3GPP TSG SA WG3 Security — S3#13 **S3-000355**

23-26 May, 2000

Yokohama, Japan

(Ad-hoc meeting on MAP Security, Yokohama, 23 May, 2000)

Source: **Motorola**

Title: **Layer III MAP Message Body in Protection Mode 2**

Document for:

Agenda Item:

---

1. Proposal

We propose that in protection mode 2 of layer III MAP secuirty, we encrypt first and then add a MAC for integrity. The reason for doing it in this order is that integrity can be checked without the need to decrypt first, so a false MAP message can be discarded with much less computation. This more efficient integrity protection provides a degree of protection against denial of service attack by flooding a node with false MAP messages.

We propose to replace TSGS3-000312 with the following:

7.4.2.3 Protection Mode 2

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

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

where "Cleartext" is the original MAP message in cleartext. Message confidentiality is achieved by encrypting cleartext, TVP and integrity check value with the confidentiality session key KSXY(con). Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function *H* to the concatenation of Time Variant Parameter TVP, MAP Header, Security Header and Ciphertext. The integrity is performed on the encrypted message so that integrity can be checked before decryption.

[Note1: There is need for replay protection of Layer III messages; it is envisaged to use TVP for this purpose. The precise definition of the use of TVP is ffs.]