3GPP TSG CN Plenary
Meeting #10, Bangkok, Thailand
6th – 8th December 2000

Tdoc NP-000637

Source: TSG_CN WG 4

Title: CRs to R99 Work Item Security

Agenda item: 7.3

Document for: APPROVAL

Introduction:

This document contains 2 CRs on R99 Work Item Security, that have been agreed by TSG_CN WG4, and is forwarded to TSG_CN Plenary meeting #10 for approval.

SMG#	TDoc	SPEC	CR	RE	PHAS	VERS	SUBJECT	CAT
CN10	N4-001006	29.060	157		R99	3.6.0	Correction of Security parameters length	F
CN10	N4-001064	29.060	161		R99	3.6.0	Clarifications to the usage of CKSN and KSI for security type	F

3GPP TSG-CN WG4 Meeting #5
Paris, France, 13-17 November 2000

Tdoc N4-001006

CR-Form-v3

CHANGE REQUEST

⌘ **29.060** **CR** **157** ⌘ rev **-** ⌘ Current version: **3.6.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Correction of Security parameters length
Source:	⌘	CN4
Work item code:	⌘	Security
Date:	⌘	6/Nov/2000
Category:	⌘	**F** Critical correction
Release:	⌘	R99

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	Octet number of the security related field shall be corrected.
Summary of change:	⌘	1. Field length of CK and IK in figure 41 and 42A shall be corrected as 16 octet length. Start octet of Quintuplet in figure 42 shall be corrected as 16. Some space allocation bitween words should be corrected. 2. Field length of RAND, CK and IK in figure 49 shall be corrected as 16 octet length.
Consequences if not approved:	⌘	

Clauses affected:	⌘	7.7.28, 7.7.35
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications
	⌘	
Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

7.7.28 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 Area Update procedure.

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

Ciphering Key Sequence Number (CKSN) is described in 3G TS 24.008. 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).

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 if GSM key is indicated in the Security Mode.

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

IK is the UMTS integrity key currently used by the old SGSN. IK shall be present if 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 present if indicated in the Security Mode.

The Quintuplet array contains Quintuplets encoded as the value in the Authentication Quintuplet information element. The Quintuplet shall be present if indicated in the Security Mode.

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. MS Network Capability and MS Network Capability Length are coded as in the value part described in 3G TS 24.008.

DRX parameter is coded as described in 3G TS 24.008, the value part only.

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

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 3G TS 24.008.

