3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010078**

13 September, 2001, Sophia Antipolis, France

3GPP TSG-SA3 Meeting #19 ***S3-010349***
London, UK, July 3-6 2001

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** **006** ⌘ 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:	⌘	Identification of MAPSec algorithms
Source:	⌘	Alcatel
Work item code:	⌘	SEC1-MAPAL ***Date:*** ⌘ June 20, 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:	⌘	Allocation of identifiers for MAPsec algorithms in 33.200 dealing only with manual key management is unnecessary and confusing.
Summary of change:	⌘	Suppress identification of MAPsec algorithms with integer values.
Consequences if not approved:	⌘	Confusion in specification which unnecessarily sets identifiers for algorithms. This task should be left to the MAPsec DoI specification.
Clauses affected:	⌘	5.4, 5.6
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	Original text in clause 5.4 on MEK is also misleading since the MAPsec DoI does not use the algo identifier to set the key length (this is the role of an attribute in MAPsec DoI). This shows that 33.200 should not make use of identifiers. There is also no need to specify the exact synatx format of the lifetime (stating that this is an absolute time is sufficient). Section 5.6.2 is also erroneously titled (encryption instead of integrity).

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.4 MAPsec security association attribute definition

The MAPsec security association ~~is a sequence of~~contains the following data elements:

~~*MAPsec security association = MEA || MEK || MIA || MIK || PPI || Fallback || SA lifetime*~~

- **MAP Encryption Algorithm identifier (MEA):**

  Identifies the encryption algorithm. Mode of operation of algorithm is implicitly defined by the algorithm identifier. ~~Mapping of~~Possible algorithms ~~identifiers is~~ are defined in clause 5.6.

- **MAP Encryption Key (MEK):**

  Contains the encryption key. ~~Length is defined according to the algorithm identifier.~~

- **MAP Integrity Algorithm identifier (MIA):**

  Identifies the integrity algorithm. Mode of operation of algorithm is implicitly defined by the algorithm identifier. ~~Mapping of~~Possible algorithms ~~identifiers is~~ are defined in section 5.6.

- **MAP Integrity Key (MIK):**

  Contains the integrity key. Length is defined according to the algorithm identifier.

- **Protection Profile Identifier (PPI):**

  Identifies the protection profile. Length is 16 bits. Mapping of profile identifiers is defined in section 6.

- **Fallback to Unprotected Mode Indicator (FALLBACK):**

  In the case that protection is available, this parameter indicates whether fallback to unprotected mode is allowed. This is a one bit indicator where the value one indicates that fall back to unprotected mode is permitted and value zero indicates that fallback to unprotected mode is not permitted.

  Editor's note: The fallback indicator may be moved to the SPD.

- **SA Lifetime:**

  Defines the actual expiry time of the SA. The expiry of the lifetime shall be given in UTC time.

  ~~Editor's Note: The exact format and length to be defined.~~

If the SA is to indicate that MAPsec is not to be applied then all the algorithm attributes shall contain a NULL value.

5.6 MAPsec algorithms

5.6.1 ~~Mapping of~~ MAP-SA encryption algorithms ~~identifiers~~

The MEA algorithm indication fields in the MAP-SA ~~are~~ is used to identify the encryption algorithm and algorithm mode to be used. The ~~mapping of~~following algorithms ~~identifiers is~~ have currently been defined ~~below:~~.

- NULL.

- AES in stream cipher mode (MANDATORY).

Table 1: MAP encryption algorithm identifiers

MAP Encryption Algorithm identifier	Description
0	Null
1	AES 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 the 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.

5.6.2 Mapping of MAP-SA encryption integrity algorithms identifiers

The MIA algorithm indication fields in the MAP-SA are is used to identify the integrity algorithm and algorithm mode to be used. The mapping offollowing algorithms identifiers is have currently been defined below.:

- NULL

- AES in CBC MAC mode (MANDATORY).

Table 2: MAP integrity algorithm identifiers

MAP Integrity Algorithm identifier	Description
0	Null
1	AES in a CBC MAC mode (MANDATORY)
:	-not yet assigned-
15	-not yet assigned-

5.6.1.1 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. See ISO/IEC 9797 [6] for more information.

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

5.6.3 Construction of IV

The IV used in the encryption shall be constructed as follows:

$$IV = TVP \,||\, NE\text{-}Id \,||\, Prop \,||\, Pad$$

The padding field is used to expand *TVP* || *NE-Id* || *Prop* to the *IV* length required by the cryptographic scheme in use.

The IV length shall be 16 octets. The padding (Pad) shall be 2 octets with all bits set to zero.