Technical Specification Group Services and System Aspects
Meeting #13, Beijing, China, 24-27 September 2001

TSGS#13(01)0492

Source: **SA WG3**

Title: **1 CR to 33.102: Removing the list of access type codes from authentication failure report (Rel-4)**

Document for: **Approval**

Agenda Item: **7.3.3**

Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New	Doc-2nd-Level
33.102	155	1	Rel-4	F	Removing the list of access type codes from authentication failure report	4.1.0	4.2.0	S3-010394

3GPP TSG-SA WG 3 Security - S3#19 ***S3-010394***
Newbury, UK, 4-6. July 2001

CR-Form-v3

CHANGE REQUEST

⌘ **33.102** **CR** **155** ⌘ rev **1** ⌘ Current version: **4.1.0** ⌘

*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:	⌘	Removing the list of access type codes from authentication failure report
Source:	⌘	S3
Work item code:	⌘	SEC1 ***Date:*** ⌘ 27-06-01
Category:	⌘	**F** ***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:	⌘	The access type parameter in authentication failure report can only have values that may be used in CS-domain (e.g. location update). In addition to these, there are several access types that exist only in PS-domain (e.g. routing area update) To avoid updating the list when new access type codes need to be added, the exhaustive list is removed from this stage 2 specification and kept only in TS 29.002.
Summary of change:	⌘	Allowing the use of all possible access types in authentication failure report
Consequences if not approved:	⌘	Fraud detection capabilities are limited into CS-domain. The list is needed to be updated always when an access type is added.

Clauses affected:	⌘	6.3.6
Other specs affected:	⌘	☒ Other core specifications ⌘ 29.002 ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	Related to CR 29.002-302

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.

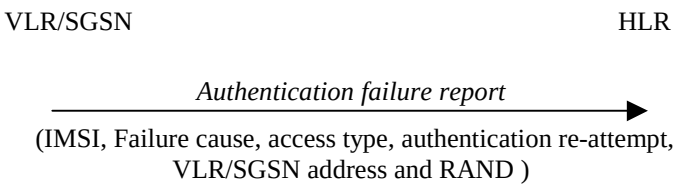

Figure 13: Reporting authentication failure from VLR/SGSN to HLR

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 ~~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. 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.