3GPP TSG SA WG3 Security — S3#18 **S3-010230**

21 - 24 May, 2001

Phoenix, USA

Title: **Reply LS on the handling of retransmitted authentication requests**

Source: **SA3**

To: **CN1**

Reference LS: **N1-010480 (enclosed)**

Contact:

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

In response to a recent LS from CN1, SA3 would like to report that CR140 on 33.102 was agreed at S3#17 (27 Feburary – 1 March) and was approved at SA#11. This CR implemented the changes to the handling of retransmitted authentication requests proposed by CN1 in a recent LS (N1-010480 enclosed).

An extract from the latest version of 33.102 (v3.8.0) is included below for information.

6.3.3 Authentication and key agreement

[…]

Re-use and re-transmission of (RAND, AUTN)

The verification of the SQN by the USIM will cause the MS to reject an attempt by the VLR/SGSN to re-use a quintet to establish a particular UMTS security context more than once. In general therefore the VLR/SGSN shall use a quintet only once.

There is one exception however: in the event that the VLR/SGSN has sent out an *authentication request* using a particular quintet and does not receive a response message (*authentication response* or *authentication reject*) from the MS, it may re-transmit the *authentication request* using the same quintet. However, as soon as a response message arrives no further re-transmissions are allowed. If after the initial transmission or after a series of re-transmissions no response arrives, retransmissions may be abandoned. If retransmissions are abandoned then the VLR/SGSN shall delete the quintet. At the MS side, in order to allow this re-transmission without causing additional re-synchronisation procedures, the ME shall store for the PS domain (and optionally the CS domain) the last received RAND as well as the corresponding RES, CK and IK. If the USIM returned SRES and Kc (for GSM access), the ME shall store these values. When the ME receives an *authentication request* and discovers that a RAND is repeated, it shall re-transmit the response. The ME shall delete the stored values RAND, RES and SRES (if they exist) as soon as the 3G security mode command or the GSM cipher mode command is received by the ME or the connection is aborted. If the ME can handle the retransmission mechanism for CS domain then it shall be able to handle the retransmission for both PS and CS domain simultaneously.

3GPP TSG-CN-WG1, Meeting #16 ***Tdoc N1-010480***
26 February 2001 to 01 March 2001,
Sophia France.

Title: Re-transmission of authentication requests

Reference LS **---**
(If available)

Source: **[CN1]**

TO [1]: **SA3**

Cc: **---**

WI: **Security**

Contact Person:
Name: **Robert Zaus**
E-mail Address: **robert.zaus@icn.siemens.de**
Tel. Number: **+49 170 331 5485**

Attachments: **N1-010477**
(Please list documents numbers to be attached)

Date: **01 March 01**

During the last two meetings, CN1#15 and CN1#16, CN1 discussed the possibility to implement the CR 33.102-130 (S3-000725), “Re-transmission of authentication request using the same quintet”, in the R’99 version of TS 24.008.

- Some delegates stated that a SIM-based solution would be more appropriate. Some delegates were also concerned that an implementation of the feature as specified by SA3 would delay the availability of standard compliant UMTS R’99 terminals.

- Other delegates were concerned that if the feature was not supported, this would greatly reduce the efficiency and grade of service of the whole system, due to a higher number of synchronisation failures and higher consumption of security quintets.

- There was a consensus that the most critical procedure for which re-transmission was expected to occur with the highest probability is the UMTS Authentication procedure via the Gb interface.

[1] Please write any action required from the groups in a clear way.

As a compromise between the points of view expressed by different delegates, CN1 agreed the change request to TS 24.008 that is attached to this liaison statement for R'99, and an identical CR for Rel-4.

CN1 hope that the agreed solution is acceptable to SA3, and kindly ask SA3 to adapt their specification TS 33.102 accordingly.

The following MM and GMM state descriptions from TS 24.008 are provided in order to help SA3 with the interpretation of the attached CR:

4.1.2.1 MM sublayer states in the mobile station

....

4.1.2.1.1 Main states

0 NULL

The mobile station is inactive (e.g. power down). Important parameters are stored. Only manual action by the user may transfer the MM sublayer to another state.

....

19. MM IDLE

There is no MM procedure running and no RR connection exists except that a local MM context may exist when the RR sublayer is in Group Receive mode. This is a compound state, and the actual behaviour of the mobile station to Connection Management requests is determined by the actual substate as described hereafter.

....

4.1.3.1 GMM states in the MS

....

4.1.3.1.1 Main states

4.1.3.1.1.1 GMM-NULL

The GPRS capability is disabled in the MS. No GPRS mobility management function shall be performed in this state.

4.1.3.1.1.2 GMM-DEREGISTERED

The GPRS capability has been enabled in the MS, but no GMM context has been established. In this state, the MS may establish a GMM context by starting the GPRS attach or combined GPRS attach procedure.