3GPP TSG SA WG3 Security — S3#18 **S3-010163**

21 - 24 May, 2001

Phoenix, USA

3GPP T3 (USIM) Meeting #19
St. John, US VI, 8 – 11 May, 2001

Tdoc T3-010379

Liaison Statement

From: **T3**

To: **SA, SA1, SA3, T, T2, CN1**

Cc: **CN**

Subject: **Rejection of 2G Authentication and Key Agreement by 3G ME with USIM in UTRAN**

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

During the work on TR 31.900 – SIM/USIM Internal and External Interworking Aspects, T3 have identified the following issue.

There is a requirement in 3G TS 33.102, section 6.8.1.4, that a "*R99+ ME with a USIM inserted and attached to a UTRAN shall only participate in UMTS AKA and shall not participate in GSM AKA*." In other words: A 3G ME with a UICC (which always contains a USIM) shall not perform 2G authentication and key agreement (AKA) in a 3G network (UTRAN).

The ME is the only entity that knows all of the implied conditions,

a) UICC (with USIM) inserted,
b) UTRAN accessed,
c) 2G authentication parameter (RAND only) received,

and by adhering to the above requirement it should reject the authentication request in this case. This means that no service (except for emergency calls) can be obtained by the user.

Now, network operators who are seeking a smooth migration path to 3G may deploy 3G UICCs much earlier than the actual UMTS network launch, i.e. before there are 3G HLR/AuCs in place. This is to minimise the number of card replacements that may come up after official introduction of UMTS services. The UICCs would comprise a SIM and a USIM application with shared identity, i.e. shared IMSI and shared secret key, while the subscriptions would have to go into a 2G HLR which certainly can only perform 2G AKA.

This scenario is fully compliant to the standards, however a user who would insert this UICC into a 3G ME and access a 3G network, would be denied service as the above requirement is followed. There are important consequences:

1) If a network operator issues UICCs in order to enable his users to use a 3G access network (at home or while roaming), the related subscriptions should be installed in a 3G HLR/AuC. Otherwise authentication will fail, since a 3G ME should not participate in 2G AKA. This can easily be satisfied by the operator in his HPLMN, as the 3G access network can only be activated after the HLRs have been migrated to 3G, but is completely out of control when his users are roaming onto other 3G networks. Hence, service problems cannot be excluded.

2) The reaction of the ME – apart from not responding to the authentication request – is, as yet, unclear. Will the user be notified? Is there any possible strategy, e.g. to try an available 2G network instead? Is there a risk for repeated access attempts? What would be the reaction of the network? It should further be noted that this is the first time that an important part of network security is entirely dependant on the ME.

3) Currently there is no means to generally prevent the ME in such a situation from accessing 3G networks in order to save the user from disappointing display messages and the 3G networks from unwanted signalling load.

T3 are already looking at point 3) from the USIM perspective, but would like to make the addressed groups aware of this issue and its potential ramifications, which have been discovered only recently.