Technical Specification Group Services and System Aspects **TSGS#19(03)0070**

Meeting #19, Birmingham, UK, 17-20 March 2003

3GPP TSG SA WG3 Security — S3#27 S3-030136

25 - 28 February 2003

Sophia Antipolis, France

Title: **LS to SA on back up algorithms for UTRAN**

Response to:

Source: **SA3**

To: **TSG SA**

Cc:

Contact Person:
Name: **Per Christoffersson**
Tel. Number: **+46 705925100**
E-mail Address: **per.e.christoffersson@telia.se**

Attachments: **S3-030085, S3-030135**

1 Introduction

In SA meeting #18 the concept of second UMTS encryption and integrity protection algorithms (UEA2 and UIA2) for backup purposes was introduced (TD SP-020812). The principle of creating backup algorithms was agreed by SA.

SA WG3 was then asked to provide figures for the expected funding costs and to inform TSG SA whether a mandatory implementation date for the new algorithms was intended, and if so, the expected timing for this. This LS is the response to SA on this topic.

2 SA 3 decisions

In the SA3 meeting #27 a provisional work plan (TD S3-030085) for a SAGE-led Task Force was presented. It indicates a 7-10 months working period. The shorter period is envisaged if no external evaluation of the resulting algorithms is considered to be needed (e.g. because sufficient confidence has been attained by other means). The extended period is needed in case external evaluation is deemed necessary. Start of work is possible already in March 2003

SA3 approved the work plan at the meeting. At the same time a Requirement Specification was agreed and sent to ETSI SAGE (TD S3-030135).

SA3 did not take a position on the need for an external evaluation at this meeting but chose to wait for the results from the SAGE Task Force and a recommendation from SAGE as to if external evaluation should be needed.

The budget for the work is estimated to be 16 MM (man months) in case of no external evaluation. To cater for an eventual external evaluation a further budget of 4 MM should be reserved.

SA3 has not yet discussed possible implementation dates for the new algorithms.

3 Proposed action by SA

SA is asked to allocate the requested budget.

4 Next SA3 Meetings

Meeting	Date	Location
SA3#28	06-09 May 2003	Berlin, Germany
SA3#29	15-18 July 2003	San Francisco, USA

3GPP TSG SA WG3 Security — S3#27 **S3-030085**

25. – 28. November 2002

Sophia Antipolis, France

Source: **Vodafone**
Title: **Requirements list for UEA2 and UIA2**
Document for: **Approval**
Agenda Item: **6.5**

---

1. Introduction

SA plenary #18 has agreed the principle to create new encryption and integrity protection algorithms as a backup (see S3-030003, section 7.3.2). This contribution contains a list of draft requirements for these new algorithms. A provisional workplan for the algorithm design and evaluation is provided in a separate contribution to SA3#27 (S3-03xxxx).

SA3 is kindly requested to review the requirements list and to send the final approved version to ETSI SAGE.

2. Requirements list

The encryption and integrity protection algorithms (UEA2/UIA2) shall comply with the following requirements:

2.1 Technical requirements

The algorithms shall fulfil the requirements listed in 3GPP TS 33.105 V4.1.0 section 5.2 and 5.3 (see Annex A).

Note: The requirements on implementation complexity in TS 33.105 section 5.2.5 need to be reviewed. In particular, new requirements are required regarding gate count (currently 10000), maximum bit rate (currently 2Mbit/s) and clock speed (currently 20MHz). Guidance is needed from manufacturers regarding implementation complexity. Furthermore rather than list gate count, bit rate and clock speed separately it may be more useful to indicate a example combination of gate count, bit rate and clock speed which should be achieved. This allows for other implementations which support the same bit rate with lower gate count and higher clock speed, for example.

2.2 Design and evaluation principles

The algorithms should be designed with a view to their continued use for a period of at least 20 years. Successful attacks with a work load significantly less than exhaustive key search through the effective key space should be impossible.

In addition the cryptographic foundations of the algorithms shall be different from KASUMI, so that it is unlikely that a successful attack against UEA1/UIA1 can be applied to UEA2/UIA2 (and vice versa).

