3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010094**

13 September, 2001, Sophia Antipolis, France

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** ⌘ ev **-** ⌘ Current version: **4.0.0** ⌘

*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 **X**

Title:	⌘	MAC calculation in PM2
Source:	⌘	Ericsson
Work item code:	⌘	MAPsec
Date:	⌘	13-09-2001
Category:	⌘	**F**
Release:	⌘	Rel-4

Use one of the following categories:
- ***F*** *(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:	⌘	Wrong definition of MAC calculation in PM2.
Summary of change:	⌘	Correct how MAC is computed in chapter 5.5. Miscellaneous editorial modifications in chapter 5.6.2.
Consequences if not approved:	⌘	Unclear/inconsistent specification.

Clauses affected:	⌘	5.5, 5.6.2
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications
	⌘	
Other comments:	⌘	

5.5 MAPsec structure of protected messages

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 operations protected by means of MAPsec consist of a Security Header and the Protected Payload. Secured MAP 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 message. For integrity and authenticity in protection mode~~s~~ 1~~ and 2~~, the message authentication code is calculated on the security header and the payload of the original MAP message in cleartext and it is included in the protected payload. The message authentication code in protection mode 2 is calculated on the security header and the encrypted payload of the original MAP message. In protection mode 0 no protection is offered, therefore the protected payload is identical to the payload of the original MAP message.

5.6.2 Mapping of MAP-SA ~~encryption~~ integrity algorithm identifiers

The MIA algorithm indication fields in the MAP-SA are used to identify the integrity algorithm and algorithm mode to be used. The mapping of algorithm identifiers is defined below.

Table 2: MAP integrity algorithm identifiers

MAP Integrity Algorithm identifier	Description
0	Null
1	AES in a CBC MAC mode (MANDATORY)
:	-not yet assigned-
15	-not yet assigned-

5.6.2~~1~~.1 Description of MIA-1

The MIA-1 algorithm is the ISO/IEC 9797 Part 1: padding method 2, MAC algorithm 1 (initial transformation=1, output transformation=1). No IV used. See ISO/IEC 9797 [6] for more information.

Editor's Note: More specification on the mode of operation for MIA-1 may be required.