

13 September, 2001, Sophia Antipolis, France

CR-Form-v4	
<b>CHANGE REQUEST</b>	
⌘ <b>33.200 CR</b> ⌘ ev <b>-</b> ⌘ Current version: <b>4.0.0</b> ⌘	

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

<b>Title:</b>	⌘ MIA key length unspecified ⌘		
<b>Source:</b>	⌘ Siemens Atea ⌘		
<b>Work item code:</b>	⌘ MAPsec ⌘	<b>Date:</b>	⌘ 06-09-2001 ⌘
<b>Category:</b>	⌘ <b>F</b> ⌘	<b>Release:</b>	⌘ Rel-4 ⌘
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> 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)

<b>Reason for change:</b>	⌘ The MIA algorithm identifiers has to include the key length ⌘
<b>Summary of change:</b>	⌘ 128-bit key is intended for Rel-4 ⌘
<b>Consequences if not approved:</b>	⌘ 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. ⌘

<b>Clauses affected:</b>	⌘ 5.6.2 ⌘		
<b>Other specs affected:</b>	⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/> Test specifications ⌘ <input type="checkbox"/> O&M Specifications ⌘		
<b>Other comments:</b>	⌘ ⌘		

## 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 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.~~