If possible the algorithms should be based on existing (well analysed) algorithms.

The algorithms shall be openly published for public scrutiny.

It may be required to have a number of independent and qualified parties evaluate the strength of the algorithms prior to publication. This will be particularly important if the algorithms are not based on existing (well analysed) algorithms. A final decision on this will be made by SA3 with guidance from SAGE.

2.3 World-wide availability and use

Legal restrictions on the use or export of equipment containing cryptographic functions may prevent the use of such equipment in certain countries.

It is the intention that UEs which embody such algorithms should be free from restrictions on export or use, in order to allow the free circulation of 3G terminals. Network equipment, including RNC, may be expected to come under more stringent restrictions. It is the intention is that RNCs which embody such algorithms should be exportable under the conditions of the Wassenaar Arrangement.

2.4 Ownership

The algorithms and all copyright and IPR to the algorithms and test data specifications shall be owned exclusively by 3GPP. It is desirable that the algorithm will be free of intellectual property considerations to aid free distribution.

2.5 Documentation

The designer of the algorithms shall provide reports similar to 33.201 – 33.204 and 33.908.

Annex A: Excerpt from 33.105 V 4.1.0

5.2 Data confidentiality

5.2.1 Overview

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

f8 UMTS encryption algorithm.

Figure 1 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.

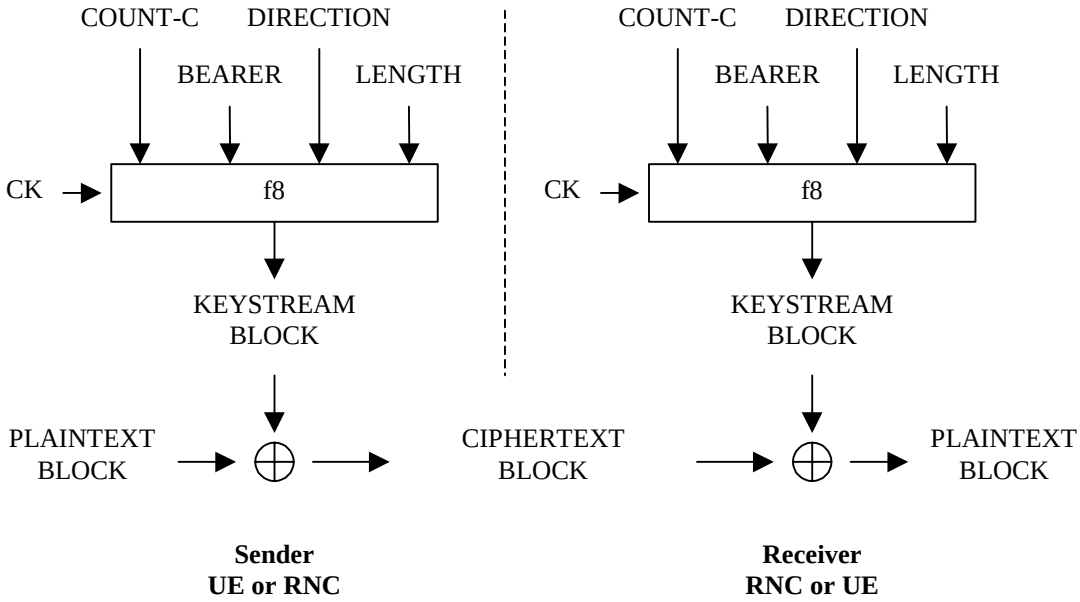

Figure 1: Ciphering user and signalling data transmitted over the radio access link

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.

5.2.2 Use

The function f8 shall only be used to protect the confidentiality of user data and signalling data sent over the radio access link between UE and RNC.

5.2.3 Allocation

The function f8 is allocated to the UE and the RNC.
Encryption will be applied in the Medium Access Control (MAC) sublayer and in the Radio Link Control (RLC) sublayer of the data link layer (Layer 2).

5.2.4 Extent of standardisation

The function f8 shall be fully standardized.

