3GPP TSG-SA WG3 Meeting #17 ***S3-010056***
Göteborg, Sweden, 27 February-2 March 2001

CR-Form-v3

CHANGE REQUEST

⌘ **33.102** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **3.7.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Additional Parameters in Authentication Failure Report
Source:	⌘	Ericsson
Work item code:	⌘	Security Architecture
Date:	⌘	27-Feb-01
Category:	⌘	**C**
Release:	⌘	Rel-4

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	Provide additional information to HE to detect fraud conditions.
Summary of 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. Including these data in the message so that the HE would gather this information for fraud detection can enhance the AFR procedure (then, they could be sent towards a FDS either in an automatic or manual way).
Consequences if not approved:	⌘	

Clauses affected:	⌘	6.3.6
Other specs Affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

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.

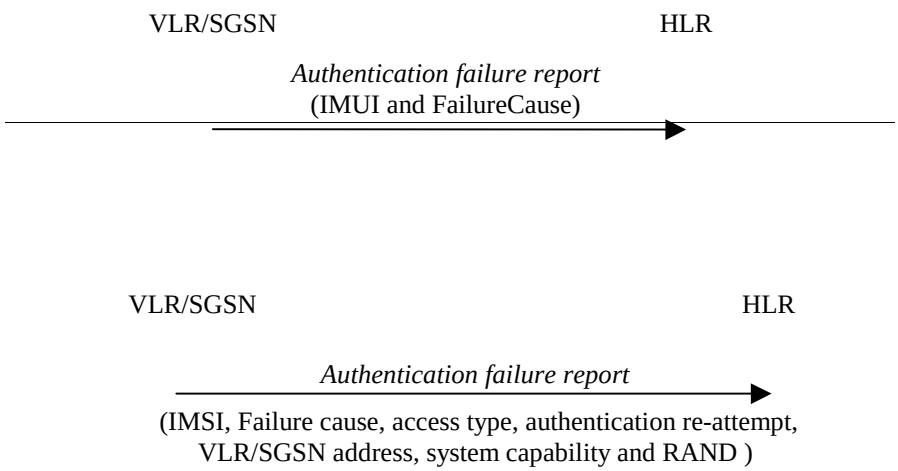

Figure 13: Reporting authentication failure from VLR/SGSN to HLR

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

1. ~~the s~~Subscriber identity~~. and~~

2. ~~a f~~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 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. 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. System Capability. This indicates the security capability of a serving node and whether it is a 3GPP or 3GPP2 system.

7. 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*~~.shall store the received data so that further processing to detect possible fraud situations could be performed.

TSG-SA WG3 (Security) meeting #17 ***S3-010xxx***
Göteborg, Sweden, 28th – 2nd March 2001

Agenda Item: 10.1

Source: Ericsson, Lucent

Title: Additional Parameters in Authentication Failure Report Procedure

Document for: Discussion and Decision

---

1 Scope and Objectives

Document S3-000675 presented at last S3#16 meeting in Sophia Antipolis, proposed the introduction of additional parameters into the Authentication Failure Report (AFR) procedure. The added information is valuable for the HE in order to determine fraud scenarios.

The principles of the proposal were well perceived by S3 so it was agreed to progress the work in this field and perform a deeper analysis in order to identify other candidate information to be also considered here. Lucent and Ericsson have worked together during this time and as a result of the analysis two more parameters are proposed to be included in the AFR procedure:

- System Capability,
- RAND.

The content of this contribution and its accompanying CR is based on the original proposal in S3-000675.

2 Introduction

2.1 Authentication Failure Report

In the main body of the TS 33.102 v3.5.0 (clause 6.3.6) a procedure, which is invoked by the serving network VLR/SGSN when the authentication procedure fails is detailed. The purpose of this procedure is to inform the Home Environment (HE) about an authentication failure.

This *authentication failure report* (AFR) message currently contains the subscriber identity and a failure cause code, indicating whether the user (i.e., the USIM) rejected the network signature or that the user authentication response was rejected by the Serving Node (note that synchronisation failures are reported by a different procedure). Based on the failure mode reported by the VRL/SGSN, the HE may take appropriate actions, such as cancelling the location of the user.

2.2 Fraud Detection System

Mobile network Operators may use a network element, called Fraud Detection System (FDS) that can analyse patterns and identify potential fraud scenarios. Based on information received from the SN or HE.

