TSG SA #5, Kyongju, 11-13 Oct. 1999 ***TSGS#5(99)418***

Source: S3
Subject: CRs to 33.105 for approval

CR	to version	topic	in S3 Tdoc	agreed at	CAT
33.105-001	3.0.0	Resources for cryptographic algorithms in the USIM	S3-99335	S3#6	C
33.105-002	3.0.0	MAC used for data integrity of signalling messages	S3-99337	S3#6	C
33.105-003	3.0.0	Cipher keystream block length	S3-99301	correspondence between S3#5 and S3#6	C

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** **001** Current Version: V3.0.0

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

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

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 [X] ME [ ] UTRAN [ ] Core Network [ ]
(at least one should be marked with an X)

Source: TSG SA WG3 **Date:** 99-10-01

Subject: Resources for cryptographic algorithms in the USIM

3G Work item: Security

Category:

F	Correction	[ ]
A	Corresponds to a correction in a 2G specification	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[X]
D	Editorial modification	[ ]

(only one category shall be marked with an X)

Reason for change: Due to progress in TSG T WG3, additional information is available on the resources for cryptographic algorithms in the USIM. This information gives the requirements to design authentication and key agreement algorithms (f0 – f5).

Clauses affected: 5.1.5

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:

5.1.5 Implementation and operational considerations

The functions f1—f5 and f1* shall be designed so that they can be implemented on an IC card equipped with a 8~~X1~~-bit microprocessor running at 3.25~~X2~~ MHz with 8 kbyte ROM and 300byte RAM~~X3 kbits of memory~~ and produce AK, MAC-A, ~~and~~ RES ~~in less than 500X4 ms , and~~ CK and IK in less than 500~~X5~~ ms execution time.

~~The functions f0—f5 and f1* shall be designed so that they can be implemented either in software or in hardware in the AuC on a X6-bit microprocessor running at X7 MHz and with X8 kbits of memory and produce MAC-A, XRES, CK, IK and AK in less than X9 ms.~~

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** **002** Current Version: V3.0.0

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

For submission to TSG SA#5 for approval [X]
list TSG meeting no. here ↑ for information [ ]
(only one box should 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:** 99-10-01

Subject: MAC used for data integrity of signalling messages

3G Work item: Security

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

F	Correction	
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	X
D	Editorial modification	

Reason for change: In order to prove data integrity of signalling messages, the ETSI SAGE 3GPP Algorithms Task Force has recommended that “direction bit” is introduced and the length of MAC-I (MAC used for data integrity of signalling messages) is increased from 24 bits to 32 bits.

Clauses affected: 5.3

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

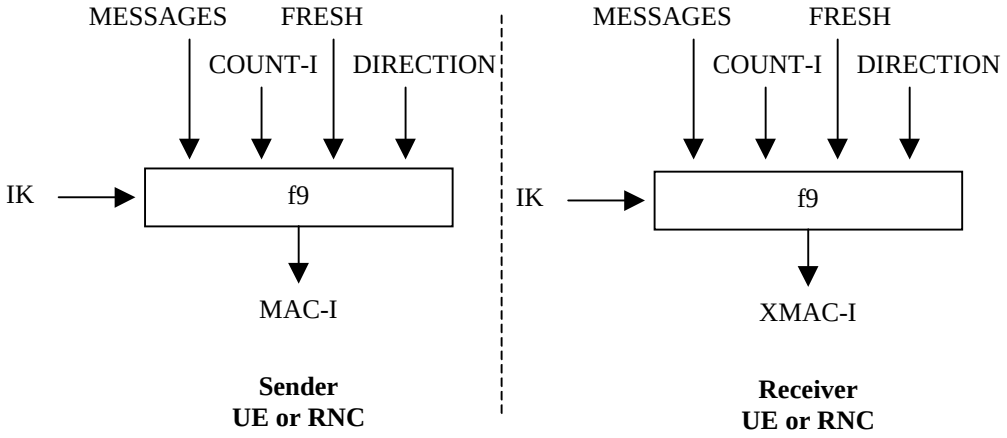

Figure 1: Derivation of MAC-I (or XMAC-I) on a signalling message

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. ~~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 parameter cannot be specified at present. However,~~ The length of COUNT-I parameter~~it~~ is assumed to be ~~a~~ 32 bit~~s counter~~.

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~~5~~ 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~~X20-1~~]

The length of MAC-I is 32 ~~24~~ bits.

Technical Specification Group Services and System Aspects Meeting #5, ***S3-99301***

TSG SA WG3 #5, Sophia Antipolis, 3-6 August, 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** **003** Current Version: V3.0.0

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

For submission to TSG SA#5 *list TSG meeting no. here ↑* for approval [X] for information [ ] *(only one box should 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:** 99-08-03

Subject: Cipher keystream block length

3G Work item: Security

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

F	Correction	[ ]
A	Corresponds to a correction in a 2G specification	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[X]
D	Editorial modification	[ ]

Reason for change: Due to progress in TSG R2, additional information is available on the size of keystream blocks to be generated each physical layer, UM RLC or AM RLC frame. Information is also available on the minimum size of RLC frames (the size of physical layer frames was already given). This extra information allows more details to be provided on implementation and operational considerations regarding the encryption algorithm and on the specification of the LENGTH parameter.

Clauses affected: 5.2.5, 5.2.7.5

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:

5.2.5 Implementation and operational considerations

The algorithm should be designed to accommodate a range of implementation options including hardware and software implementations. For hardware implementations, it should be possible to implement one instance of the algorithm using less than 10,000 gates (working assumption).

A wide range of UE with different bearer capabilities is expected, so the encryption throughput requirements on the algorithm will vary depending on the implementation. However, based on the likely maximum user traffic data rates, it must be possible to implement the algorithm to achieve an encryption speed in the order of 2Mbit/s on the downlink and on the uplink.

~~The exact throughput requirements will depend on the RLC PDU / MAC SDU size and the number of RLC PDUs / MAC SDUs which may be sent in a single physical layer 10ms frame. In addition, within each 10ms frame, the algorithm will need to be reinitialised (or reinstantiated) for each different bearer and for each transmission direction.~~

For each mode of encryption the following parameters are given:

1. RLC-transparent mode:
   - New keystream block required every physical layer frame (10ms)
   - Maximum number of bits per physical layer frame of 5114 bits
   - Minimum number of bits per physical layer frame of 1 bit.
   - Granularity of 1 bit on all possible intermediate values
2. For UM RLC mode:
   - New keystream block required every RLC frame (minimum 156µs)
   - Maximum number of bits per UM RLC frame of 1016 bits (ongoing specification work in TSG-R2 could extend this to 5000 bits)
   - Minimum number of bits per UM RLC frame of 16 bit.
   - Granularity of 8 bit on all possible intermediate values
3. For AM RLC mode:
   - New keystream block required every RLC frame (minimum 156µs)
   - Maximum number of bits per AM RLC frame of 1024 bits (ongoing specification work in TSG-R2 could extend this to 5000 bits)
   - Minimum number of bits per AM RLC frame of 24 bit.
   - Granularity of 8 bit on all possible intermediate values

The encryption throughput requirements should be met based on clock speeds upwards of 20MHz (typical clock speeds are expected to be much greater than this).

5.2.7.5 LENGTH

LENGTH: the required length of keystream.
LENGTH[0], LENGTH[1], …, LENGTH[X18-1]

The length of LENGTH is X18 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.~~

LENGTH shall be able to specify the required number of bits in each keystream block according to the parameters defined in section 5.2.5. Where the required granularity cannot be achieved with the specified LENGTH parameter size, a larger keystream block may be generated and unused bits discarded.