3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010073**

13 September, 2001, Sophia Antipolis, France

3GPP TSG SA WG3 Security — S3#19 **S3-010322**

3 - 6 July, 2001, Newbury, UK

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** **001** ⌘ 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 **X**

Title:	⌘	All messages of the same application context shall be applied MAPsec or not at all
Source:	⌘	Siemens Atea
Work item code:	⌘	MAPsec
Date:	⌘	29-06-2001
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:	⌘	If within a dialogue one (or more) component needs protection (PM1 or PM2) then all components which do not need protection from a security point of view must be "protected" with PM0. 29.002 is very clear on this. 33.200 needs to be aligned. Technical reason: MAP-messages are sent within TCAP-dialogues. A TCAP dialogue is identified by the Application Context (AC). Within a given AC only well defined operations are allowed, and for a given operation only well defined errors are allowed. E.g. if the AC is 40 (secureTransportHandling) the operation must be 78,79,80, or 81 (SecureTransportClassx). If the Operation is 78 (SecureTransportClass1) only the errors 4, 35 and 36 are allowed. Sending cleartext messages rather than PM0-messages within a protected dialogue (AC40) means to allow a mismatch between AC, Operation, and Error, which is not acceptable for TCAP.
Summary of change:	⌘	Remove implementation option of Clause 5.5.2.1
Consequences if not approved:	⌘	Implementations that use that implementation option as suggested by the TS33.200 V4.0.0 clause 5.5.2.1 will run into TCAP problems

Clauses affected:	⌘	5.5.2.1
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

5.5.2 Protected payload

5.5.2.1 Protection Mode 0

Protection Mode 0 offers no protection at all. Therefore, the protected payload of Secured MAP messages in protection mode 0 is identical to the original MAP message payload in cleartext.

~~For cases where Protection Mode 0 is to be used the protection level will be identical to the original unprotected MAP message. It is therefore allowed as an implementation option to let Protection Mode 0 operations be sent without the security header.~~

5.5.2.2 Protection Mode 1

The protected payload of Secured MAP messages in protection mode 1 takes the following form:

Cleartext|| f7(Security Header||Cleartext)

where "Cleartext" is the payload of the original MAP message in cleartext. Therefore, in Protection Mode 1 the protected payload is a concatenation of the following information elements:

- Cleartext
- Message authentication code (MAC-M) calculated by the function f7

Authentication of origin and message integrity are achieved by applying the message authentication code (MAC-M) function f7 with the integrity key defined by the security association to the concatenation of Security Header and Cleartext. The MAC-M length shall be 32 bits.

5.5.2.3 Protection Mode 2

The protected payload of Secured MAP Messages in protection mode 2 takes the following form:

f6(Cleartext) || f7(Security Header|| f6(Cleartext))

where "Cleartext" is the original MAP message payload in cleartext. Confidentiality is achieved by encrypting Cleartext using the encryption function f6 with the confidentiality key defined by the security association and the initialisation vector (IV). Authentication of origin and integrity are achieved by applying the message authentication code (MAC-M) function f7 with the integrity key defined by the security association to the concatenation of Security Header and ciphertext. The MAC-M length shall be 32 bits. The length of the ciphertext is the same as the length of the cleartext.