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.

1. RLC-transparent mode:
   - New keystream block required every physical layer frame (10ms)
   - Maximum number of bits per physical layer frame of 20000 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 per UMD PDU
   - Maximum number of bits in UMD PDU is 5000 bits
   - Minimum number of bits in UMD PDU is 16 bits
   - Granularity of 8 bit on all possible intermediate values.
3. For AM RLC mode:
   - New keystream block required per AMD PDU
   - Maximum number of bits in AMD PDU is 5000 bits
   - Minimum number of bits in AMD PDU is 24 bits
   - 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).

5.2.6 Type of algorithm

The function f8 should be a symmetric synchronous stream cipher.

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:

$CK[n] = CK[n \bmod k]$, for all n, such that $k \leq n < 128$.

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]

The length of BEARER is 5 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 maximum RLC PDU / MAC SDU size is 5000 bits. 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 for a given bearer and transmission direction. It may consist of user traffic or signalling data:

- For RLC UM mode, the plaintext block is the UMD PDU excluding the first octet, i.e. excluding the RLC UM PDU header (see TS 25.322 [19]).
- For RLC AM mode, the plaintext block is the AMD PDU excluding the two first octets, i.e. excluding the RLC AM PDU header (see TS 25.322 [19]).
- For RLC TM on DCH, the plaintext block consists of all the MAC SDUs containing data for one and the same radio bearer and sent in one Transmission Time Interval. In this case, the CFN part of COUNT-C for the plaintext block is the CFN for the first radio frame of the Transmission Time Interval containing the plaintext block. (see TS 25.321 [18]).

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.

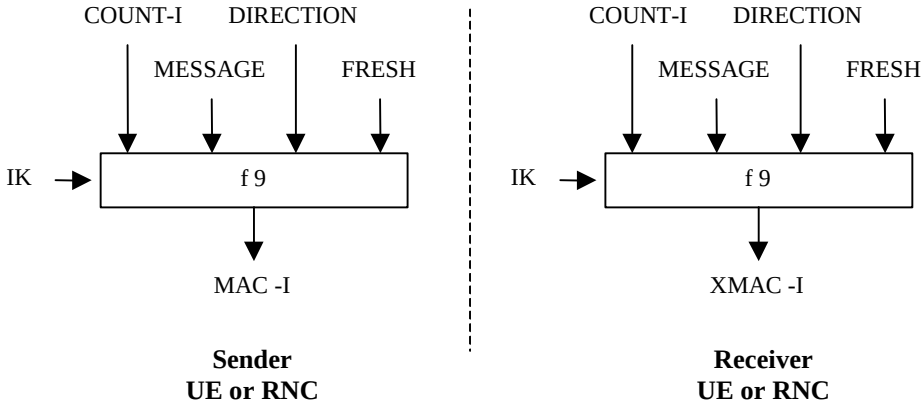

Figure 2: Derivation of MAC-I (or XMAC-I) on a signalling message

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[X-1]

The length of MESSAGE is X.

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.

3GPP TSG SA WG3 Security — S3#27 **S3-030135**
25 - 28 February 2003
Sophia Antipolis, France

Title: **LS on Requirements list for UEA2 and UIA2**
Response to:
Release:
Work Item:

Source: **TSG SA3**
To: **ETSI SAGE**
Cc:

Contact Person:
Name: Benno Tietz
Tel. Number: +49 211 533 2168
E-mail Address: benno.tietz@vodafone.com

Attachments: UEA2UIA2_requirements_list.doc

---

1. Overall Description:

The attached requirement list for UEA2 and UIA2 has been agreed at SA3-#27. The values for the maximal gate count and the clock speed will be provided by the next SA3 meeting. Members of 3GPP2 have offered usage of their corresponding algorithms as input for the ETSI SAGE's work. Also the workplan has been approved by SA3.

2. Actions:

To ETSI SAGE

ACTION: ETSI SAGE is kindly asked to start the work as soon as the funding has been granted by TSG SA.

