S3-000151

Technical Specification Group Services and System Aspects Meeting #7,

TSG SA WG3 #11, Mainz, Germany, 22nd Feb-24 Feb 2000

DRAFT 3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

TS 33.102 **CR** **073** Current Version: V3.3.0

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG SA#7 for approval [X] *(only one box should be marked with an X)*
list TSG meeting no. here ↑ for information [ ]

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: USIM [ ] ME [ ] UTRAN [ ] Core Network [X]
(at least one should be marked with an X)

Source: TSG SA WG3 **Date:** 99-17-02

Subject: MAP Security

3G Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	[ ]
A	Corresponds to a correction in a 2G specification	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[ ]
D	Editorial modification	[X]

Reason for change: Further details on Encrypted MAP Message structure requested by CN2

Clauses affected: 7.4

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other 2G core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

7.4 Layer III Message Format

7.4.1 General Structure of Layer III Messages

Layer III messages are transported via the MAP protocol, that means, they form the payload of a MAP message after the original MAP message header. For Layer III Messages, three levels of protection (or protection modes) are defined providing the following security features:

Protection Mode 0: No Protection

Protection Mode 1: Integrity, Authenticity

Protection Mode 2: Confidentiality, Integrity, Authenticity

[Note: GTP based transmission data will also contain sensitive data. This data will require an equal level of security (e.g. authentication parameters, subscriber profile information, etc.). The specifications will extended to address GTP based transmissions using industry standard techniques (such as IPSEC) where appropriate. The possibility of extending these mechanisms to secure CAP/INAP signalling is also being investigated.]

Layer III messages consists of a Security Header and the Layer III Message Body that is protected by the symmetric encryption algorithm, using the symmetric session keys that were distributed in layer II. Layer III Messages have the following structure:

Security Header	Layer III Message Body

In all three protection modes, the security header is transmitted in cleartext. It shall comprise the following information:

- protection mode;
- other security parameters (if required, e.g. IV, Version No. of Key Used, Encryption Algorithm Identifier, Mode of Operation of Encryption Algorithm, ~~etc~~cf. 7.4.3.).

Both parts of the Layer III messages, security header and message body, will become part of the "new" MAP message body. Therefore, the complete "new" MAP messages take the following form in this proposal:

MAP Message Header	MAP Message Body

	Layer III Message

MAP Message Header	Security Header	Layer III Message Body

Like the security header, the MAP message header is transmitted in cleartext. In protection mode 2 providing confidentiality, the Layer III Message Body is essentially the encrypted "old"

MAP message body. For integrity and authenticity, an encrypted hash calculated on the MAP message header, security header and the "old" MAP message body in cleartext is included in the Layer III Message Body in protection modes 1 and 2. In protection mode 0 no protection is offered, therefore the Layer III Message Body is identical to the "old" MAP message body in cleartext in this case.

Summing up, the Protected MAP Message (i.e. the Layer III Message) is a sequence of data elements consisting of the MAP Message Header, the Security Header and the Layer III Message Body. In the following subchapters, the contents of the Layer III Message Body for the different protection modes and the security header will be specified in greater detail.

7.4.2 Format of Layer III Message Body

7.4.2.1 ~~7.4.2.1~~Protection Mode 0

Protection Mode 0 offers no protection at all. Therefore, the Layer III message body in protection mode 0 is identical to the original MAP message body in cleartext.

7.4.2.2 ~~7.4.2.2~~Protection Mode 1

The message body of Layer III messages in protection mode 1 takes the following form:

Cleartext||TVP||$E_{KSXY(i)}$(*Hash*(MAP Header||Security Header||Cleartext||TVP))

where "Cleartext" is the message body of the original MAP message in cleartext. Therefore, in Protection Mode 1 the Layer III Message Body is a sequence of the following data elements and data types:

- Cleartext (OCTET STRING)
- Time Variant Parameter (UTCTime)
- Integrity Check (OCTET STRING)

Authentication of origin is achieved by encrypting the hash value of the cleartext, since only a network element knowing $KS_{XY}(i)$ can encrypt in this way. Message integrity and validation is achieved by hashing and encrypting the cleartext.

[Note: The case X=Y, i.e. only one key for sending and receiving, corresponds to internal use inside network X.]

Note that protection mode 1 is compatible to the present MAP protocol, since everything appended to the cleartext may be ignored by a receiver incapable of decrypting.

7.4.2.3 ~~7.4.2.3~~Protection Mode 2

The Layer III Message Body in protection mode 2 takes the following form:

$E_{KSXY(i)}$(Cleartext||TVP||*Hash*(MAP Header||Security Header||Cleartext||TVP))

where "Cleartext" is the original MAP message in cleartext. Therefore, in protection mode 2 the Layer III message body is just an OCTET STRING which can only be interpreted after having decrypted it. After decryption, the data structure is similar to that in Protection Mode 1.

Message confidentiality is achieved by encrypting with the session key. This also provides for authentication of origin, since only a network element knowing KSXY(i) can encrypt in this way. Message integrity and validation is achieved by hashing the cleartext. TVP is a random number that avoids traceability.

[Note1: There is need for replay protection of Layer III messages; this is for further study. By making use of a TVP as timestamp (perhaps derived from an overall present master time) this could be achieved.]

[Note2: In protection mode 2, the original MAP message body will be encrypted in order to achieve confidentiality. For integrity and authenticity, an encrypted hash calculated on the MAP message header and body in cleartext (i.e. the original MAP message) is appended to the messages in protection mode 1 and 2. All protection modes need a security header to be added.
When implementing these changes, care has to be taken that the maximum length of a MAP message (approx. 250 byte) is not exceeded by the protected MAP messages of Layer III, otherwise substantial changes to the underlying SS7 protocol levels (TCAP and SCCP) would have to be made.]

7.4.3 ~~7.4.3~~ Structure of Security Header

The security header is a sequence of the following data elements and data types:

- Protection Mode (INTEGER)
- Key Identifier (INTEGER)
- Algorithm Identifier (AlgorithmIdentifier)
- Mode of Operation (INTEGER)
- Initialisation Vector (OCTET STRING OPTIONAL)

[Note: Whether the Initialisation Vector is needed depends on the mode of operation of the encryption algorithm]