3GPP TSG SA WG3 Security — S3#26 **S3-020648**

19 – 22 November 2002

Oxford, UK

Source: **Vodafone**

Title: **Introduction of a second UMTS encryption and integrity protection algorithm**

Document for: **Discussion and decision**

Agenda Item: **tbd**

1. Introduction

As the past has taught us (e.g. GEA2) the deployment of a new encryption (and integrity protection) algorithm into the networks and the handsets takes some years (from the very beginning - writing the requirements - to the sale of handsets supporting the new algorithm). Therefore it is not possible to react within a short time period in the case that the first algorithm (KASUMI) should be broken. Therefore it is sensible to start with the development of a new algorithm now to have a second one in place and ready to use.

2. Requirements

A requirements list is needed. As a basis the requirements list of KASUMI (3G TS 33.105 V 4.1.0 see below) could be used and reviewed (e.g. number of gates, bit rates). It might be useful to add some requirements (e.g. the cryptographic foundations should be different from KASUMI). This could be done in a small working group (*during S3#26?*) of interested parties.

3. Algorithm Designer and Evaluation.

It is proposed that the actual work should be done by ETSI SAGE. Similar to KASUMI an evaluation by (invited and paid) experts is recommended. The terms and conditions for usage and distribution of the algorithm might be the same as for KASUMI.

4. Funding

It is proposed that 3GPP should provide the money. The costs for the KASUMI-based algorithms were funded by ETSI, but other SAGE work has been funded by GSMA or 3GPP.

S3 is kindly asked to consider the above four proposals.

Except 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.

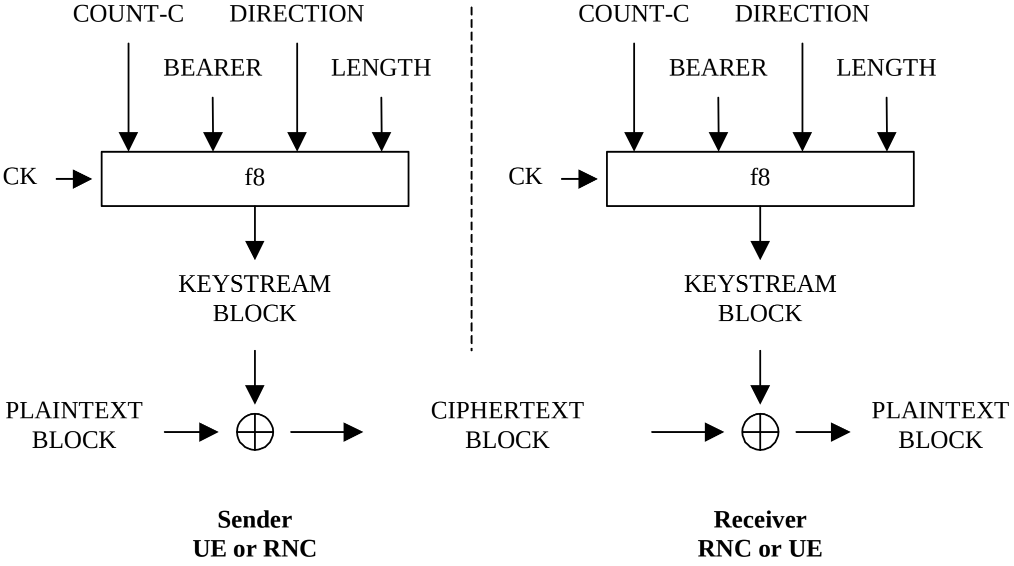

Figure 1: Ciphering user and signalling data transmitted over the radio access link

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 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]

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.

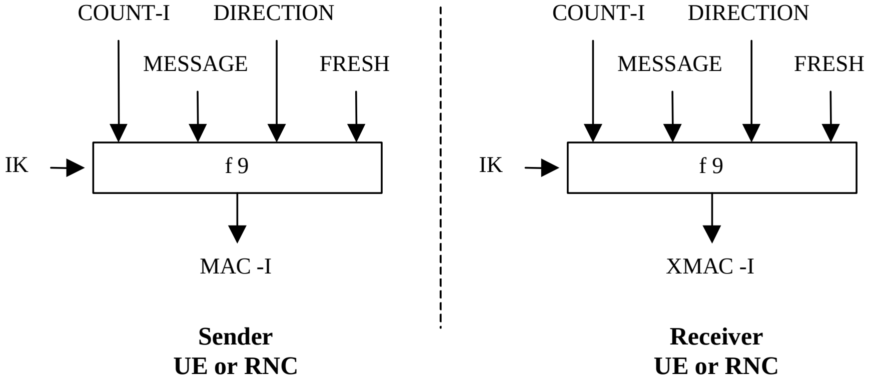

Figure 2: Derivation of MAC-I (or XMAC-I) on a signalling message

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.