Source **TSG-SA WG3**

Title **2 Functional Release 1999 CRs to 33.102**

S3 Tdoc.	Spec.	Ver.	CR	Rev.	Cat.	Rel.	Subject
S3-000261	33.102	3.4.0	089		C	R99	Addition of another variant of sequence number generation
S3-000263	33.102	3.4.0	091		C	R99	Inclusion of the radio bearer identity to the integrity mechanism

3GPP TSG SA WG 3 Security #12
Stockholm, Sweden, 11-14. April 2000

***Document* S3-000261**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102	CR	089	Current Version:	3.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG SA # 8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio	X	Core Network	

Source: SA WG3 **Date:** 9. April 2000

Subject: Addition of another variant of sequence number generation

Work item:

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature	X		Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: The variant is beneficial if more static data base structure in AuC is preferred.

Clauses affected: Annex C

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other GSM core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

Annex C (informative): Management of sequence numbers

This annex is devoted to the management of sequence numbers for the authentication and key agreement protocol.

C.1 Generation of sequence numbers in the Authentication Centre

According to section 6.3 of this specification, authentication vectors are generated in the authentication centre (AuC) using sequence numbers. This section specifies how these sequence numbers are generated. It is taken into account that authentication vectors may be generated and sent by the AuC in batches such that all authentication vectors in one batch are sent to the same SN/VLR.

(1) In its binary representation, the sequence number consists of two concatenated parts $SQN = SEQ \,||\, IND$.
SEQ is the batch number, and *IND* is an index numbering the authentication vectors within one batch. *SEQ* in its turn consists of two concatenated parts $SEQ = SEQ1 \,||\, SEQ2$. *SEQ1* represents the most significant bits of *SEQ*, and *SEQ2* represents the least significant bits of *SEQ*. *IND* represents the least significant bits of *SQN*.
If the concept of batches is not supported then *IND* is void and *SQN* = *SEQ*.

(2) There is a counter SEQ_{HE} in the HE. $SEQ = SEQ1 \,||\, SEQ2$ is stored by this counter. SEQ_{HE} is an individual counter, i.e. there is one per user.

(3) There is a global counter, e.g. a clock giving universal time. For short we call the value of this global counter at any one time *GLC*. If *GLC* is taken from a clock it is computed mod p, where $p = 2^n$ and n is the length of *GLC* and of *SEQ2* in bits.

(4) If *GLC* is taken from a clock then there is a number $D > 0$ such that the following holds:
(i) the time interval between two consecutive increases of the clock (the clock unit) shall be chosen such that, for each user, at most *D* batches are generated at the AuC during any *D* clock units;
(ii) the clock rate shall be significantly higher than the average rate at which batches are generated for any user;
(iii) $D << 2^n$.

(5) When the HE needs new sequence numbers *SQN* to create a new batch of authentication vectors, HE retrieves the (user-specific) value of $SEQ_{HE} = SEQ1_{HE} \,||\, SEQ2_{HE}$ from the database.
(i) If $SEQ2_{HE} < GLC < SEQ2_{HE} + p - D + 1$ then HE sets $SEQ = SEQ1_{HE} \,||\, GLC$;
(ii) if $GLC \le SEQ2_{HE} \le GLC+D - 1$ or $SEQ2_{HE} + p - D + 1 \le GLC$ then HE sets $SEQ = SEQ_{HE} + 1$;
(iii) if $GLC+D - 1 < SEQ2_{HE}$ then HE sets $SEQ = (SEQ1_{HE} + 1) \,||\, GLC$.
(iv) The i-th authentication vector in the batch receives the sequence number $SQN = SEQ \,||\, i$.
(v) After the generation of the first authentication vector in the batch has been completed SEQ_{HE} is reset to *SEQ*.

NOTES

1. The clock unit and the value *D* have to be chosen with care so that condition (4)(i) is satisfied for every user at all times. Otherwise, user identity confidentiality may be compromised. When the parameters are chosen appropriately sequence numbers for a particular user do not reveal significant information about the user's identity. In particular, *IND* is to be sufficiently short so that no unacceptably long contiguous strings of sequence numbers are generated.
   If authentication vectors for the CS and the PS domains are not separated by other means it is recommended to choose $D > 1$ as requests from the two different domains may arrive completely independently.

