3GPP TSG SA WG3 Security – S3#21bis

S3z020043
revised: *S3z020035*

January 31st– February 1st, 2002
Antwerp, Belgium

Title: ~~**[DRAFT]**~~ Response to the LS from RAN2 on START value calculation
Source: SA WG3 (e-mail approved)
To: RAN2
Cc:
Response to: R2-012775
Release: R'99

Contact Person:
Name: **David Castellanos-Zamora**
Tel. Number: +46 84045920
E-mail Address: david.castellanos-zamora@era.ericsson.se

Attachments: None

Overall Description:

This LS is an answer to the questions raised by RAN2 in R2-012775.
S3 thanks RAN 2 for questions and is pleased to provide the following answers to RAN 2's questions.

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.

2. Actions:

To [S3] group.

ACTION: *RAN2 asks [S3] group to give their guidance of whether COUNT-C values for non ciphered UM or AM user plane RBs shall be included in the START value calculation or not.*
Furthermore RAN2 would like to know whether the COUNT-C values for unciphered AM and UM radio bearers need to be reinitialised when ciphering is started for those SRBs.

Answer to actions:

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~~ ALL radio bearers and signalling radio bearers ~~should always~~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.

Date of Next S3 Meetings:

SA3_22	25 - 28 Feb 2002	2002	Bristol.