

25 - 28 February 2002

Bristol, UK

---

3GPP TSG GERAN2 #7bis  
Helsinki, Finland  
January 14<sup>th</sup>-18<sup>th</sup>, 2002

Tdoc GERAN G2 020145  
Agenda Item 6

Source: TSG GERAN2

1 (3)

---

## Liaison Statement on Count Input to Ciphering Algorithm

Source: TSG GERAN2 To: TSG SA3

Contact: Guillaume SEBIRE, Nokia  
<mailto:guillaume.sebire@nokia.com>

---

### 1. INTRODUCTION

For GERAN Iu (Release 5 of 3GPP) the definition of the input parameters to the ciphering algorithm is yet to be completed. Precisely, the *count input* to the ciphering algorithm in case of *layer 2 signalling*, as well as in case of *RLC Transparent* mode is still pending. Although a working assumption was agreed based upon TSG SA3's suggestion that the 28-bit *count input* be defined as an *extended TDMA Frame Number* (see attached document S3-000455), it was argued later in TSG GERAN that a *HFN* similar to the HFN used in UTRAN should be used instead, and therefore no agreement could be reached on either of these proposals for the following reasons:

*Extended TDMA Frame Number:*

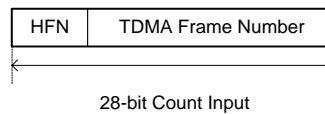
In case of a handover (cell change) the same TDMA frame number as was used in the source cell might be used again in the target cell, which should be avoided as it would lead otherwise to using the same mask in the target cell and in the source cell. This problem is similar to the GSM case today.

*HFN:*

In case of *RLC Transparent* mode, no RLC protocol information is added, therefore if an RLC block is lost when transmitted over the air interface, the synchronization of the input parameters is lost i.e. different HFN values are used on both transmitter (HFN) and receiver (HFN-1) sides, hence deciphering cannot be performed on receiver side as no sequence number may be added to counteract this.

## 2. PROPOSAL

In order to avoid the problems presented above, it was proposed to use a *combination* of HFN and TDMA frame number as shown below and with the following rules:



**Figure 1. 28-bit Count Input**

- Every time the TDMA Frame number reaches 0 the HFN is incremented by 1.
- When a handover is performed, the HFN is also incremented by 1.
- In order not to cipher twice the same message with two different set of parameters (this could happen in case of a handover: the message is first sent in the old cell, and then resent in the new cell), a sequence number must be introduced in this *message* to make its content differ when retransmitted: 1 bit is sufficient.
- The HFN must be kept in the mobile station's memory until a new authentication is needed (in which case the HFN is reset) whether the MS is in RRC-Idle or RRC-Connected modes. The HFN shall be incremented by 1 at every new RRC connection and informed to the network within RRC Connection Request similarly to UTRAN, this in order to avoid repetition of the same count value in-between two authentications.

It is proposed to use a 11-bit HFN and 17-bit TDMA frame number (equivalent to about 6.5 minutes). This TDMA frame number is a simple truncation of the 22-bit GSM TDMA frame number: the 5 MSBs of the T1 part are allocated to the HFN.

However, it was commented in TSG GERAN#7 that having such *fixed rules for the evolution of the HFN might lead to a security threat*. In UTRAN, similar rules are defined, but integrity protection allows to avoid any security problem with them, whereas in GERAN integrity protection is not available for layer 2 signalling, nor in RLC Transparent mode.

Therefore, TSG GERAN2 kindly asks TSG SA3:

- **whether the *principle* of combining a HFN with a TDMA Frame Number and the *corresponding rules* are acceptable from security standpoint, and**
- **if yes,**
  - **whether the proposed 11-bit HFN and 17-bit TDMA Frame Number (by truncation of the T1 part of the 22-bit GSM TDMA Frame Number) is acceptable; otherwise to suggest the size of the HFN and of the TDMA Frame Number**
- **if not,**
  - **to provide guidance and detailed recommendations.**

