Technical Specification Group Services and System Aspects   *TSGS#12(01)0315*

Meeting #12, Stockholm, Sweden, 18-21 June 2001

Source:	**SA WG3**
Title:	**1 CR to 33.102: Include reference to TS 43.041 GERAN Stage 2 specification (Rel-5)**
Document for:	**Approval**
Agenda Item:	**7.3.3**

Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New	Doc-2nd-Level
33.102	148		Rel-5	B	Include reference to TS 43.041 GERAN Stage 2 specification	4.0.0	5.0.0	S3-010236

CR-Form-v3

CHANGE REQUEST

| ⌘ | **33.102** CR **148** | ⌘ | rev | **-** | ⌘ | Current version: | **4.0.0** | ⌘ |

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘   (U)SIM ☐   ME/UE ☐   Radio Access Network ☒   Core Network ☒

Title: ⌘	Include reference to TS 43.041 GERAN Stage 2 specification	
Source: ⌘	TSG SA3	
Work item code: ⌘	SEC1	***Date:*** ⌘ 22/05/2001
Category: ⌘	**B**	***Release:*** ⌘ REL-5

Use <u>one</u> of the following categories:
   F *(essential correction)*
   A *(corresponds to a correction in an earlier release)*
   B *(Addition of feature),*
   C *(Functional modification of feature)*
   D *(Editorial modification)*
Detailed explanations of the above categories can
be found in 3GPP TR 21.900.

Use <u>one</u> of the following releases:
   2   (GSM Phase 2)
   R96 (Release 1996)
   R97 (Release 1997)
   R98 (Release 1998)
   R99 (Release 1999)
   REL-4 (Release 4)
   REL-5 (Release 5)

Reason for change: ⌘	Following decision was made at the Joint GERAN/SA3 Adhoc in Madrid (27 April 2001) and approved at 3GPP TSG SA WG3#18: The stage 2 for GERAN security will be included temporarily in 3GPP TS 43.051 and a reference to 3GPP TS 43.051 will be included in 3GPP TS 33.102**Error! Reference source not found.**. When the stage 2 becomes stable and the stage 3 changes commence, (at least part of) the stage 2 in 3GPP TS 43.051 will be moved into 3GPP TS 33.102.
Summary of change: ⌘	Include reference to TS 43.051
Consequences if not approved: ⌘	Lack of reference to needed information in 33.102 Rel-5

Clauses affected: ⌘	2, 6.5, 6.6, 6.7 (New), 6.8 (New)
Other specs affected: ⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments: ⌘	

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1]   3GPP TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2]   3GPP TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[3]   3GPP TR 21.905: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications (Release 1999)".

[4]   3GPP TS 23.121: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Architecture Requirements for Release 99".

[5]   3GPP TS 31.101: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics".

[6]   3GPP TS 22.022: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Personalisation of UMTS Mobile Equipment (ME); Mobile functionality specification".

[7]   3GPP TS 23.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Security Mechanisms for the USIM application toolkit; Stage 2".

[8]   ETSI GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[9]   3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[10]   ISO/IEC 9798-4: "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function".

[11]   3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications".

[12]   3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification".

[13]   3GPP TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementers' test data".

[14]   3GPP TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data".

[15]   3GPP TS 31.111: "3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT)".

[16]   3GPP TS 02.48: "Security Mechanisms for the SIM Application Toolkit; Stage 1".

[17]   3GPP TS 25.331: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RRC Protocol Specification".

[18]   3GPP TS 25.321: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; MAC protocol specification".

[19]   3GPP TS 25.322: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RLC Protocol Specification".

[20]   3GPP TS 31.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Characteristics of the USIM Application".

[21]   3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Service principles".

[22]   3GPP TS 43.051: "3rd Generation Partnership Project; Technical Specification Group GERAN; GSM/EDGE Radio Access Network (GERAN); Overall Description - Stage 2".

6.5   Access link data integrity for UTRAN

6.5.1   General

Most control signalling information elements that are sent between the MS and the network are considered sensitive and must be integrity protected. A message authentication function shall be applied on these signalling information elements transmitted between the ME and the RNC.

After the RRC connection establishment and execution of the security mode set-up procedure, all dedicated MS <–> network control signalling messages (e.g. RRC, MM, CC, GMM, and SM messages) shall be integrity protected. The Mobility Management layer in the MS supervises that the integrity protection is started (see section 6.4.5).

All signalling messages except the following ones shall then be integrity protected:

HANDOVER TO UTRAN COMPLETE

PAGING TYPE 1

PUSCH CAPACITY REQUEST

PHYSICAL SHARED CHANNEL ALLOCATION

RRC CONNECTION REQUEST

RRC CONNECTION SETUP

RRC CONNECTION SETUP COMPLETE

RRC CONNECTION REJECT

RRC CONNECTION RELEASE (CCCH only)

SYSTEM INFORMATION (BROADCAST INFORMATION)

SYSTEM INFORMATION CHANGE INDICATION

TRANSPORT FORMAT COMBINATION CONTROL (TM DCCH only)

6.5.2 Layer of integrity protection

The UIA shall be implemented in the ME and in the RNC.

Integrity protection shall be applied at the RRC layer.

