

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 XX

Current Version: **3.3.1**

3G specification number ↑

↑ CR number as allocated by 3G support team

For submission to TSG **SA #7** for approval **X** (only one box should
list TSG meeting no. here ↑ for information 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

UTRAN

Core Network

Source:

Ericsson

Date:

2000-01-17

Subject:

Clarification on enhanced Distribution of authentication data within one serving network domain

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

Reason for change:

This CR specifies the behaviour of new VLR/SGSN when the keys of the current security context have been received from old VLR/SGSN.

Clauses affected:

6.3.4

Other specs affected:

Other 3G core specifications	<input checked="" type="checkbox"/>	→ List of CRs:	29.002
Other 2G core specifications	<input type="checkbox"/>	→ List of CRs:	
MS test specifications	<input type="checkbox"/>	→ List of CRs:	
BSS test specifications	<input type="checkbox"/>	→ List of CRs:	
O&M specifications	<input type="checkbox"/>	→ List of CRs:	

Other comments:



help.doc

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

6.3.4 Distribution of IMSI and temporary authentication data within one serving network domain

The purpose of this procedure is to provide a newly visited MSC/VLR or SGSN with temporary authentication data from a previously visited MSC/VLR or SGSN within the same serving network domain.

The procedure is shown in Figure 11.

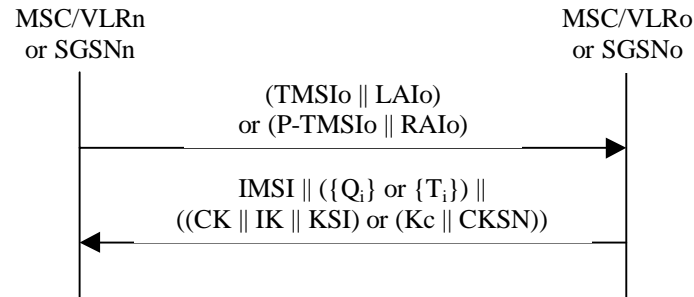


Figure 11: Distribution of IMSI and temporary authentication data within one serving network domain

The procedure shall be invoked by the newly visited MSC/VLRn (resp. SGSNn) after the receipt of a location update request (resp. routing area update request) from the user wherein the user is identified by means of a temporary user identity TMSIo (resp. P-TMSIo) and the location area identity LAIo (resp. routing area identity RAIo) under the jurisdiction of a previously visited MSC/VLRo or SGSNo that belongs to the same serving network domain as the newly visited MSC/VLRn or SGSNn.

The protocol steps are as follows:

- a) The MSC/VLRn (resp. SGSNn) sends a *user identity request* to the MSC/VLRo (or SGSNo), this message contains TMSIo and LAIo (resp. P-TMSIo and RAIo).
- b) The MSC/VLRo (resp. SGSNo) searches the user data in the database.

If the user is found, the MSC/VLRo (resp. SGSNo) shall send a *user identity response* back that

- i) shall include the IMSI,
- ii) may include a number of unused authentication vectors (quintets or triplets) and
- iii) may include the current security context data: CK, IK and KSI (UMTS) or Kc and CKSN (GSM).

The MSC/VLRo or SGSNo subsequently deletes the authentication vectors which have been sent and the data elements on the current security context.

If the user cannot be identified the MSC/VLRo or SGSNo shall send a *user identity response* indicating that the user identity cannot be retrieved.

- c) If the MSC/VLRn or SGSNn receives a *user identity response* with an IMSI, it creates an entry and stores any authentication vectors and any data on the current security context that may be included. [Note that if a different security context is required at MSC/VLRn \(resp. SGSNn\), the information regarding current security context data received from MSC/VLRo \(resp. SGSNo\) can not be used to authenticate the subscriber using local authentication. A new authentication and key agreement procedure shall be performed in this case.](#)

If the MSC/VLRn or SGSNn receives a *user identity response* indicating that the user could not be identified, it shall initiate the user identification procedure described in 6.2.