3GPP TSG SA WG3 Security — S3#17 **S3-010053**

27 February – 2 March, 2001

Gothenburg, Sweden

Title: **UE-triggered re-authentication during connections**

Source: **Vodafone**

Agenda: **8.2**

For: **Decision**

The 3GPP R99 specifications currently contain a mechanism to allow the operator to set a CK/IK lifetime threshold on the USIM whereby a re-authentication is triggered by the MS at the start of a connection if the threshold was exceeded at the end of the previous connection. In REL-4 it has been proposed to extend this to allow a re-authentication to be triggered by the MS if the threshold is exceeded *during* a connection.

The CK/IK lifetime control is an attempt to reduce the level of trust that a user and home environment needs to place in a serving network to implement an appropriate authentication policy by allowing the USIM/UE to trigger authentication once a certain key lifetime has been exceeded. For operators who choose to implement this feature the threshold value must be selected based on the following criteria:

- the threshold should be low so that it is effective in forcing an authentication when a serving network does not implement the stated policy in the roaming agreement

- the threshold should be high so that roamers are not denied service when the serving network cannot obtain fresh vectors (e.g. because the link to the HLR fails)

Although the basic R99 mechanism makes use of existing signalling procedures, the proposed REL-4 enhancement will require additional signalling and hence additional complexity in the terminal and in the network. Furthermore, while the support of the R99 mechanism was optional in the USIM, the REL-4 mechanism relies on the feature being supported in all terminals and all networks. In addition, SA3 have not yet started to define the exact requirements on the new signalling procedures that would have to be developed. In particular, a number of open issues have yet to be resolved:

1. Synch/MAC failures

   If the UE asks for a re-authentication during a connection, and the network obliges, but then the new authentication procedure fails for some reason, what should the behaviour be now?

2. THRESHOLD value on USIM is set by operators

   What is to prevent a network operator setting a very low threshold value and thus trigger several re-authentications per connection?

3. Authentication not performed

   What should the behaviour of the MS be if the threshold value is passed and the UE asks the network to re-authenticate it, but the network does not? Should the connection be dropped? Should the terminal behave as if network authentication had failed?

4. New keys not applied

   What would be the behaviour of the UE if the network did re-authenticate it, but never sent the SECURITY MODE COMMAND message, and therefore the new keys are never 'activated'?

Because of the above reasons, it is recommended that this feature is not included in the REL-4 specifications. In addition SA3 are asked to consider whether this feature should be considered for inclusion in the REL-5 specifications.