3GPP TSG SA WG3 Security — S3#36 **S3-040967**

23 - 26 November 2004

Shenzhen, China

Title: **Detecting a falsified SMSC address**

Source: **Nokia**

Document for: **Discussion/Decision**

Agenda Item: **6.2**

1. Introduction

This contribution provides a follow-up of the discussion on 'SMS fraud countermeasures'. This paper adds a method to TCAP handshake mechanism for the receiving MSC to detect a falsified SMSC address.

2. Solution

In [S3-040802] it was discussed how the receiving MSC can detect a falsified SMSC address within the TC_Continue message (mt-forwardSM with payload).

> *A first easy to use (but also to detect) possibility is to include a falsified SMSC address within the TC_Continue (mt-forwardSM with payload). This can be detected by the receiving MSC by checking if the received SMSC address (in the third message) matches with the SS7-address the message is received from, and consequently the transaction can be rejected in real-time. This requires that the MSC implements a table of allowed addresses including a list of SMSC-addresses and the allowed SS7 addresses may be sent from (table 1). This must match with the SS7-address of the first TCAP-message. Alternatively if such a table would not be used then all addresses can be logged and analyzed afterwards. Such a table could also be beneficially used to reject SMS traffic from a malicious party that predicted the TCAP-ID in the third message but sent it from a wrong SS7-address.*

The proposed table here would be very big and it will take quite long time for MSC to go through the table to check whether or not the SMSC address is allowed. Such table would be also hard for operator to maintain. Therefore we propose that the receiving MSC implements a table of not allowed SMSC addresses, i.e. SMSC barring, to detect a falsified SMSC address. The SMSC barring table would be much smaller and thus faster for the MSC to check. This enables, for example, that a Short Message Service Center from a foreign country (suspected falsified SMSC address) can be restricted. Also this method solves the charging and network load problem which is caused by the big amount of free SMSs that arrive from an internet address via a foreign SMSC (again suspected falsified SMSC address).

3. Conclusions

We propose that SMSC barring table as an additionally method to TCAP handshake short term solution is documented within an informative Annex to TS 33.200.

4. References

[S3-040802] SA3#35: SMS Fraud countermeasure (Siemens).