3GPP TSG SA WG3 Security — S3#17 **S3-010066**

27 February – 2 March, 2001

Gothenburg, Sweden

CR-Form-v3

CHANGE REQUEST

⌘ **33.105 CR ?** ⌘ rev **-** ⌘ Current version: **3.6.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [X] Radio Access Network [X] Core Network [X]

Title:	⌘	Add bit ordering convention
Source:	⌘	Vodafone
Work item code:	⌘	?
Date:	⌘	2001-02-23
Category:	⌘	**F**
Release:	⌘	REL-99

Use one of the following categories:
- ***F*** *(essential 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)*

Reason for change:	⌘	The bit ordering of parameters is ambiguous. Some examples: 1) SQN is defined as a 48-bit string SQN[0]..SQN[47]. In the scheme in section C.1.1.1, SQN = SEQ||IND, and in normal operation the AuC may set SEQhe = SEQ+1. This is ambiguous unless we know which numbered bit is the msb. 2) AUTN = SQN [(+)AK] || AMF || MAC-A, where the component parts are formally defined as arrays of bits numbered from 0. This is ambiguous unless we know whether bit 0 of each array is the leftmost or rightmost bit. 3) COUNT-I is defined as a 32-bit counter COUNT-I[0]..COUNT-I[31] that increments by one for each integrity protected message. That is ambiguous unless we know whether COUNT-I[0] or COUNT-I[31] is the msb.
Summary of change:	⌘	A new section is added to specify the bit ordering convention.
Consequences if not approved:	⌘	Serious risk of protocol breakdown if different manufacturers make different bit ordering assumptions.

Clauses affected:	⌘	3		
Other specs affected:	⌘	[X] Other core specifications [ ] Test specifications [ ] O&M Specifications	⌘	33.102-CR-xxx 33.103-CR-xxx
Other comments:	⌘	The most important thing is to establish a consistent bit ordering; exactly which ordering is chosen is a secondary issue. However, the proposed convention is the one that will allow for the most efficient implementations of the security algorithms designed by ETSI SAGE.		

3 Definitions, symbols, abbreviations and conventions

3.1 Definitions

For the purposes of the present document, the following definitions apply:

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

||	Concatenation
⊕	Exclusive or
f0	random challenge generating function
f1	network authentication function
f1*	the re-synchronisation message authentication function;
f2	user authentication function
f3	cipher key derivation function
f4	integrity key derivation function
f5	anonymity key derivation function for normal operation
f5*	anonymity key derivation function for re-synchronisation
f8	UMTS encryption algorithm
f9	UMTS integrity algorithm

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AK	Anonymity key
AuC	Authentication Centre
AUTN	Authentication token
COUNT-C	Time variant parameter for synchronisation of ciphering
COUNT-I	Time variant parameter for synchronisation of data integrity
CK	Cipher key
IK	Integrity key
IMSI	International Mobile Subscriber Identity
IPR	Intellectual Property Right
MAC	Medium access control (sublayer of Layer 2 in RAN)
MAC	Message authentication code
MAC-A	MAC used for authentication and key agreement
MAC-I	MAC used for data integrity of signalling messages
PDU	Protocol data unit
RAND	Random challenge
RES	User response
RLC	Radio link control (sublayer of Layer 2 in RAN)
RNC	Radio network controller

SDU	Signalling data unit
SQN	Sequence number
UE	User equipment
USIM	User Services Identity Module
XMAC-A	Expected MAC used for authentication and key agreement
XMAC-I	Expected MAC used for data integrity of signalling messages
XRES	Expected user response

3.4 Conventions

All data variables in this specification are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.