3GPP TSG SA WG3 Security — S3#15bis **S3z000032**

Ad hoc meeting, 8-9 November, 2000

Munich, Germany

Title:	**Reply LS on GERAN integrity protection**
Source:	**TSG SA WG3 Ad-Hoc**[1]
To:	**TSG GERAN**
Contact Person:	**Email: Marc.Blommaert@siemens.atea.be**

S3 ad hoc would like to thank GERAN for their LS on integrity protection (GAHW-000096 - S3-000011). S3 ad hoc have studied the proposals for integrity protection and have noted GERAN's concerns that, when it causes message segmentation, integrity protection may result in a significant and unacceptable overhead on the radio interface.

The LS proposed three alternatives to reduce the overhead. S3 ad hoc offer the following comments:

- *To adapt the method of UTRAN for GERAN, by defining a message authentication code smaller than 32 bits in GERAN in order to limit the overhead*

  A reduction in the message authentication code length for all protected messages is considered unacceptable by S3 ad hoc since it would reduce the effectiveness of the integrity protection mechanism. A 24-bit message authentication code was considered for UTRAN, but the algorithm design authority recommended a 32-bit message authentication code (see LS from ETSI SAGE in Tdoc S3-99317).

- *To set integrity protection as optional, i.e. to be set on or off by the network operator*

  Unlike ciphering, it must not be possible for the network to switch off integrity protection for all messages, since this would undermine the effectiveness of the integrity protection mechanism. To prevent an attacker from being able to turn off integrity protection, a secure mechanism for turning integrity protection on and off would have to be developed. Such a mechanism does not exist in UTRAN and its development may delay GERAN.

- *Not to include integrity protection in GERAN*

  S3 have previous stated to TSG GERAN that the level of security provided by GERAN should be aligned with the level of security provided by UTRAN. S3 ad hoc believe that this principle should be maintained since integrity protection is required in UTRAN and GERAN to protect users and operators against new threats. Furthermore, in many cases operators will provide services over both UTRAN and GERAN. Since the radio access technology will be transparent to the user, it would be desirable for both RANs to offer the same level of protection.

Conclusion:

S3 ad hoc requires that a 32-bit message authentication code shall be added to all messages where any resulting message segmentation can be tolerated. S3 ad hoc currently considers handover messages to be the only time-critical messages where adding integrity protection may lead to an unacceptable failure rate on the radio interface when the handover dialogue cannot be completed in time because the uplink resource was not available for adding a 32-bit message authentication code.

S3 are currently considering solutions for these time-critical messages in GERAN. To assess these solutions, it would be useful if GERAN could provide to S3 a list of time-critical messages that are likely to be segmented due to the addition of a 32-bit message authentication code and justify the effects on failure rates and message overhead. S3 ad hoc also ask GERAN to consider whether any improvements can be made to the GERAN protocols which might allow 32-bit integrity protection to be added without causing any disadvantageous affects.

[1] This reply LS was approved by an **S3 ad hoc** meeting. It will be considered for full S3 plenary approval at S3#16, 28-30 November.