3GPP TSG SA WG3 Security — S3#20 **S3-010413**

16 - 19 October, 2001

Sydney, Australia

TSG-RAN Working Group 2 (Radio L2 and Radio L3) ***R2-011763***

Berlin, Germany, 9 - 13 July 2001

Source: **TSG-RAN WG2**

To: **TSG-SA WG3**

Title: **LS on Guidance Needed Concerning Security Mode Reconfiguration**

Contact: **Richard Kuo**
Email: Richard_kuo@asus.com.tw

One R99 contribution R2-011576 (attached below) concerned about the usage of COUNT-C and COUNT-I for SRBs when the security mode is reconfigured.

To clarify the behavior of the UE when the security mode reconfiguration takes place, TSG-RAN WG2 would kindly like to ask the opinion of TSG-SA WG3 on the following question.

Question*: Is it possible that the ciphering algorithm or/and the integrity protection algorithm is changed while the security key set is kept unchanged during the security mode reconfiguration?*

3GPP TSG RAN WG2 #22 **Tdoc R2-011576**

Berlin, Germany, 9 - 13 July, 2001

Source **: ASUSTeK**

Title **:** Issue on the usage of COUNT-C and COUNT-I for SRBs at CN domain switching

Agenda Item **:** 6.2

Document for **: Discussion and decision**

Current Security Architecture Specifications (Background):

1. There may be one integrity key (IK) for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user. The same statement is also true for cipher key (CK).

2. The signalling radio bearers (SRB) are used for transfer of signalling data for services delivered by both CS and PS service domains. These signalling radio bearers are data integrity protected by the IK of the service domain for which the most recent security mode negotiation took place. The same statement is also true for ciphering.

Problems:

According to the current security architecture specification [TS 33.102 V 3.8.0], it is clear that the signalling radio bearers should be switched to the new CN domain (which means to use the UMTS security context of the new CN domain) when a new security mode negotiation is performed on a different CN domain. But the current RRC specification [TS 25.331 V 3.7.0] does not cover anything about the CN domain switching for the signalling radio bearers. It might cause inconsistency in security context usage between the UE and UTRAN if there is any ambiguity existing.

To clarify the UE's behavior when a new security mode negotiation is performed on a different CN domain, consider the following scenario:

1. RRC connection is setup.

   → The IE "START list" which contains the $START_{PS}$ and $START_{CS}$ is sent to UTRAN in the RRC CONNECTION SETUP COMPLETE message.

2. A PS call is established and security mode is started for this domain.

   → The HFNs of COUNT-Cs and COUNT-Is of the SRBs on the PS domain are initialized with $START_{PS}$.

3. A CS call is established and security mode is started for this domain.

   →The SRBs are switched to the CS domain.

   → The HFNs of COUNT-Cs and COUNT-Is of the SRBs on the CS domain are initialized with $START_{CS}$.

4. Security mode is reconfigured for PS domain.

   → The SRBs are switched back to the PS domain.

   → The HFNs of COUNT-Cs and COUNT-Is of the SRBs are also switched back to the PS domain.

   → The HFNs might be incremented by 1 to avoid reusing the old counter values (**To Be Clarified!**).

If the above concepts about the UE's behavior are correct, the following solution is proposed.

Proposed Solution:

The solution is to store the HFNs of COUNT-C and COUNT-I in the security context for each SRB per CN domain and to switch the SRBs to the new CN domain when a new security mode negotiation is performed on a different CN domain.

Based on the proposed solution, ASUSTeK will provide the CR for this issue in the next meeting held in Helsinki.