3GPP TSG SA 3 meeting #11
Mainz, Germany, 22-24 February 2000

***Document* S3-000133**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

25.301	**CR**		Current Version:	3.3.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ ↑ *CR number as allocated by MCC support team*

For submission to:	SA 7	for approval	X	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM	X	ME	X	UTRAN / Radio	X	Core Network	

Source:	Siemens Atea	**Date:**	
Subject:	Ciphering and Integrity		
Work item:	Security		

Category:	F	Correction		**Release:**	Phase 2	
	A	Corresponds to a correction in an earlier release			Release 96	
(only one category	B	Addition of feature			Release 97	
shall be marked	C	Functional modification of feature			Release 98	
with an X)	D	Editorial modification	X		Release 99	X
					Release 00	

Reason for change: Detail on ciphering is removed from TS 25.301. Instead a reference to the security architecture is put in place. Besides ciphering, also data integrity is discussed.

Clauses affected: 8

Other specs affected:	Other 3G core specifications		→ List of CRs:	
	Other GSM core specifications		→ List of CRs:	
	MS test specifications		→ List of CRs:	
	BSS test specifications		→ List of CRs:	
	O&M specifications		→ List of CRs:	

Other comments:

help.doc

<---------- double-click here for help and instructions on how to create a CR.

8 ~~Ciphering~~Security

The ciphering architecture is specified in TS 33.102 [15], clause 6.6.

The integrity architecture is specified in TS 33.102 [15], clause 6.5.

~~8.1 Location of ciphering function in the UTRAN protocol architecture~~

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

- ~~If a logical channel is expected to be supported on common transport channel and has to be ciphered, it can not use the transparent mode of RLC (it should use the UM RLC mode instead).~~
- ~~If a logical channel is using a non-transparent RLC mode (AM or UM), ciphering is performed in the RLC sub-layer.~~
- ~~If a logical channel is using the transparent RLC mode, ciphering is performed in the MAC sub-layer (MAC-d entity).~~

~~According to this model, ciphering when applied is performed in the SRNC and the UE, and the context needed for ciphering (CK, HFN, etc.) is only known in SRNC and the UE.~~

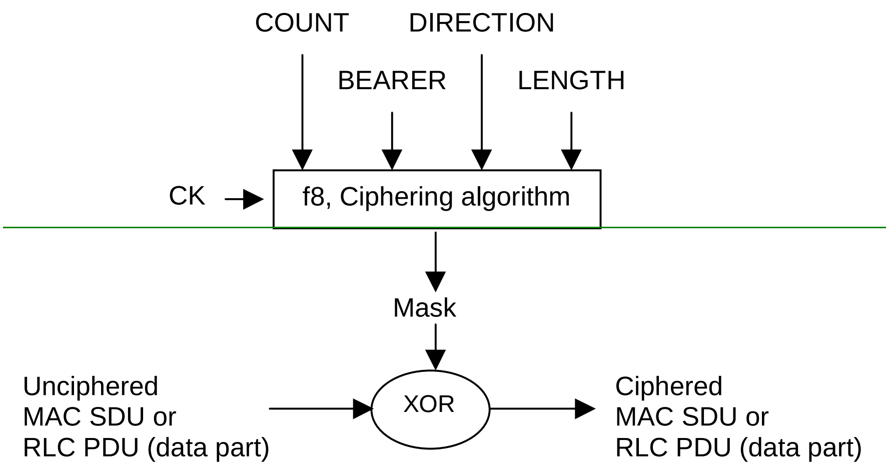
~~8.2 Input parameters to the ciphering algorithm~~

~~8.2.1 Overview~~

~~When ciphering is performed in the RLC sub-layer, it performs the encryption/decryption of the ciphering unit of an RLC PDU, based on XOR combining with a mask obtained as an output of the ciphering algorithm. For UM RLC, the ciphering unit is defined as the UMD PDU minus the first octet. The first octet comprises the sequence number used as LSB of the COUNT parameter. For AM RLC, the ciphering unit is defined as the AMD PDU minus the two first octets. These two octets comprise the sequence number used as LSB of the COUNT parameter.~~

~~When ciphering is performed in the MAC sub-layer, it performs the encryption/decryption of a MAC SDU (RLC PDU), based on XOR operation with a mask obtained as an output of the ciphering algorithm.~~

