3GPP TSG SA WG3 Security — S3#13 **S3-000351**

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. In order to complete this work we will need to know more about how CN4 intends to implement MAP-over-IP.

One particularly important issue to S3 is how the addressing of MAP over IP is done. Our working assumption is that MAP-over-IP will use IP addresses for end-to-end addressing between the sending and receiving node.

This will allow the sending node to encrypt the entire contents of the MAP-over-IP message/operation, possibly including the IP header, and encapsulate it in an outer IP packet. The encrypted packet will then be sent to the receiving node which will decrypt the MAP-over-IP packet. In particular, we assume that no intermediate node/router will be able to or need to decrypt the confidentiality protected MAP-over-IP operation. S3 explicitly assumes that intermediate nodes **do not** need to decrypt the protected MAP message/operation.

Given that MAP over IP addressing is done end-to-end, the use of IPsec will be applicable for both GTP and MAP-over-IP.

Should our working assumption be false it will have a serious impact on how security for MAP-over-IP is to be provided. S3 will therefore ask CN4 for a quick response on our addressing assumption as well as more information on MAP-over-IP in general.