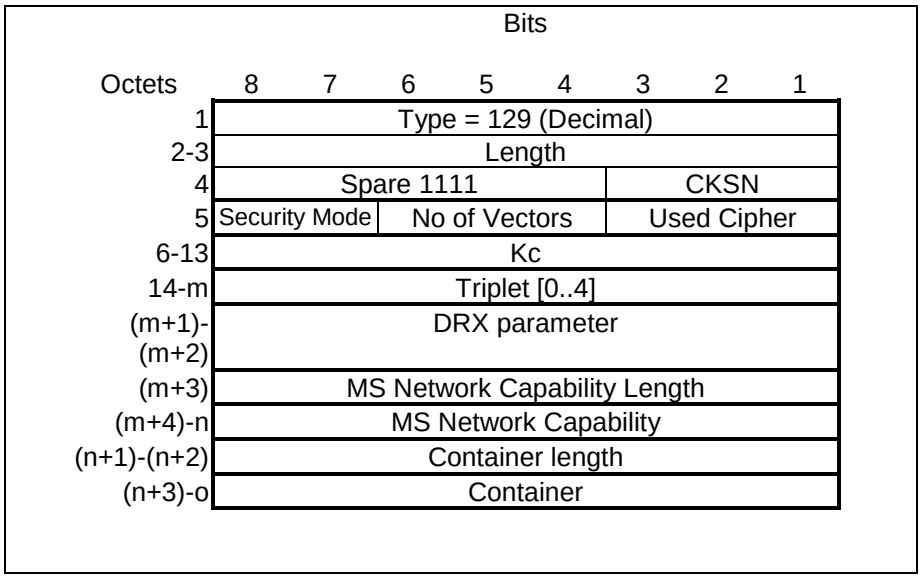


Figure 40: MM Context Information Element with GSM Key and Triplets

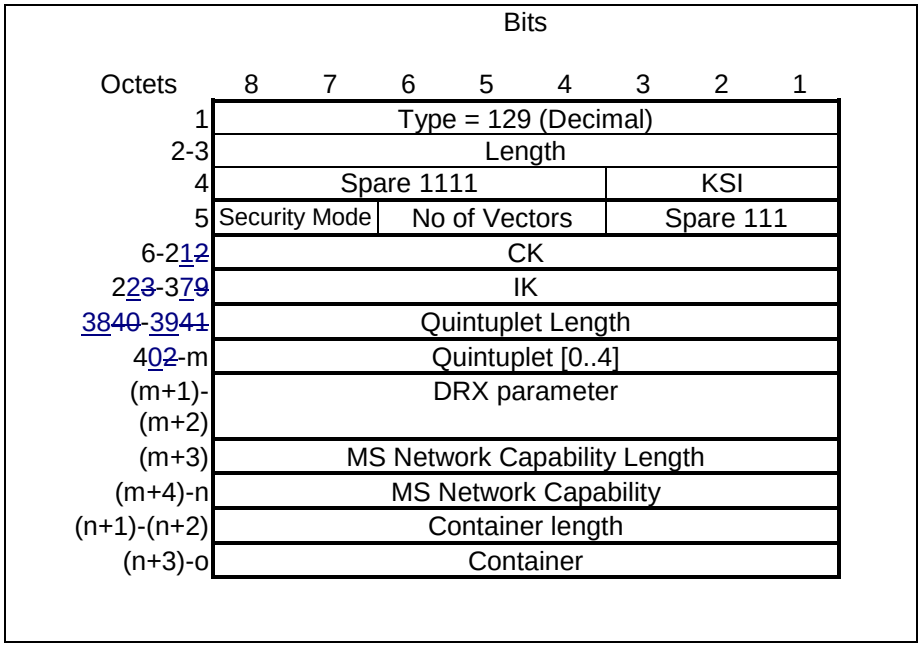
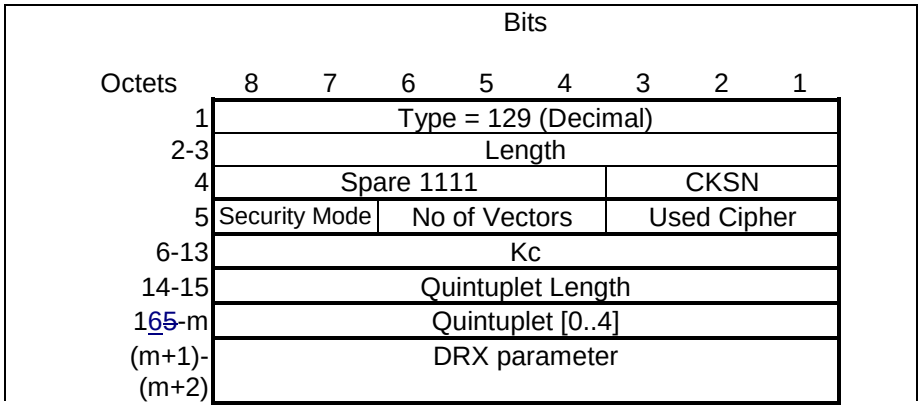


Figure 41: MM Context Information Element with UMTS Keys and Quintuplets



(m+3)	MS Network Capability Length
(m+4)-n	MS Network Capability
n+1-n+2	Container length
n+3-o	Container

Figure 42: MM Context Information Element with GSM Keys and UMTS Quintuplets

Bits

Octets	8	7	6	5	4	3	2	1
1	Type = 129 (Decimal)							
2-3	Length							
4	Spare 1111					CKSN		
5	Security Mode		No of Vectors			Used Cipher		
6-21	CK							
22-37	IK							
38-39	Quintuplet Length							
40-m	Quintuplet [0..4]							
(m+1)-(m+2)	DRX parameter							
(m+3)-(m+4)	MS Network Capability							
(m+5)-(m+6)	Container length							
(m+7)-n	Container							

Figure 42A: MM Context Information Element with Used Cipher value, UMTS Keys and Quintuplets

Table 46: Used Cipher Values

Cipher Algorithm	Value (Decimal)
No ciphering	0
GEA/1	1
GEA/2	2
GEA/3	3
GEA/4	4
GEA/5	5
GEA/6	6
GEA/7	7

