3GPP TSG SA WG3 Security — S3#10 **S3-000077**

19-21 January, 2000

Antwerpen, Belgium

To: **SA, CN, N2**

Copy: **PCG**

From: **S3**

Title: **LS on MAP security**

A 3GPP S3 ad hoc meeting, with experts from ~~N1 and~~ N2 invited, was held in Darmstadt on 10-11 January 2000 to try to resolve the open security issues in 3GPP Release 99. The aim is to complete the appropriate specifications for late inclusion into 3GPP Release 99 in March.

At the meeting it was agreed in principle that N2 should be able to draft the enhancements to the MAP specification for the protection of ~~to show how~~ some sensitive MAP messages ~~can be protected~~. However, ~~all~~ the manufacturers represented ~~(Alcatel, Ericsson, Nokia, Nortel Networks and Siemens)~~ were reluctant to progress the work in N2 because of tight time constraints and the following concerns: ~~.~~

~~Two main concerns were raised:~~

- *Manufacturers emphasised the desirability of introducing security mechanisms in lower layers of the protocol stack; IP security mechanisms were ~~repeatedly~~ mentioned.*

  Provision of security in the lower layers of the protocol stack is ~~may be~~ desirable in the future. However, a solution is required in the short to medium term to address the very real threats that exist in today's signalling networks. It is ~~imperative~~necessary that we provide a solution in R99. The only workable proposal available now is to provide security in the application layer by making appropriate changes to sensitive MAP dialogues in the R99 specifications. Note that an IP based transport layer solution would always be limited to those links that use IP based transmission; there is no guarantee that everyone will switch over to MAP-over-IP. Furthermore, the necessary standards for MAP-over-IP are some way off.

- *There were concerns that the transport mechanisms for key management for MAP security, which are outside the control of N2, would not be fully specified in time for the March plenaries. There were also concerns that the key management for the R99 solution may not meet the requirements for the future solution for IP-based core networks.*

  It must be emphasised that the protocols for key management are fully specified by S3 and S3 believes that the standardisation of transport mechanisms for these protocols is achievable within the timescales for late inclusion into Release 99. An LS has already been sent to S2 to progress this. In the meantime, S3 is ~~will~~ consider ing what further specification work needs to be done. ~~at their meeting in Antwerp on 19-21 January~~. ~~I~~it should be noted ~~however~~ that the lack of standards for transport mechanisms for the key management protocols does not prevent N2 from specifying the necessary changes to MAP.

Second generation core network security has long been identified as a problem area which must be tackled in 3G. ~~From~~ The threats include eavesdropping and

modification of customer information., ~~to large scale~~ denial of service and fraud.. ~~t~~The range of possible “false network” attacks is alarming. The threats to current systems should not be underestimated, and new possibilities will be created for fraudsters and adversaries in the future if we do not deal with this problem ~~now~~. For those who doubt the severity of the attacks, demonstrations could be provided.

We have an excellent opportunity with the Release 99 specifications to provide a solution for core network signalling security to ensure that critical~~these~~ problems do not persist. It is vital that the standardisation work is progressed in all involved groups so that MAP security can be provided in Release 99.

We would appreciate your support in getting these absolutely essential features in place in R99. ~~The vast majority of the work has been in place in S3 for some months; to delay the completion would be to devalue the effort that S3 has put in.~~