3GPP TSG SA WG3 Security — S3#11 **S3-000157**

22-24 February, 2000

Mainz, Germany

From: **S3**

To: **R2**

Title: **Draft Reply to the LS R2-000282**

In their LS R2-000282 (= S3-000102) the RAN2 group asked S3 to consider the security issues related to the proposed UTRAN procedure which checks whether a new cipher key is correct and in the case of the negative result the old key is reverted to the use.

More specifically, the following questions were asked:

- 1) Does the scenario that is described in the attached document exist?
- 2) If the answer is yes, is it addressed by higher layers?
- 3) If the answer is no to the second question, does the proposed solution solve it?

S3 answers as follows:

1) The key generation is always coupled with the full mutual authentication of the user and the network. This means, in particular, that if a wrong cipher key appears in the UE because of transmission error on the radio interface, there is a very high probability that the authentication fails totally. This is implied by the fact that the random challenge is always associated to a message authentication code inside the authentication token AUTN. This message authentication code is calculated in both the USIM and the 3G-AuC based on the secret master key K of the subscriber.

Also, the coupling with authentication protects against wrong cipher keys because of computation errors in either USIM or in 3G-AuC.

S3 sees two additional reasons why a wrong cipher key may appear in either UE or in the RNC: a transmission error between USIM and the UE in the first case and a transmission error on Iu interface in the latter case.

S3 is not in the place to estimate the probability of these errors but the following comments can be made:

- If an erronous message gets through the Iu i/f then it is likely that there are many bit errors in this. This would imply typically that either also the integrity key would be erroneous or the whole message is rejected. If the integrity key is erroneous the S3 already has developed some measures to recover from this situation.
- Also, for the case of the USIM-UE i/f it seems likely that the transferred integrity key is erroneous if the cipher key is.

2) As indicated in theprvious answer the scenario exists to some degree. Also, there are countermeasures built in the higher layers. These are implemented via the coupling to authentication and integrity protection mechanisms.

3) The answer to (2) is yes.

S3 wants to add that there are security issues related to reverting to an older key. The mechanisms of mutual authentication and integrity protection are primarily developed in

order to prevent false elements (e.g. false BTS or false MS) to appear in the network. It is typically in the interest of such false elements to use old keys as long as possible. This gives them an advantage in the case some keys are compromised.