TSG-SA WG3 (Security) meeting #16 **_S3-000675_**
Sophia Antipolis, France, 28th – 30th November 2000

Agenda Item: 10.1

Source: Ericsson

Title: Additional Parameters in Authentication Failure Report Procedure

Document for: Discussion and Decision

1 Introduction

1.1 Authentication Failure Report

In the main body of the TS 33.102 v3.5.0 (chapter 6.3.6) it is described a procedure, invoked by the serving network VLR/SGSN when the authentication procedure fails, to inform the Home Environment (HE) about that failure.

This *authentication failure report* (AFR) message contains the subscriber identity and a failure cause code, being the possible failure causes either that the network signature was wrong or that the user response was wrong (synchronisation failures are reported by a different procedure). Then, the HE may decide to cancel the location of the user after receiving an *authentication failure report*.

1.2 Fraud Detection System

Mobile network Operators might use an element called FDS (Fraud Detection System) that, by means of indicators, analyses the existence of fraud.

The mentioned indicators can be classified as:

- **Primary indicators.** Those indicators that, in principle, can be employed in isolation to detect fraud.
  Example: Number of call forwarding within a defined time interval.
- **Secondary indicators**. Those indicators from which, in principle, useful information can be gained if they are considered in isolation, but which should not be used to detect fraud.
  Example: Classification by cell site(s) or switch area(s). Call selling for certain destinations are concentrated in areas where the buyers live.
- **Tertiary indicators.** Those indicators from which no useful information can be gained if they are considered in isolation, but which can, in principle, be used to provide essential information in connection with the detection of fraud.
  Example: Number of successful handovers within a defined time interval. Fraudsters need to have a stable position to initiate call selling services so mobiles with a low mobility indicate possible fraudulent activities. Obviously, many mobiles may have this low mobility behaviour so further investigations are needed.

2 Enhanced procedure

2.1 Current Situation

In one hand, the data sent currently in the Authentication Failure Report procedure, as described in TS 33.102, cannot be used by the HLR to take any decision since this node doesn't have the functionality to perform an evaluation of possible fraud. But not even and FDS could use those data since they don't fit with any of the indicators used by an FDS (described in chapter 1.2).

On the other hand, there are some data related with unsuccessful authentication that can be considered as secondary indicators and that are not sent to the FDS. Those data and its foreseen utility from a fraud-detection point of view are described following:

- **Access type.** – In order to distinguish if the authentication procedure was initiated due to a call, an emergency call, a location updating, a supplementary service procedure or a short message transfer. This parameter can be used to evaluate the seriousness of the failure since it can be considered more serious a failure produced in a location updating than in a call set up, and this one more serious than one produced in a short message transfer. These considerations are based in some facts; e.g. a successful location updating has to be performed formerly to an unsuccessful call attempt.
- **Authentication reattempt.** – It 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). An authentication reattempt is performed in current networks since the failure could be provoked by a TMSI mismatch or by erroneous Authentication Vectors received from the previous MSC server (the re-attempt is performed after requesting new Authentication Vectors to the HLR). When the authentication reattempt is performed, this is done with the correct IMSI (User Identity Request performed) and with correct Authentication Vectors (Send Authentication Info performed), thus an error in this case is of higher importance.
- **VLR/SGSN address.** – This data shall be included in order to have a reference of the physical location where the failure has been produced. The usefulness of this data from a fraud-detection point of view resides on the fact that some frauds (mainly call selling) in current mobile network are associated to concrete geographical location.

  The VLR/SGSN performing the authentication handles all these data but, since they are not included in any CDR (Call Data Record) and this is the way to send indicators towards the FDS, they are not received by the FDS. Moreover a manual gathering is quite complex since the VLR/SGSN and the subscription can be from different operators.

2.2 Enhancement for fraud detection

The VLR/SGSN shall include the three mentioned data in the AFR message so that the HE would gather that fraud information. Once the data are stored in the HE, it should be possible to send this information towards a FDS either in a manual or automatic way (this is out of he scope of this contribution).

3 Conclusions

The chapter 6.3.6 in TS 33.102 v3.6.0 should be updated so that the following data are included in the message *authentication failure report*:

- Access type.
- Authentication re-attempt.
- VLR/SGSN address.

