3GPP TSG SA WG3 Security — S3#14 **S3-000474**

2-4 August, 2000

Oslo, Norway

Source: **TSG SA WG3** (contact: Valtteri.Niemi@nokia.com)

To: **TSG GERAN**

Title: **Proposed LS on GERAN security issues**

S3 would like to inform TSG GERAN and its subgroups that the work on technical details on the work item of GERAN security has begun in S3.

The best progress has been achieved on the ciphering feature. The S3 working assumptions can be found in the attached Tdoc S3-000455. TSG GERAN may base their stage 3 specification work on these working assumptions.

As regards integrity protection, the working assumption of S3 is to introduce it into GERAN in a form which is similar to the respective UTRAN mechanism. However, the details have not been elaborated yet. At the moment, we can only refer to the relevant part in TS 33.102. In brief, integrity protection mechanism adds a 32-bit cryptographic checksum to each RRC signalling message, with a few exceptions which are listed in TS 33.102.

As regards authentication and (ciphering/integrity) key agreement, the mechanism would be exactly the same for UTRAN and GERAN because it is executed on higher layers between USIM, SGSN (resp. VLR) and AuC.

Furthermore, S3 would like to point out that there are messages sent over Iu interface which are essential for security of UMTS (e.g. SECURITY MODE COMMAND including keys). This is a strong argument in favor of introducing both Iu-CS and Iu-PS interfaces into GERAN architecture.

3GPP TSG SA WG3 Security — S3#14 **S3-000455**

2-4 August, 2000

Oslo, Norway

Source: **Nokia**

Title: **Ciphering parameters in GERAN**

Document for: **Discussion/Decision**

Agenda Item:

Introduction

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

Implicit synchronization of ciphering including handover cases

Similar approach for RT and non-RT services

Incremental redundancy

Re-using of existing ciphering principles and schemes

Multiplexing several users on the same timeslot

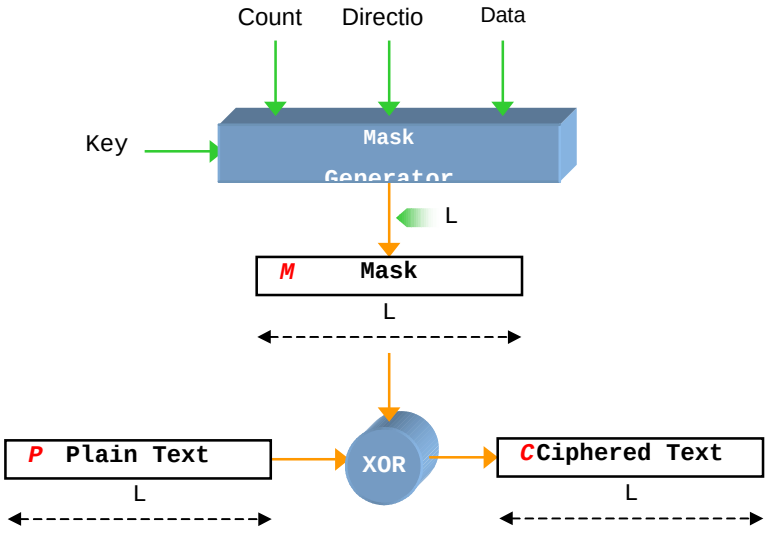
Multiplexing several bearers to the same MS

Multislot operation

It was commonly viewed in SMG2GERAN#2 workshop that ciphering 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], similarily as is done in UTRAN, or on the physical layer. It is suggested in [9] that UTRAN Ciphering 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 ciphering algorithm for GERAN.

Main Principle

The figure below describes the main principle used for ciphering 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:

$$\begin{array}{ll} & P_1 \oplus M = C_1 \\ \oplus & P_2 \oplus M = C_2 \\ \hline & P_1 \oplus P_2 = C_1 \oplus C_2 \end{array}$$

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:

RLC Mode	Non-transparent	Transparent
Protocol	RLC	MAC
Counter	RLC Sequence Number: 7 or 11 bits: 0..127 or 0..2047 RBid indicator[1]: 1 bit:: 1 (RBid exists) HFN: 24 or 20 bits *Total: 32 bits*	Extended TDMA Frame Number: 28 bits: 0…2^{28}-1 Slot number: 3 bits: 0..7 Rbid indicator: 1 bit:: 1 (RBid exists) *Total: 32 bits*
Direction	0 Uplink / 1 Downlink	0 UL / 1 DL
Data Id	RBid	Radio Bearer Identifier (RBid see [8])
L	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.
Applies to	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:

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

[1] 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, "Ciphering for GSM/EDGE RAN", Ericsson, Nokia, Siemens, 2-4 August, 2000, Oslo, Norway