### 3. MEETING SCHEDULE

Meeting	Week	Dates	Place
GERAN2 #8	6	5-7 Feb, 2002	Rome
GERAN2 #8bis	11	11-15 Mar, 2002	Tbd
GERAN2 #9	16	16-18 Apr, 2002	[USA]
GERAN2 #9bis	22	27-31 May, 2002	Tbd
GERAN2 #10	26	25-27 Jun, 2002	[Europe]

### 4. ATTACHMENTS

S3-000455: Ciphering\_parameters\_in\_GERAN

---

2-4 August, 2000

Oslo, Norway

**Source:** Nokia**Title:** Cipherring parameters in GERAN**Document for:** Discussion/Decision**Agenda Item:**

## Introduction

This paper proposes a solution for cipherring in GERAN. Due to requirements for real-time bearers and new architecture aligned with UTRAN, the adoption of existing cipherring schemes for GERAN'00 is not straightforward. However general requirements that shall be met are listed below:

Implicit synchronization of cipherring including handover cases

Similar approach for RT and non-RT services

Incremental redundancy

Re-using of existing cipherring principles and schemes

Multiplexing several users on the same timeslot

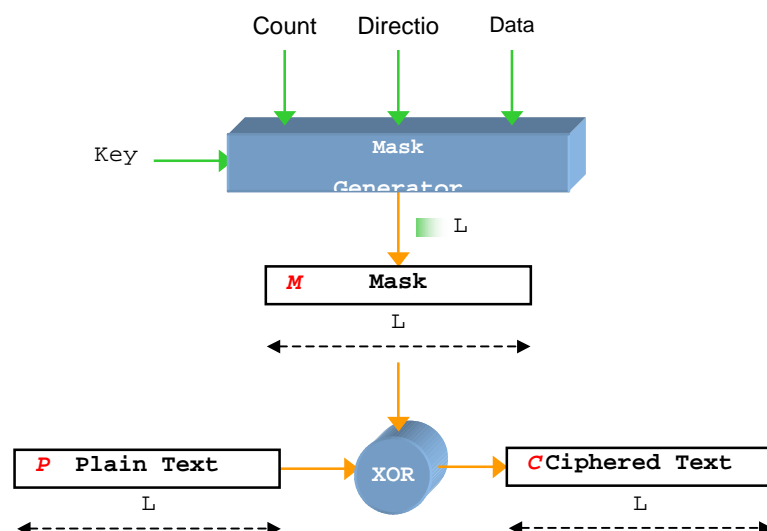
Multiplexing several bearers to the same MS

Multislot operation

It was commonly viewed in SMG2GERAN#2 workshop that cipherring should not be placed on PDCP layer but below, however, diverging opinions were expressed that it could be either located on RLC and MAC layers [2][3], similarly as is done in UTRAN, or on the physical layer. It is suggested in [9] that UTRAN Cipherring Algorithm be used in GERAN, which implies that GERAN shall use the same (but not identical) input parameters (number of inputs and associated length shall be identical). This paper proposes how to set the input parameters of the cipherring algorithm for GERAN.

## Main Principle

The figure below describes the main principle used for cipherring in UTRAN.



A mask  $M$  is generated that is applied to the incoming data (Plain text)  $P$  to yield the ciphered data  $C$ , according to the following equation:

$$C = M \oplus P \quad (1)$$

Several parameters (key, counter, direction, data id) are needed for generating the mask, among which the most important is the ciphering key, the other ones being to apply different ciphering processes (masks) between the blocks of one or more data flows, and therefore to avoid having twice the same mask on two different data blocks, which would lead to a significant security loss as the ciphered and non-ciphered data are then linked together without the mask:

$$\begin{array}{l} P_1 \oplus M = C_1 \\ \oplus \quad P_2 \oplus M = C_2 \\ \hline P_1 \oplus P_2 = C_1 \oplus C_2 \end{array}$$

The length of the mask has to be identical to the length  $L$  of the incoming data.

The different parameters are as follows:

- Key: ciphering key.
- Counter: incoming data block number or frame number
- Direction: uplink or downlink.
- Data id: identifies the data flow.

