

8-11 October 2002**Munich, Germany**

Title: Reuse of COUNT-C Values for Cipherring of RB Using RLC TM During Handover
Response to: LS R2-022684
Source: SA3
To: RAN2
Cc: -

Contact Person:

Name: Lee Valerius
Tel. Number: + 1 972 684 5526
E-mail Address: Valerius@nortelnetworks.com

Attachments: none

1. Description:

SA3 kindly thanks RAN2 for its LS R2-022684 (=S3-020482) on re-use of COUNT-C values for cipherring of radio bearers using RLC transparent mode during SRNS relocation. SA3 has the following responses to the questions from RAN2.

- “RAN2 kindly asks SA3 whether they consider that the R’99 handling of cipherring of RB using RLC TM during SRNS relocation by re-using COUNT-C values is a security problem that needs correction in further releases (R4 onwards).”
 - SA3 affirms that reuse of the COUNT-C values in this situation is a security problem that needs correction in releases beyond Release 99.
- “If the answer to the first question is yes, RAN2 asks SA3 if the attached proposal is in line with the SA3 principles, is more secure compared to the solution adopted in R’99 and looks acceptable as far as they are concerned.”
 - SA3 believes that the attached proposal does solve the problem and is acceptable given that backwards compatibility with R99 mobiles is ensured (i.e. the new IE is only included in the handover message by the Target RNC when the Target RNC is aware that the UE will understand this IE). Also, SA3 recommends that with respect to Target RNC choice of the ‘MAC-d HFN initial value’, a minimum value of the margin variable ‘x’ in the formula be agreed by RAN2 in such a way that no values of COUNT-C are repeated.

2. Actions to RAN2:

RAN2 are asked to take into account the recommendation above when developing the necessary CRs to their specifications.

3. Dates of Next TSG-SA3 Meetings:

SA3-26	19 th – 22 nd November 2002	Oxford, UK
SA3-27	25 th – 28 th February 2003	Sophia Antipolis, France