3GPP TSG SA WG3 Security — S3#17bis **S3z010032**
23rd April – 24th April
Madrid, Spain

CR-Form-v3

S3 Editors CHANGE REQUEST

⌘	**33.200**	**CR**	**CR-Num**	⌘	rev	**-**	⌘	Current version:	**0.3.2**	⌘

*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:	⌘	Cleanup of MAPsec structure of protected operations			
Source:	⌘	Ericsson			
Work item code:	⌘	Network Domain Security	***Date:***	⌘	23-April-01
Category:	⌘	**D**	***Release:***	⌘	

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:	⌘	The chapters about MAPsec structure of protected operations have been inherited from R99 and need some cleaning up.
Summary of change:	⌘	R99 concepts have been removed and the text has been cleaned up: - Edictorial changes, - "KSXY" notation removed from PM1 and PM2 - "MAPHeader" removed from PM2
Consequences if not approved:	⌘	

Clauses affected:	⌘	7.2.5		
Other specs affected:	⌘	□ Other core specifications	⌘	
		□ Test specifications		
		□ O&M Specifications		
Other comments:	⌘			

7.2.5 MAPsec structure of protected ~~operations~~messages

7.2.5.1 MAPsec protection modes

MAPsec provides for three different protection modes and these are defined as follows:

Protection Mode 0: No Protection

Protection Mode 1: Integrity, Authenticity

Protection Mode 2: Confidentiality, Integrity, and Authenticity

MAP operation protected by means of MAPsec consists of a Security Header and the Protected Payload. Secured MAP ~~operations~~ messages have the following structure:

Security Header	Protected Payload

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

In protection mode 2 providing confidentiality, the protected payload is essentially the encrypted payload of the original MAP ~~operation~~ message (see chapter 7.2.5.4). For integrity and authenticity in protection modes 1 and 2, the message authentication code is calculated on the security header and the payload of the original MAP ~~operation~~ message in cleartext and it is included in the protected payload. In protection mode 0 no protection is offered, therefore the protected payload is identical to the payload of the original MAP ~~operation~~message.

~~[EDITOR: I got the impression that a container operation "SecureTransport" is being specified and that it would take a protected operations as its payload. This is not yet reflected in the most current version of TR 33.800 and the the material here may not be completely up to date. This affects 7.2.5.2-5.~~

~~**Input from companies with CN4 delegates is wanted.**~~]

7.2.5.2 Protection Mode 0

Protection Mode 0 offers no protection at all. Therefore, the protected payload of Secured MAP ~~operations~~ messages in protection mode 0 is ~~functionally and security wise~~ identical to the original MAP ~~operation~~ message payload in cleartext.

For cases where Protection Mode 0 is to be used the protection level will be identical to the original unprotected MAP ~~operation~~message. It is therefore allowed as an implementation option to let Protection Mode 0 operations be sent without the security header.

7.2.5.3 Protection Mode 1

The protected payload of Secured MAP ~~operations~~ messages in protection mode 1 takes the following form:

TVP||Cleartext|| H~~$_{KSXY(int)}$~~(TVP|| Security Header||Cleartext)

where "Cleartext" is the payload of the original MAP operation in clear text. Therefore, in Protection Mode 1 the protected payload 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)~~ defined by the security association to the concatenation of Time Variant Parameter TVP, Security Header and Cleartext.

The TVP used for replay protection of Secured MAP operations is a 32 bit time-stamp. The receiving network entity shall~~will~~ accept an operation 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.

7.2.5.4 Protection Mode 2

The ~~Secured MAP Message Body~~ protected payload of Secured MAP ~~operations~~ Messages in protection mode 2 takes the following form:

TVP|| E~~$_{KSXY(con)}$~~(Cleartext) || H~~$_{KSXY(int)}$~~(TVP|| ~~MAP Header~~||Security Header|| E~~$_{KSXY(con)}$~~(Cleartext))

where "Cleartext" is the original MAP ~~message~~ ~~operation~~ message payload in clear text. ~~Message c~~Confidentiality is achieved by encrypting Cleartext with the confidentiality ~~session~~ key defined by the security association ~~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 defined by the security association ~~KS$_{XY}$(int)~~ to the concatenation of Time Variant Parameter TVP, ~~MAP Header,~~ Security Header and encrypted~~E$_{KSXY(con)}$(~~Cleartext~~)~~.

The TVP used for replay protection of Secured MAP messages is a 32 bit time-stamp. The receiving network entity ~~will~~ shall 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.

It is further recommended ~~the~~to use ~~of~~ protection mode 2 whenever possible as this makes replay attacks even more difficult.