Technical Specification Group Services and System Aspects
Meeting #15, Cheju Island, Korea, 11-14 March 2002

TSGS#15(02)0114

Source:	**SA WG3**
Title:	**CR to 33.200: NIST Special Publication 800-38A updates on MEA-1 (Rel-4)**
Document for:	**Approval**
Agenda Item:	**7.3.3**

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	SA WG3 doc#
SP-020114	33.200	020		Rel-4	NIST Special Publication 800-38A updates on MEA-1	F	4.2.0	S3-020147

3GPP TSG-SA3 Meeting #22 **S3-020147**

25 - 28 February 2002
Bristol, UK, 25.-28.2.

CR-Form-v5

CHANGE REQUEST

⌘	**33.200**	**CR**	**020**	⌘ **rev**	**-**	⌘	Current version:	**4.2.0**	⌘

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:	⌘	NIST Special Publication 800-38A updates on MEA-1	
Source:	⌘	SA WG3	
Work item code:	⌘	SEC1-MAP	***Date:*** ⌘ 19.02.2002
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 NIST Special Publication 800-38A “Recommendation for Block Cipher Modes of Operation" has been published in December 2001.
Summary of change:	⌘	The draft NIST Special Publication 800-XX references are changed according to the recently published NIST SP 800-38A.
Consequences if not approved:	⌘	Draft NIST Special Publication 800-XX references would be used.

Clauses affected:	⌘	2 and 5.6.1, 5.6.2	
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments:	⌘		

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~~XX~~ "Recommendation for Block Cipher Modes of Operation" December~~July~~ 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.

[7] FIPS Publication 197: Specification for the Advanced Encryption Standard (AES), November 26, 2001.

5.6.1 Mapping of MAPsec-SA encryption algorithm identifiers

The MEA algorithm indication fields in the MAPsec-SA are used to identify the encryption algorithm and algorithm mode to be used. The mapping of algorithm identifiers is defined below.

Table 1: MAP encryption algorithm identifiers

MAP Encryption Algorithm identifier	Description
0	Null
1	AES in counter mode with 128-bit key length (MANDATORY)
:	-not yet assigned-
15	-not yet assigned-

5.6.1.1 Description of MEA-1

The MEA-1 algorithm is AES [7] used in counter mode with a 128-bit key and 128-bit counter blocks as described ~~is the~~ in clause 6~~5~~.5 of FIPS 800-38A~~XX~~ 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>=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 5.5 of [5]).~~

5.6.2 Mapping of MAPsec-SA integrity algorithm identifiers

The MIA algorithm indication fields in the MAPsec-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-