3GPP TSG SA WG3 Security — S3#13 **S3-000342**

23-26 May, 2000

Yokohama, Japan

Source: **Nokia**

Title: **CR to 33.105**

Document for: **Approval**

Agenda Item:

This CR is associated with an earlier one to 33.102 (Tdoc S3-000262). Creation was an Action Point given to Nokia in Stockholm meeting S3#12.

3GPP TSG SA WG3#13
Yokohama, Japan, 24-26 May 2000

Document ??99???
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.

33.105 CR Current Version: 3.3.0

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 ☒	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: (U)SIM □ ME ☒ UTRAN / Radio ☒ Core Network □
(at least one should be marked with an X)

Source: SA3 (Security) **Date:** 22 May 2000

Subject: Clarification of BEARER and DIRECTION parameters

Work item: Security

Category:	F	Correction	☒	**Release:** Phase 2	□
	A	Corresponds to a correction in an earlier release	□	Release 96	□
(only one category	B	Addition of feature	□	Release 97	□
shall be marked	C	Functional modification of feature	□	Release 98	□
with an X)	D	Editorial modification	□	Release 99	☒
				Release 00	□

Reason for change: To get 33.105 in line with 33.102. The BEARER parameter cannot be the logical channel identity because that is not unique for one UE; instead the radio bearer identity must be used. Values for the DIRECTION bit have to be defined.

Clauses affected:

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.

5.2.7 Interfaces to the algorithm

5.2.7.1 CK

CK: the cipher key

CK[0], CK[1], …, CK[127]

The length of CK is 128 bits. In case the effective key length k is smaller than 128 bits, the most significant bits of CK shall carry the effective key information, whereas the remaining, least significant bits shall repeat the effective key information:

CK[n] = CK[n mod k], for all n, such that k ≤ n < 128.

5.2.7.2 COUNT-C

COUNT-C: the cipher sequence number.

COUNT-C[0], COUNT-C[1], …, COUNT-C[31]

The length of the COUNT-C parameter is 32 bits.

Sychronisation of the keystream is based on the use of a physical layer (Layer 1) frame counter combined with a hyperframe counter introduced to avoid re-use of the keystream. This allows the keystream to be synchronised every 10ms physical layer frame. The exact structure of the COUNT-C is specified in TS 33.102.

5.2.7.3 BEARER

BEARER: the radio bearer identifier.

BEARER[0], BEARER[1], …, BEARER[4~~3~~]

The length of BEARER is 5~~4~~ bits.

The same cipher key may be used for different radio bearers simultaneously associated with a single user which are multiplexed onto a single 10ms physical layer frame. To avoid using the same keystream to encrypt more than one bearer, the algorithm shall generate the keystream based on the identity of the radio bearer.

5.2.7.4 DIRECTION

DIRECTION: the direction of transmission of the bearer to be encrypted.

DIRECTION[0]

The length of DIRECTION is 1 bit.

The same cipher key may be used for uplink and downlink channels simultaneously associated with a UE, which are multiplexed onto a single 10ms physical layer frame. To avoid using the same keystream to encrypt both uplink and downlink transmissions, the algorithm shall generate the keystream based on the direction of transmission.

The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

An explicit direction value is required in preference to splitting the keystream segment into uplink and downlink portions to allow for asymmetric bearer services.

5.2.7.5 LENGTH

LENGTH: the required length of keystream.

LENGTH[0], LENGTH[1], …, LENGTH[15]

The length of LENGTH is 16 bits.

For a given bearer and transmission direction the length of the plaintext block that is transmitted during a single physical layer frame may vary. The algorithm shall generate a keystream block of variable length based on the value of the length parameter.

The input parameter LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

The format of LENGTH cannot be specified at present since the number and sizes of RLC PDUs / MAC SDUs in each 10ms physical layer frame have not yet been fully specified. However, a maximum RLC PDU / MAC SDU size in the region of 1000 bits has been informally indicated by 3GPP TSG RAN2. The range of values of the length parameter will depend not only on the RLC PDU / MAC SDU size but also the number of RLC PDUs / MAC SDUs which may be sent in a single physical layer 10ms frame for a given bearer and transmission direction.

Not all values between the maximum and minimum values shall be required but it is expected that the ability to produce length values of whole numbers of octets between a minimum and a maximum value will be required.

5.2.7.6 KEYSTREAM

KEYSTREAM: the output keystream.

KS [0], KS [1], …, KS [LENGTH-1]

The length of a keystream block equals the value of the input parameter LENGTH.

5.2.7.7 PLAINTEXT

PLAINTEXT: the plaintext.

PT[0], PT[1], …, PT[LENGTH-1]

The length of a keystream block equals the value of the input parameter LENGTH.

