Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 **Annex K of S3-99203**

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	011	Current Version:	3.0.0

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

For submision to TSG SA#3 *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 [ ] ME [X] UTRAN [ ] Core Network [X]

Source: SA WG3 **Date:** 99-06-18

Subject: Precision of the status of annex B

3G Work item: 3G Security architecture

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	[X]
D	Editorial modification	[ ]

Reason for change: Modification of status of annex B on user identity confidentiality

Clauses affected: Annex B

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.

Annex B (Informative): Enhanced user identity confidentiality

This mechanism allows the identification of a user on the radio access by means of the permanent user identity encrypted by means of a group key. The mechanism described here can be used in combination with the mechanism described in 6.2 to provide user identity confidentiality in the event that the user not known by means of a temporary identity in the serving network.

The mechanism assumes that the user belongs to a user group with group identity GI. Associated to the user group is a secret group key GK which is shared between all members of the user group and the user's HE, and securely stored in the USIM and in the HE.

The mechanism is illustrated in Figure B.1.

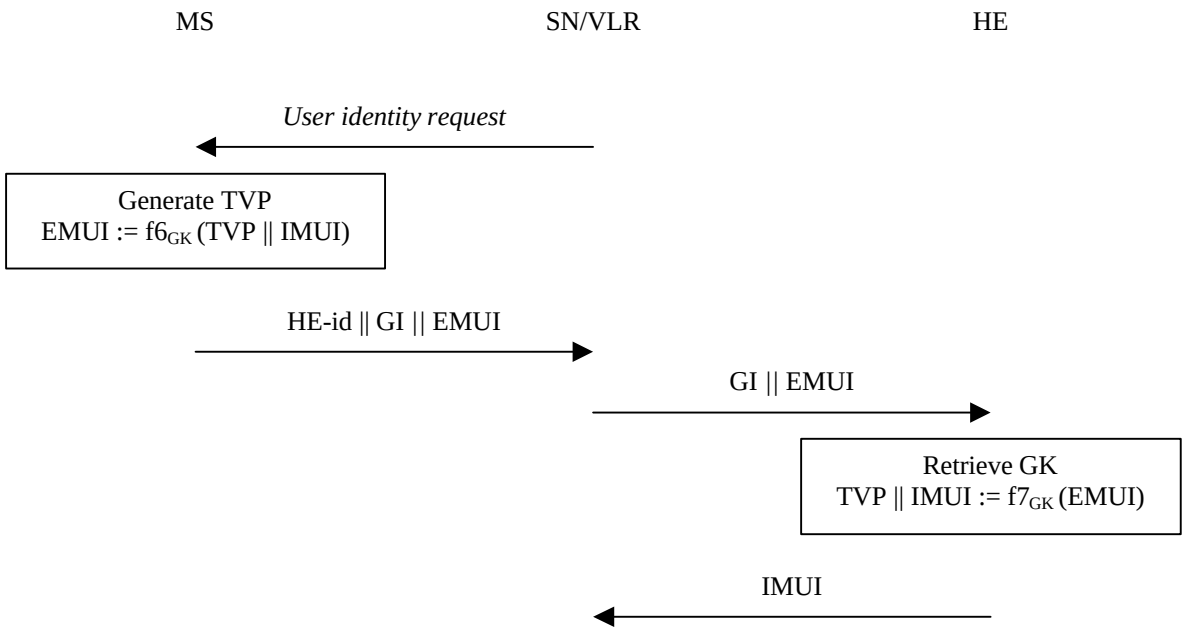

Figure B.1: Identification by means of the IMUI encrypted by means of a group key

The user identity procedure is initiated by the visited VLR. The visited VLR requests the user to send its permanent user identity.

Upon receipt the user generates a time variant parameter TVP. The user encrypts the time variant parameter TVP and the IMUI with enciphering algorithm f6 and his group key GK. The TVP prevents traceability attacks. The user sends a response to the VLR that includes the HE identity, the group identity GI and the encrypted mobile user identity (EMUI).

Upon receipt of that response the SN/VLR should resolve the user's HE address from HE-identity and forwards the group identity GI and the user's EMUI to the user's HE.

Upon receipt the HE retrieves the group key GK associated with the group identity GI. The HE then decrypts EMUI with the deciphering algorithm f7 ($f7 = f6^{-1}$) and the group key GK and retrieves TVP and IMUI. The HE then sends the IMUI in a response to the visited SN/VLR.