## 3GPP TSG SA WG3 Security — S3#25

#### 8 - 11 October 2002

### S3-020503

# Munich, Germany

							от	1			CR-Form-v7
CHANGE REQUEST											
ж <mark>Т</mark>	<mark>S 33</mark>	. <mark>102</mark> (	CR <mark>C</mark>	RNum	жrev	-	Ħ	Current vers	ion:	5.0.0	ж
For <b>HELP</b> on using this form, see bottom of this page or look at the pop-up text over the $\Re$ symbols.											
Proposed change	e affec	t <b>s:</b> UI	CC app	s# 📃	ME	Rad	dio A	ccess Netwo	rk	Core Ne	etwork
Title:	₩ <mark>US</mark>	I <mark>M supp</mark>	ort in GI	ERAN only	terminal	S					
Source:	<mark>₩ Sie</mark>	mens									
Work item code:	₩ <mark>Se</mark> o	curity						Date: ೫	3/10	0/2002	
Catagory	ж <mark>г</mark>							Release: ೫	Dol	E	
Category:	Use	F (corre A (corre B (addit C (funct D (edito iled expla	ction) esponds t ion of fea ional mod rial modil	dification of lication) of the above	on in an ea feature)		elease	Use <u>one</u> of 2	the for (GSM (Relea (Relea (Relea (Relea (Relea		
Reason for chang	<b>де:</b> Ж							5.7.0 on the s	uppoi	rt of USIN	/l in
		GERAN only terminals for Rel-5 or later. SP-020051 is the approved CR for TS 22.101.									
Summary of char	nge:	require	ement is		l within T	S 22.1		ng requireme GERAN only			
Consequences if not approved:	ж	TS 33	.102 will	be incons	istent wit	h the a	abov	e mentioned	specif	ication.	

Clauses affected:	Ж <mark>6</mark>	. <mark>8.1</mark>	.4		
	Y	Ν			
Other specs affected:	ж	N N N	Other core specifications Test specifications O&M Specifications	Ħ	
Other comments:	ж	·	• •		

#### 6.8.1.4 R99+ ME

Release 99+ ME that has UTRAN radio capability shall support the USIM-ME interface as specified in TS 31.102 [20].

Release 99+ ME that has no UTRAN radio capabilities may support the USIM-ME interface as specified in TS 31.102 [20].

R99+ ME capable of UMTS AKA with a USIM inserted and attached to a UTRAN shall only participate in UMTS AKA and shall not participate in GSM AKA.

R99+ ME capable of UMTS AKA with a USIM inserted and attached to a GSM BSS shall participate in UMTS AKA and may participate in GSM AKA. Participation in GSM AKA is required to allow registration in a R98- VLR/SGSN.

A R99+ ME that does not support the USIM-ME interface (not capable of UMTS AKA) with a USIM inserted can only participate in GSM AKA.

The execution of UMTS AKA results in the establishment of a UMTS security context; the UMTS cipher/integrity keys CK and IK and the key set identifier KSI are passed to the ME. If the USIM supports conversion function c3 and/or GSM AKA, the ME shall also receive a GSM cipher key Kc derived at the USIM.

The execution of GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the ME.