~~Requirements and interfaces to the generic algorithm are specified in TS 33.105 and described in the following figure.~~



~~**Figure 28: Ciphering algorithm and parameters**~~

~~8.2.2 Ciphering algorithms parameters~~

~~8.2.2.1 COUNT~~

~~COUNT shall be at least 32 bits long. It is composed of a 'long' sequence number called Hyper Frame Number HFN, and a 'short' sequence number, which depends on the ciphering mode, as described below. There is one ciphering sequence per logical channel using AM or UM mode plus one for all logical channels using the transparent mode (and mapped onto DCH).~~

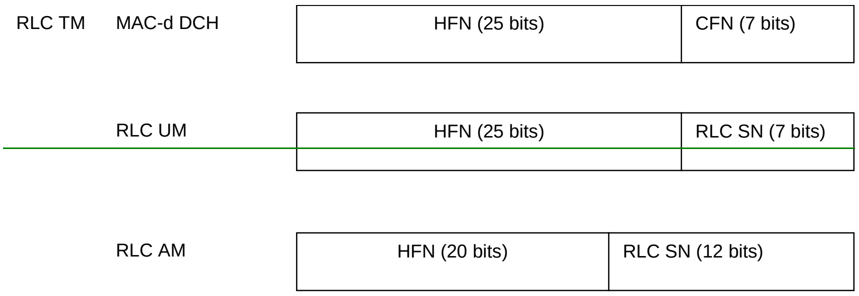
~~The Hyper Frame Number (HFN) is initialised by the UE and signalled to the SRNC before ciphering is started. It is used as initial value for each ciphering sequence, and it is then incremented independently in each ciphering sequence, at each cycle of the 'short' sequence number. When a new RAB / logical channel is created during a RRC connection, the highest HFN value currently in use is incremented, and used as initial value for the ciphering sequence of this new logical channel. The highest HFN value used during a RRC connection (by any ciphering sequence) is stored in the USIM, and the UE initialises the new HFN for the next session with a higher number than the stored one. If no HFN value is available in USIM, the UE randomly selects a HFN value.~~

~~Depending on the requirements (e.g. how many successive RRC Connections can use the same ciphering key), it may be sufficient to use only the most significant bits of HFN in the re-initialisation (and set LSBs implicitly to zero). This may be necessary at least if the HFN value needs to be included in the RRC Connection Request message.~~

~~The 'short' sequence number is:~~

- ~~For RLC TM on DCH, the CFN of the UEFN is used and is independently maintained in UE MAC and SRNC MAC-d. The ciphering sequence number is identical to the UEFN.~~
- ~~For RLC UM and AM modes, the RLC sequence number is used, and is directly available in each RLC PDU at the receiver side (it is not ciphered). The HFN is incremented at each RLC SN cycle.~~

~~The figure below presents some examples of the different COUNT parameters, assuming various sizes for the 'short' sequence numbers. This proposal permits to exchange a unique HFN and also to use a unique CSN size, which should permit to reduce the implementation complexity of the ciphering function. In this example, the HFN is 25 bits long, and only the 20 MSB are used for the CSN of the RLC AM mode.~~



~~Figure 29: Example of ciphering sequence number for all possible configurations~~

~~8.2.2.2 Ciphering key, CK~~

~~CK is established between the UE and SRNC 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 3G-MSC (CK-CS). The PS-domain bearers are ciphered with the most recent cipher key agreed between the user and the3G-SGSN (CK-PS). The signalling link is ciphered with the most recent cipher key established between the user and the network, i.e., the youngest of CK-CS and CK-PS.~~

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

- ~~Each logical traffic channel can only transfer the information 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.~~

~~8.2.2.3 BEARER~~

~~This parameter indicates the logical channel identity, which shall be unique within a RRC connection. It is used as input parameter of the ciphering algorithm to ensure that the same ciphering mask is not applied to two or more parallel logical channels having the same CK and same COUNT. Each logical channel is ciphered independently.~~

~~8.2.2.4 Direction~~

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

~~8.2.2.5 Length~~

~~This parameter indicates the length of the keystream block (mask) to be generated by the algorithm. It is not an input to the keystream generation function.~~