3GPP TSG SA WG3 Security — S3#22 **S3-020017**

25 - 28 February 2002

Bristol, UK

TSG-RAN Working Group 2 (Radio L2 and Radio L3) *R2-012776*
Makuhari, Japan, 26 - 30 November 2001

Title:	LS on HFN initialisation at CN domain switch for SRBs
Source:	RAN2
To:	S3
Cc:	
Response to:	
Release:	R'99

Contact Person:

Name:	**Patrick Fischer**
Tel. Number:	+33 1 30 77 53 56
E-mail Address:	Patrick.fischer@alcatel.fr

Attachments:

1. Overall Description:

RAN 2 asks S3 for guidance on the way to initialise the HFN part of the COUNT-C and COUNT-I for signalling radio bearers at CN domain switch.

RAN2 has identified the following scenario:
An Iu connection to a CN domain A is established. In the RRC connection setup complete messaqe the UE will report the IE START list. Those values would be used for initialising the HFN values of COUNT-C and COUNT-I of the signalling radio bearers that have been setup in the RRC connection setup procedure. The COUNT-C and COUNT-I values are initialised during the security mode command procedure. The signalling radio bearers are then ciphered and integrity protected using Cka and Ika.

When a Iu connection to a second CN domain B is established and a security mode procedure is started, the signalling radio bearers shall be ciphered and integrity protected after this procedure with Ckb and Ikb. In order to guarantee protection, as soon as the Ckb and Ikb are used (at the activation time for each RB) the HFN values of the COUNT-C and COUNT-I values for the signalling radio bearers need to be initialised with an appropriate value for the CN domain B.

RAN2 is unclear about which value is supposed to be used in order to initialise the second CN domain. RAN2 proposes to use either

1. The START value for the CN domain B that has been transmitted from the UE to UTRAN in the RRC connection setup complete message.
2. The last START value for CN domain B that has been transmitted from the UE to UTRAN in any message.

It could now happen that the Iu connection to CN domain A is released. At that point in time the signalling radio bearers will still be ciphered with CKb and IKb.

After releasing the Iu connection to CN domain A a new CN domain connection to CN domain A can be established. After the security mode procedure for this CN domain Ika and CKa shall be used for the signalling radio bearers. Therefore the HFN components of the COUNT-I and the COUNT-C values shall be initialised with a START value that is appropriate for CN domain A. The option 1. above is felt to be not possible since this would mean reusing the same COUNT-C values as used before, and the option 2. may not be possible since the UE may not have transmitted any START value for CN domain A.

RAN2 has identified the following possibilities to initialise the HFN components of the COUNT-C and COUNT-I values for the signalling radio bearers:

1. Calculate locally in the UE and in UTRAN a START value for CN domain A based on the HFN that were used for signalling radio bearer or radio bearers before the Iu connection for CN domain A has been released. RAN2 has identified an eventual desynchronization problem between the value calculated in UTRAN and UE in case some UM PDUs are lost just before release of the last RB of CN domain A that would have incremented the HFN at the transmitter and not at the receiver.
2. Locally store in UE and UTRAN the HFN component of each signalling radio bearer at the activation time of ciphering configuration for CN domain B and use these values incremented by 1 for initialising the HFNs for the signalling RBs.
3. As a variation from 2 the HFN components of the signalling RBs at the respective activation times of ciphering configuration of domain B could be used to calculate a local $\text{START}_{\text{SRBA}}$ value which would be only valid for the signalling radio beares.

2. Actions:

To [S3] group.

ACTION: RAN2 asks [S3] group to S3 to explain their preferred solution to the described scenario, or propose another solution if the above stated are not satisfying.

3. Date of Next RAN2 Meetings:

RAN2_26	7 – 11 January 2002	Sophia Antipolis, France.
RAN2_27	18 – 22 February 2002	Orlando, FL, USA.