3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102 **CR** **056r1** Current Version: 3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG: SA #7 *list TSG meeting no. here ↑*
for approval **X**
for information
(only one box should be marked with an X)

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: *(at least one should be marked with an X)* USIM **X** ME **X** UTRAN **X** Core Network **X**

Source: S3 **Date:** 2000-Feb-23

Subject: Identification of temporary identities

3G Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	**X**

Reason for change: Clarification of the relation to GSM 03.20 and GSM 23.060 for identification of temporary identities.
Terminology clean-up.

Clauses affected: 2.1; 6.1.1

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other 2G core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

2.1 Normative references

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

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

[3] UMTS 33.21, version 2.0.0: "Security requirements".

[4] UMTS 33.22, version 1.0.0: "Security features".

[5] UMTS 33.23, version 0.2.0: "Security architecture".

[6] Proposed UMTS Authentication Mechanism based on a Temporary Authentication Key.

[7] TTC Work Items for IMT-2000 – System Aspects.

[8] Annex 8 of "Requirements and Objectives for 3G Mobile Services and systems" – "Security Design Principles".

[9] ETSI GSM 09.02 Version 4.18.0: Mobile Application Part (MAP) Specification.

[10] ISO/IEC 11770-3: *Key Management – Mechanisms using Asymmetric Techniques*.

[11] ETSI SAGE: Specification of the BEANO encryption algorithm, Dec. 1995 (confidential).

[12] ETSI SMG10 WPB: SS7 Signalling Protocols Threat Analysis , Input Document AP 99-28 to SMG10 Meeting#28, Stockholm, Sweden.

[13] 3G TS 33.105: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Cryptographic Algorithm Requirements".

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

6.1 Identification by temporary identities

6.1.1 General

This mechanism allows the identification of a user on the radio access link by means of a temporary mobile ~~user~~ subscriber identity (TMS~~U~~I/P-TMSI). A TMS~~U~~I/P-TMSI has local significance only in the location area or routing area in which the user is registered. Outside that area it should be ~~a~~ accompanied by an appropriate Location Area Identification (LAI) or Routing Area Identification (RAI) in order to avoid ambiguities. The association between the permanent and temporary user identities is kept by the Visited Location Register (VLR/SGSN) in which the user is registered.

The TMS~~U~~I/P-TMSI, when available, is normally used to identify the user on the radio access path, for instance in paging requests, location update requests, attach requests, service requests, connection re-establishment requests and detach requests.

The procedures and mechanisms are described in GSM 03.20 and TS 23.060. The following subchapters contain a summary of this feature.