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

S3-010394

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		

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

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.

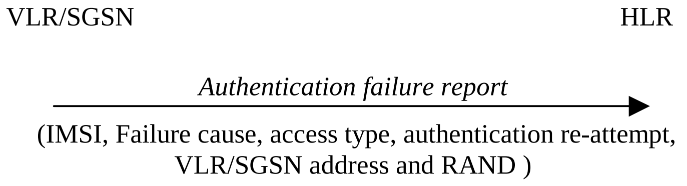
VLR/SGSN
HLR
Authentication failure report
(IMSI, Failure cause, access type, authentication re-attempt,
VLR/SGSN address and RAND)

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.