3GPP TSG SA WG 3 (Security) meeting #13
Yokohama (Japan), 24—26 May, 2000

Document **S3-000336**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

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:	3.2.0

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

For submission to:	SA #8	for approval	X	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: *(at least one should be marked with an X)* (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]

Source: Ericsson **Date:** 2000-05-19

Subject: Removal of MAP Security from 33.103

Work item: Security

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

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

Release:

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

Reason for change: As per SA#7 decision, MAP Security is not a R99 feature. MAP Security is therefore removed from 33.103.

Clauses affected: 5

Other specs affected:

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

5 Provider domain security

5.1 Functional security architecture

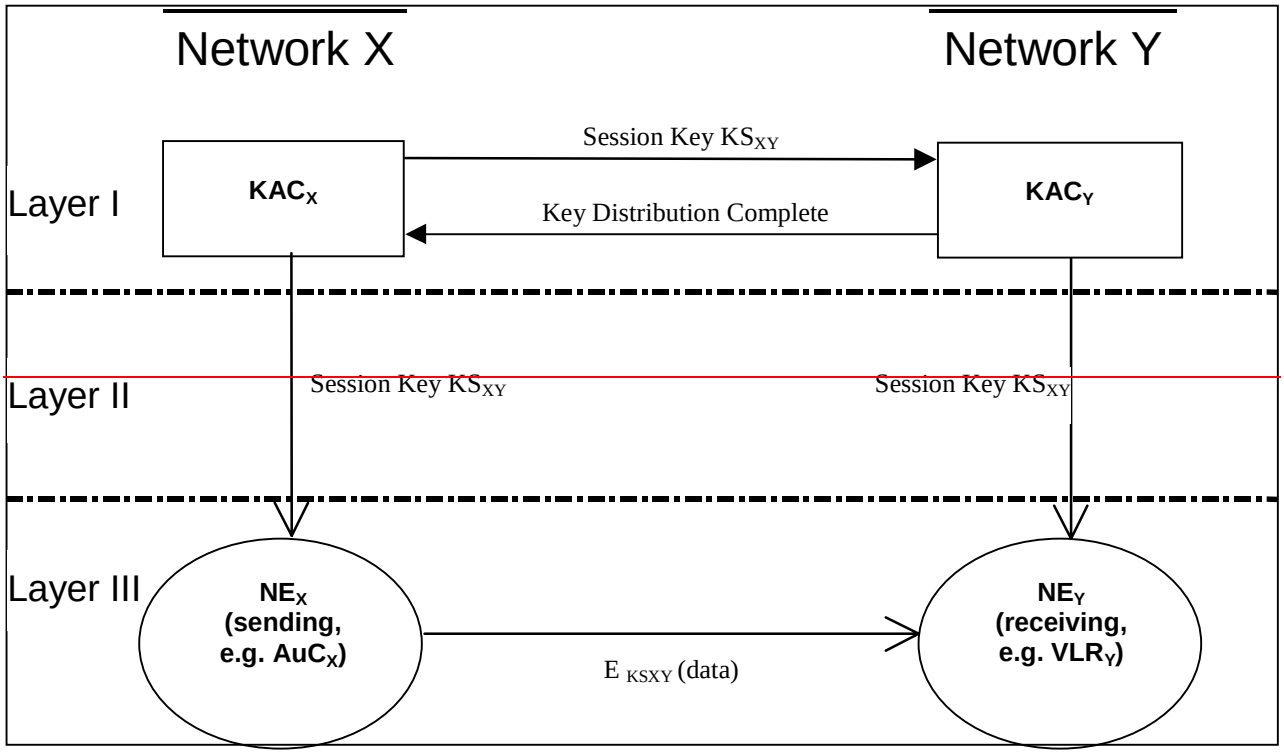

Figure 5: Overview of Proposed Mechanism

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

A secret key transport mechanism based on an asymmetric crypto-system i used to agree on a symmetric session key for each direction of communication between two networks X and Y.

The party wishing to send sensitive data initiates the mechanism and chooses the symmetric session key it wishes to use for sending the data to the other party. The other party shall choose a symmetric session key of its own, used for sending data in the other direction. This second key shall be transported immediately after the first key has been successfully transported. The session symmetric keys are protected by asymmetric techniques. They are exchanged between certain elements called the *Key Administration Centres* (KACs) of the network operators X and Y.

Transport of Session Keys

In order to establish a symmetric session key with version no. i to be used for sending data from X to Y, the KAC_X sends a message containing the following data to the KAC_Y:

$$E_{PK(Y)}\{X||Y||i||KS_{XY}(i)||RND_X||Text1||D_{SK(X)}(Hash(X||Y||i||KS_{XY}(i)||RND_X||Text1))||Text2||Text3$$

After having successfully distributed the symmetric session key received by network X to its own network entities, network Y sends to X a Key Distribution Complete Message. This is an indication to KAC_X to start with the distribution of the key to its own entities, which can then start to use the key immediately.

The message takes the form

$$KEY\_DIST\_COMPLETE||Y||X||i||RND_Y||D_{SK(Y)}(Hash(KEY\_DIST\_COMPLETE||Y||X||i||RND_Y)$$

where i indicates the distributed key and RND_Y is a random number generated by Y. The digital signature is appended for integrity and authenticity purposes. Y includes RND_Y to make sure that the message contents determined by X will be modified before signing.

Since most of the signalling messages to be secured are bidirectional in character, immediately after successful completion the procedure described here shall be repeated, now with Y choosing a key $KS_{YX}(i)$ to be used in the reverse direction, and X being the receiving party. Thereby keys for both directions are established.

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
PVTK-s	Network's own Private Key (signing)	1	According to roaming agreement	< or = 2048 bits	Mandatory
PVTK-d	Network's own Private Key (decryption)	1	According to roaming agreement	< or = 2048 bits	Mandatory
$PUBKv_1$	PKR_1 Public Key for network #1 (verify)	1 per roaming agreement	According to roaming agreement	< or = 2048 bits	Mandatory
$PUBKe_1$	PKR_1 Public Key for network #1 (encryption)	1 per roaming agreement	According to roaming agreement	< or = 2048 bits	Mandatory
$KS_{XY}(i)$	Symmetric Send Key #i for sending data from X to Y	1 per session	According to roaming agreement	128 bits	Mandatory
$KS_{YX}(j)$	Symmetric Send Key #j for sending data from Y to X	1 per session	According to roaming agreement	128 bits	Mandatory
I	Session key Sequence Number (for sending data from X to Y)	1 per session	According to roaming agreement	32 – 64 bits	Mandatory
J	Session key Sequence Number (for sending data from Y to X)	1 per session	According to roaming agreement	32 – 64 bits	Mandatory
RND_X	Unpredictable Random Value generated by X	1 per session	Session	128 bits	Mandatory
RND_Y	Unpredictable Random Value generated by Y	1 per session	Session	128 bits	Mandatory

Table 23: Signalling Protection - Cryptographic Functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
BEANO	Block Encryption Algorithm for Network Operators	1	Permanent	Standardised	Mandatory