3GPP TSG SA WG3 Security — S3#22 **S3-020149**

25 - 28 February 2002

Bristol, UK

Source: **S3**

To: **RAN2**

Title: **DRAFT Reply LS on START value calculation and Additional principles adopted by TSG-RAN WG2**

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

S3 thanks RAN2 for their response LS R2-020594 (=S3-020139).

RAN2 requested S3 feedback on the following additional principles adopted by RAN2:

"

1. The Security Mode Command cannot be used to "modify" Integrity protection on the same CN Domain unless new keys have been received.
2. Change of algorithms is possible only through Reconfiguration messages on RNC decision. i.e.Change of algorithms is not possible through the Security Mode Command.
3. UEA0 will be used to stop ciphering through Reconfiguration messages at relocation; the previous mechanism through the use of a code point for "stop" has been removed from all messages.
4. In case of signalling connections to both domains, the same ciphering algorithm needs to be applied on both domains. The status of ciphering (i.e. started or not started) shall be the same for both domain.
5. In case ciphering is started in one CN domain, a subsequently established signalling connection on the other CN domain also needs to be ciphered (with the same ciphering algoprithm).
6. At Inter-rat handover to UTRAN, a mechanism is applied where the UE uses a fixed HFN value for ciphering, without incrementing the HFN when the CFN cycle wraps around. The value of the HFN is given by the START value transferred by the UE via the BSC to UTRAN prior to the handover. This HFN is used until the handover to UTRAN COMPLETE command is received in UTRAN, in which the UE includes a new START value for ciphering. Thus, until the "Handover to UTRAN complete" message is received in UTRAN (a few 100ms) it is possible that the HFN part of COUNT-C used for ciphering is reused.
7. For timing-initialised hard handover a similar mechanism as for the inter-rat handover to UTRAN is adopted, with the exception that the UE uses the latest transmitted START value before the handover until the responce message is received in UTRAN.

"

As already observed by RAN2, the principles 6 and 7 conflict with the security principle which states that the COUNT-C value should never be re-used while all other inputs (except the message and its length) to the ciphering algorithm stay constant. However, S3 is ready to accept these deviations from the general principle in order to get Release 99 specifications on ciphering completed. All principles 1-5 are also endorsed by S3.

The LS from RAN2 continued with the following:

" In the context of Release 4 RAN WG2 has discussed the issue of integrity protection/ciphering of TM RLC mode Signalling radio bearers (SRBs). These SRBs are not integrity protected. It is proposed by RAN WG2 that these will also not be ciphered. RAN WG2 does not forsee significant security issues with this proposal due to the functionality associated with these TM mode SRBs in Release 4. RAN WG2 requests feedback from SA WG3 on this proposal."

S3 did not have enough information in their meeting about the functionality associated with Rel.4 TM mode SRBs to be able to give any feedback on the proposal. As soon as more information is available for S3 they will inform RAN2 whether the proposal could be accepted.