3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010079**

13 September, 2001, Sophia Antipolis, France

3GPP TSG-SA3 Meeting #19 ***S3-010350***
London, UK, July 3-6 2001

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** **003** ⌘ 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:	⌘	Assignment of bit numbers to Protection Profiles
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:	⌘	There is no need to set bit identifiers for protection profiles in 33.200. This should be done in MAPsec DoI specification and other automatic key management specifications.
Summary of change:	⌘	Remove assignment of bit numbers for protection profiles.
Consequences if not approved:	⌘	Confusion in specifications.

Clauses affected:	⌘	5.4, 6.3.
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

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 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 algorithm identifiers is 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 algorithm identifiers is 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~~Possible profiles ~~identifiers is~~ are 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.

6.3 MAPsec protection profiles

Protection profiles can be individual protection groups or particular combinations of protection groups. ~~MAP protection profiles are coded as a 16 bit binary number where each bit corresponds to a protection group.~~ Currently only 5 groups are defined~~, the rest are reserved for future use~~.

- No protection
- Reset
- Authentication information except handover situations
- Authentication information in handover situations
- Non-location dependaent HLR data.

~~**Table 8: Protection profile encoding**~~

~~**Protection profile bit**~~	~~**Protection group**~~
~~0~~	~~No protection~~
~~1~~	~~Reset~~
~~2~~	~~Authentication information except handover situations~~
~~3~~	~~Authentication information in handover situations~~
~~4~~	~~Non-location dependant HLR data~~
~~5-15~~	~~Reserved~~

The following protection profiles are defined.

Table 9~~8~~: Protection profile definition

Protection profile name	**Protection group**				
	PG(0) *No protection*	PG(1) *Reset*	PG(2) *AuthInfo except handover situations*	PG(3) *AuthInfo in handover situations*	PG(4) *Non-location dependaent HLR data*
Profile A	✓				
Profile B		✓	✓		
Profile C		✓	✓	✓	
Profile D		✓	✓	✓	✓
Profile E		✓	✓		✓