3GPP TSG SA WG3 Security — S3#20 **S3-010538**

16 - 19 October, 2001

Sydney, Australia

CR-Form-v4

CHANGE REQUEST

⌘ **33.200 CR 012** ⌘ ev **-** ⌘ Current version: **4.1.0** ⌘

*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:	⌘	MEA encryption algorithm update		
Source:	⌘	SA WG3		
Work item code:	⌘	MAPsec	***Date:*** ⌘	09-Oct-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 counter mode of operation, that is currently referred to, is described in a not publicly available draft version of an ISO standard that is targetted for completion in 2003.
Summary of change:	⌘	The NIST specified counter mode of operation shall be used.
Consequences if not approved:	⌘	Inconsistent counter mode implementations may arise as there will be no official ISO IEC 10116:200x available including a counter mode of operation until begin 2003. A publicly available draft version will be available end of 2002. This may delay the implementation and use of MAPsec Rel-4.

Clauses affected:	⌘	2 ; 5.6.1	
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-XX Recommendation for Block Cipher Modes of Operation July 2001 ~~ISO/IEC 10116: "Information technology -- Security techniques -- Modes of operation for an n-bit block cipher", Ed.2, 1997-04-17.~~

[6] ISO/IEC 9797: "Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher"**,** Ed.1, 1999-12-16.

***** next modified chapter ****

5.6 MAPsec algorithms

5.6.1 Mapping of MAP-SA encryption algorithm identifiers

The MEA algorithm indication fields in the MAP-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~~in a stream cipher mode~~ (MANDATORY)
:	-not yet assigned-
15	-not yet assigned-

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 5.5 of FIPS 800-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]).

~~ISO/IEC 10116 Counter Mode with parameter j=128 bits, SV=IV and truncation of the last block is according to the method described in ISO/IEC 10116 Annex A.5.3. See ISO/IEC 10116 [5] for more information.~~

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