

CHANGE REQUEST

⌘ **33.102 CR XXX** ⌘ rev **6.0.0** ⌘ Current version: **6.0.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Clarification on Authentication re-attempt parameter		
Source:	⌘ SA WG3		
Work item code:	⌘ TEI6	Date:	⌘ 12/05/2004
Category:	⌘ F	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)	2 (GSM Phase 2)	
	A (corresponds to a correction in an earlier release)	R96 (Release 1996)	
	B (addition of feature),	R97 (Release 1997)	
	C (functional modification of feature)	R98 (Release 1998)	
	D (editorial modification)	R99 (Release 1999)	
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	⌘ The authentication re-attempt parameter was introduced in REL4 to be used by a Fraud Detection System (FDS) in the Home Network to help identify and manage potential fraud scenarios. However, it was pointed out by the CN4 LS (S3-030672) that the detailed usage of this parameter is unclear. Besides, CN4 requested SA3 in the later LS (N4-040247) to provide more information in the 33.102 about the criteria when the authentication re-attempt parameter is set in VLR and SGSN. Therefore, this CR proposes to provide all criteria the authentication re-attempt parameter is set in VLR and SGSN.
Summary of change:	⌘ This CR proposes to add new sub clause to describe the all criteria the authentication re-attempt parameter is set in VLR and SGSN.
Consequences if not approved:	⌘ Due to unclear definition of the authentication re-attempt parameter, VLR and SGSN may not be designed properly and this may lead the FDS function ineffective.

Clauses affected:	⌘ 6.3.6										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td>X</td> <td></td> </tr> <tr> <td></td> <td>X</td> </tr> <tr> <td></td> <td>X</td> </tr> </table>	Y	N	X			X		X	Other core specifications	⌘ 23.012, 23.018 and possibly 29.002
Y	N										
X											
	X										
	X										
		Test specifications									
		O&M Specifications									
Other comments:	⌘										

First modification

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.

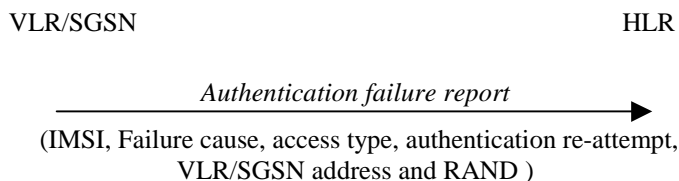


Figure 13: Reporting authentication failure from VLR/SGSN to HLR

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;
4. Authentication re-attempt. This indicates whether the failure was produced in a normal authentication attempt or it was due to an authentication re-attempt (there was a previous unsuccessful authentication). [Details are provided in subclause 6.3.6.1](#);
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.

6.3.6.1 Authentication re-attempt

The serving network sets the Authentication re-attempt to “true” if the second authentication described in the following cases results in an authentication failure report.

- Authentication with (P-)TMSI failed in MS (reject cause 'MAC failure') and new authentication procedure (re-attempt) is taken because an IMSI obtained by the followed IDENTITY REQUEST procedure does not match to the original IMSI that linked with (P-)TMSI.
- Authentication failed in MS (reject cause 'GSM authentication unacceptable') and new authentication procedure (re-attempt) is taken after MSC obtains UMTS authentication vectors from HLR.
- Authentication failed in MS (reject cause 'synch failure') and new authentication procedure (re-attempt) is taken after MSC obtains new authentication vectors from HLR for re-synchronisation.
- SRES mismatches with (P-)TMSI in VLR/SGSN and new authentication procedure (re-attempt) is taken because an IMSI obtained by the followed IDENTITY REQUEST procedure does not match to the original IMSI that linked with (P-)TMSI.

Error! No text of specified style in document.

3

Error! No text of specified style in document.

[Otherwise Authentication re-attempt is set to "False"](#)