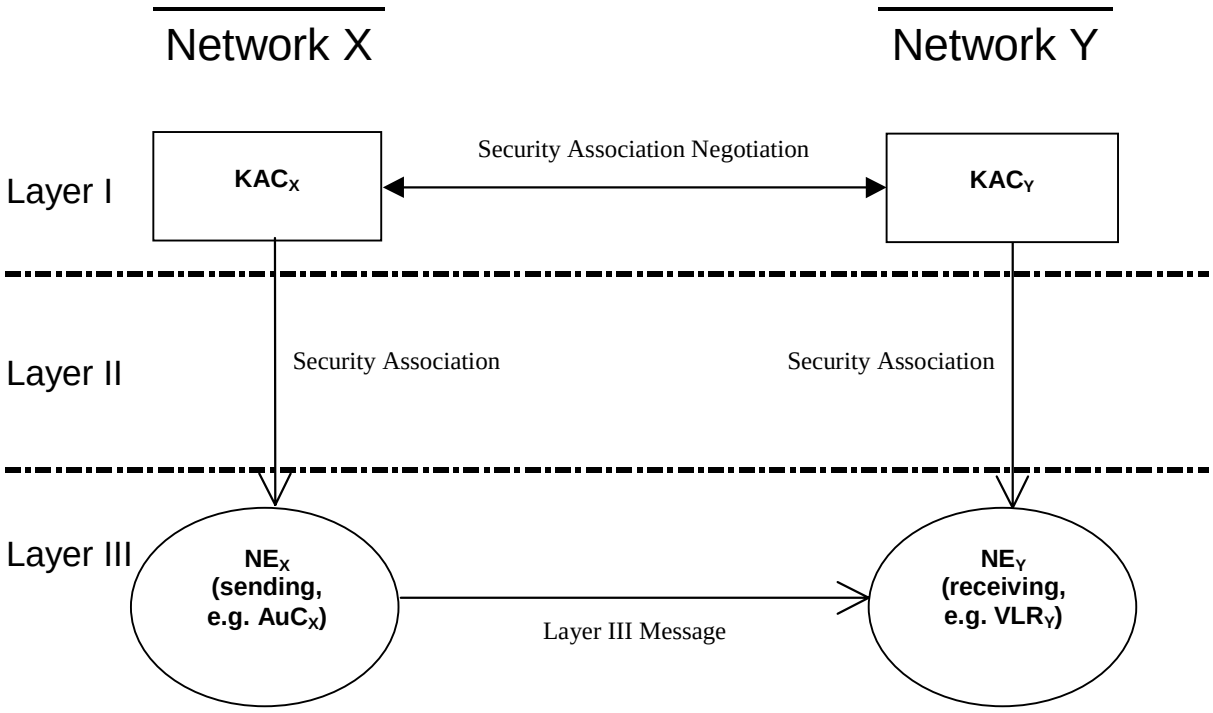

Figure 5: Overview of Proposed Mechanism

This mechanism establishes a secure signalling link between network nodes, in particular between VLR/SGSNs and HE/AuCs. Such procedures may be incorporated into the roaming agreement establishment process.

5.2 Key Authentication Centre

Details in security architecture to be finalised

5.3 Core network entities

Table 22: Signalling Protection- Data Elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
KS_{XY}(int)	Symmetric Integrity Key for integrity of data sent between X and Y	1 per session	According to roaming agreement	128 bits	Mandatory
KS_{XY}(con)	Symmetric Confidentiality Key for confidentiality of data sent between X and Y	1 per session	According to roaming agreement	128 bits	Mandatory
TVP	Time Variant Parameter (time stamp)	1 per message	message	32 bits	Mandatory

Table 23: Signalling Protection –Cryptographic Functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional