3GPP/SMG Meeting #14
Oslo, Norway, 01-04 August 2000

***Document* S3-000430**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

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		Current Version:	3.5.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: SA#14	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑	For information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [X] ME [ ] UTRAN / Radio [ ] Core Network [X]

Source: Ericsson **Date:** 2000-07-25

Subject: Replace IMUI and TMUI with IMSI and TMSI

Work item: Security

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

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Change IMUI to IMSI and TMUI to TMSI

Clauses affected: Contents, 5.1.1, 6.1, 6.3.6

Other specs Affected:

Other 3G core specifications		→ List of CRs:
Other GSM 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.

Contents

5.1.1 User identity confidentiality

The following security features related to user identity confidentiality are provided:

- **user identity confidentiality:** the property that the permanent user identity (~~IMUI~~IMSI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link;

- **user location confidentiality:** the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link;

- **user untraceability:** the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

To achieve these objectives, the user is normally identified by a temporary identity by which he is known by the visited serving network, or by an encrypted permanent identity. To avoid user traceability, which may lead to the compromise of user identity confidentiality, the user should not be identified for a long period by means of the same temporary or encrypted identity. To achieve these security features, in addition it is required that any signalling or user data that might reveal the user's identity is ciphered on the radio access link.

Clause 6.1 describes a mechanism that allows a user to be identified on the radio path by means of a temporary identity by which he is known in the visited serving network. This mechanism should normally be used to identify a user on the radio path in location update requests, service requests, detach requests, connection re-establishment requests, etc..

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 subscriber identity (TMSI/P-TMSI). A TMSI /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 TMSI/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 subclauses contain a summary of this feature.

6.1.2 ~~TMUI~~TMSI reallocation procedure

The purpose of the mechanism described in this subsection is to allocate a new ~~TMUI~~TMSI/LAI pair to a user by which he may subsequently be identified on the radio access link.

The procedure should be performed after the initiation of ciphering. The ciphering of communication over the radio path is specified in clause 6.6. The allocation of a temporary identity is illustrated in Figure 3.

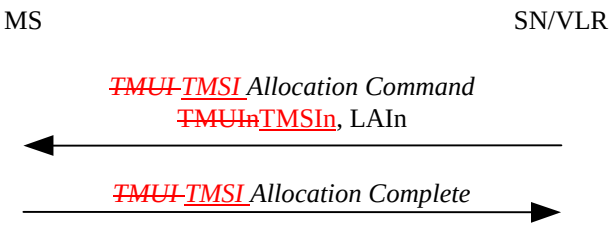

Figure 3: TMSI allocation

The allocation of a temporary identity is initiated by the VLR.

The VLR generates a new temporary identity (~~TMUIn~~TMSIn) and stores the association of ~~TMUIn~~TMSIn and the permanent identity ~~IMUI~~IMSI in its database. The ~~TMUI~~TMSI should be unpredictable. The VLR then sends the ~~TMUIn~~TMSIn and (if necessary) the new location area identity LAIn to the user.

Upon receipt the user stores ~~TMUIn~~TMSIn and automatically removes the association with any previously allocated ~~TMUI~~TMSI. The user sends an acknowledgement back to the VLR.

Upon receipt of the acknowledgement the VLR removes the association with the old temporary identity ~~TMUIo~~TMSIo and the ~~IMUI~~IMSI (if there was any) from its database.

6.1.3 Unacknowledged allocation of a temporary identity

If the serving network does not receive an acknowledgement of the successful allocation of a temporary identity from the user, the network shall maintain the association between the new temporary identity ~~TMUIn~~TMSIn and the ~~IMUI~~IMSI and between the old temporary identity ~~TMUIo~~TMSIo (if there is any) and the ~~IMUI~~IMSI.

For a user-originated transaction, the network shall allow the user to identify itself by either the old temporary identity ~~TMUIo~~TMSIo or the new temporary identity ~~TMUIn~~TMSIn. This allows the network to determine the temporary identity stored in the mobile station. The network shall subsequently delete the association between the other temporary identity and the ~~IMUI~~IMSI, to allow the temporary identity to be allocated to another user.

For a network-originated transaction, the network shall identify the user by its permanent identity (~~IMUI~~IMSI). When radio contact has been established, the network shall instruct the user to delete any stored ~~TMUI~~TMSI. When the network receives an acknowledgement from the user, the network shall delete the association between the ~~IMUI~~IMSI and any ~~TMUI~~TMSI to allow the released temporary identities to be allocated to other users.

Subsequently, in either of the cases above, the network may initiate the normal ~~TMUI~~TMSI reallocation procedure.

Repeated failure of ~~TMUI~~TMSI reallocation (passing a limit set by the operator) may be reported for O&M action.

6.1.4 Location update

In case a user identifies itself using a ~~TMUIo~~TMSIo/LAIo pair that was assigned by the visited VLRn the ~~IMUI~~IMSI can normally be retrieved from the database. If this is not the case, the visited VLRn should request the user to identify itself by means of its permanent user identity. This mechanism is described in 6.2.

In case a user identifies itself using a ~~TMUIo~~TMSIo/LAIo pair that was not assigned by the visited VLRn and the visited VLRn and the previously visited VLRo exchange authentication data, the visited VLRn should request the previously visited VLRo to send the permanent user identity. This mechanism is described in 6.3.4, it is integrated in the mechanism for distribution of authentication data between VLRs. If the previously visited VLRo cannot be contacted or cannot retrieve the user identity, the visited VLRn should request the user to identify itself by means of its permanent user identity. This mechanism is described in 6.2.

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.

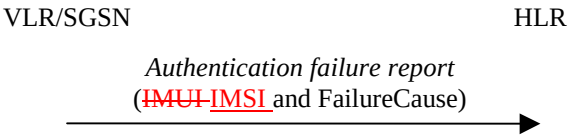

Figure 13: Reporting authentication failure from VLR/SGSN to HLR

The procedure is invoked by the serving network VLR/SGSN when the authentication procedure fails. The *authentication failure report* shall contain the subscriber identity and a failure cause code. The possible failure causes are either that the network signature was wrong or that the user response was wrong.

The HE may decide to cancel the location of the user after receiving an *authentication failure report*.