3GPP TSG SA WG3 Security — S3#15 **S3-000507**

12-14 September, 2000

Washington D.C., USA

3GPP TSG T3 #15 ***Tdoc T3-000406***
San Diego, USA, 16–18 August 2000

Liaison Statement

From: **T3** (Contact: Stefan Kaliner, stefan.kaliner@t-mobil.de)

To: **S3**

Subject: **Limitation of Lifetime of Keys CK and IK**

TS 33.102 specifies a mechanism to limit the lifetime of the keys CK and IK, which imposes particular requirements on the USIM: "The USIM shall send CK / IK under the condition that 1) a valid CK / IK is available, 2) the current value of START in the USIM is "up-to-date" and 3) START has not reached THRESHOLD" (see TS 33.102, sections 6.5.4.2 and 6.6.4.2).

Regarding these requirements, T3 would like to raise the following comments:

1. The meaning of the term "up-to-date" is unclear. How could this be checked by the USIM?

2. The required mechanism is currently not supported in TS 31.102. To change that, a new USIM command would be necessary to check the validity of the START values and reply either with the keys, if these have not reached THRESHOLD, or with a dedicated response, if THRESHOLD is reached. However, a new USIM command should only be introduced, if it is indispensable.

T3 would like to recommend that the checking of the START values is done in the ME rather than in the USIM. In the beginning of a session the ME should read the value of THRESHOLD from the USIM and store it. When a connection is established, the ME should read the current value of $START_{CS}$ or $START_{PS}$ from the USIM and compare it to the stored value of THRESHOLD. If this is reached, the ME should trigger a new authentication and reset the START values in the USIM to zero.

This alternative procedure transfers the checking operation from the USIM to the ME. Compared to the procedure assumed by S3, this is certainly not less secure, since the USIM does not have control over the START values (as these are delivered by the ME) anyway. Furthermore, it is in line with many similar procedures, where the USIM serves as a storage entity for data and the related evaluations are done by the ME. No additional functions are needed for the USIM to support the proposed procedure.

S3 are kindly invited to consider these arguments and eventually modify their specifications.