3GPP TSG SA WG3 Security — S3#29 **S3-030465**
15 - 18 July 2003, San Francisco, USA

CR-Form-v7

CHANGE REQUEST

⌘ **33.102** CR **CRNum** ⌘rev **-** ⌘ Current version: 5.2.0 ⌘

*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:	⌘	Clarification on the usage of the c3 conversion function
Source:	⌘	Siemens, Nokia, T-Mobile
Work item code:	⌘	Security
Date:	⌘	08/07/2003
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change: ⌘
- The support of the USIM Service n° 27: called "GSM Access" is optional. With this service the USIM generates the 2G ciphering key Kc required by the 2G air interface. The Kc is derived from the CK and IK with the conversion function c3. The c3 algorithm is described in section 6.8.1.2 of TS 33.102. The function c3 may only be performed in the network and the USIM. If an operator decides to issue USIMs without USIM Service n° 27 it is the intention of the operator that *64-bit 2G ciphering* shall not be possible. Thus c3 shall not be performed in the ME if the USIM Service n° 27 is not available. This essential mandatory requirement for the ME is not explicitly stated in TS 33.102.
- Erroneous sentence on the lack of c3 function on the USIM, specifying that the ME cannot operate under any BSS.
- The last sentence in 6.8.1.5 has been corrected.

Summary of change: ⌘
- It is clarified that the conversion function c3 shall not be performed in the ME.
- It is clarified that with the lack of c3 function on the USIM, the ME cannot operate under BSS with *ciphering enabled.*
- Split of the last sentence of 6.8.1.5 to correct the logic of the sentence.

Consequences if not approved: ⌘ Risk of erroneous ME implementations which are performing the c3 in the ME, completely bypassing the operator's intentions to forbid 64-bit 2G ciphering.

Clauses affected: ⌘ 6.8.1.5

Other specs affected: ⌘

Y	N		
X		Other core specifications	TR 31.900
	X	Test specifications	
	X	O&M Specifications	

Other comments: ⌘

***** Begin of Change ****

6.8.1.5 USIM

The USIM shall support UMTS AKA and may support backwards compatibility with the GSM system, which consists of:

Feature 1: GSM cipher key derivation (conversion function c3) to access GSM BSS attached to a R99+ VLR/SGSN using a dual-mode R99+ ME;

Feature 2: GSM AKA to access the GSM BSS attached to a R98- VLR/SGSN or when using R99+ ME not capable of UMTS AKA or R98- ME;

Feature 3: SIM-ME interface (GSM 11.11) to operate within R98- ME or R99+ ME not capable of UMTS AKA.

When the ME provides the USIM with RAND and AUTN, UMTS AKA shall be executed. If the verification of AUTN is successful, the USIM shall respond with the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The USIM shall store CK and IK as current security context data. If the USIM supports access to GSM cipher key derivation (feature 1), the USIM shall also derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK using conversion function c3 and send the derived Kc to the R99+ ME. In case the verification of AUTN is not successful, the USIM shall respond with an appropriate error indication to the R99+ ME.

When the ME provides the USIM with only RAND, and the USIM supports GSM AKA (Feature 2), GSM AKA shall be executed. The USIM first computes the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The USIM then derives the GSM user response SRES and the GSM cipher key Kc using the conversion functions c2 and c3. The USIM then stores the GSM cipher key Kc as the current security context and sends the GSM user response SRES and the GSM cipher key Kc to the ME.

In case the USIM does not support GSM cipher key derivation (Feature 1) or GSM AKA (Feature 2), the R99+ ME shall be informed. An ME with a~~A~~ USIM that does not support GSM cipher key derivation (Feature 1) shall not perform the GSM cipher key derivation (conversion function c3) in the ME and therefore cannot operate in any GSM BSS with 64-bit key ciphering enabled. An ME with a~~A~~ USIM that does not support GSM AKA (Feature 2) cannot operate under a R98- VLR/SGSN. ~~-~~A USIM that does not support GSM AKA (Feature 2) cannot work within ~~or in a both~~ a ~~R99+~~ ME that is not capable of UMTS AKA ~~-~~and cannot work within a~~in~~ R98- ME.

**** end of change ****