3GPP TSG-CN SWG2B
Milano, Italy, 14-16 Feb 2000

S3-000144
Document N2B000352
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.

29.060	**CR**	**067r1**	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: CN#7	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: (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]
(at least one should be marked with an X)

Source: Ericsson **Date:** 15 Febr 2000

Subject: Distribution of security data

Work item: GTP Enhancements

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

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature	X		Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Transfer of
GSM security context and unused UMTS authentication vectors (quintuplets) between R99+ SGSNs needed.

Clauses affected:

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.

7.7.18 MM Context

The MM Context information element contains the Mobility Management, MS and security parameters that are necessary to transfer between SGSNs at the Inter SGSN Routeing Update procedure.

The ~~Authentication Type~~ Security Mode indicates the type of security keys (GSM/UMTS) and Authentication Vectors (quintuplets/triplets) that are passed to the new SGSN.~~Authentication mechanism that is the GSM or UMTS.~~

The Ciphering Key Sequence Number (CKSN) is described in GSM 04.08. Possible values are integers in the range [0; 6]. The value 7 is reserved. The Ciphering Key Sequence Number is applicable to GSM as well as UMTS security key(s). ~~shall be presented if Authentication Type is GSM.~~

~~The Key Set Identifier (KSI) is described in UMTS 23.060. Possible values are integer in the range [0; 6]. The value 7 is reserved. The Key Set Identifier shall be presented if Authentication Type is UMTS.~~

The Used Cipher indicates the GSM ciphering algorithm that is in use.

Kc is the GSM ciphering key currently used by the old SGSN. Kc shall be present~~ed~~ if ~~Authentication Type is GSM~~ GSM keys is indicated in the Security Mode.

CK is the UMTS ciphering key currently used by the old SGSN. CK shall be present~~ed~~ if ~~Authentication Type is UMTS~~. UMTS keys are indicated in the Security Mode.

IK is the UMTS integrity key currently used by the old SGSN. IK shall be present~~ed~~ if ~~Authentication Type is UMTS~~ UMTS keys are indicated in the Security Mode.

The Triplet array contains triplets encoded as the value in the Authentication Triplet information element The Triplet array shall be presented if ~~Authentication Type is GSM.~~indicated in the Security Mode.

The Quintuplet array contains Quintuplets encoded as the value in the Authentication Quintuplet information element. The Quintuplet shall be presented if ~~Authentication Type is UMTS~~ indicated in the Security Mode.

The Triplet array contains triplets encoded as the value in the Authentication Triplet information element.

The DRX parameter indicates whether the MS uses DRX mode or not.

MS Network Capability provides the network with information concerning aspects of the MS related to GPRS.

The DRX parameter and the MS Network Capability are coded as described in GSM 04.08.

The two octet Container Length holds the length of the Container, excluding the Container Length octets.

The Container contains one or several optional information elements as described in the sub-clause ‘Overview’, from the clause ‘General message format and information elements coding’ in GSM 04.08.

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 129 (Decimal)							
2-3	Length							
4	spare 1 1 1 1 1					CKSN		
5	Security		No of Vectors			Used Cipher		
6-13	Kc							
14-m	Triplet [0..4]							
(m+1)-(m+2)	Container length							
(m+3)-n	Container							

Figure 31: MM Context element ~~in~~ with GSM keys and triplets

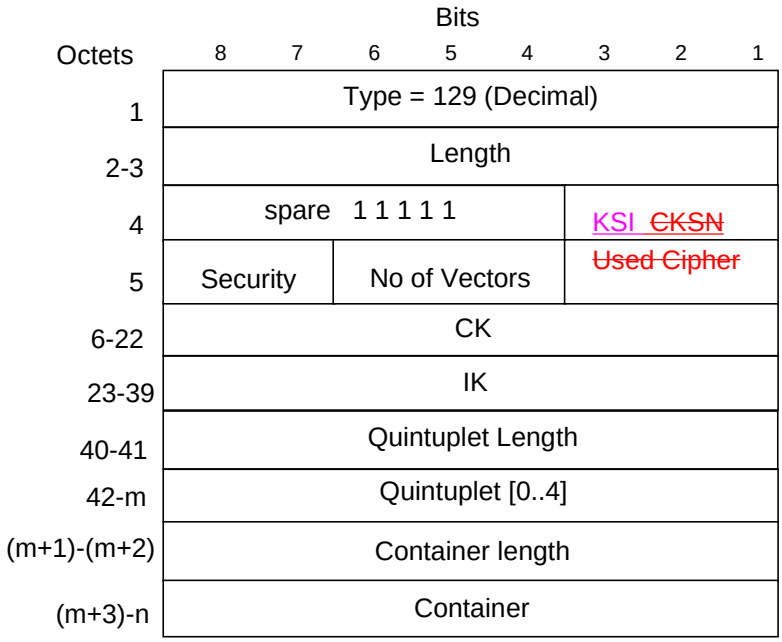

Figure 32: MM Context element ~~in~~ with UMTS keys and quintuplets

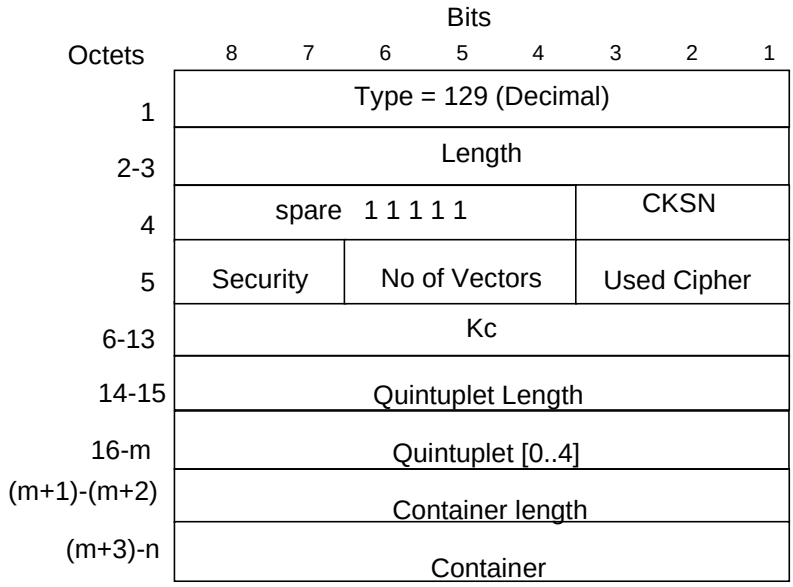

Figure 33: MM Context element with GSM keys and UMTS quintuplets

Table 44: Used Cipher values

Cipher Algorithm	Value (Decimal)
No ciphering	0
GEA/1	1

Table 45: Security ~~Type~~ Mode Values

Security ~~Type~~ Mode	Value (Decimal)
GSM key and triplets	1~~3~~
GSM key and quintuplets	3~~2~~
UMTS key and quintuplets	2