

CR-Form-v7
CHANGE REQUEST
⌘ TS 33.102 CR CRNum ⌘ rev - ⌘ Current version: 5.1.0 ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Handling of START values stored on a ME for use with a SIM		
Source:	⌘ Siemens, Nokia, Vodafone		
Work item code:	⌘ Security	Date:	⌘ 28/4/2003
Category:	⌘ F	Release:	⌘ Rel-5
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)		2 (GSM Phase 2)
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)
	B (addition of feature),		R97 (Release 1997)
	C (functional modification of feature)		R98 (Release 1998)
	D (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	⌘ TS 33.102 contains some unclear text about storing START values on a ME for handling a SIM.		
Summary of change:	⌘ Clarify the intention of the specification in a clearer way: This includes making explicit following requirements in clause 6.8.2.4 which may only be derived by interpretation of the referenced clause 6.4.8: Issue-A: Start values stored on a ME for use with SIM shall survive a controlled power-off (I.e. the start values on the ME shall be stored in non-volatile memory). Issue-B: When the SIM is replaced, the ME shall reset the START values to zero and delete the old keys.		
Consequences if not approved:	⌘ There may be either a performance (issue-A) or a security issue (issue-B) if the specification can be interpreted in different ways. For issue-A: User of ME's, with ME-stored START values, that don't survive a controlled power off, will experience each time an authentication delay. For issue-B: When inserting SIM1 from ME1 into ME2, and ME2 is not able to detect that SIM2 was formerly used then the COUNT values for SIM1 might be reused.		

Clauses affected:	⌘ 6.8.2.4						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
	Y	N					
	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Test specifications				
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	O&M Specifications				
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
Other comments:	⌘						

***** Start of change *****

6.8.2.4 R99+ ME

R99+ ME with a SIM inserted, shall participate only in GSM AKA.

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.

When the user is attached to a UTRAN, R99+ ME shall derive the UMTS cipher/integrity keys CK and IK from the GSM cipher key Kc using the conversion functions c4 and c5. The ME shall handle the START_{CS} and START_{PS} as described in section 6.4.8 with the exception that the START values ~~shall be~~ stored in non-volatile memory on the ME rather than on the GSM SIM. ~~If the ME loses the current START value for a particular domain (e.g. due to power off) If a different SIM is inserted then the ME~~ shall delete the ~~corresponding~~ GSM cipher keys for the PS and CS domain (Kc), the derived UMTS cipher/integrity keys (CK and IK) for the PS and CS domain, and reset the START values to zero. The ME shall then trigger a new authentication and key agreement at the next connection establishment by indicating to the network that no valid keys are available for use using the procedure described in section 6.4.4.

When the user is attached to a UTRAN, a R99+ ME with a SIM inserted shall use a default value of all ones for maximum value of START_{CS} or START_{PS}. The ME shall handle the maximum value of START_{CS} or START_{PS} as described in section 6.4.3 with the exception that the maximum value of START_{CS} or START_{PS} is stored on the ME rather than on the GSM SIM.

***** End of change *****