3GPP TSG SA WG3 Security — S3#21 **S3-010657**

27-30 November, 2001

Sophia Antipolis, France

Source: **SA 3**

To: **RAN 3**

Title: **Draft** Response LS on Security of Rel5 IP Transport in UTRAN

Contact Person:

Name: Tiina Koskinen, Nokia

E-mail Address: tiina.s.koskinen@nokia.com

SA 3 thanks RAN 3 for their LS R3-013064 on security of Rel5 IP Transport in UTRAN. The following questions were asked in the LS:

Can TSG-SA WG3 confirm the working assumption of TSG-RAN WG3, that the Rel5 IP UTRAN transport networks can be seen as closed environments?

If not:

N1. What is the level of security needed to be standardised in Rel5 UTRAN IP option? (authentication, integrity protection, encryption, for some signalling messages, e.g., ciphering keys, for all signalling messages, for all traffic…)

N2. Would TGS-SA WG3 be willing to take the responsibility of standardising the needed transport security for TGS-RAN WG3 to be then incorporated in its Rel5 Transport Network Layer specifications?

If yes:

Y1: Does TSG-SA WG3 confirm that the threat of internal attacks (from inside this closed environment) is negligible? If not, which type of protection against such internal attacks would be proposed by TSG-SA WG3?

Y2. Does TSG SA3 confirm that the assumption of a closed network holds even in the case where two or more "UTRAN islands" are interconnected via a Virtual Private Network?

No clear-cut "yes or no" -answer can be given to the first question. Indeed, the issue on "closed environments" depends more on the physical structure and characteristics of individual UTRAN transport networks than on standardized functionality of UTRAN networks. This is true for both ATM-based and IP-based UTRAN transport networks. The fact that these networks are typically controlled by a single operator provides some justification for the RAN 3 working assumption about "closed environments".

In light of the above, SA 3 cannot confirm that the threat of internal attacks is negligible. The most effective protection against such attacks can be created by combining cryptographic protection (integrity protection and encryption) of the network interfaces and physical protection of security keys in the network elements.

SA 3 is willing to take the responsibility of standardizing the needed transport security. SA 3 has already started this work by extending the scope of the work on NDS/IP (Network domain security: IP layer security; TS 33.210). On the other hand, most probably only a limited part of UTRAN interface protection can be covered in Rel. 5 time frame. This is due to several reasons in addition to the time pressure for finalizing Rel. 5 specs. The NDS/IP work is relying heavily on IPSEC specifications which are controlled by IETF. Currently, SCTP and IPSEC protocols do not fully interoperate which complicates issues on UTRAN interface protection.