3GPP TSG SA WG3 Security — S3#22 **S3-020156**

25 - 28 February 2002

Bristol, UK

Source: **S3**

To: **GERAN**

Title: **DRAFT Reply LS on COUNT INPUT TO CIPHERING ALGORITHM**

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

S3 thanks GERAN for their LS G2-020145 (=S3-020028).

GERAN asked the following questions from S3 :

"

- whether the *principle* of combining a HFN with a TDMA Frame Number and the *corresponding rules* are acceptable from security standpoint, and
- if yes,
- whether the proposed 11-bit HFN and 17-bit TDMA Frame Number (by truncation of the T1 part of the 22-bit GSM TDMA Frame Number) is acceptable; otherwise to suggest the size of the HFN and of the TDMA Frame Number
- if not,
- to provide guidance and detailed recommendations.

"

S3 accepts the proposed principle. The rules were listed as follows:

"

- Every time the TDMA Frame number reaches 0 the HFN is incremented by 1.
- When a handover is performed, the HFN is also incremented by 1.
- In order not to cipher twice the same message with two different set of parameters (this could happen in case of a handover: the message is first sent in the old cell, and then resent in the new cell), a sequence number must be introduced in this *message* to make its content differ when retransmitted: 1 bit is sufficient.
- The HFN must be kept in the mobile station's memory until a new authentication is needed (in which case the HFN is reset) whether the MS is in RRC-Idle or RRC-Connected modes. The HFN shall be incremented by 1 at every new RRC connection and informed to the network within RRC Connection Request similarly to UTRAN, this in order to avoid repetition of the same count value in-between two authentications.

"

These rules are also acceptable from security viewpoint. In fact, the third rule can be left out without degrading the security. It is very important that two different messages are never ciphered

using the same set of input parameters but the same message can be ciphered using two different sets of input parameters.

The proposed lengths for HFN and TDMA frame number parameters are also acceptable. They seem to provide a good balance between different cases where HFN is incremented.