3GPP TSG SA WG3 Security — SA3#33 **S3-040216**
10-14 May 2004, Beijing, China

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.220 CR CRNum** ⌘ **rev** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	Introducing the Special-RAND mechanism for GBA_U		
Source:	⌘	Siemens		
Work item code:	⌘	SSC-GBA	***Date:*** ⌘	07/04/2004
Category:	⌘	**B** *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.	***Release:*** ⌘	Rel-6 *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:	⌘	Introducing a special RAND format that tells the UICC to run the key derivation procedures as described by GBA_U (section 5 of TS 33.220)
Summary of change:	⌘	Introducing a special RAND format to securely execute GBA on the UICC
Consequences if not approved:	⌘	UICC based key management for MBMS cannot be based on GBA.

Clauses affected:	⌘	New normative Annex C				
		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

***** BEGIN OF CHANGE *****

Annex C (normative): Structure of the RAND for GBA_U

This section specifies the structure of the special-RAND for GBA_U. A GBA-aware UICC shall recognize the GBA_U special-RAND and perform the key derivations that are described within section 5 and Annex B. An HSS (AuC) that supports GBA_U shall only generate the special-RANDs defined within this Annex C when, for a GBA-aware UICC, an Authentication Vector Request originates from a GBA_U aware BSF.

The ME takes the received RAND unmodified as the input to the authentication and ciphering key generation algorithms A3 and A8.

The structure of special RAND values is the following for GBA_U:

0 31	32 35	36 127
Flag	Context	Non predictable bits

Bit 0 is the most significant bit of RAND and bit 127 is the least significant bit of RAND.

- length of Flag: 32 bits;
- length of Context: 4 bits;
- length of Non predictable bits: 92 bits.

Flag:

In special-RAND values, the flag is set to a particular binary pattern (all 32 bits set to 1) to indicate that bits 32-35 (Context bits) shall be interpreted by the UICC.

Context:

The value 0000 is used for GBA_U.