3GPP TSG SA WG3 Security — S3#10 **S3-000075**

19-21 January, 2000

Antwerpen, Belgium

TSG-SA WG3 (Security) meeting #9 ***TSGS-WG3#9(99)550***

Helsinki, 7-9 December, 1999

From: **S3**

To: **N1, R2, T3**

Title: **USIM triggered authentication and key setting during PS connections**

3G TS 33.102 v3.2.0 section 6.4.3 specifies a mechanism which allows the USIM to trigger authentication at the start of an RRC connection if a counter on the UE exceeds an operator controlled threshold set by the USIM. It is proposed to extend this so that authentication can be triggered by the UE on a value provided by the USIM during a PS connection. Note that section 6.4. in 33.102 v3.2.0 already specifies that the network should be able to initiate authentication and key setting during a PS connection. See also the S3-approved CR to this section in S3-99552 (attached).

USIM triggered authentication and key setting during a connection may be useful in the PS mode where long connections lasting several days might be expected. One of the objectives for 3G security is to minimise the amount of trust that needs to be placed in the serving network. USIM triggered authentication during a PS connection can help to minimise the trust that the home environment needs to place in the serving network to implement an appropriate re-authentication policy for long PS connections.

In order to provide this capability three things are necessary:

- It shall be possible that the security mode negotiation can be run during a PS connection and that the new keys are taken into use immediately. Note that this is also required for network-originated re-authentication during a PS connection. R2 are asked to confirm that this can be done.
- It shall be possible for the USIM to transfer the operator-controlled threshold value to the UE at the start of an RRC connection and for the UE to monitor whether the current HFN exceeds the threshold at the start of a CS mode connection or during a PS mode connection. T3 are asked to confirm that appropriate functionality can be provided in the UE and the USIM.
- It shall be possible for the UE to indicate to the MSC/SGSN during a connection that the-authentication and key setting procedure should be run. This could be done, for example, by including KSI as part of an existing or new Layer 3 signalling message (KSI would be set to all 1s to indicate that no valid key set is available for use). N1 are asked to confirm that such and indication can be made to the network during a connection.

USIM and network initiated authentication and key setting during a CS connection is for further study.