3. Date of Next TSG-SA3 Meetings:

TSG-SA3 Meeting #28	6th – 9th May 03	Berlin, Germany.
TSG-SA3 Meeting #29	15th – 18th July 2003	San Francisco, USA
TSG-SA3 Meeting #30	7th – 10th October 2003	Italy (tbc)
TSG SA Plenary # 19	17th - 20th March 2003	Birmingham, UK

Requirement List for UEA2/UIA2

1.1 Technical requirements

The algorithms shall fulfil the requirements listed in 3GPP TS 33.105 V4.1.0 section 5.2 and 5.3 (see Annex A).

Differing from the above mentioned specification the maximal bit rate is 10 Mbit/s (formerly 2 Mbit/s). The requirements on gate count and clock speed are currently under investigation and will be fixed by SA3#28.

1.2 Design and evaluation principles

The algorithms should be designed with a view to their continued use for a period of at least 20 years. Successful attacks with a work load significantly less than exhaustive key search through the effective key space should be impossible.

In addition the cryptographic foundations of the algorithms shall be different from KASUMI, so that it is unlikely that a successful attack against UEA1/UIA1 can be applied to UEA2/UIA2 (and vice versa).

If possible the algorithms should be based on existing (well analysed) algorithms.

The algorithms shall be openly published for public scrutiny.

It may be required to have a number of independent and qualified parties evaluate the strength of the algorithms prior to publication. This will be particularly important if the algorithms are not based on existing (well analysed) algorithms. A final decision on this will be made by SA3 with guidance from SAGE.

1.3 World-wide availability and use

Legal restrictions on the use or export of equipment containing cryptographic functions may prevent the use of such equipment in certain countries.

It is the intention that UEs which embody such algorithms should be free from restrictions on export or use, in order to allow the free circulation of 3G terminals. Network equipment, including RNC, may be expected to come under more stringent restrictions. It is the intention is that RNCs which embody such algorithms should be exportable under the conditions of the Wassenaar Arrangement.

1.4 Ownership

It is desirable that the algorithms and all copyright and IPR to the algorithms and test data specifications are owned exclusively by 3GPP or that the algorithms will be free of intellectual property considerations to aid free distribution.

1.5 Documentation

The designer of the algorithms shall provide reports similar to 33.201 – 33.204 and 33.908.

Annex A: Excerpt from 33.105 V 4.1.0

5.2 Data confidentiality

5.2.1 Overview

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

f8 UMTS encryption algorithm.

Figure 1 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.