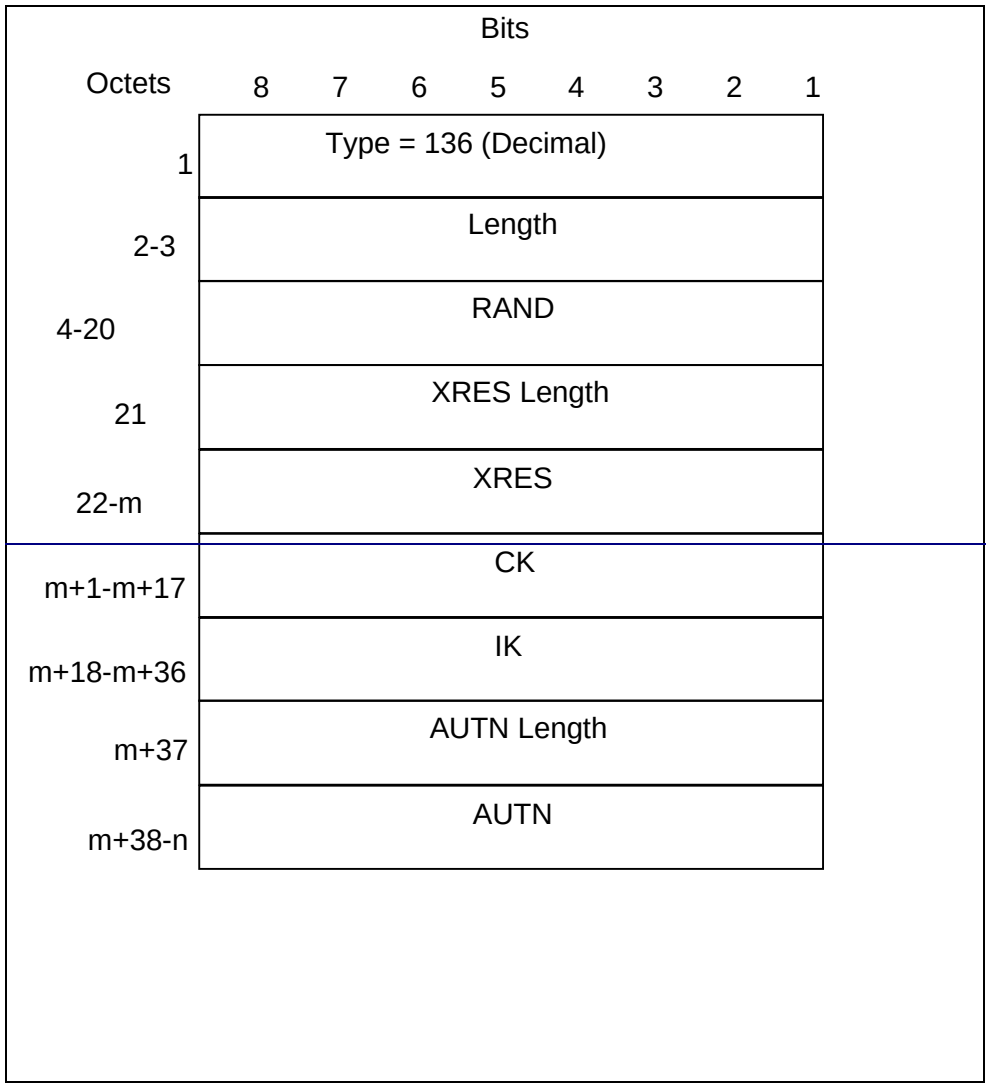
Table 47: Security Mode Values

Security Type	Value (Decimal)
GSM key and triplets	1
GSM key and quintuplets	3
UMTS key and quintuplets	2
Used cipher value, UMTS Keys and Quintuplets	0

*** NEXT MODIFIED SECTION ***

7.7.35 Authentication Quintuplet

An Authentication Quintuplet consists of a Random challenge (RAND), an Expected user response (XRES), a Cipher key (CK), an Integrity key (IK), an Authentication token (AUTN) (see 3G TS 33.102).



