Technical Specification Group Services and System Aspects Meeting #11, Palm Springs, CA, USA, 19-22 March 2001

TSGS#11(01)0134

Source: **SA WG3**

Title: **3 Corrective CRs to 33.105 version 3.6.0**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CRs were agreed at SA WG3 meeting #17 and are presented to TSG SA #11 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
33.105	016		R99	Add bit ordering convention	F	3.6.0	S3	S3-17	S3-010066
33.105	017		R99	RES has to be a multiple of 8 bits	F	3.6.0	S3	S3-17	S3-010048
33.105	018		R99	Minimum clock frequency updated	F	3.6.0	S3	S3-17	S3-010111

3GPP TSG-SA WG3 #17 ***Tdoc S3-010048***
Gothenberg, Sweden, 27 Februar- 3 March 2001

CR-Form-v3

CHANGE REQUEST

⌘ **33.105** **CR** **017** ⌘ 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 ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	RES has to be a multiple of 8 bits
Source:	⌘	SA WG3
Work item code:	⌘	Security ***Date:*** ⌘ 19/2/2001
Category:	⌘	**F** ***Release:*** ⌘ R99

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:	⌘	-Other specifications have no protocol-provisions to handle bits for XRES A) TS 29.002 (MAP) specify XRES as OCTET STRING. "XRES **::= OCTET STRING (SIZE (4..16))"** B) TS 24.008 (Mobile Radio layer 3 Specification) specify RES as number of octets. **"**The Authentication Response parameter (extension) IE is a type 4 information element with a minimum length of 3 octets and a maximum length of 14 octets" - All other Authentication Parameters are specified as bits, but match a multiple of 8 bits.
Summary of change:	⌘	RES definition is aligned to 8bits (Octet).
Consequences if not approved:	⌘	TS 29.002 and TS 24.008 have to be adapted to handle bit-variable RES.

Clauses affected:	⌘	5.1.7.8
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

5.1.7.8 RES (or XRES)

RES: the user response

RES[0], RES[1], …, RES[n-1]

The length n of RES and XRES is at most 128 bits and at least 32 bits, and shall be a multiple of 8 bits. RES and XRES constitute to entity authentication of the user to the network.

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

27 February – 2 March, 2001

Gothenburg, Sweden

CR-Form-v3

CHANGE REQUEST

⌘ **33.105 CR 016** ⌘ 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:	⌘	SA WG3
Work item code:	⌘	Security
Date:	⌘	2001-02-23
Category:	⌘	**F**
Release:	⌘	R99

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 ⌘ 33.102-CR 136, 33.103-CR-013
- [ ] Test specifications
- [ ] O&M Specifications

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.

3GPP TSG-SA WG3 #17 ***Tdoc S3-010111***
Gothenberg, Sweden, 27 February- 3 March 2001

CR-Form-v3

CHANGE REQUEST

⌘ **33.105** **CR** **018** ⌘ 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 [ ] Core Network [ ]

Title:	⌘	Minimum clock frequency updated
Source:	⌘	SA WG3
Work item code:	⌘	Security ***Date:*** ⌘ 1/3/2001
Category:	⌘	**F** ***Release:*** ⌘ R99

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:	⌘	Advise from T3 is taken into account
Summary of change:	⌘	Minimum clock frequency used by the terminal during USIM sessions is updated from 3.25 MHz to 3 MHz
Consequences if not approved:	⌘	The requirements for authentication algorithm are a bit too loose.

Clauses affected:	⌘	5.1.5
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

5.1.5 Implementation and operational considerations

The functions f1—f5, f1* and f5* shall be designed so that they can be implemented on an IC card equipped with a 8-bit microprocessor running at 3~~.25~~ MHz with 8 kbyte ROM and 300byte RAM and produce AK, XMAC-A, RES, CK and IK in less than 500 ms execution time.