3GPP TSG SA WG3 Security — S3#25 **S3-020482**
8 - 11 October 2002
Munich, Germany

TSG-RAN Working Group 2 Meeting #32 *R2-022684*
Xi'an, China, 23- 27 September 2002

Title: LS on re-used of START value for ciphering of RB using RLC TM during SRNS relocation

Release: Rel-4
Work Item:

Source: **RAN WG2**
To: **SA WG3**

Contact Person:
Name: **Tania Le Goff**
Tel. Number: +33 1 39 44 37 75
E-mail Address: tlegoff@nortelnetworks.com

Attachments:

R2-022550 Discussion Paper on 25.331 [Rel-4] Ciphering of radio bearer using RLC TM during SRNS relocation (Nortel Networks)

---

1. Overall Description:

RAN2 would like to inform SA3 about the fact that a new, more secure, solution has been proposed in R4 for the handling of ciphering of radio bearers using RLC TM during a Timing re-initialised hard handover.

In order to avoid the reuse of COUNT-C values during some time after the handover procedure (around 2 seconds), a proposal has been made (see attached document) that the Target RNC sends a 'MAC-d HFN initial value' to the UE in the message that will trigger the handover.
Such a solution was not adopted for R99, because when this was corrected in February this year, it was found too late to introduce a new IE in the ASN.1 of the RRC messages.

At that time, RAN2 did send a LS to SA3 asking if it was acceptable to reuse COUNT-C values for R99 during some time after the handover procedure. SA3 answered that this conflicts '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.'

2. Actions:

To SA3 group.

ACTION:

- RAN2 kindly asks SA3 whether they consider that the R'99 handling of ciphering 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).
- 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.

3. Date of Next RAN2 Meetings:

RAN2_33	12 – 15 Nov 2002	Sophia, France
RAN2_34	17 – 21 Feb 2002	Sophia-Antipolis, France

3GPP TSG-RAN WG2 meeting #32
23 – 27 September 2002
Xi'an, China

R2-022550

Agenda item: 8.2

Source: Nortel Networks

Title: Ciphering of radio bearers using RLC TM during SRNS relocation

Document for: Discussion, Decision

1 Introduction

This document proposes a more secure solution for handling of ciphering of radio bearers using RLC TM during a Timing re-initialised hard handover. The solution was not adopted for R99 because it was found too late than an IE was missing in ASN.1. The proposal is for Rel-4 only. Whether or not to use it would be up to the Target RNC. The UE would have to support it.

2 Discussion

2.1 R99 specification

During RAN2#27 in Orlando, it has been decided to solve the issue of the continuity of ciphering during the timing re-initialised Hard Handover for TM radio bearers by re-using the value of the latest transmitted IE 'START' during the gap between the activation of the radio bearer and the IE "COUNT-C activation time" included by the UE in the uplink message.

Subsection 11.5 of 25.331 v3.b.0:

If the IE "Downlink DPCH info common for all RL" is included in a message used to perform a Timing re-initialised hard handover or the IE "Downlink DPCH info common for all RL" is included in a message other than RB SETUP used to transfer the UE from a state different from Cell_DCH to Cell_DCH, and ciphering is active for any radio bearer using RLC-TM, the UE shall, after having activated the dedicated physical channels indicated by that IE:

*1> set the 20 MSB of the HFN component of **COUNT-C for TM-RLC to the value of the latest transmitted IE "START" or "START List" for this CN domain**, while not incrementing the value of the HFN component of COUNT-C at each CFN cycle; and*

1> set the remaining LSBs of the HFN component of COUNT-C to zero;

1> start to perform ciphering on the radio bearer in lower layers while not incrementing the HFN;

1> include the IE "COUNT-C activation time" in the response message and specify a CFN value other than the default, "Now" for this IE;

1> calculate the START value according to subclause 8.5.9;

1> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the response message;

1> at the CFN value as indicated in the response message in the IE "COUNT-C activation time":

2> set the 20 MSB of the HFN component of the COUNT-C variable to the START value as indicated in the IE "START list" of the response message for the relevant CN domain; and

2> set the remaining LSBs of the HFN component of COUNT-C to zero;

2> increment the HFN component of the COUNT-C variable by one;

2> set the CFN component of the COUNT-C to the value of the IE "COUNT-C activation time" of the response message. The HFN component and the CFN component completely initialise the COUNT-C variable;

2> step the COUNT-C variable, as normal, at each CFN value, i.e. the HFN component is no longer fixed in value but incremented at each CFN cycle.

At that time, it was felt that it was not very 'secure' to re-used already an old 'START' value. The proposed alternative was to send the new initialisation value to apply from the Target SRNC to the UE, which would allow for no re-use of old values after handover. However as it was too late to modify any RRC messages for R99, the simplest solution was adopted. The following paragraph re-introduces the alternative that was not selected for R99.

2.2 Proposed alternative

In order to avoid the reused of an old START value during the gap, it is proposed that the Target RNC sends a 'MAC-d HFN initial value' to the UE in the message that will trigger the handover. The UE would then use this value to initialised the COUNT-C for the TM RB similarly to want is currently done. The HFN would not be incremented during the gap.

The Target RNC would chose the 'MAC-d HFN initial value' by evaluating the current COUNT-C of the TM bearers included in the Source to Target 'SRNS RELOCATION INFO' and taking some margin to prevent for possible CFN wrap around, i.e. (24 MSB of the COUNT-C) +x.

The Source RNS would always include the IE 'COUNT-C list' in the Source to Target 'SRNS RELOCATION INFO'. And it would be up to the Target RNC to decide if it wants to use the more secure method or not.

The UE would know which method the UTRAN wants to used by the presence or absence of the 'MAC-d HFN initial value' IE.

2.3 Changes needed

The following modification are necessary for the more secure solution:

- Addition on the optional IE 'MAC-d HFN initial value' in the IE 'Downlink DPCH info common for all RL'.

3 Proposal

It is proposed to agree on the inclusion of the described more secure solution for Rel-4. A CR would then be prepared for RAN2#33 in Sophia.