3GPP TSG SA #6 **Tdoc TSG SA SP-99587**
Nice, FRANCE
15th - 17th December 1999

Source: TSG SA WG3

Subject: R99 CRs to 33.105
Agenda item: 5.3.3

This document contains CRs to 33.105 version 3.1.0 agreed by SA WG3 to be presented to SA#6 for approval.

CR	REV	CAT	SUBJECT	WG_DOC	3G_PHASE
004		D	Time variant parameter for synchronisation of ciphering	S3-99384	99
005		D	Direction bit in f9	S3-99455	99

DRAFT 3G CHANGE REQUEST

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

TS 33.105	**CR**	**004**	Current Version:	V3.1.0

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG	SA#6	for approval	X	*(only one box should*
list TSG meeting no. here ↑		for information		*be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

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

Source:	TSG SA WG3	**Date:**	99-10-27
Subject:	Time variant parameter for synchronisation of ciphering		
3G Work item:	Security		

Category:	F	Correction	
	A	Corresponds to a correction in a 2G specification	
(only one category	B	Addition of feature	
shall be marked	C	Functional modification of feature	
with an X)	D	Editorial modification	X

Reason for change: On the algorithms for both data confidentiality and data integrity, one of input parameters is COUNT, a time variant parameter for synchronisation. Due to progress in TSG S3, it is better to use a time variant parameter separately in order to improve security. A time variant parameter used for ciphering is renamed COUNT-C.

Clauses affected: 3.3, 5.2.1, 5.2.7.2

Other specs affected:			
	Other 3G core specifications		→ List of CRs:
	Other 2G 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:

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
CK	Cipher key
COUNT-C	Time variant parameter for synchronisation of ciphering
COUNT-I	Time variant parameter for synchronisation of data integrity
EMUI	Encrypted Mobile User Identity
GK	User group key
IK	Integrity key
IMUI	International Mobile User 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
SEQ_UIC	Sequence for user identity confidentiality
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

5.2 Data confidentiality

5.2.1 Overview

The mechanism for data confidentiality of user data and signalling data that is described in 6.4 of [1] requires the following cryptographic function:

f8 UMTS encryption algorithm.

Figure 2 illustrates the use of f8 to encrypt plaintext by applying a keystream using a bitwise XOR operation. The plaintext may be recovered by generating the same keystream using the same input parameters and applying it to the ciphertext using a bitwise XOR operation.

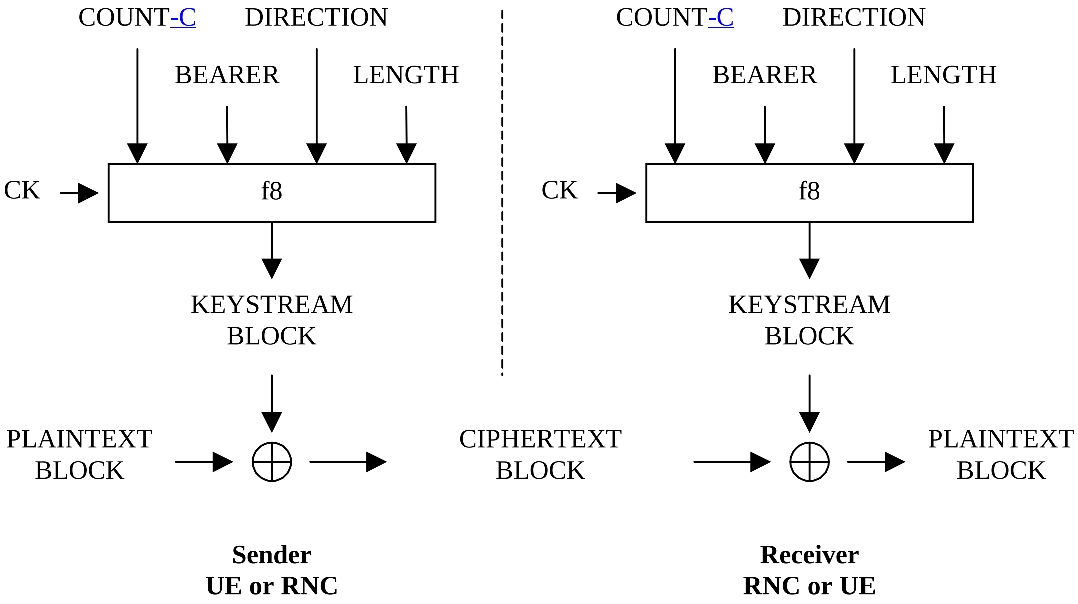

Figure 2: Ciphering user and signalling data transmitted over the radio access link

The input parameters to the algorithm are the Cipher Key (CK), a time dependent input (COUNT-C), the bearer identity (BEARER), the direction of transmission (DIRECTION) and the length of the keystream required (LENGTH). Based on these input parameters the algorithm generates the output keystream block (KEYSTREAM) which is used to encrypt the input plaintext block (PLAINTEXT) to produce the output ciphertext block (CIPHERTEXT).

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

5.2.7.2 COUNT-C

COUNT-C: a time dependent input.

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

The length of the COUNT-C parameter is 32 bits. It is assumed that sychronisation of the keystream will be 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 parameter cannot be specified at present. However, it is assumed to be a 32 bit counter.

