Title:	**Current status of stage 2**
Source:	Vodafone
Date:	19th April 2001
Document for:	Decision

1 Introduction

This contribution intends to point out the incomplete status of the security matters currently contained in the stage 2 for GERAN Release 5, 3GPP TS 43.051 [1].

2 Discussion

2.1 Ciphering

Currently, the stage 2 for GERAN Release 5 [1] only addresses ciphering. Sub-clause 7 of the latest version (v5.0.0) has been included as Annex A of this contribution. SA3 are kindly invited to review it. More specifically, it should be checked that how the inputs to the ciphering algorithm are chosen in GERAN satisfy SA3's security requirements (see tables in sub-clause 7.2.5).

Furthermore, there are still (at least) a couple of issues for further study, appearing as notes in the first of the tables. It is advisable that these two issues are solved at this meeting.

2.2 Other issues

2.2.1 Integrity protection

So far, only ciphering is addressed in the stage 2 for GERAN. However, there are other GERAN security items / features / problems that are not mentioned in this specification. The most obvious one is integrity protection. It is important that the current working assumptions on integrity protection are captured on the stage 2, at least temporarily, while GERAN works on the CRs to the stage 3.

2.2.2 Iur-g interface

Work on the Iur-g interface is ongoing at the moment in TSG GERAN and, to some extent, SA2 and RAN3. Scenarios when the Iur-g interface is used need further study, since there are security implications that need to be considered.

As depicted in Figure 1, the Iur-g interface is used to connect two BSSs or a BSC and an RNC. As in UTRAN, the MS/UE can reselect a cell on a different BSC/RNC. In certain states of *inactivity*, it is possible that the MS/UE does not indicate the change of cell. It is in those scenarios (shown in Figure 2) when the Iur-g interface is used for. TSG GERAN is currently working on these procedures and the specification of this interface is not stable. It could be suggested that the following procedures might be executed while the MS/UE is in this situation:

- Mobile terminated call/session establishment
- Mobile originated call/session establishment
- Cell Update procedure
- GRA/URA update procedure
- Relocation procedure

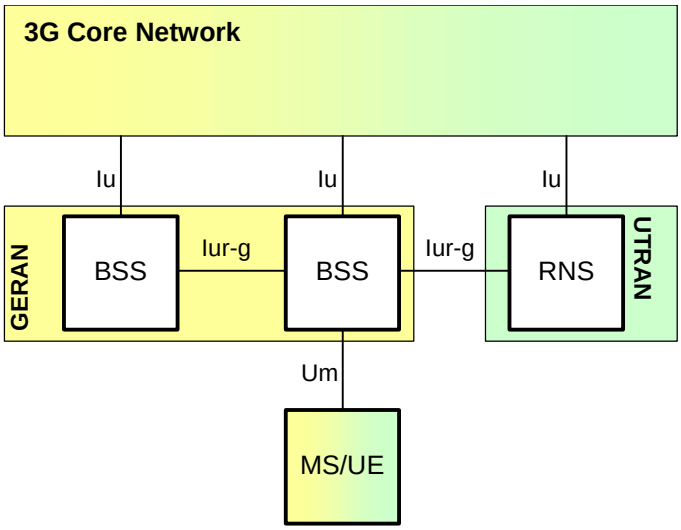

Figure 1 – Simplified 3G reference architecture

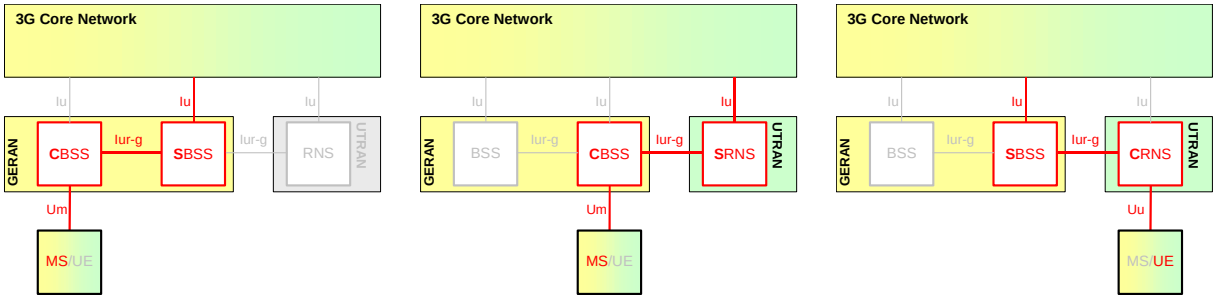

Figure 2 – Scenarios of Iur-g interface usage

2.3 Responsibility of stage 2

It needs to be decided at this meeting which TS(s) is/are more suitable to contain the stage 2 for GERAN security, i.e. either 3GPP TS 43.051 [1], 3GPP TS 33.102 [2] or both. In the latter case, the scope of each TS should be clarified in order to avoid redundancies and facilitate updates.

3 Conclusion

It is recommended that:

- A decision be made at this meeting as to where the stage 2 description of the GERAN security should be, along whit the scope if it is to be split between different specifications.
- SA3 confirm the validity of the working assumptions regarding ciphering; the remaining open points should be closed at this meeting.
- The sub-clause in the stage 2 is enhanced so that other issues regarding GERAN security are dealt with; these at least include integrity protection.
- The scenarios where the Iur-g interface is used are studied from the security point of view so that security matters can be considered by GERAN during the ongoing work on this interface.

