

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 064r1 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: **S3** **Date:** **2000-02-23**

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

Work item: **Security**

| | | |
|---|--|--|
| Category: (only one category shall be marked with an X) | F Correction <input checked="" type="checkbox"/> | Release: Phase 2 <input type="checkbox"/> |
| | A Corresponds to a correction in an earlier release <input type="checkbox"/> | Release 96 <input type="checkbox"/> |
| | B Addition of feature <input type="checkbox"/> | Release 97 <input type="checkbox"/> |
| | C Functional modification of feature <input type="checkbox"/> | Release 98 <input type="checkbox"/> |
| | D Editorial modification <input type="checkbox"/> | Release 99 <input checked="" type="checkbox"/> |
| | | Release 00 <input type="checkbox"/> |

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 | <input type="checkbox"/> | → List of CRs: <input type="text"/> |
| Other GSM core specifications | <input type="checkbox"/> | → List of CRs: <input type="text"/> |
| MS test specifications | <input type="checkbox"/> | → List of CRs: <input type="text"/> |
| BSS test specifications | <input type="checkbox"/> | → List of CRs: <input type="text"/> |
| O&M specifications | <input type="checkbox"/> | → List of CRs: <input type="text"/> |

Other comments:



<----- 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 distribution of authentication data (unused authentication vectors and/or current security context data) between R99+ VLRs/SGSNs of the same service network domain is performed according to chapter 6.3.4. The following four cases are distinguished related to the distribution of authentication data between VLRs/SGSNs (of the same or different releases). 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 and used between R99+ VLRs/SGSNs.

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 shall be discarded and the R99+ VLR/SGSN shall request fresh AVs (either triplets or quintuplets) to HE.

For the same reason, a R99+ SGSNs shall discard current security context data received from a R98- SGSN.

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