Technical Specification Group Services and System Aspects
Meeting #13, Beijing, China, 24-27 September 2001

TSGS#13(01)0502

Source: **SA WG3**

Title: **1 CR to 33.200: MIA key length unspecified (Rel-4)**

Document for: **Approval**

Agenda Item: **7.3.3**

Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New	Doc-2nd-Level
33.200	010		Rel-4	F	MIA key length unspecified	4.0.0	4.1.0	S3z010091

3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010091**

13 September, 2001, Sophia Antipolis, France

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** **010** ⌘ 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 ☒

Title:	⌘	MIA key length unspecified
Source:	⌘	SA WG3 (MAP ad-hoc)
Work item code:	⌘	MAPsec
Date:	⌘	06-09-2001
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:	⌘	The MIA algorithm identifiers has to include the key length
Summary of change:	⌘	128-bit key is intended for Rel-4
Consequences if not approved:	⌘	Specification is left incomplete, implementers can only assume that a 128-bit key was intended too be used. Removal of editors note is not possible.

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

5.6.2 Mapping of MAP-SA encryption 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 with a 128-bit key (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. The MAC-length m is 32-bits (See clause 5.6.1). See ISO/IEC 9797 [6] for more information.

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