3GPP TSG SA WG3 Security — S3#31 **S3-030672**
18 - 21 November 2003
Munich, Germany

3GPP TSG CN WG4 Meeting #21 ***N4-031152***
Bangkok, Thailand, 27th – 31st October 2003

Title:	**LS to SA3 on Clarification on use of Re-attempt Information element in Authentication Failure Report service**
Release:	**6**
Work Item:	**Security**
Source:	**NEC (TSG CN4)**
To:	**TSG SA3**
Cc:	

Contact Person:
Name: Toshiyuki Tamura
Tel. Number: +81-4-7185-7167
E-mail Address: tamurato@aj.jp.nec.com

Attachments: **None**

1. Overall Description:

It was discussed in CN4#21 meeting in Bangkok that the use of the 'Re-attempt' parameter in Authentication Failure Report Service is not clear in current specifications how it could be used. Therefore, TSG CN4 kindly ask TSG SA3 to provide guidance on this question.

2. Background

The 'Re-attempt' parameter was introduced as the REL4 feature about 2 years ago. This parameter is used in Authentication Failure Report Service in order to indicate whether the failure occurred in a normal authentication attempt or in an authentication reattempt (there was a previous unsuccessful authentication). However, it is not clear for NEC what is the “normal authentication attempt” meant and what is the “an authentication reattempt” meant.

The 'Re-attempt' IE is currently defined in TS 29.002 is as follows.

> === Quotation from TS 29.002 ===
> 7.6.7.10 Re-attempt
> It indicates whether the failure occurred in a normal authentication attempt or in an authentication reattempt (there was a previous unsuccessful authentication).
> === Quotation end ===

Additionally, the related description in TS 33.102 is as follows.

> === Quotation from TS 33.102 ===
> 6.3.6 Reporting authentication failures from the SGSN/VLR to the HLR
>
> The purpose of this procedure is to provide a mechanism for reporting authentication failures from the serving environment back to the home environment.
> The procedure is shown in Figure 13.

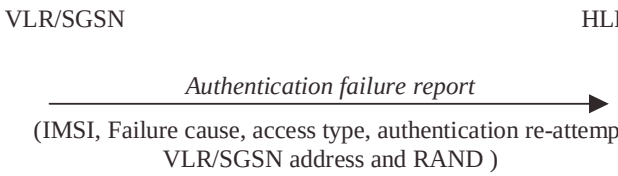

Figure 13: Reporting authentication failure from VLR/SGSN to HLR

The procedure is invoked by the serving network VLR/SGSN when the authentication procedure fails. The authentication failure report shall contain:

1. Subscriber identity;
2. Failure cause code. The possible failure causes are either that the network signature was wrong or that the user response was wrong;
3. Access type. This indicates the type of access that initiated the authentication procedure;
4. Authentication re-attempt. This indicates whether the failure was produced in a normal authentication attempt or it was due to an authentication reattempt (there was a previous unsuccessful authentication);
5. VLR/SGSN address;
6. RAND. This number uniquely identifies the specific AV that failed authentication.

The HE may decide to cancel the location of the user after receiving an authentication failure report and may store the received data so that further processing to detect possible fraud situations could be performed.
=== Quotation end ===

3. Discussion

Based on our analysis, the follows 4 cases could be a case where the 'Re-attempt' is set.

1) 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)

2) Authentication failed in MS (reject cause 'GSM authentication unacceptable') and new authentication procedure (re-attampt) is taken after MSC obtains UMTS authentication vectors from HLR. See TS 24.008 section 4.3.2.6 c)

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

4) 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

For 2) case, this is not a failure case since it may happen as the normal procedure especially along the GSM/UMTS broader. Therefore, CN4 consider that **the 'Re-attempt' parameter is set in the Authentication Failure Report Request message if the second authentication procedure is failed after the case 1), 3) or 4) procedure executed.**

4. Actions

To SA3 group.

ACTION: CN4 would like to ask following 2 questions in order for CN4 to put more clarity in TS 29.002 on use of ‘Re-attempt’ parameter. Moreover, if SA3 would conclude that TS 33.102 is also relevant to be put more clarity on use of ‘Re-attempt’ parameter, please update TS 33.102 and inform to CN4 so that CN4 could make an alignment with an update of TS 33.102.

Question 1: What is the purpose of the ‘Re-attempt’ parameter to be included in Authentication Failure Report Service? Particularly, how the HLR utilize this information.

Question 2: What is a situation where ‘Re-attempt’ parameter is set in VLR and SGSN.

5. Date of Next CN4 Meeting

CN4 #22 16th February – 20th February 2004, Atlanta, USA