3GPP TSG SA WG 3 (Security) meeting #1	1
Mainz, 22—24 February, 2000	

S3-000212 Document (Rev. of S3-000209) 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	064	lr2	Cu	irrent Versi	on: 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 a for info	X strategic (for s non-strategic use o version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form					only)		
Proposed change affects: (U)SIM ME UTRAN / Radio Core Network X (at least one should be marked with an X)											
Source:		S3						Date:	2000-03-08		
Subject: Distribution and Use of Authentication Data between VLRs/SGSNs											
Work item:		Security									
Category: (only one category shall be marked with an X)	F A B C D	Addition of	modification of fe		rlier rel	ease	X	<u>Release:</u>	Phase 2 Release 96 Release 97 Release 98 Release 99 Release 00	X	
<u>Reason for</u> <u>change:</u>		and/or curre releases) a A new chap	ecifies the conditi ent security conte nd use of such in oter under section serted: Chapter 6 Ns'.	ext data) formation 6.8 ('Int	betwee n at VL eropera	n VLRs Rn/SG ation ar	s/SGSN SNn. nd hanc	Ns (of the s	ame or differe	ent	
Clauses affect	ted	: 6.8									
Other specs affected:	C C N E	- Dther 3G cor	cifications	3	\rightarrow List \rightarrow List \rightarrow List \rightarrow List \rightarrow List	of CRs of CRs of CRs					
<u>Other</u> comments:	3	3.3.1. ("Inters	new chapter doe system HO for CS re it instead.							02	
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 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) <u>R99+ VLR/SGSN to R99+ VLR/SGSN</u>

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

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

- i) <u>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 $\leftarrow \rightarrow$ R'98 UE) when the user registers at VLRn/SGSNn.</u>
- ii) <u>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).</u>

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

b) <u>R98- VLR/SGSN to R98- VLR/SGSN</u>

<u>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.</u>

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) <u>R99+ VLR/SGSN to R98- VLR/SGSN</u>

<u>R99+ VLR/SGSN can distribute to a new R98- VLR/SGSN triplets originally provided by HLR/AuC for GSM</u> 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) <u>R98- VLR/SGSN to R99+ VLR/SGSN.</u>

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.

In all other cases, R99+ VLR/SGSN shall request fresh AVs (either triplets or quintuplets) to HE. In the event, the R99+ VLR/SGSN receives quintuplets, it shall discard the triplets provided by the R98- VLR/SGSN.

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

<u>R98-</u>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).