3GPP TSG SA WG3 Security — S3#32 **S3-040028**
09 - 13 February 2004
Edinburgh, Scotland, UK

Title: **Draft Reply to S3-030672 on use of authentication re-attempt IE**

Work Items: UTRAN network access security

Source: 3GPP SA3
To: 3GPP CN4
Cc:

Contact Person:
Name: Colin Blanchard
Tel. Number: +44 1473 605353
E-mail Address: colin.blanchard@bt.com

Attachments: S3-010056

SA3 thanks CN4 for their analysis of the use of the 'Re-attempt' parameter in the Authentication Failure Report (AFR) Service.

The authentication re-attempt indicator is intended to be used by a Fraud Detection System (FDS) in the Home Network to help identify and manage potential fraud scenarios. More information can be found in S3-010056 attached. The indicator can be used on its own, or more usually conjunction with other information from the Authentication Failure Report and call records. It was SA3's intention that an authentication error that occurs outside the normal operation and allowed error conditions should be given the higher priority.

SA3's requirements on the operation of this feature are as follows:

The serving network performs the authentication re-attempt procedure and sets *Re-attempt* to "true" after a failed first authentication when and only when

- New Authentication Vectors are received from the HLR/AuC). (Send Authentication Info performed)

- An updated IMSI is required (User Identity Request performed)

Otherwise *Re-attempt* is set to "False"

Thus failures caused by a TMSI mismatch or an erroneous Authentication Vectors received from the previous serving MSC could be allocated a different priority in the FDS processing.

SA3 believe that this is inline with the following cases identified in the CN4 analysis.

- Authentication with (P-)TMSI failed in MS (reject cause 'MAC failure') and new authentication procedure (re-attempt) is taken because an IMSI obtained by the followed IDENTITY REQUEST procedure does not match to the original IMSI that linked with (P-)TMSI. See TS 24.008 section 4.3.2.6 c) **[Case 1]**

- Authentication failed in MS (reject cause 'synch failure') and new authentication procedure (re-attempt) is taken after MSC obtains new authentication vectors from HLR for re-synchronisation. See TS 24.008 section 4.3.2.6 c) **[Case 3]**

- SRES mismatches with (P-) TMSI in VLR (SGSN) and new authentication procedure (re-attempt) is taken because an IMSI obtained by the followed IDENTITY REQUEST procedure does not match to the original IMSI that linked with (P-)TMSI. See TS 23.012 section 4.1.2.2 Procedure Authenticate_VLR, and TS 23.018 section 7.1.2.6 Procedure Authenticate_VLR [**Case 4]**

The additional scenario **[Case 2]** identified by CN4, where the authentication failed in MS (reject cause 'GSM authentication unacceptable') and new authentication procedure (re-attempt) is taken after MSC obtains UMTS authentication vectors from HLR. See TS 24.008 section 4.3.2.6 c) should also set re-attempt to “true” as pointed out by CN4, as this is an allowed error condition when operating at a GSM/UMTS boarder.

Action on CN4:

To confirm that the SA3 requirement as described above can be implemented so that SA3 can update TS33.102 if necessary.

Date of Next SA3 Meetings:

S3#32 09-13 Feb 2004 Edinburgh	EF3
S3#33 11-14 May 2004 Beijing	Samsung
S3#34 06-09 July 2004 Chicago	"NA Friends of 3GPP"