The information elements (indicators) analysed by a FDS can be classified as:

- **Primary indicators.** Those are indicators that, in principle, can be employed in isolation to detect fraud patterns.
  Example: monitor the number of call forwarding within a pre-defined time interval.
- **Secondary indicators**. Those are indicators that, in principle, provide useful information when they are considered in isolation, but they should not be used to detect fraud on their own.
  Example: Classification by cell site(s) or switch area(s), e.g., call selling operations are concentrated in areas where the buyer lives.
- **Tertiary indicators.** Those are indicators from which no useful information can be gained, if they are considered in isolation. On the other hand, the data can be used to provide essential information in connection with other fraud detection mechanisms.

Example: Number of successful handovers within a pre-defined time interval. Fraudsters need to have a stable position to provide call selling services, therefore mobiles with a low mobility may indicate possible fraudulent activity. Obviously, many legitimate mobiles may have this low mobility behaviour, therefore further investigations may be required.

3 Enhanced procedure

3.1 Current Situation

The data currently sent in an AFR, as described in TS 33.102, cannot be used effectively by the HLR to detect fraudulent call patterns, since this node doesn't have the functionality to perform an evaluation of all possible fraud scenarios (note that the HE can cancel the registration upon receiving the AFR). Even a FDS cannot use the data, since the data received cannot be associated with any of the current indicators used by an FDS (described in chapter 1.2).

On the other hand, some data related to an unsuccessful authentication can be considered equivalent to secondary indicators, but is not sent to the FDS. The data elements and their potential use, from a fraud-detection point of view, are described below:

- **Access type.** – Parameter needed to differentiate among authentication failure detected during a regular access attempt, 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 a failure produced by a location update procedure can be considered more severe than a failure detected during a call set up procedure, which in turn may be more severe than a failure detected during a short message transfer. These considerations are based in some facts; e.g. a successful location updating has to be performed before a call attempt is attempted.
- **Authentication re-attempt.** – It indicates whether the failure was produced during an initial normal authentication attempt or it was due to an authentication re-attempt (following an unsuccessful 1st authentication attempt). An authentication re-attempt is performed by the serving network, since the failure could be generated by a TMSI mismatch or by an erroneous Authentication Vectors received from the previous serving MSC (the reattempt is executed after a new Authentication Vectors is received from the HLR/AuC). When the authentication re-attempt is performed, it is done with the updated IMSI (User Identity Request performed) and with an updated Authentication Vector (Send Authentication Info performed), thus an error in this case is of higher importance.
- **VLR/SGSN address.** – This parameter is required to associate the failure with a physical location. The usefulness of this data, from a fraud-detection point of view, resides on the fact that some fraudulent activity (mainly call selling) is associated to a fixed geographical location.
- **System Capability** – parameter which potentially can be used to identify the Serving Node as a 3GPP or 3GPP2 system and as well as indicate to the HE the security capability of a serving node. This parameter is part of the ANSI-41 information flow[1], and the parameter is needed for interworking between a 3GPP and 3GPP2 system.
- **RAND** – The RAND number can be used to uniquely identify the specific AV that failed authentication. This parameter is part of the ANSI-41 information flow, and the parameter is needed for interworking between a 3GPP and 3GPP2 system.

The VLR/SGSN performing the authentication has access to all the data associated with an authentication failure, but since the data is not included in any CDR (Call Data Record) used to transfer the information to the FDS, this critical information is never received by an FDS. Moreover, a manual data gathering is quite complex, since the VLR/SGSN and the subscription can belong to different operators.

3.2 Enhancement for fraud detection

The VLR/SGSN shall include the above mentioned data elements in the AFR message, enabling the HE to gather relevant fraud information. Once the data is stored in the HE, it should be possible to send this information towards a FDS, either manually or automatically (this is out of he scope of this contribution).

[1] The ANSI_41 document is based-line, and changes may occur before it is balloted and approved.

4 Conclusions

The clause 6.3.6 in TS 33.102 v3.6.0 should be updated to include the following data elements in the message *authentication failure report*:

- Access type.
- Authentication re-attempt.
- VLR/SGSN address.
- System Capability
- RAND

A short description of the parameter should be included as well, stating that the HE should temporarily store this data before it can be forwarded to a FDS for processing.

The attached CR proposes the corresponding changes to TS 33.102 specification. Note that the addition of these parameters into the AFR procedure is being proposed for R4 and not for R99 (R99 functionality should be frozen at this stage).