3GPP TSG SA WG3 Security — S3#22 **S3-020139**

25 - 28 February 2002

Bristol, UK

TSG-RAN Working Group 2 Meeting #27 *R2-020594*
Orlando, FL, USA, 18 - 22 February 2002

Title:	**Response to LS (S3z020043) on START value calculation and Additional principles adopted by TSG-RAN WG2**
Source:	**RAN2**
To:	**S3**
Cc:	
Response to:	**LS (S3z020043) on START value calculation**
Release:	**R'99**

Contact Person:
Name: Ravi Kuchibhotla
Tel. Number:
E-mail Address: Ravi.Kuchibhotla@motorola.com

Attachments: None

1. Overall Description:

This LS is a response to the issue originally raised by RAN2 in R2-012775. In addition RAN WG2 would like to apprise SA WG3 on the latest set of principles assumed and adopted by RAN WG2 in specifying the security features for Release 99.

RAN WG2 thanks SA WG3 for their response..

Question:

RAN 2 asks S3 for guidance on how to calculate the START value for the initialisation of HFN components of COUNT-C and COUNT-I.

When ciphering is not applied for AM and UM user plane radio bearers the COUNT-C values for those UM and AM RBs are anyway maintained, i.e. initialised and incremented in order to be used in the counter check procedure.

However it is not clear whether those COUNT-C values shall be used for calculating the START value or not.

S3 Response:
According to TS 33.102, only COUNT-C values of these RBs being protected should be included in the START value calculation.

However, S3 believes that the COUNT-C values for ALL radio bearers and signalling radio bearers could be included in the START value calculation, regardless of whether the bearers are ciphered or not.

S3 understands that this may potentially shorten the lifetime of the keys but this is not considered to be a security problem. If in this case the THRESHOLD had been reached, then as would normally occur, the outcome is that an authentication would be triggered the next time the RRC connection is established.

Either of these alternatives will be acceptable from an S3 point of view.

S3 kindly asks RAN2 to consider this input and inform S3 of RAN2's final decision so that S3 could prepare corresponding CRs to 33.102 if needed.

RAN WG2 Action (February 18-22, 2002) :

RAN WG2 has decided to not include the unciphered bearers in the calculation of the START value. This requires no modifications to the current versions of TS 33.102 per our understanding of the current status.

Additionally the following principles were adopted in RAN WG2 #27, February 18-22, 2002 in agreeing to modifications (CRs) to TS 25.331 v3.9.0 and which will be presented to the RAN plenary (March 5-8, 2002) for approval.

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.

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.

2. Actions:

To S3 group.

ACTION: No action needed for the START value calculation issue raised in the earlier LS to S3. RAN2 requests S3 group to review the additional principles adopted by RAN WG2 and provide their feedback as necessary.

3. Date of Next RAN2 Meetings:

RAN2_28	8 – 12 April 2002	Kobe, Japan.
RAN2_29	13 – 17 May 2002	Gyeongju, Korea.