3GPP TSG SA WG3 Security — S3#17 **S3-010110**

27 February - 02 March, 2001

Gothenburg, Sweden

Title: **LS to CN4 on Additional Parameters in AFR procedure**

Source: **TSG SA WG3**
To: **TSG CN WG4**
Contact Person: **david.castellanos-zamora@era.ericsson.se**

S3 would like to inform CN4 that at our S3#17 meeting, the CR in Tdoc S3-010104 was agreed (this is a CR on 33.102 for R4).

This CR incorporates the following additional parameters into the Authentication Failure Report procedure:

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

This information will be valuable for the HE in order to identify fraud scenarios.

S3 kindly asks CN4 to consider this change in order that it is further accommodated into the corresponding CN4 specifications (i.e. 29.002 Rel 4).

3GPP TSG-SA WG3 Meeting #17 ***S3-010104***
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.

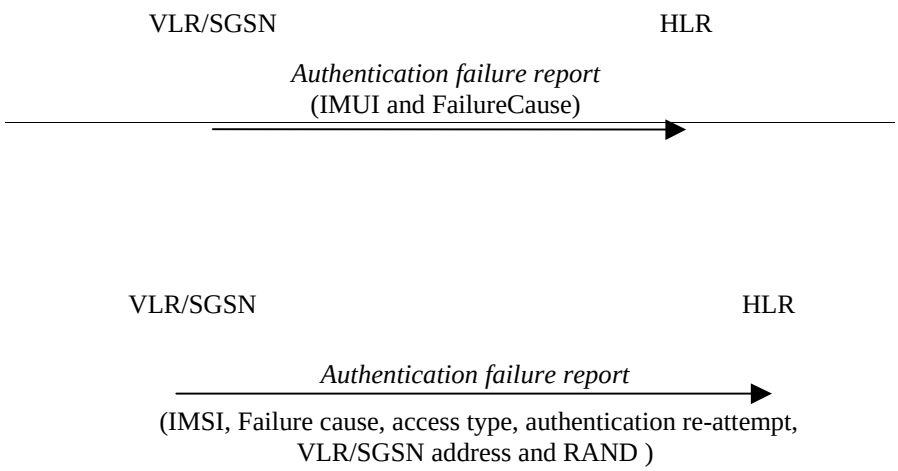

Figure 13: Reporting authentication failure from VLR/SGSN to HLR

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.

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

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.