Technical Specification Group Services and System Aspects ***S3-99455***
Meeting #5,

TSG SA WG3 #58, Sophia Antipolis, 16-19 November, 1999

DRAFT 3G CHANGE REQUEST

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

TS 33.105 CR 005 Current Version: V3.1.0

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG	SA#5	for approval	X	*(only one box should*
list TSG meeting no. here ↑		for information		*be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects:	USIM		ME	X	UTRAN	X	Core Network	

(at least one should be marked with an X)

Source:	TSG SA WG3	**Date:**	99-11-19
Subject:	Direction bit in f9		
3G Work item:	Security		

Category:	F	Correction	
	A	Corresponds to a correction in a 2G specification	
(only one category	B	Addition of feature	
shall be marked	C	Functional modification of feature	
with an X)	D	Editorial modification	X

Reason for change:	The direction bit as input for f9 has been agreed in an earlier CR. The direction bit should also be shown in the figure 3 as well.
Clauses affected:	5.3.1

Other specs affected:	Other 3G core specifications		→ List of CRs:
	Other 2G 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:	

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

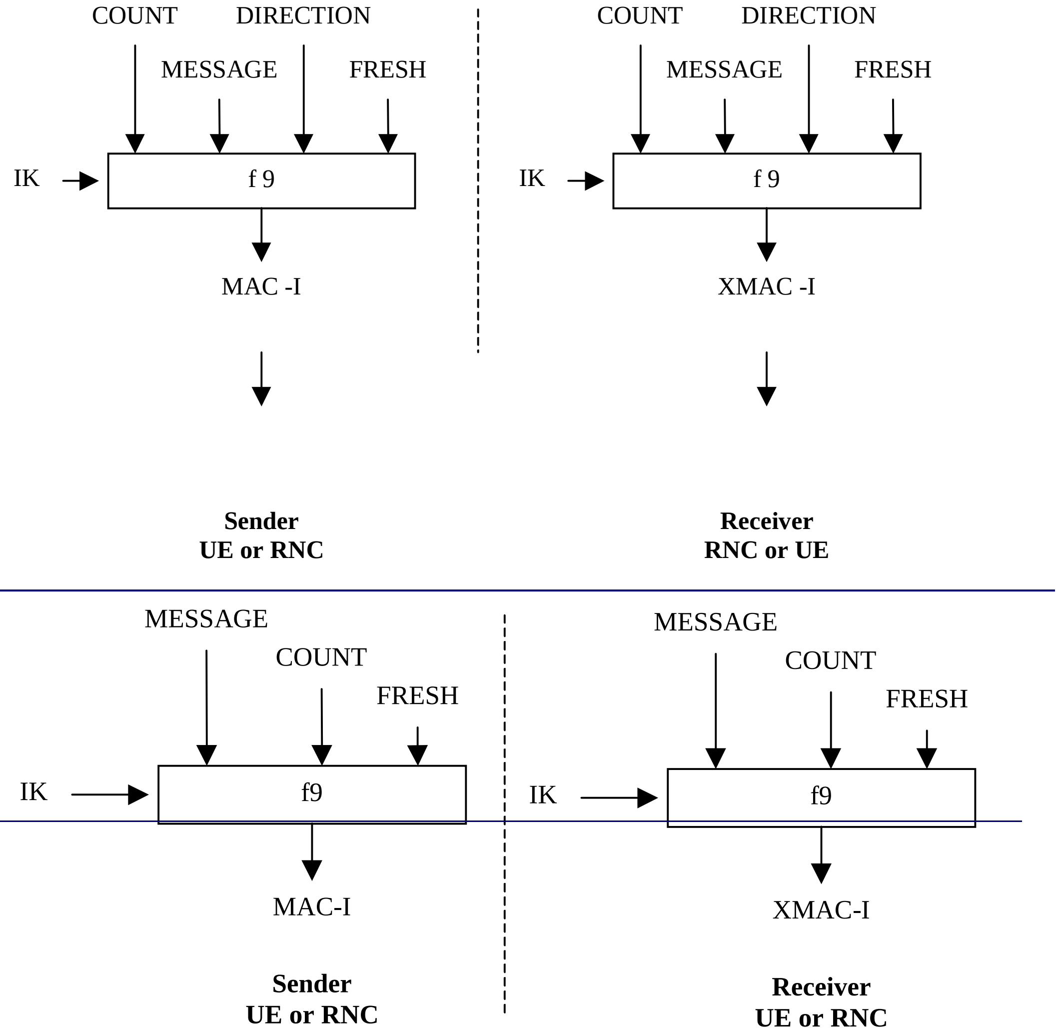

Figure 1: Derivation of MAC-I (or XMAC-I) on a signalling message

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.

The exact position of MAC algorithm in the radio network architecture has not yet been fully specified. The current working assumption is that it will be closely integrated with the ciphering algorithm.

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. In case the effective key length should need to be made smaller than 128 bits, the most significant bits of IK shall carry the effective key information, whereas the remaining, least significant bits shall be set zero.

5.3.7.2 COUNT-I

COUNT-I: a frame dependent input.

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

The keystream should be initialised with a time dependent input parameter.

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. The length of COUNT-I parameter is assumed to be 32 bits.

5.3.7.3 FRESH

FRESH: a random number generated by the RNC.

FRESH[0], FRESH[1], …, FRESH[31]

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.

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.