3GPP TSG SA WG3 Security — SA3#35 **S3-040708**
October 5-8, 2004
St Paul's Bay, Malta

3GPP TSG-CN1 Meeting #35 Tdoc N1-041519
Sophia Antipolis, France, 16-20 August 2004

Title:	LS on Re-authentication and key set change during inter-system handover
Response to:	LS (R2-041261/N1-041322) on Re-authentication and key set change during inter-system handover from RAN2
Release:	Release 5
Work Item:	---
Source:	CN1
To:	RAN2
Cc:	SA3, RAN3

Contact Person:
Name: Robert.Zaus
E-mail Address: robert.zaus@siemens.com

Attachments: ---

1. Overall Description:

CN1 would like to thank RAN2 for their reply liaison statement on "re-authentication and key set change during inter-system handover" and give the following answers to RAN2's questions.

Question from RAN2:

1) Since these problems occur only when the UE and MSC have new keys but they are not activated, RAN2 would like to clarify what is the normal operation of these procedures. Is it the understanding that the specifications permit that the AKA procedure providing new keys to the UE may be performed significantly in advance of the corresponding Security/Ciphering Control procedures that activate these new keys? If so, in what proportion of cases does this currently occur?

Answer from CN1:

There are separate procedures for authentication and starting ciphering, so a short period of time when the new keys are available but not in use yet cannot be completely excluded, even if the operator intends to start ciphering “immediately”.

Normal operation of the procedures is as follows:

If authentication and ciphering are used in the network, then ciphering is turned on as soon as possible.

Currently, CN1 is not aware of any scenario where re-authentication on the already ciphering- and/or integrity-protected CS connection would be required for security reasons. Accordingly, there seems to be no MSC implementation that would perform such a re-authentication.

Question from RAN2:

2) Are the new keys that are not activated considered as new keys in the next signalling connection? (i.e. “Key Status” to RNC is indicated as ‘new’ in the security mode command.)

Answer from CN1:

From the CN protocol viewpoint the keys are always new after authentication, but it is up to the RANAP protocol to encode the indication of key status.

2. Actions:

To RAN2.

ACTION: CN1 asks RAN2 to take these answers into account when further discussing the CRs to TS 25.331.

3. Date of Next TSG-CN1 Meetings:

CN1_36 15th – 19th November 2004 Asia?