References

[1] 3GPP TS 43.051, "3rd Generation Partnership Project; Technical Specification Group GERAN; GSM/EDGE Radio Access Network (GERAN); Overall Description – Stage 2"

[2] 3GPP TS 33.102; "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture"

Annex: sub-clause 7 of the stage 2

7 Ciphering

The ciphering architecture is specified in TS 33.102 and is identical to that of UTRAN (f8). The ciphering principle with input parameters to the algorithm is illustrated in figure 18.

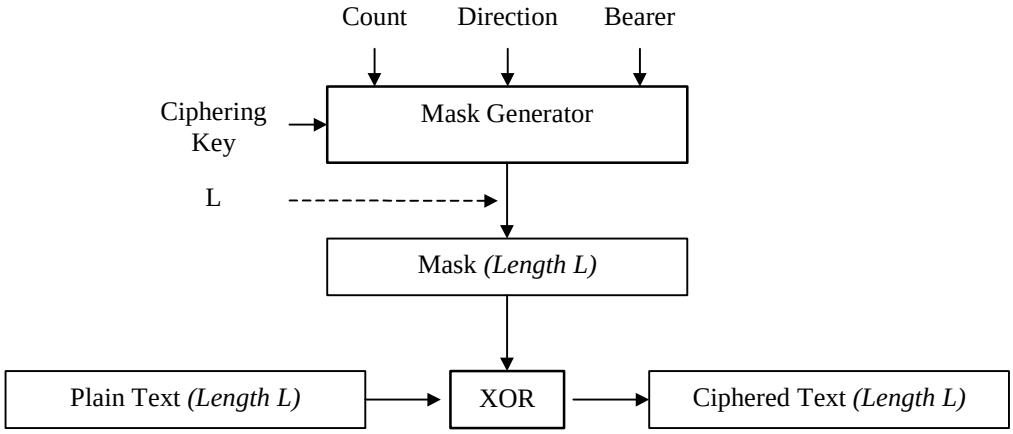

Figure 18: Ciphering Principle

7.1 Location of ciphering in the GERAN protocol architecture

The ciphering function is performed either in the RLC sub-layer or in the MAC sub-layer, according to the following rules:

- In case of non-transparent RLC mode (acknowledged or unacknowledged), ciphering is performed in the RLC sub-layer for layer 2 user data blocks only. Layer 2 signalling is ciphered in the MAC sub-layer.
- In case of transparent RLC mode, ciphering is performed in the MAC sub-layer.

According to this model, ciphering when applied is performed in the BSS and the MS, and the context needed for ciphering (input parameters) is only known in BSS and the MS.

7.2 Inputs to the ciphering algorithm

7.2.1 Ciphering Key

The ciphering key is 128 bit long.

The ciphering key is established between the MS and BSS during the authentication phase. In the two-key solution, the CS-domain bearers are ciphered with the most recent cipher key agreed between the user and the MSC (CK-CS). The PS-domain bearers are ciphered with the most recent cipher key agreed between the user and the SGSN (CK-PS).

To ensure performing the right ciphering function at the RLC and MAC layers, three conditions must be met:

- A Radio Bearer is either from CS-domain or PS-domain, but not from both.
- RRC maps a given Radio Bearer to a given domain in order to derive the correct key to utilise for each RB.
- The RLC and MAC layers receive the Radio Bearer IDs and CKs they should use from RRC.

7.2.2 Bearer

This parameter indicates the radio bearer identity (when available), which shall be unique within a RRC connection. It is used as input parameter to the ciphering algorithm to ensure that the same ciphering mask is not applied to two or more parallel Radio Bearers having the same ciphering key and count. Each Radio Bearer is ciphered independently.

In case no radio bearer identity is available (layer 2 signalling), the data id shall be equal to a unique value.

To ensure that the same ciphering mask is not applied to layer 2 signalling (no RBid available) and layer 2 user data (RBid available), RBid indicator is used in the count parameter to inform whether RBid is available or not.

7.2.3 Direction

This parameter indicates the direction of transmission (uplink/downlink).

7.2.4 Length

This parameter indicates the length of the mask to be generated by the algorithm (this length is equal to that of the data to be ciphered). It is not an input to the mask generator.

7.2.5 Parameter Settings

The following tables defines how to set the input parameters to the ciphering algorithm that applies to layer 2 user data blocks and layer 2 signalling respectively:

Table 3: Input parameters for user data blocks

Input parameters	Size (bits)	Non-transparent RLC Mode	Transparent RLC Mode
Count	**32**	RLC Sequence Number: a) 7 bits or b) 11 bits a) 0…127 or b) 0…2047	Slot number: 3 bits 0…7
		RBid indicator: 1 bit 1 (RBid available)	
		HFN: 24 or 20 bits a) 0…16777215 or b) 0…1048575	Extended TDMA Frame Number: 28 bits or HFN (see note 2) 0…268435455
Direction	**1**	1 bit 0 (Uplink) or 1 (Downlink)	
Bearer	**5**	Radio Bearer Identifier (RBid) 0…31	
Length	**16**	Length of the input data to be ciphered: the fields included in the input parameters shall not be ciphered. 0…65535	Full block size
NOTE 1: Whether RBid is carried in RLC PDUs is ffs. NOTE 2: Whether GSM time numbering (TDMA frame number) or HFN similar to UTRAN is used is ffs.			

Table 4: Input Parameters for layer 2 signalling

Input parameters	Size (bits)	Non-transparent RLC mode
Count	**32**	Slot number: 3 bits 0…7
		RBid indicator: 1 bit 0 (RBid not available)
		Extended TDMA Frame Number: 28 bits or HFN (see note 2 in table 3) 0…268435455
Direction	**1**	1 bit 0 (Uplink) or 1 (Downlink)
Bearer	**5**	"00000"
Length	**L**	Full block size