3GPP TSG SA WG3 Security — S3#33 **S3-040207**
10 - 14 May 2004
Beijing, China

3GPP TSG-CN1 Meeting #33 Tdoc N1-040501
Atlanta, Georgia, USA 16 – 20 February 2004

Title: LS on Re-authentication and key set change during inter-system handover
Release: Release 5
Work Item: ---

Source: CN1
To: RAN2, RAN3, SA3
Cc: ---

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

Attachments: ---

---

1. Overall Description:

During their last meeting, CN1 discussed and agreed a CR on re-authentication and key set change during inter-system handover. It is CN1's understanding that the following principles apply for the key set change after re-authentication of an ongoing, already ciphering and/or integrity protected RR/RRC connection or PS signalling connection:

i) in the CS domain: If a new GSM or UMTS security context is created during an ongoing, already ciphering and/or integrity protected RR or RRC connection, the ciphering and integrity keys of the new context will be taken into use only when the MSC initiates a new Security Mode Command procedure or Ciphering Mode Command procedure.

ii) in the PS domain: In GERAN A/Gb mode the new GSM or UMTS security context is taken into use immediately after the Authentication and Ciphering procedure creating the new context.
In UTRAN or GERAN Iu mode an explicit Security Mode Command procedure initiated by the SGSN is necessary to take the new keys into use.
If an inter-system change from UTRAN/GERAN Iu mode to GERAN A/Gb mode occurs before the SGSN initiated a Security Mode Command procedure, the new keys will be taken into use immediately after the inter-system change. The same applies if an inter-system change from GERAN A/Gb mode to UTRAN/GERAN Iu mode occurs, before an Authentication and Ciphering procedure initiated in GERAN A/Gb mode could be completed.

CN1 have noticed that there are several issues in the current 3GPP specifications which are not completely in line with these principles:

1) CN1 has become aware of a CR agreed during RAN2 meeting #37 on “Handling of key sets at Inter-RAT Handover to UTRAN” (CR 1991, R2-031856) that clarified the usage of security keys after handover to UTRAN for the case that new keys have been created in GERAN A/Gb mode, but have not been taken into use before the handover occurs.

According to the CR, immediately after the handover the UE starts to use the key set stored on the SIM/USIM for ciphering in UMTS, i.e. the key set created during the last authentication procedure, even if this key set was not yet used in GERAN A/Gb mode at the time the inter-system handover was initiated.

CN1 would like to point out that there is a reason for the strict requirement for the CS domain that an explicit signalling between MSC and UE is required to take the new keys into use:

It is possible that an inter-MSC handover from an anchor MSC-A to an MSC-B occured, before the subsequent inter-system handover to UTRAN takes place inside MSC-B. If the anchor MSC has triggered an re-authentication where new security keys have been generated by the SIM/USIM shortly before the inter-system handover is initiated, the MSC-B is not aware of the re-authentication, because the re-authentication procedure between the anchor MSC and the UE is transparent for the MSC-B. The new keys are not available in MSC-B, until the anchor MSC intiates a MAP procedure towards MSC-B including a RANAP Security Mode Command. Therefore, in this scenario, after an inter-system handover to UTRAN the UE and the network would use different keys for ciphering and intergrity protection, the handover would fail and possibly the call would be dropped.

CN1 therefore kindly ask RAN2 to align their specification TS 25.331 with the above principles.

Since CN1 considers a re-authentication during an ongoing, already ciphering protected connection in the CS domain as a quite rare event, it is CN1's opinion that a correction from release 5 onwards shall be sufficient.

2) CN1 noticed that according to TS 33.102, v 5.3.0, subclause 6.8.5, Intersystem handover for CS Services – from GSM BSS to UTRAN:

> The integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed. The Serving RNC will do this by initiating the RRC security mode control procedure when the first RRC message (i.e. the Handover to UTRAN complete message) has been received from the MS.

It is CN1's understanding of the specification that the RNC will initiate this without receiving an explicit RANAP Security Mode Command procedure from the MSC.

Furthermore it is CN1's understanding of the RANAP specification TS 25.413 that during the inter-system handover the MSC can provide only one key set to the RNC with the RANAP Relocation Request message, and that this is the old key set.

Can SA3, RAN2 and RAN 3 confirm this interpretation?

If yes, then it has to be ensured that after the inter-system handover, the first RRC Security mode control procedure, which was not intiated by the MSC with an explicit RANAP Security Mode Command procedure, will not trigger a change of the key set, if a new security context was already created before the inter-sytem handover, but not yet taken into use.

CN1 kindly ask RAN2 whether their specification TS 25.331 fulfils this requirement.

2. Actions:

To RAN2, RAN3, and SA3.

ACTION: CN1 kindly ask RAN2, RAN3, and SA3 to reply to the questions above and to align their specifications where necessary.

3. Date of Next TSG-CN1 Meetings:

CN1_34	10th – 14th May 2004	Zagreb, Croatia (EF3)
CN1_35	16th – 20th August 2004	Sophia Antipolis, France (ETSI)