3GPP TSG SA WG3 Security — SA3#37
February 21-25, 2005
Sophia Antipolis, France

S3-050071
(comment to S3-050012)

Source:	**Siemens (was** T-Mobile)
Title:	**Comments to (**Next Steps for MAPsec: S3-050012)
Agenda item:	MAPsec
Document for:	Discussion/Decision

1 Introduction

Several changes need to be introduced into TS 33.200 in order to realize the gateway principle. This paper lists some aspects of the work to be done, open questions, and some proposals.

2 MAPsec Changes

2.1 Protection Profiles

The protection profiles were intended to minimise processing overhead on existing NE when they are upgraded to MAPsec. With the new gateway approach, this special effort is no longer necessary. Typical IPsec gateways today can handle throughput of several hundreds of Megabits per second. For MAPsec, similar encryption and integrity algorithms will be used, so the figures should be comparable. Therefore, it is recommended to apply both confidentiality and integrity protection to all traffic passed through the gateway.

Siemens agrees with the principle to slim down the protection profiles possibilities in other to make the 'MAPsec' Gateway MAP-payload type agnostic. However in analogy with IPsec gateways, it should be considered to have the choice between applying integrity only and both integrity and confidentiality protection.

2.2 Protected Protocol Layers

Without the protection profiles, there is no need to analyse the MAP protocol within the gateway. The gateway could just protect the whole MAP payload. There were discussions whether lower layers should be included into the protection. SCCP is required for message routing, therefore it must be kept in the clear. TCAP does not contain sensitive information, so there is no need to protect it. However, it does make sense to protect any protocol on top of TCAP. CAP, as an important protocol for prepaid roaming, could then also benefit from the security provided on the inter-operator interface.

A drawback of this "TCAPsec" idea could be that SA3 is not responsible for TCAP. In that case protection could be applied to CAP and MAP only, which both should be of SA3's concern.

Siemens agrees that it could be studied if a gateway concept could be developed to apply to both CAP and MAP, reusing the protected Messages Format from TS 33.200. Without changes to TS 29.002, the MAP-SECURE-TRANSPORT-CLASS-x services would be used for transporting CAP messages. CN4 should be invited to check the feasibility and to agree the most elegant way forward to document this.

2.3 Protected Message Format

The current definition of TS 33.200 V6.0.0 section 5.5 could be kept, but it would apply to at least CAP and MAP.

2.4 Spoofing Countermeasures

Currently, TS 33.200 does not mandate verification of source address (SCCP Calling Party Address) against MAPsec Sending PLMN-Id and the keys used (at least not explicitly).

The threat scenario is that a fraudulent party agrees to use MAPsec, but still intends to spoof (source) addresses. In that case it would insert a spoofed source address, but sign the message with its own key. According to 33.200 Appendix B, a receiver does not have to match source address to SPI and SA. The receiving entity just uses the SPI to look up the policy table. It then uses the key (looked up using SPI, step 7.) to verify the message and would not detect a spoofed origin address. Address use is only mentioned explicitly in the sending case (but as destination address, in step 1).

Siemens: The received SPI within the ‘MAPsec’ security header is used to retrieve from the SADB (in addition to other data like the MAPsec keys) the source PLMN of the received MAPsec message. After checking the applied integrity protection, the Gateway is sure about the PLMN that has applied the MAPsec protection. If a check towards the SCCP calling party address or the MAP-payload address (e.g SM-RP-OA) is needed, then it could be done at that point of time.

No NE behind the gateway will be able to perform this check, as the SA terminates in the gateway. Any traffic that passes the gateway will be considered verified. Therefore, the gateway should perform this check.

Siemens: The above paragraph means that it is very important to enforce all traffic through the existing MAPsec enabled gateways.

2.5 Coexistence with a MAPsec Rel-4 NE-based solution ?

It is proposed that a Gateway solution should not be able to handle configurations where it communicates with a MAPsec NE. Such a requirement might complicate the gateway design and might delay the standardization of the MAPsec gateway. If that view is supported then a way should be found within the 3GPP documentation to withdraw the MAPsec Rel-4 NE-based solution (without affecting the TCAP handshake alternative in TS 33.200).

2.6 The need for automatic key distributions solutions

As the number of needed gateways at the network borders is anticipated in the same order as the needed VPN gateways (i.e. low) there seems to be no urgent need for an automatic key management mechanism. The policy negotiation complexity (protection profiles/Ze-interface) could be reduced significantly if the suggestions of section 2.1 are followed. This might result in a new (and simplified) key management concept with no need for KAC’s.

2 Summary

SA3 is kindly asked to consider the following proposals, and accept them as working assumptions.

1. ~~MAPsec protection profiles will be dropped for~~ T~~t~~he gateway concept will only include two ‘protection profiles’: ‘Integrity only and ’integrity and confidentiality’.~~.~~

2. Any protocol on top of TCAP will be protected when passing through the gateway.

3. Explicit verification of SCCP and MAP-payload ~~source~~ addresses against MAPsec SPI ~~spoofing~~ will be studied~~shall be added to the TS~~.

4. The MAPsec Gateway concept and the MAPsec Rel-4 NE-based solution need not coexist. A solution needs to be found, how to ‘delete’ the MAPsec Rel-4 NE-based solution from the 3GPP specs.

It is proposed to ask CN4 feedback on the above proposals..