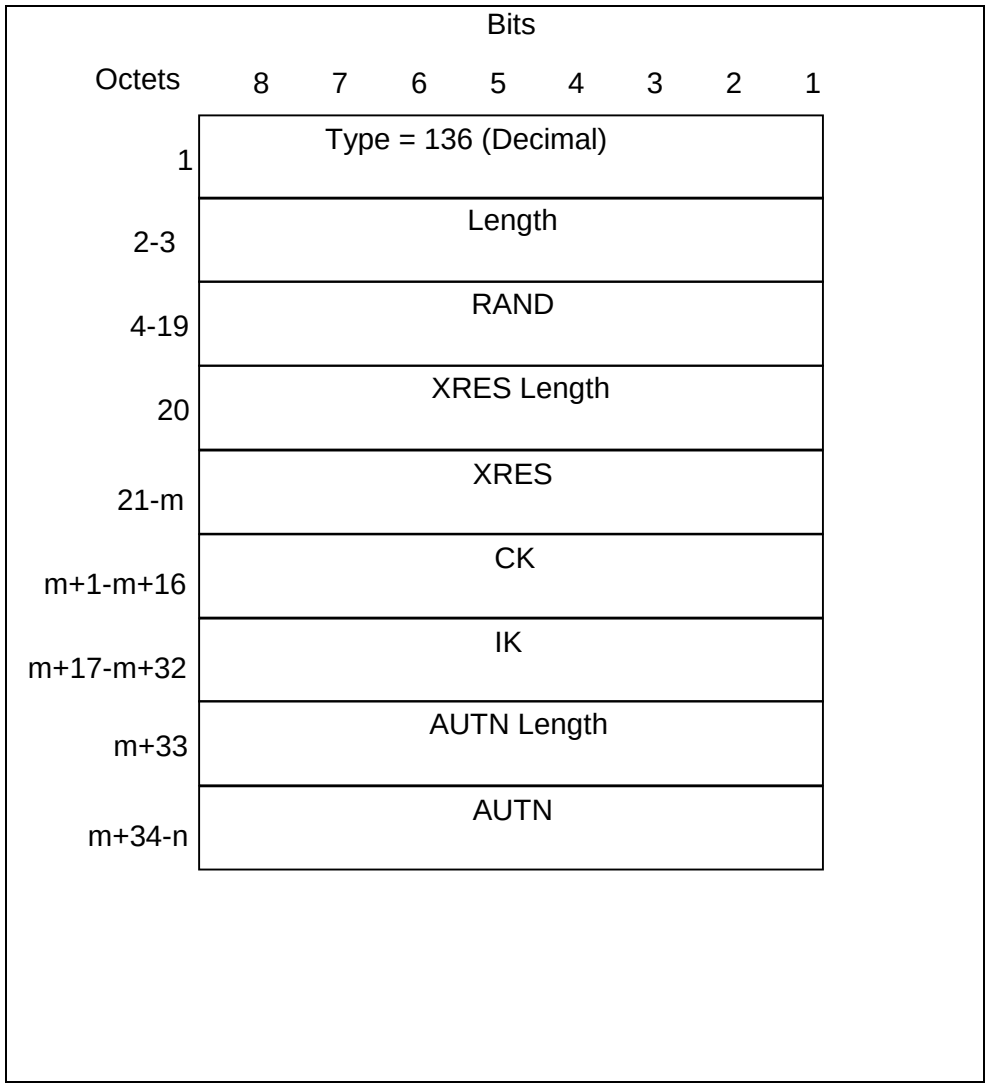


Figure 49: Authentication Quintuplet Information Element

3GPP-CN4 Meeting # 5
Paris, France 13-17 November 2000

Document ***N4-001064***

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**	**161**	Current Version:	3.6.0

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

For submission to:	CN#10	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: CN4 **Date:** 14 November 2000

Subject: Clarifications to the usage of CKSN and KSI for security type 0

Work item: Security

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

F	Correction	X	**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			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change:

CR is supported by consensus in the CN4.

According to 33.102v3.6.0 For an UMTS subscriber the 3G-SGSN may send to 2G-SGSN MM Context of the Security type 0. Figure 42A allocates three list significant digits of the octet 5 to CKSN.
However, 3G-SGSN does not have CKSN IE at all. Rather, 3G-SGSN keeps KSI IE.

It is proposed to clarify how the CKSN is related to KSI during the Inter SGSN Intersystem Change and to modify Figure 42A.

Clauses affected: 7.7.28

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.

7.7.28 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 Area Update procedure.

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

Ciphering Key Sequence Number (CKSN) is described in 3G TS 24.008. 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).~~ CKSN identifies Kc. During the Intersystem Change to 3G-SGSN, the KSI shall be assigned the value of CKSN.

Key Set Identifier (KSI) identifies CK and IK. During the Intersystem Change to 2G-SGSN, the CKSN shall be assigned the value of KSI.

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 if GSM key is indicated in the Security Mode.

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

IK is the UMTS integrity key currently used by the old SGSN. IK shall be present if 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 present if indicated in the Security Mode.

