3GPP TSG SA WG3 Security — S3#13 **S3-000364**

23-26 May, 2000

Yokohama, Japan

Source: **SA WG3**

Title: **Security for MAP over IP**

Document for: **Discussion**

Agenda Item:

From: **TSG SA WG3**

To: **TSG CN WG4**

Security for MAP over IP

S3 is currently in the process of specifying security requirements and functions for MAP and GTP. At the moment we are looking at how to protect MAP-over-IP and we have realised that we need more information from CN4 on how MAP-over-IP will be implemented.

We see two main alternatives to provide security for MAP-over-IP:

- to provide security at the application layer using the Layer III-security mechanisms currently specified for MAP over SS7;
- to provide security at the network layer using the IPSec protocol specified by the IETF.

In order to be able to assess the feasibility of the second alternative S3 needs more information related in particular to the following issues:

One important issue to S3 is how the addressing of MAP-over-IP is done. In particular, it is important for us to know whether MAP-over-IP will use IP addresses for end-to-end addressing between the sending and receiving node (network entity) or if addressing is done in a hop-by-hop manner. This may impact not only how IPsec may be used (e.g. transport mode or tunnel mode), but also the viability of using IPsec as a solution.

If we assume end-to-end addressing at the network layer then it may be possible for the sending node and the receiving node to establish an IP security association between them. The protection of the IP packets could then be end-to-end between the two nodes and would not have to rely on any intermediate nodes.

But we are aware that there may be a need for network address translation on the path between the two nodes. E.g. network addresses may be translated at border gateways at the edge of the sending and receiving networks (PLMNs) so that the addresses of nodes within one particular network need not be known outside that network. If such a network address translation occurs at an intermediate node then the IP security association will probably have to terminate at that node. There may also be other reasons for terminating an IP security association at an intermediate node, e.g. the provision of firewall functionality.

In such cases, the intermediate node may have to decrypt and re-encrypt packets. Consequently, the sending and receiving nodes will have to trust the intermediate node for security. This is not considered a problem as long as the intermediate node (e.g. a border gateway) resides in either the sending or the receiving network, but it is considered unacceptable that the sending and the receiving nodes have to trust an intermediate node in a third network for providing adequate security protection between them.

For these reasons, information about how addressing is done for MAP-over-IP is essential for the S3 security work on MAP-over-IP.

S3 therefore kindly asks CN4 for more information on how MAP-over-IP will be implemented in general, and on the above-mentioned issues in particular. S3 would greatly appreciate if the desired information could be circulated well in advance of the joint S3-N4 meeting in mid June. S3 recognises, however, that the work on security for MAP-over-IP has different time-frame from that on security for MAP-over-SS7.

Contact person:

Geir M. Køien (Telenor)

Phone: +47 90752914

Email: geir-myrdahl.koien@telenor.com