

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 064

Current Version: **3.3.1**

GSM (AA.BB) or 3G (AA.BBB) specification number ↑

↑ CR number as allocated by MCC support team

For submission to: **SA #7**
list expected approval meeting # here ↑

for approval
for information

strategic
non-strategic (for SMG use only)

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: (U)SIM ME UTRAN / Radio Core Network
(at least one should be marked with an X)

Source: Ericsson **Date:** 2000-02-16

Subject: Distribution and Use of Authentication Data between VLRs/SGSNs

Work item: Security

Category: F Correction
A Corresponds to a correction in an earlier release
B Addition of feature
C Functional modification of feature
D Editorial modification
(only one category shall be marked with an X)

Release: Phase 2
Release 96
Release 97
Release 98
Release 99
Release 00

Reason for change: This CR specifies the conditions for the distribution of authentication data (unused AVs and/or current security context data) between VLRs/SGSNs (of the same or different releases) and use of such information at VLRn/SGSNn.
A new chapter under section 6.8 ('Interoperation and handover between UMTS and GSM') is introduced: Chapter 6.8.3 'Distribution of Authentication Data between VLRs/SGSNs'.

Clauses affected: 6.8

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.

6.8.3 Distribution and use of authentication data between VLRs/SGSNs

The following four cases are distinguished related to the distribution of authentication data (unused authentication vectors and/or current security context data) between VLRs/SGSNs. Conditions for the distribution of such data and for its use when received at VLRn/SGSNn are indicated for each case:

a) R99+ VLR/SGSN to R99+ VLR/SGSN

UMTS and GSM authentication vectors can be distributed between R99+ VLRs/SGSNs. Note that originally all authentication vectors (quintuplets for UMTS subscribers and triplets for GSM subscribers) are provided by the HLR/AuC.

Current security context data can be distributed between R99+ VLRs/SGSNs. VLRn/SGSNn shall not use current security context data received from VLRo/SGSNo to authenticate the subscriber using local authentication in the following cases:

- i) Security context to be established at VLRn/SGSNn requires a different set of keys than the one currently in use at VLRo/SGSNo. This change of security context is caused by a change of UE release (R'99 UE \leftrightarrow R'98 UE) when the user registers at VLRn/SGSNn.
- ii) Authentication data from VLRo includes Kc+CKSN but no unused AVs and the subscriber has a R'99 UE (under GSM BSS or UTRAN). In this situation, VLRn have no indication of whether the subscriber is GSM or UMTS and it is not able to decide whether Kc received can be used (in case the subscriber were a GSM subscriber).

In these two cases, received current security context data shall be discarded and a new AKA procedure shall be performed.

b) R98- VLR/SGSN to R98- VLR/SGSN

Only triplets can be distributed between R98- VLRs/SGSNs. Note that originally for GSM subscribers, triplets are generated by HLR/AuC and for UMTS subscribers, they are derived from UMTS authentication vectors by R99+ HLR/AuC. UMTS AKA is not supported and only GSM security context can be established by a R98- VLR/SGSN.

R98- VLRs are not prepared to distribute current security context data.

Since only GSM security context can be established under R98- SGSNs, security context data can be distributed and used between R98- SGSNs.

c) R99+ VLR/SGSN to R98- VLR/SGSN

R99+ VLR/SGSN can distribute to a new R98- VLR/SGSN triplets originally provided by HLR/AuC for GSM subscribers or can derive triplets from stored quintuplets originally provided by R99+ HLR/AuC for UMTS subscribers. Note that R98- VLR/SGSN can only establish GSM security context.

R99+ VLRs shall not distribute current security context data to R98- VLRs.

Since R98- SGSNs are only prepared to handle GSM security context data, R99+ SGSNs shall only distribute GSM security context data (Kc, CKSN) to R98- SGSNs.

d) R98- VLR/SGSN to R99+ VLR/SGSN.

In order to not establish a GSM security context for a UMTS subscriber, triplets provided by a R98- VLR/SGSN can only be used by a R99+ VLR/SGSN to establish a GSM security context under GSM-BSS with a R98- UE.

R99+ VLR/SGSN shall discard triplets received from R98- VLR/SGSN and shall request fresh AVs (either triplets or quintuplets) to HE in all other cases.

R99+ VLR/SGSN shall not distribute triplets received from a R98- VLR/SGSN to any other R99+ VLR/SGSN since it is unknown if the triplets belong to a GSM subscriber or UMTS subscriber (derived from quintuplets).

R98- VLRs are not prepared to distribute current security context data.

R98- SGSNs can distribute GSM security context data only. The use of this information at R99+ SGSNn shall be

performed according to the conditions stated in a).