3GPP TSG CN Meeting #27 **NP-050090**
9th - 11th March 2005. Tokyo, Japan.

Title:	**Misalignment amongst the 3GPP specifications, "Re-authentication and key set change during inter-system handover"**
Source:	**CN1**
Agenda item:	**5**
Document for:	**INFORMATION**

3GPP TSG-CN1 Meeting #37 Tdoc N1-050270
Sydney, Australia, 14-18 February 2005

Title:	Misalignment amongst the 3GPP specifications, "Re-authentication and key set change during inter-system handover"
Response to:	R2-042611
Work Item:	TEI-5
Source:	CN1
To:	SA
Cc:	SA3, CN, RAN, RAN3, RAN2

Contact Person:
Name: Rouzbeh Farhoumand
Tel. Number: +1 469 682 9924
E-mail Address: rouzbeh.farhoumand@ericsson.com

Attachments: None

---

1. Overall Description:

A year ago, at CN1#33 meeting in February 2004, a misalignment amongst the 3GPP specifications on handling of key sets from R99 between the terminal and the network was identified. At that meeting, CN1 concluded that the inter-system handover from GERAN to UMTS procedures after re-authentication (i.e. 'late AKA') would always fail, if the handover occurred before the new keys were taken into use. Since CN1 was of the opinion that a re-authentication in the CS domain may be a rare event in R99 and also to avoid creating problems for the existing R99 mobiles, corrections in Rel-5 and onwards were judged to be sufficient.

The misalignment among 3GPP specifications leads to undesirable effects and call drops in the CS domain, because ciphering and/or integrity protection fails. In that end, CN1 informed all affected Working Groups via LS in N1-040501 to verify CN1's understanding and if so, align their respective specifications accordingly.

CN1 has approved Rel-5/6 CRs in NP-040099 and N1-040498 in CN1#33, and further in N1-041074, N1-041075 in CN1#34.

SA3 informed CN1 in N1-041319 (S3-040436) that SA3 shared the understanding of CN1 in regards to the inconsistency on key set use after intersystem handover if AKA was run prior to intersystem handover, and aligned TS 33.102 accordingly.

RAN3 informed CN1 in N1-041321 (R3-040944) that CN1's understanding was correct that the MSC can provide only one key set to the RNC with the RANAP Relocation Request message. The key set provided in the message will be used by RNC after the handover.

After exchange of a few more LSes between CN1 and RAN2 (N1-041322, N1-041519), RAN2 finally informed CN1#37 in N1-042013 (R2-042611) that RAN2 will not align their TS 25.331 with approved stage 2 and stage 3 in other Working Groups. In this LS RAN2 states:

"To introduce this change now would lead to many UEs which are using the current version of the specifications to suffer more problems whenever the proposed behaviour will occur. It is also noted that because the situation raised does not exist in current network deployments, the impact of not accepting this change will be minimal."

CN1#37's understanding and response to RAN2's conclusions are:

1. RAN2 does acknowledge that the problem exists, but yet is not willing to change their specification in Rel-5 and onwards.
2. In CN1's view, the statement about *"pre-Rel-5 UEs suffering more problems when the proposed behaviours occur"* is incorrect. Those UEs would continue behaving as today, i.e. drop the call if late AKA happens before the handover.

There is at least one MSC implementation that would perform late AKA. The reason for the situation not to exist in the current deployments at this time is that the function can be switched off by the operator to avoid 'late AKA', in order not to cause troubles with existing R99 mobiles after handover. But this is at the cost of reduced security in the system and as such, for Rel-5/6 this 'security hole' must be closed. As an example, in GSM it is possible that MSC omits authentication for a specific access, because subscriber was authenticated in a previous access. When MSC then starts ciphering and algorithms supported in MSC and MS does not match, BSC then may choose 'no encryption' for the connection (GSM TS 12.03, chapter 4.3.1). In this case, MSC should do a 'late authentication' after it realizes that the connection will be unencrypted (GSM TS 12.03, chapter 6.2.1).

If an operator chooses to enable the feature in Rel-5, the system would fail. The result would be increased call drops, decreased revenue for operators and a bad user perception.

At this junction, CN1 would like to bring the issue to the attention of the SA plenary and to seek guidance.

2. Actions:

To SA group.

ACTION: CN1 kindly requests SA to provide a way forward on this issue. Either RAN2 shall align their specification with SA3 and CN1 from Rel-5 onwards, or CRs must be produced to revert the already plenary approved CRs by SA3 and CN1, and accepting the flaw in the system that the inter-system handover from GERAN to UMTS procedures after re-authentication would always fail, if the handover occurred before the new keys were taken into use.

3. Date of Next TSG-CN1 Meetings:

CT1_38	25th -29th April 2005	Cancun, Mexico