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

TSGS#11(01)0133

Source: **SA WG3**

Title: **1 Corrective CR to 33.103 version 3.4.0**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CR was agreed at SA WG3 meeting #17 and is presented to TSG SA #11 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
33.103	013		R99	Add bit ordering convention	F	3.4.0	S3	S3-17	S3-010065

3GPP TSG SA WG3 Security — S3#17 **S3-010065**

27 February – 2 March, 2001

Gothenburg, Sweden

CR-Form-v3

CHANGE REQUEST

⌘ **33.103 CR 013** ⌘ rev **-** ⌘ Current version: **3.4.0** ⌘

*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, 33.105-CR 016
- [ ] 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, ~~and~~ abbreviations and conventions

3.1 Definitions

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

Authentication vector: either a quintet or a triplet.

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.

GSM Entity authentication and key agreement: Entity authentication according to GSM 03.20.

GSM security context: a state that is established between a user and a serving network domain usually as a result of the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.

GSM subscriber: a mobile station that consists of user equipment with a SIM inserted.

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.

Mobile station, user: the combination of user equipment and a user access module.

Quintet, UMTS authentication vector: temporary authentication data that enables an MSC/VLR or SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

SIM – GSM Subscriber Identity Module. In a security context, this module is responsible for performing GSM subscriber authentication and key agreement. This module is **not** capable of handling UMTS authentication nor storing UMTS style keys.

Temporary authentication data: either UMTS or GSM security context data or UMTS or GSM authentication vectors.

Triplet, GSM authentication vector: temporary authentication data that enables an MSC/VLR or SGSN to engage in GSM AKA with a particular user. A triplet consists of three elements: a) a network challenge RAND, b) an expected user response SRES and c) a cipher key Kc.

User access module: either a USIM or a SIM

USIM – User Services Identity Module. In a security context, this module is responsible for performing UMTS subscriber and network authentication and key agreement. It should also be capable of performing GSM authentication and key agreement to enable the subscriber to roam easily into a GSM Radio Access Network.

UMTS Entity authentication and key agreement: Entity authentication according to this specification.

UMTS security context: a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI.

UMTS subscriber: a mobile station that consists of user equipment with a USIM inserted.

3.2 Symbols

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

||	Concatenation
⊕	Exclusive or
f1	Message authentication function used to compute MAC
f1*	Message authentication function used to compute MAC-S
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK in normal operation
f5*	Key generating function used to compute AK for re-synchronisation
f6	Encryption function used to encrypt the IMSI
f7	Decryption function used to decrypt the IMSI ($=f6^{-1}$)
f8	Integrity algorithm
f9	Confidentiality algorithm
f10	Deriving function used to compute TEMSI
K	Long-term secret key shared between the USIM and the AuC

3.3 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
$D_{SK(X)}$(data)	Decryption of "data" with Secret Key of X used for signing
$E_{KSXY(i)}$(data)	Encryption of "data" with Symmetric Session Key #i for sending data from X to Y
$E_{PK(X)}$(data)	Encryption of "data" with Public Key of X used for encryption
EMSI	Encrypted Mobile Subscriber Identity
EMSIN	Encrypted MSIN
Hash(data)	The result of applying a collision-resistant one-way hash-function to "data"
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
IV	Initialisation Vector
KAC_X	Key Administration Centre of Network X
KS_{XY}(i)	Symmetric Session Key #i for sending data from X to Y
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAP	Mobile Application Part
MAC	Message Authentication Code
MAC-A	The message authentication code included in AUTN, computed using f1
MS	Mobile Station
MSC	Mobile Services Switching Centre
MSIN	Mobile Station Identity Number
MT	Mobile Termination
NE_X	Network Element of Network X
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier

RAND	Random challenge
RND_X	Unpredictable Random Value generated by X
SQN	Sequence number
SQN_{UIC}	Sequence number user for enhanced user identity confidentiality
SQN_{HE}	Sequence number counter maintained in the HLR/AuC
SQN_{MS}	Sequence number counter maintained in the USIM
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TE	Terminal Equipment
TEMSI	Temporary Encrypted Mobile Subscriber Identity used for paging instead of IMSI
Text1	Optional Data Field
Text2	Optional Data Field
Text3	Public Key algorithm identifier and Public Key Version Number (eventually included in Public Key Certificate)
TMSI	Temporary Mobile Subscriber Identity
TTP	Trusted Third Party
UE	User equipment
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UIDN	User Identity Decryption Node
USIM	User Services Identity Module
VLR	Visitor Location Register
X	Network Identifier
XEMSI	Extended Encrypted Mobile Subscriber Identity
XRES	Expected Response
Y	Network Identifier

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.