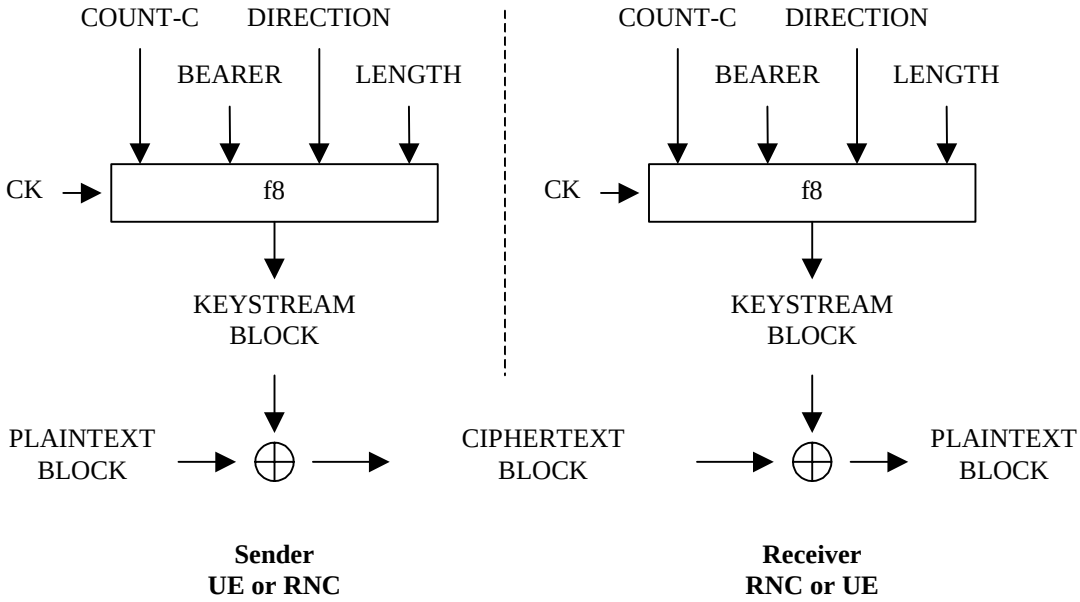

Figure 1: Ciphering user and signalling data transmitted over the radio access link

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.

5.2.2 Use

The function f8 shall only be used to protect the confidentiality of user data and signalling data sent over the radio access link between UE and RNC.

5.2.3 Allocation

The function f8 is allocated to the UE and the RNC.
Encryption will be applied in the Medium Access Control (MAC) sublayer and in the Radio Link Control (RLC) sublayer of the data link layer (Layer 2).

5.2.4 Extent of standardisation

The function f8 shall be fully standardized.

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.

1. RLC-transparent mode:
   - New keystream block required every physical layer frame (10ms)
   - Maximum number of bits per physical layer frame of 20000 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 per UMD PDU
   - Maximum number of bits in UMD PDU is 5000 bits
   - Minimum number of bits in UMD PDU is 16 bits
   - Granularity of 8 bit on all possible intermediate values.
3. For AM RLC mode:
   - New keystream block required per AMD PDU
   - Maximum number of bits in AMD PDU is 5000 bits
   - Minimum number of bits in AMD PDU is 24 bits
   - 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).

5.2.6 Type of algorithm

The function f8 should be a symmetric synchronous stream cipher.

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:

$CK[n] = CK[n \bmod k]$, for all n, such that $k \leq n < 128$.

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]

The length of BEARER is 5 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 maximum RLC PDU / MAC SDU size is 5000 bits. 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 for a given bearer and transmission direction. It may consist of user traffic or signalling data:

- For RLC UM mode, the plaintext block is the UMD PDU excluding the first octet, i.e. excluding the RLC UM PDU header (see TS 25.322 [19]).
- For RLC AM mode, the plaintext block is the AMD PDU excluding the two first octets, i.e. excluding the RLC AM PDU header (see TS 25.322 [19]).
- For RLC TM on DCH, the plaintext block consists of all the MAC SDUs containing data for one and the same radio bearer and sent in one Transmission Time Interval. In this case, the CFN part of COUNT-C for the plaintext block is the CFN for the first radio frame of the Transmission Time Interval containing the plaintext block. (see TS 25.321 [18]).

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.

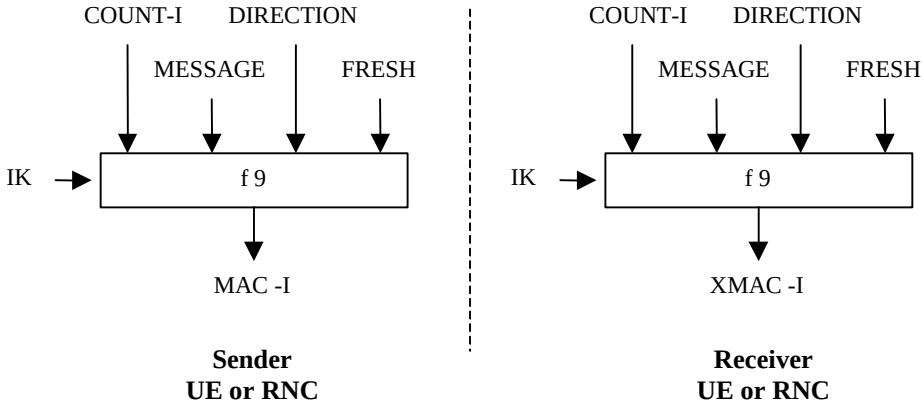

Figure 2: Derivation of MAC-I (or XMAC-I) on a signalling message

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[X-1]

The length of MESSAGE is X.

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.