## Location of Ciphering

In UTRAN, the location of ciphering in a given protocol layer (MAC, RLC) implies that there is only one possible physical place where ciphering is performed. In GERAN though where various locations of PCU are allowed (BSC, BTS), the physical spot of ciphering depends on the selected architecture, if performed in the same protocol layer(s) as in UTRAN. In case PCU locates in BTS, ciphering should be performed on a possible radio link between BSC and BTS. In case PCU locates in BSC, no extra ciphering is needed between BSC and BTS.

## Ciphering parameters

RLC/MAC ciphering is preferred to be applied to GERAN'00 in a similar way as done in UTRAN in order to reach an equivalent security level in an acceptable time schedule, i.e. without any need for redesigning a new algorithm. Using the same algorithm as in UTRAN implies that similar inputs (number of inputs and bit length) be used for GERAN. However the content of the inputs may be different between UTRAN and GERAN.

This section describes how to perform ciphering on RLC/MAC in GERAN'00 as well as the associated parameters to set up the ciphering function.

The approach here is similar as that of UTRAN.

Data transmitted over a non-transparent RLC mode (either Acknowledged Mode or Unacknowledged Mode) are ciphered in the RLC sub-layer. Data transmitted over the transparent RLC mode is ciphered at the MAC sub-layer.

The following table lists the parameters that are needed to set up the ciphering function, on the user plane:

<b>RLC Mode</b>	Non-transparent	Transparent
<b>Protocol</b>	RLC	MAC
<b>Counter</b>	RLC Sequence Number: 7 or 11 bits: 0..127 or 0..2047 RBid indicator <sup>1</sup> : 1 bit:: 1 (RBid exists) HFN: 24 or 20 bits  <i>Total: 32 bits</i>	Extended TDMA Frame Number: 28 bits: 0...2 <sup>28</sup> -1 Slot number: 3 bits: 0..7 Rbid indicator: 1 bit:: 1 (RBid exists)  <i>Total: 32 bits</i>
<b>Direction</b>	0 Uplink / 1 Downlink	0 UL / 1 DL
<b>Data Id</b>	RBid	Radio Bearer Identifier (RBid see [8])
<b>L</b>	Payload size (without RBid) Or Full block without RBid neither RLC sequence number.	Full block size Note: the RBid is not carried in the data flow, but agreed before data transfer starts.
<b>Applies to</b>	Payload only without RBid, header non-ciphered to recover the RLC sequence number. Or payload and header but RLC sequence number and RBid.	Whole block.

**Table 1: Ciphering Parameters for user data**

For the control plane, L2 control messages need to be ciphered on the MAC layer, with the following parameters:

<b>RLC mode</b>	-
<b>Protocol</b>	MAC
<b>Counter</b>	Extended TDMA Frame Number: 28 bits Slot number: 3 bits RBid indicator: 1 bit:: 0 (RBid does not exist) <i>Total: 32 bits</i>
<b>Direction</b>	0 UL / 1 DL
<b>Data Id</b>	"00000" 5 bits
<b>L</b>	Full block size
<b>Applies to</b>	Whole block

**Table 2: Ciphering parameters for signalling**

The length of 32 bits for the counter was introduced in UTRAN to ensure that the cycle of the counter is long enough. In "old" GSM the TDMA frame number of 22 bits is used as an input parameter for the ciphering algorithm. This means that the counter reaches its maximum in about 3.5 hours of continuous execution of ciphering. In the proposed solution the RBid indicator takes 1 bit which stays constant during a connection. Also, in the MAC case the time slot number may stay constant if e.g. only one time slot is in use. This leaves 28 bits as the "effective counter" as regards absolute time. This is 64 times more than the current GSM cycle time and is adequate in practice.

If even longer cycle is required then the RBid indicator and/or time slot number has to be embedded into the ciphering key parameter which of course reduces the "effective key length". Since the key length is 128 bits this would not imply any significant decrease in the security level. However, the key is provided by the authentication and key agreement procedure in AuC and in SIM/USIM that should not be modified. If this alternative is selected then the HFN parameter (HyperFrame Number) in RLC ciphering and the extended TDMA frame number are made longer accordingly.

