3GPP TSG SA WG3 Security — S3#13 **S3-000379**

23-26 May, 2000

Yokohama, Japan

Source: **3GPP TSG SA WG 3 (Security)**

To: **SMG 2**

Title: **Reply to an LS about Security functions in GERAN**

Contact: Valtteri.Niemi@nokia.com

S3 / SMG10 has studied the issues raised in the LS from SMG2 (Tdoc SMG2 1130/00).

SMG2 wrote:

" GERAN R00 implies a major redesign of the R99 GSM/GPRS control plane and offers a good opportunity to refresh in a future proofed manner the design of major functionalities of the GERAN."

S3 is very happy about this opportunity and would like to utilize it to enhance the security of GSM (as SMG2 already suggests in their LS). However, S3 felt they have not enough information available about the GERAN architecture to be able to give detailed guidance in all security issues.

That is why S3 would kindly invite expert(s) of GERAN to give a presentation about GERAN architecture in the next meeting of S3/SMG10 in Oslo, Norway, 1-4 August 2000.

S3 has included GERAN security as one of their work items for R00 specification work. The leading principle in designing security for GERAN is to get it to an equal level with UTRAN. Also, it is beneficial if the security architectures of GERAN and UTRAN allow the core network (and the terminals) to deal with both as uniformly as possible.

SMG2 asked guidance on the following specific issues. We give initial response to each of those.

- Requirements on ciphering in GERAN with respect to e.g. synchronization including handover cases, different bearers (Real-Time, non-Real Time), etc.

  Answer: Full requirements cannot be given at this stage. The corresponding requirements for UTRAN (see TS 33.102 and TS 33.105) serve as a starting point for this work.

- SMG2 is currently discussing location (protocol) of the ciphering function and would like to know where it is best to place the ciphering function, e.g. before/after channel coding and before/after retransmission protocol.

  Answer: The most important matter is to terminate the ciphering in BSC instead of BTS. The location in the protocol stack is less relevant from the security point of view.

- The list and the description of the parameters needed for the ciphering function in GERAN

  Answer: The parameter set shall include at least: the secret ciphering key (preferably 128 bits), direction bit (uplink/downlink), a counter (at least 32 bits; it counts the ciphered communication units). Probably also a bearer identity is needed to avoid situations where exactly the same set of input parameters are used more than once.

- Requirements on integrity protection in GERAN.

  Answer: Ideally both user plane and control plane traffic should be integrity protected. Integrity protection of the control plane is required, and protection of the user plane is under study. This is most probably done by adding 32-bit integrity checksum to transmitted communication units at some layer. The integrity protection should also terminate in the BSC.

- The list and the description of the parameters needed for the integrity function in GERAN

Answer: This resembles the answer on the ciphering case. The parameter set shall include at least: the secret integrity key (probably 128 bits), direction bit (uplink/downlink), a counter (at least 32 bits). Probably also a bearer identity is needed to avoid situations where exactly the same set of input parameters are used more than once.

SMG2 also raised the concern that the ciphering algorithm to be used in the future releases of GERAN would be designed in time to be introduced in R00 onwards. S3 has already started the process of designing a new algorithm for GSM-GPRS-EDGE, and this new algorithm is intended be suitable for this purpose. It is too early to estimate when the design is finalized, but S3 is confident that the ciphering algorithm will be delivered in time for R00.