2. The use of *IND* is only for the benefit of the USIM (see note 4 in Annex C.2). When *D* is chosen sufficiently large then several authentication vectors can be generated at the same time by (5)(ii) even when *IND* is not present.

Another variant of the sequence number generation mechanism is described below.

The part *SEQ* is not divided into two parts. The global counter *GLC* is thus as long as *SEQ*. Instead of storing the individual counter SEQ_{HE} in the HE there is a value *DIF* stored in the HE which is individual for each user. The *DIF* value represents the current difference between generated *SEQ* values for that user and the *GLC*.

When the HE needs new sequence numbers *SQN* to create a new batch of authentication vectors, HE retrieves the (user-specific) value of *DIF* from the data base and calculates *SEQ* values as *SEQ = GLC +DIF*.

The *DIF* value needs to be updated in the HE only during the re-synchronization procedure.

3GPP TSG SA WG 3 Security #12
Stockholm, Sweden, 11-14. April 2000

***Document* S3-000263**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102	CR	091	Current Version:	3.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG SA # 8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio	X	Core Network	

Source: SA WG3 **Date:** 9. April 2000

Subject: Inclusion of the radio bearer identity to the integrity mechanism

Work item:

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature	X		Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: The radio bearer identity has to affect the message authentication code calculated by the integrity algorithm.

Clauses affected: 6.5.4.5

Other specs affected:

Other 3G core specifications	X	→ List of CRs:
Other GSM core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments: Impact upon RAN WG2 specification 25.331.


help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.5.4 Input parameters to the integrity algorithm

6.5.4.1 COUNT-I

The integrity sequence number COUNT-I is 32 bits long.

There is one COUNT-I value per logical signalling channel.

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number is the 4-bit RRC sequence number RRC SN that is available in each RRC PDU. The "long" sequence number is the 28-bit RRC hyperframe number RRC HFN which is incremented at each RRC SN cycle.

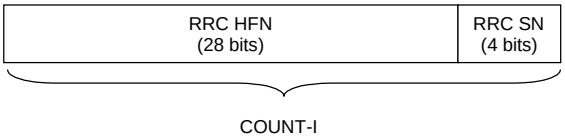

Figure 16a: The structure of COUNT-I

The hyperframe number RRC HFN is initialised by means of the parameter START, which is transmitted from UE to RNC during *RRC connection establishment*. The UE and the RNC then initialise the X most significant bits of the RRC HFN to START; the remaining (28-X) LSB of the RRC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel used for signalling.

Editor's note: The value of X still needs to be added.

Editor's note: The description of how START is managed in the UE needs to be added.

6.5.4.2 IK

The integrity key IK is 128 bits long.

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user. Which integrity key to use for a particular connection is described in 6.5.6.

For UMTS subscribers IK is established during UMTS AKA as the output of the integrity key derivation function f4, that is available in the USIM and in the HLR/AuC. For GSM subscribers, that access the UTRAN, IK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 6.8.2.

IK is stored in the USIM and a copy is stored in the UE. IK is sent from the USIM to the UE upon request of the UE. The USIM shall send IK under the condition that 1) a valid IK is available, 2) the current value of START in the USIM is up-to-date and 3) START has not reached THRESHOLD. The UE shall delete IK from memory after power-off as well as after removal of the USIM.

IK is sent from the HLR/AuC to the VLR or SGSN and stored in the VLR or SGSN as part of a quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) *security mode command*. The MSC/VLR or SGSN shall assure that the IK is updated at least once every 24 hours.

At handover, the IK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed, and the synchronisation procedure is resumed. The IK remains unchanged at handover.

6.5.4.3 FRESH

The network-side nonce FRESH is 32 bits long.

There is one FRESH parameter value per user. The input parameter FRESH protects the network against replay of signalling messages by the user. At connection set-up the RNC generates a random value FRESH and sends it to the user in the (RRC) *security mode command*. The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection. This mechanism assures the network that the user is not replaying any

old MAC-Is.

At handover with relocation of the S-RNC, the new S-RNC generates its own value for the FRESH parameter and sends it in a new *security mode command* to the user.

6.5.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the integrity algorithm used to compute the message authentication codes would use an identical set of input parameter values for the up-link and for the down-link messages.

6.5.4.5 MESSAGE

The signalling message itself with the radio bearer identity. The latter is appended in front of the message. Note that the radio bearer identity is not transmitted with the message but it is needed to avoid that for different instances of message authentication codes the same set of input parameters is used.