The HFN parameter in the RLC case may be stored between connections either on the terminal side in SIM/USIM (as is done in UTRAN) or in the network. The decision upon which way to go is partially dependent on how the transmission of the most significant bits of HFN can be embedded in some of the early messages in the connection before ciphering is started.

The extended TDMA frame number utilizes the same idea as HFN. Currently in GSM the 11 most significant bits of the TDMA frame number are used to count the so-called multiframes. This counter T1 should be made longer (17-21 bits depending on which of the above-mentioned alternatives is

<sup>1</sup> The RBid indicator bit is needed so that the same ciphering process does not apply in two different configurations: see section 2.

chosen). Also, the handling of this extended T1 parameter may be done similarly as the handling of HFN in the RLC case.

The UTRAN management of stored HFN values can be adopted. The extended T1 parameter can be called HFN in the MAC case. Between connections the highest value of the most significant bits (e.g. 17-21) of all HFNs in all radio bearers is stored. Then only one value has to be communicated in the start of the next connection and that value is used when initiating the ciphering for that new connection (In UTRAN the value is called START). Whenever a new radio bearer is set up during one connection the highest value of HFN that is in use in that connection shall be used as the initialization value for the new radio bearer.

The use of Radio Bearer identifier indicator is needed because for layer 2 signalling there exists no RBid. Instead "00000" is used input to the algorithm. This may cause the problem of section 2 to appear in case a user plane radio bearer with RBid "00000" is in use. An alternative solution would be to forbid the use of "00000" as a legitimate RBid value. This solution would however limit the number of possible radio bearers.

## **Handover GERAN/UTRAN**

The solution allows for using the same ciphering key in GERAN and UTRAN when moving from GERAN (resp. UTRAN) to UTRAN (resp. GERAN) by means of e.g. handover.

The problem described in section 0 appears again in case counter values are identical between GERAN and UTRAN after the move. To tackle this, it is proposed that the most significant part of the highest counter (i.e. 20 MSB when moving from GERAN to UTRAN, and the 17 MSB in the other way) is transferred to the targetted RAN and taken into use incremented by 1. Therefore the differences between UTRAN/GERAN in the least significant part (e.g. RBid indicator, slot number, etc) do not have any impact.

Note that this problem is tied to the fact that the same algorithm is used in UTRAN and GERAN, and not to the different fields (counter, etc.) defined. The same principle is applicable even if different fields than the ones previously defined are used.

## **Conclusion**

This paper proposes that GERAN ciphering be performed on RLC/MAC layer, using the same algorithm as defined in UTRAN, in order to reach equivalent security level in an acceptable time schedule for GERAN'00. Details on how to set the inputs to the parameters are given to enable such ciphering.

## **References**

- [1] SMG2#36, Tdoc 2-00-1095, "GERAN Overall Description – Stage 2", SMG2GERAN#2, 22-26 May, 2000, Biarritz, France
- [2] SMG2GERAN#2, Tdoc 2E00-122, "Ciphering Issues for GERAN", Ericsson, 8-12 May, 2000, Seattle, WA, USA
- [3] SMG2GERAN#2, Tdoc 2E00-148, "Ciphering in GERAN", Siemens, 8-12 May, 2000, Seattle, WA, USA
- [4] SMG2#36, Tdoc 2-00-1085, "Ciphering Issues for GERAN", Ericsson, 22-26 May, 2000, Biarritz, France
- [5] SMG2#36, Tdoc 2-00-1119, "Ciphering in GERAN", Siemens, 22-26 May, 2000, Biarritz, France
- [6] SMG2#36, Tdoc 2-00-1130, "LS on Security Functions in GERAN", SMG2#36, 22-26 May, 2000, Biarritz, France

- [7] SMG2#36, Tdoc 2-00-1221, "Reply to an LS about security functions in GERAN", 3GPP TSG SA WG 3, 22-26 May, 2000, Biarritz, France
- [8] SMG2#36, Tdoc 2-00-1101, "MAC Design for GERAN", Nokia, 22-26 May, 2000, Biarritz, France
- [9] 3GPP TSG SA3, Doc S3-000408, "Cipherring for GSM/EDGE RAN", Ericsson, Nokia, Siemens, 2-4 August, 2000, Oslo, Norway