3GPP TSG SA WG3 Security — S3#34 **S3-040462**
06 - 09 July 2004
Alcapulco, Mexico

3GPP TSG-RAN WG2 Meeting#42 **R2-041261**
Montreal, Canada, 10-14 May 2004

Title: Response LS (to N1-040501) on Re-authentication and key set change during inter-system handover

Release: Release 5

Work Item: ---

Source: RAN WG2

To: CN1, SA3, RAN3

Cc: GERAN2

Contact Person:

Name: Toby Proctor
Tel. Number: +44 1794 833226
E-mail Address: toby.proctor@roke.co.uk

1. Response:

RAN2 thanks CN1 for their LS (N1-040501) and would like to respond to the two points within.

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

RAN2 discussed a draft CR which corrects 25.331 to the requested (original) behaviour. However, before the CR could be agree the following points were noted:

Since the RAN 2 meeting #37 where CR1991 was agreed some UE manufacturers have already implemented CR 1991, and hence the problem of legacy UEs must be considered. In this case, a UE which has implemented CR1991 and operates in a network in which the behaviour has been corrected, where the UE has completed the ciphering procedures but not activated the new keys in the old RAT will activate the new keys immediately upon entering the cell while the network will operate according to the CN1/SA3 understanding of the behaviour (using the old keys). This will lead to a mismatch in the keys used between RAN and UE.

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?

It is also noted that if RAN2 agree to the proposal from CN1, then for this issue the legacy UE problem will become less common due to the tendency of users to upgrade handsets, and if RAN2 leave the behaviour as currently specified then this problem will be a permanent “feature” of the UTRAN.

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

RAN2 confirm that this is the case, however in 25.331 it is noted that in the case ciphering was not already ongoing in the previous RAT then the first SECURITY MODE CONTROL procedure in the UTRAN will be the one triggered by the CN.

2. New issue:

Other concerns have been raised in RAN2 regarding security procedure **within UTRA**. Our understanding is that regardless of the answer to question 1, in normal operation, there is the case that the UE and MSC have new keys but they are not activated due to an unexpected signalling connection release.

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.)

Also, section 6.4.1 of 33.102 contains the following text

> *"If an authentication procedure is performed during a connection (PS or CS mode), the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the ME as part of the security mode set-up procedure (see 6.4.5) that follows the authentication procedure."*

Could SA3 clarify what the intention of their specification is, especially with respect to the following scenario?

If new keys are received during a RRC connection but they are not activated during a signalling connection and a second security mode command is received for a following signalling connection to the same domain (and same RRC connection) are those keys to be activated or not with the second security mode command?

2. Actions:

To CN1, RAN3 and SA3.

ACTION: RAN2 kindly asks CN1, RAN3 and SA3 to reply to the following questions where the answers lie within their domain of expertise:

1) 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?

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.)

3) Could SA3 clarify what the intention of their specification is, especially with respect to the scenario described above?

3. Date of Next RAN2 Meetings:

3GPPRAN2-Release 6	AH	21 - 24 Jun 2004	Cannes	FR
3GPPRAN2#43	WG	16 - 20 Aug 2004	Prague	CZ
3GPPRAN2#44	WG	4 - 8 Oct 2004	Sophia Antipolis	FR