The Quintuplet array contains Quintuplets encoded as the value in the Authentication Quintuplet information element. The Quintuplet shall be present if indicated in the Security Mode.

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. MS Network Capability and MS Network Capability Length are coded as in the value part described in 3G TS 24.008.

DRX parameter is coded as described in 3G TS 24.008, the value part only.

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

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 3G TS 24.008.

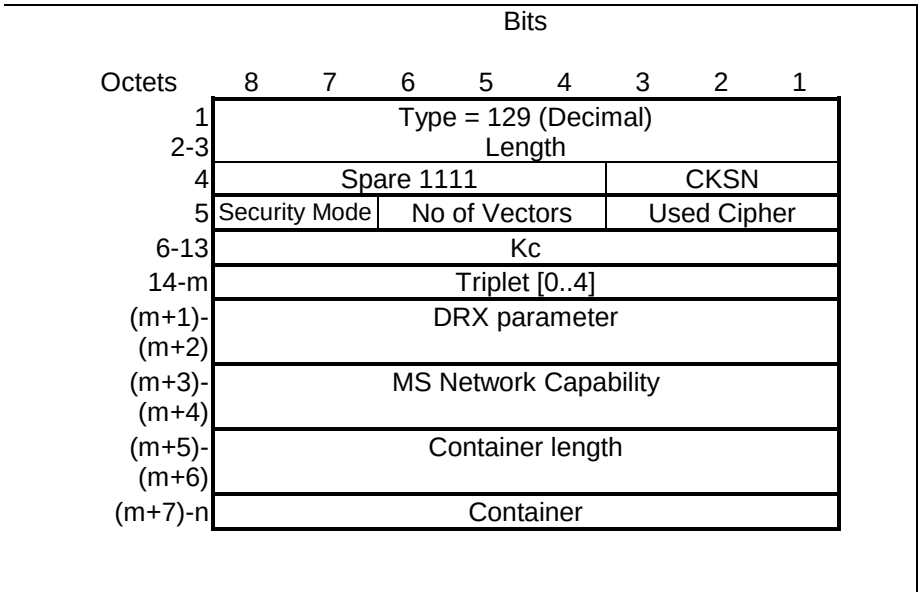


Figure 40: MM Context Information Element with GSM Key and Triplets

