3GPP TSG SA WG3 Security — S3#11 **S3-000124**

22-24 February, 2000

Mainz, Germany

Source: **Vodafone**

Title: **UE triggered authentication and key agreement during connections**

For: **Decision**

It is for discussion whether UE triggered authentication and key agreement during connections is achievable in R99. A draft LS and two CRs are attached.

From: **TSG SA WG3**

To: **TSG CN WG1**

Copy: **TSG RAN WG2, TSG T WG3**

Title: **Proposed LS on UE triggered authentication and key agreement during connections**

3G TS 33.102 v3.3.1 section 6.4.3 specifies a mechanism to allow the UE to force the authentication and key agreement procedure to be run at the start of an RRC connection if the value of the hyperframe number at the end of the previous RRC connection exceeds a maximum value. This mechanism is used to control the lifetime of the cipher and integrity keys, CK and IK. The value of the hyperframe number at the end of the previous RRC connection and its maximum permitted value are both stored on the USIM. It is intended to correct a potential weakness in this mechanism so that the authentication and key agreement procedure can be triggered by the UE during a connection if the maximum permitted hyperframe counter value is reached. It is felt that due to timescales, it may not be feasible to introduce this feature in R99. If this is the case then it should be introduced in R00.

UE triggered authentication and key agreement during a connection may be useful if long connections are expected. One of the objectives of 3G security is to minimise the amount of trust that needs to be placed in the serving network. UE triggered authentication based on a maximum permitted hyperframe number set in the USIM 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 connections. This feature is likely to be of most value in the PS domain where long connections are more likely.

In order to implement this feature, it is required that the UE is able to indicate to the core network during a connection that the authentication and key agreement procedure should be run. N1 are asked to ensure that this functionality is implemented in their specifications.

Attached: S3-000xxx (CR on key setting) and S3-000xxx (CR on key lifetime).

Contact person: Peter Howard
Email: peter.howard@vf.vodafone.co.uk
Tel: +44 1635 676206