3GPP TSG SA WG3 Security — S3#19 **S3-010373**

3 - 6 July, 2001

London, UK

From: **SA3**

To: **TSG GERAN**

Title: **Reply LS to GERAN GP 011368 on integrity protection at RLC/MAC level**

Contact: **Valtteri.Niemi@nokia.com**

TSG SA WG3 (Security) thank TSG GERAN for their attached LS. The fact that RLC/MAC messages cannot be integrity protected is acknowledged. SA3 also confirms the assumption that RLC/MAC control messages listed in S3-010150 shall be ciphered.

3GPP TSG GERAN #5
Chicago, IL, USA
May 27th-June 1st, 2001

Tdoc GERAN GP 011368
Revised from GP 011281

Source: Nokia 2 (3)

Source: **TSG GERAN**
To: **TSG SA WG3**

Title: **Reply to LS S3-010290 on integrity protection at RLC/MAC level**

Contact: Guillaume SÉBIRE, Nokia
mailto:Guillaume.Sebire@nokia.com

TSG GERAN thank TSG SA3 for their LS on integrity protection at RLC/MAC level.

TSG GERAN do not see that the requirement of having a 32-bit MAC-I in *all* possible cases for *any* of the RLC/MAC control messages listed in S3-010150 (GAHW-010245) can be fulfilled considering the following:

- Although the evaluations so far (GP-010981, S3z010016) have proved feasible the inclusion of a 32-bit MAC-I in all possible cases[1] for some of the messages, and of a variable size MAC-I for the other messages, these studies were conducted based on Release 4 features. The introduction of Release 5 features like e.g. multiple simultaneous temporary block flows will prevent, for all the messages, appending systematically a full-size MAC-I due to constraints in the maximum size of RLC/MAC control messages. Otherwise, this may prevent new features from being introduced in GERAN Rel5.

- The GERAN Rel5 architecture allows connecting BSSs together through the Iur-g interface. The major architecure difference with the UTRAN Iu-r is that only the control plane is available on Iur-g. The security context being known only in the serving BSS, RLC/MAC control messages addressed to an MS under coverage of a drift BSS (not its serving BSS) can, until serving BSS relocation occurs, neither be integrity protected nor ciphered since they originate in this drift BSS. Note however than in this case, integrity protection is possible to RRC messages since they are originated in the serving BSS.

Consequently, TSG GERAN would like to inform TSG SA3 that integrity protection will *not* be applied at RLC/MAC level, and that 3G TS 43.051 has been modified accordingly.

Following this decision, TSG GERAN however still consider the working assumption to cipher the RLC/MAC control messages listed in S3-010150, valid. In fact, some radio resource related functions (i.e. resource request, assignment, reconfiguration, release; cell change) are performed at GERAN RLC/MAC and constitute the main functionality difference with UTRAN RLC/MAC where radio resource related functions are non-existent. Those functions should be secure, therefore the corresponding RLC/MAC control messages should at least be ciphered if not integrity protected. TSG GERAN kindly ask TSG SA3 to confirm this assumption.

[1] Provided the Mobile Station is under coverage of its serving BSC and contention resolution has been performed.