3GPP TSG-SA3 Meeting #33 **S3-040251**
10th - 14th May 2004. Beijing, China.

CR-Form-v7

CHANGE REQUEST

⌘ **33.102** **CR** **XXX** ⌘ **rev** ⌘ 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 **X**

Title:	⌘	Clarification on Authentication re-attempt parameter
Source:	⌘	NEC
Work item code:	⌘	TEI6
Date:	⌘	19/April/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(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)*
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. Together with above updates, the reference section is updated accordingly.
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:	⌘	2, 6.3.6

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	23.012, 23.108 and possibly 29.002 might need some updates. However, This CR can be approved alone since this is just for clarification purpose.

First modification

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2] 3GPP TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[3] 3GPP TR 21.905: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications (Release 1999)".

[4] 3GPP TS 23.121: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Architecture Requirements for Release 99".

[5] 3GPP TS 31.101: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics".

[6] 3GPP TS 22.022: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Personalisation of UMTS Mobile Equipment (ME); Mobile functionality specification".

[7] 3GPP TS 23.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Security Mechanisms for the (U)SIM application toolkit; Stage 2".

[8] ETSI GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[9] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[10] ISO/IEC 9798-4: "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function".

[11] 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications".

[12] 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification".

[13] 3GPP TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementers' test data".

[14] 3GPP TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data".

[15] 3GPP TS 31.111: "3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT)".

[16] 3GPP TS 22.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Security Mechanisms for the (U)SIM Application Toolkit; Stage 1".

[17] 3GPP TS 25.331: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RRC Protocol Specification".

[18] 3GPP TS 25.321: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; MAC protocol specification".

[19] 3GPP TS 25.322: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RLC Protocol Specification".

[20] 3GPP TS 31.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Characteristics of the USIM Application".

[21] 3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Service principles".

[22] 3GPP TS 23.195: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Provision of User Equipment Specific Behaviour Information (UESBI) to network entities".

[23] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols - Stage 3".

[24] 3GPP TS 23.012: "Location management procedures".

[25] 3GPP TS 23.018: "Basic call handling; Technical realization".

Second 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.

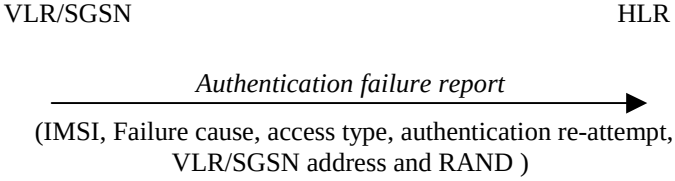

Figure 13: Reporting authentication failure from VLR/SGSN to HLR

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. Details are provided in TS 24.008 [23]
- 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. Details are provided in TS 24.008 [23]
- Authentication failed in MS (reject cause 'synch failure') and new authentication procedure (re-attampt) is taken after MSC obtains new authentication vectors from HLR for re-synchronisation. Details are provided in TS 24.008 [23]
- 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. Details are provided in TS 23.012 [24] and TS 23.018 [25]

Otherwise Authentication re-attempt is set to “False”