3GPP TSG SA WG3 Security — S3#13 **S3-000377**

23-26 May, 2000

Yokohama, Japan

Source: **Vodafone Airtouch/ Motorola/ Siemens**

Title: **Proposed LS to N4 on MAP security Layer III**

Document for: **Approval**

Agenda Item: **12**

Source: **S3**[1]

To: **N4**

Title: **MAP security Layer III**

In their meeting #13, S3 agreed two changes to MAP security Layer III as specified in TS 33.102, v3.4.0, section 7. These changes are:

- confidentiality and integrity protection are made independent of each other by making the hash function used to provide integrity protection a keyed hash function (MAC function); for a justification of this change see doc S3-000312 with the amendment described in S3-000355;
- the time variant parameter (TVP) used for replay protection is defined as a 32 bit time-stamp; for a justification of this change see doc S3-000368.

Documents 312, 355 and 368 are attached to this document.

The changes are described below.

With these changes the specification of MAP security layer III, as specified in TS 33.102, v3.4.0, section 7, is considered stable by S3. Please note that MAP security will not be part of the R'99 security architecture specification which will be frozen in TS 33.102, v.3.5.0. MAP security will be re-introduced to a later version of TS 33.102.

TS 33.102, v3.4.0, section 7.4.2.2 is replaced with the following:

7.4.2.2 Protection Mode 1

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

TVP||Cleartext|| $H_{KSXY(int)}$(TVP|| MAP Header||Security Header||Cleartext)

where "Cleartext" is the message body of the original MAP message in clear text. Therefore, in Protection Mode 1 the Layer III Message Body is a concatenation of the following information elements:

- Time Variant Parameter TVP

---

[1] Contact: Peter Howard, Vodafone Ltd; tel +44 1635 676206; email peter.howard@vf.vodafone.co.uk

- Cleartext
- Integrity Check Value

Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function *H* with the integrity session key KSXY(int) to the concatenation of Time Variant Parameter TVP, MAP Header, Security Header and Cleartext.

The TVP used for replay protection of Layer III messages is a 32 bit time-stamp. The receiving network entity will accept a message only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

TS 33.102, v3.4.0, section 7.4.2.3 is replaced with the following:

7.4.2.3 Protection Mode 2

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

$$TVP|| E_{KSXY(con)}(\text{ Cleartext}) || H_{KSXY(int)}(TVP|| \text{ MAP Header}||\text{Security Header}|| E_{KSXY(con)}(\text{ Cleartext}))$$

where "Cleartext" is the original MAP message in clear text. Message confidentiality is achieved by encrypting Cleartext with the confidentiality session key KSXY(con). Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function *H* with the integrity session key KSXY(int) to the concatenation of Time Variant Parameter TVP, MAP Header, Security Header and $E_{KSXY(con)}$(Cleartext).

The TVP used for replay protection of Layer III messages is a 32 bit time-stamp. The receiving network entity will accept a message only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

TS 33.102, v3.4.0, section 7.4.3 is replaced with the following:

7.4.3 Structure of Security Header

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

- Protection Mode
- Key Identifier
- Algorithm Identifier
- Mode of Operation
- Initialisation Vector
- Sending PLMN Id

NOTE: Whether the Initialisation Vector is needed depends on the mode of operation of the encryption algorithm.