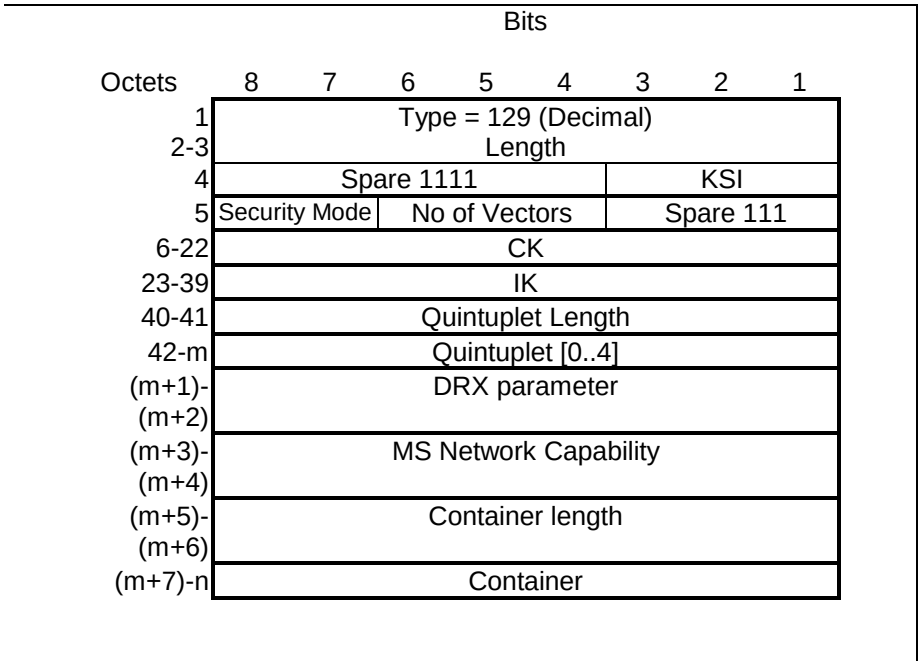


Figure 41: MM Context Information Element with UMTS Keys and Quintuplets

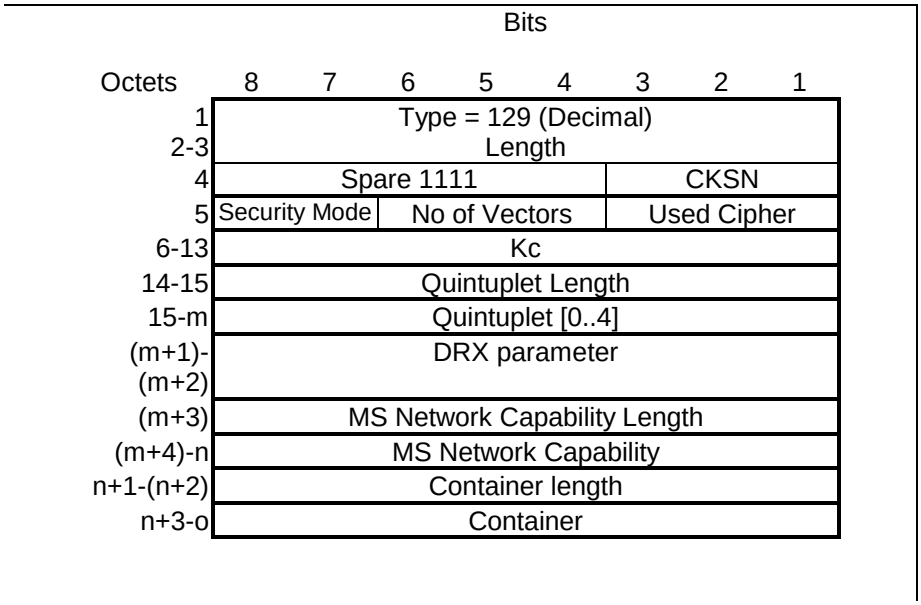


Figure 42: MM Context Information Element with GSM Keys and UMTS Quintuplets

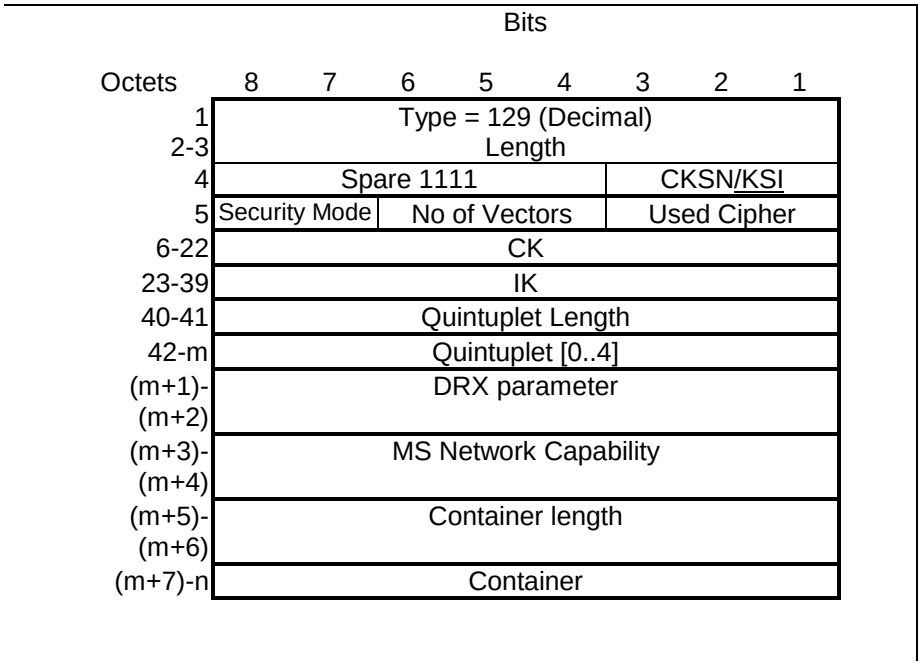


Figure 42A: MM Context Information Element with Used Cipher value, UMTS Keys and Quintuplets

Table 46: Used Cipher Values

Cipher Algorithm	Value (Decimal)
No ciphering	0
GEA/1	1
GEA/2	2
GEA/3	3
GEA/4	4
GEA/5	5
GEA/6	6
GEA/7	7

Table 47: Security Mode Values

Security Type	Value (Decimal)
GSM key and triplets	1
GSM key and quintuplets	3
UMTS key and quintuplets	2
Used cipher value, UMTS Keys and Quintuplets	0