3GPP TSG SA WG3 Security — S3#18 **S3-010153**

21 - 24 May, 2001

Phoenix, USA

TSG-RAN Working Group 2 (Radio L2 and Radio L3) ***R2-010981***
Hayama, Japan, 9 - 13 April 2001

Source: TSG-RAN WG2

To: **TSG-SA WG3, TSG-CN WG1**

Cc: **TSG-T WG3**

Title: **LS on THRESHOLD check at RRC connection establishment**

Contact: Ainkaran Krishnarajah, Ericsson
Email: Ainkaran.Krishnarajah@era.ericsson.se

TSG RAN WG2 would like to ask TSG SA WG3 to clarify the procedure for checking THRESHOLD and the deletion of keys if these are considered to be too old.

Referring to TS 33.102 v3.7.0, Section 6.4.3:

[…]

1.1.1 6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement which generates cipher/integrity keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time an RRC connection is released the values $START_{CS}$ and $START_{PS}$ of the bearers that were protected in that RRC connection are stored in the USIM. When the next RRC connection is established ~~that~~ those values are read from the USIM. The ME shall trigger the generation of a new access link key set (a cipher key and an integrity key), if $START_{CS}$ **or** $START_{PS}$ has reached a maximum value, ~~set by the operator and stored in the USIM~~ at the next RRC connection request message sent out. The maximum value is set by the operator and stored in the USIM When this maximum value is reached the cipher key and integrity key stored on USIM shall be deleted.

This mechanism will ensure that a cipher/integrity key set cannot be reused beyond the limit set by the operator.

[…]

It is unclear for TSG RAN WG2 that the checks to see if $START_{CS}$ or $START_{PS}$ have reached the maximum value (i.e. THRESHOLD) is done at RRC connection establishment or RRC connection release.

It would appear from the text in 6.4.3 that the check is performed at the RRC connection establishment phase. Assuming this, if the START stored in the USIM for *any* CN domain is greater than THRESHOLD then the keys are deleted for *both* CN domains.

TSG RAN WG2 would like to ask if this is the case or if the deletion of keys is really only necessary for the CN domain for which START is greater than THRESHOLD? If so, then this needs to be clarified in 33.102.

It is stated in 6.4.3 that when the maximum value is reached (and possible passed), then the keys stored in the USIM are deleted. This deletion should be reported to upper layer, in order to set the KSI to invalid. Although not the experts on NAS, it is the understanding that the initial NAS message that contains the Key Set Identifier (KSI) is prepared by NAS before NAS requests RRC for connection establishment. Perhaps TSG CN WG1 could confirm this procedure (refer to Figure 14 in TS 33.102 v3.7.0).

If this is correct then the following case exists, as shown in steps (i) – (vii):

i) During an ongoing RRC connection the START for a CN domain eventually passes the THRESHOLD value.

ii) The RRC connection is then naturally released and the calculated START value for each CN domain is stored in the USIM.

iii) Another RRC connection is established. The START for each CN domain read from the USIM (the START values in the USIM is then set to THRESHOLD, thereby being marked as invalid) is checked and found that the THRESHOLD value has been reached. The keys are deleted in the USIM.

iv) The RRC connection is established but this will use the old keys again, as the KSI only becomes invalid at the next RRC connection.
v) The RRC connection is released and the calculated START value for each CN domain is stored in the USIM.
vi) Another RRC connection is established. The keys are deleted in the USIM and so KSI is marked as invalid. The START for each CN domain is checked and found that the THRESHOLD value has been reached.
vii) The RRC connection is established and the ME will trigger the authentication procedure.
NOTE: The core network in this scenario has not initiated Authentication

If the assumptions above are correct then the use of the THRESHOLD is not serving its purpose and the old keys have been used in two different RRC connections.
In that case, TSG RAN WG2 would like to suggest that the THRESHOLD check and invalidation of keys be made at RRC connection release.
i) During an ongoing RRC connection the START for a CN domain eventually passes the THRESHOLD value.
ii) The RRC connection is released and the calculated START value for each CN domain is compared with THRESHOLD. If THRESHOLD has been reached or passed then:
- the keys are deleted in the USIM
- an indication of deletion of keys is informed to higher layers by RRC, and
- the calculated START value for each CN domain is stored in the USIM.
iii) Another RRC connection is established. The keys are deleted in the USIM and the KSI is already set as invalid. The START for each CN domain is read from the USIM (the START values in the USIM is then set to THRESHOLD) and is checked and found to have reached the THRESHOLD value.
iv) An authentication procedure is triggered and new keys are received.

TSG RAN WG2 sees that the second scenario ensures that the old keys are not used for too long and would suggest to TSG SA WG3 to update TS 33.102 if TSG RAN WG2s assumptions are correct. Also, minor editorial comments have been made to Section 6.4.3 above.