A short description of the parameter should be included as well, stating that the HE should store this data so that later on can be send to an FDS for processing.

The attached CR proposes how this could be reflected in the specification. Mind that the addition of these parameters into AFR procedure is being proposed for R4 and not for R99 (R99 functionality should be frozen at this stage).

3GPP TSG-SA WG 3 (Security) meeting #16 **Document *S3-000675***
Sophia Antipolis, France, 28th-30th November 2000

3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102	**CR**		Current Version: 3.6.0
3G specification number ↑		*↑ CR number as allocated by 3G support team*	

For submision to TSG SA#10 — for approval ☒ — for information □ *(only one box should be marked with an X)*
List TSG meeting no. here ↑

Form: 3G CR cover sheet, version 1.0 The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf

Proposed change affects: USIM □ ME □ UTRAN □ Core Network ☒
(at least one should be marked with an X)

Source:	Ericsson	**Date:**	2000-11-27
Subject:	Additional Parameters in Authentication Failure Report		
3G Work item:	Security		

Category:
(only one category shall be marked with an X)

F	Correction	□	**Release:**	Phase 2	
A	Corresponds to a correction in a 2G specification	□		Release 96	
B	Addition of feature	□		Release 97	
C	Functional modification of feature	☒		Release 98	
D	Editorial modification	□		Release 99	
		□		Release 00	X

Reason for change:

The data sent currently in the Authentication Failure Report (AFR) procedure, as described in TS 33.102, cannot be used by the HE to take any decision.
There are some data related with unsuccessful authentication (access type, authentication-reattempt and VLR/SGSN address) that can be considered as secondary indicators for fraud detection and that doesn't reach the FDS with current implementation.
The AFR procedure can be enhanced by including these data in the message so that the HE would gather this information for fraud detection (then, they could be sent towards a FDS either in an automatic or manual way).

Clauses affected: 6.3.6

Other specs affected:

Other 3G core specifications	□	→ List of CRs:
Other 2G core specifications	□	→ List of CRs:
MS test specifications	□	→ List of CRs:
BSS test specifications	□	→ List of CRs:
O&M specifications	□	→ List of CRs:

Other comments: This CR shall apply to the correspoding R4 version of 33.102 (i.e. v4.0.0).

help.doc

<--------- double-click here for help and instructions on how to create a CR.

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.

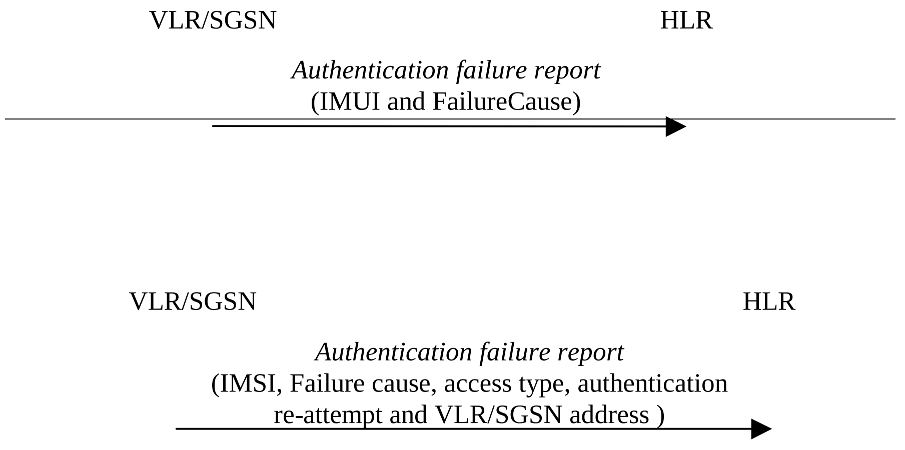
VLR/SGSN
HLR
Authentication failure report
(IMUI and FailureCause)
VLR/SGSN
HLR
Authentication failure report
(IMSI, Failure cause, access type, authentication
re-attempt and VLR/SGSN address)

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. -T~~t~~he subscriber identity.~~ and~~

2. A~~a~~ failure cause code. The possible failure causes are either that the network signature was wrong or that the user response was wrong.

3. The access type. It indicates if the authentication procedure was initiated due to a call set up, an emergency call, a location updating, a supplementary service procedure or a short message transfer.

4. Authentication re-attempt. It 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.

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