This plaintext block consists of the payload of the particular RLC PDUs / MAC SDUs to be encrypted in a single 10ms physical layer frame for a given bearer and transmission direction. It may consist of user traffic or signalling data. The structure of the plaintext block cannot be specified at present.

5.2.7.8 CIPHERTEXT

CIPHERTEXT: the ciphertext.

CT[0], CT[1], …, CT[LENGTH-1]

The length of a keystream block equals the value of the input parameter LENGTH.

5.3 Data integrity

5.3.1 Overview

The mechanism for data integrity of signalling data that is described in 6.6 of [1] requires the following cryptographic function:

f9 UMTS integrity algorithm.

Figure 3 illustrates the use of the function f9 to derive a MAC-I from a signalling message.

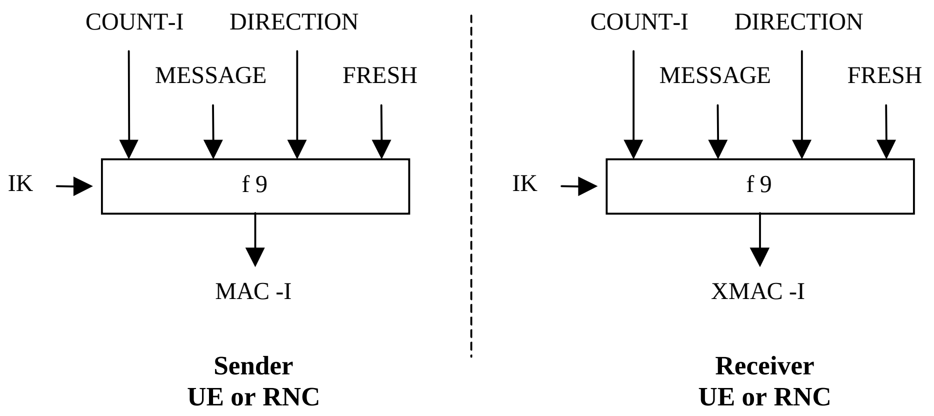

Figure 1~~2~~: Derivation of MAC-I (or XMAC-I) on a signalling message

The input parameters to the algorithm are the Integrity Key (IK), a time dependent input (COUNT-I), a random value generated by the network side (FRESH), the direction bit (DIRECTION) and the signalling data (MESSAGE). Based on these input parameters the user computes with the function f9 the message authentication code for data integrity (MAC-I) which is appended to the message when sent over the radio access link. The receiver computes XMAC-I on the messages received in the same way as the sender computed MAC-I on the message sent.

5.3.2 Use

The MAC function f9 shall be used to authenticate the data integrity and data origin of signalling data transmitted between UE and RNC.

5.3.3 Allocation

The MAC function f9 is allocated to the UE and the RNC.

Integrity protection shall be applied at the RRC layer.

5.3.4 Extent of standardisation

The function f9 is fully standardized.

5.3.5 Implementation and operational considerations

The algorithm should be designed to accommodate a range of implementation options including hardware and software implementations.

5.3.6 Type of algorithm

The function f9 shall be a MAC function.

5.3.7 Interface

5.3.7.1 IK

IK: the integrity key

IK[0], IK[1], …, IK[127]

The length of IK is 128 bits.

5.3.7.2 COUNT-I

COUNT-I: a frame dependent input.

COUNT-I[0], COUNT-I[1], …, COUNT-I[31]

The length of COUNT-I is 32 bits.

The input parameter COUNT-I protects against replay during a connection. It is a value incremented by one for each integrity protected message. COUNT-I consists of two parts: the HYPERFRAME NUMBER (HFN) as the most significant part and a RRC Sequence Number as the least significant part. The initial value of the hyperframe number is sent by the user to the network at connection set-up. The user stores the greatest used hyperframe number from the previous connection and increments it by one. In this way the user is assured that no COUNT-I value is re-used (by the network) with the same integrity key.

5.3.7.3 FRESH

FRESH: a random number generated by the RNC.

FRESH[0], FRESH[1], …, FRESH[31]

The length of FRESH is 32 bits.

The same integrity key may be used for several consecutive connections. This FRESH value is an input to the algorithm in order to assure the network side that the user is not replaying old MAC-Is.

5.3.7.4 MESSAGE

MESSAGE: the signalling data.

MESSAGE[0], MESSAGE[1], …, MESSAGE[X19-1]

The maximum length of MESSAGE is X19.

5.3.7.5 DIRECTION

DIRECTION: the direction of transmission of signalling messages (user to network or network to users).

DIRECTION[0]

The length of DIRECTION is 1 bit.

The same integrity key may be used for uplink and downlink channels simultaneously associated with a UE.

The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

5.3.7.6 MAC-I (and equivalently XMAC-I)

MAC-I: the message authentication code for data integrity authentication

MAC-I[0], MAC-I[1], …, MAC-I[31]

The length of MAC-I is 32 bits.