

25 - 28 February 2002

Bristol, UK, 25.-28.2.

CR-Form-v5	
<b>CHANGE REQUEST</b>	
⌘ <b>33.200 CR</b> ⌘ rev <b>-</b> ⌘ Current version: <b>4.2.0</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>	⌘ NIST Special Publication 800-38A updates on MEA-1		
<b>Source:</b>	⌘ NOKIA		
<b>Work item code:</b>	⌘ MAPSec	<b>Date:</b>	⌘ 11.02.2002
<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 NIST Special Publication 800-38A "Recommendation for Block Cipher Modes of Operation" has been published in December 2001.
<b>Summary of change:</b>	⌘ The draft NIST Special Publication 800-XX references are changed according to the recently published NIST SP 800-38A.
<b>Consequences if not approved:</b>	⌘ Draft NIST Special Publication 800-XX references would be used.

<b>Clauses affected:</b>	⌘ 2 and 5.6.1.1		
<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>	⌘		

---

## 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3G TS 21.133: Security Threats and Requirements.
- [2] 3G TS 21.905: 3G Vocabulary.
- [3] 3G TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2.
- [4] 3G TS 29.002: Mobile Application Part (MAP) specification.
- [5] NIST Special Publication 800-~~38A~~ "Recommendation for Block Cipher Modes of Operation"  
~~December~~<sup>July</sup> 2001.
- [6] ISO/IEC 9797: "Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher", Ed.1, 1999-12-16.

### 5.6.1.1 Description of MEA-1

The MEA-1 algorithm is AES used in counter mode with a 128-bit key and 128-bit counter blocks as described ~~is the~~ in clause 65.5 of FIPS 800-~~38A~~ Recommendation for Block Cipher Modes of Operation [5]. The initial counter block  $T_1$  is initialized with IV. Successive counter blocks  $T_j$  ( $J > 1$ ) are derived by applying an incrementing function over the entire block  $T_{j-1}$  ( $J \geq 2$ ) (see Appendix B.1: The standard incrementing function of [5]).

The MAPsec cleartext shall be cut into  $P_j$  blocks of 128 bits. If the last block  $P_n$  has less than 128-bits ( $z$  bits), then it shall be encrypted by bitwise addition with only the first  $z$  bits of output block  $n$  (Clause 65.5 of [5]).