6.5.3 Data integrity protection method

Figure 16 illustrates the use of the integrity algorithm f9 to authenticate the data integrity of a signalling message.
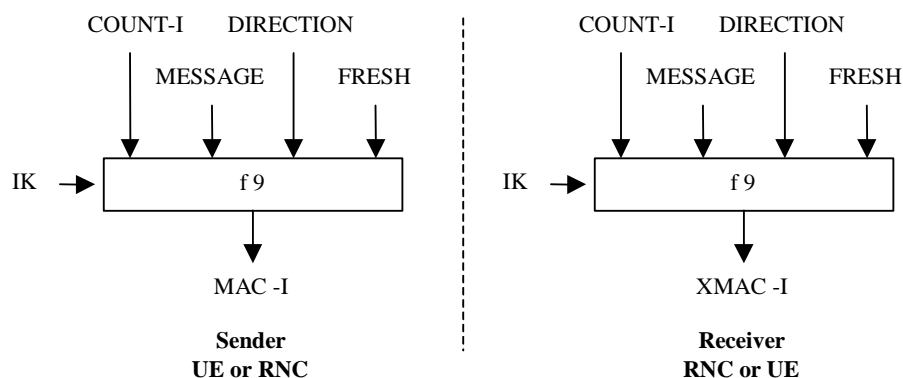

Figure 16: Derivation of MAC-I (or XMAC-I) on a signalling message

The input parameters to the algorithm are the Integrity Key (IK), the integrity sequence number (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 message authentication code for data integrity MAC-I using the integrity algorithm f9. The MAC-I is then appended to the message when sent over the radio access link. The receiver computes XMAC-I on the message received in the same way as the sender computed MAC-I on the message sent and verifies the data integrity of the message by comparing it to the received MAC-I.

6.5.4 Input parameters to the integrity algorithm

6.5.4.1 COUNT-I

The integrity sequence number COUNT-I is 32 bits long.

For signalling radio bearers (RB 0-4) there is one COUNT-I value per up-link signalling radio bearer and one COUNT-I value per down-link signalling radio bearer.

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number forms the least significant bits of COUNT-I while the "long" sequence number forms the most significant bits of COUNT-I. The "short" sequence number is the 4-bit RRC sequence number (RRC SN) that is available in each RRC PDU. The "long" sequence number is the 28-bit RRC hyper frame number (RRC HFN) which is incremented at each RRC SN cycle.
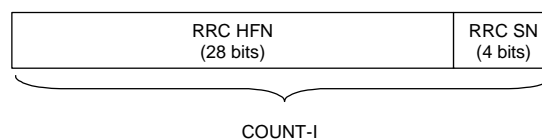
RRC HFN (28 bits)	RRC SN (4 bits)

COUNT-I

Figure 16a: The structure of COUNT-I

The RRC HFN is initialised by means of the parameter START, which is described in subclause 6.4.8. The ME and the RNC then initialise the 20 most significant bits of the RRC HFN to START; the remaining bits of the RRC HFN are initialised to 0.

6.5.4.2 IK

The integrity key IK is 128 bits long.

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user. Which integrity key to use for a particular connection is described in 6.5.5.

For UMTS subscribers IK is established during UMTS AKA as the output of the integrity key derivation function f4, that is available in the USIM and in the HLR/AuC. For GSM subscribers, that access the UTRAN, IK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 6.8.2.

IK is stored in the USIM and a copy is stored in the ME. IK is sent from the USIM to the ME upon request of the ME. The USIM shall send IK under the condition that a valid IK is available. The ME shall trigger a new authentication procedure if the current value of $START_{CS}$ or $START_{PS}$ in the USIM are not up-to-date or $START_{CS}$ or $START_{PS}$ have reached THRESHOLD. The ME shall delete IK from memory after power-off as well as after removal of the USIM.

IK is sent from the HLR/AuC to the VLR/SGSN and stored in the VLR/SGSNas part of a quintet. It is sent from the VLR/SGSN to the RNC in the (RANAP) *security mode command*.

At handover, the IK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed, and the synchronisation procedure is resumed. The IK remains unchanged at handover.

6.5.4.3 FRESH

The network-side nonce FRESH is 32 bits long.

There is one FRESH parameter value per user. The input parameter FRESH protects the network against replay of signalling messages by the user. At connection set-up the RNC generates a random value FRESH and sends it to the user in the (RRC) *security mode command*. The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection. This mechanism assures the network that the user is not replaying any old MAC-Is.

At handover with relocation of the S-RNC, the new S-RNC generates its own value for the FRESH parameter and sends it to the ME in the RRC message that indicates a new UTRAN Radio Network Temporary Identity due to a SRNC relocation (see TS 25.331 [17]).

6.5.4.4   DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that the integrity algorithm used to compute the message authentication codes would use an identical set of input parameter values for the up-link and for the down-link messages. The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

6.5.4.5   MESSAGE

The signalling message itself with the radio bearer identity. The latter is appended in front of the message. Note that the radio bearer identity is not transmitted with the message but it is needed to avoid that for different instances of message authentication codes the same set of input parameters is used.

6.5.5   Integrity key selection

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user.

The data integrity of radio bearers for user data is not protected.

The signalling radio bearers are used for transfer of signalling data for services delivered by both CS and PS service domains. These signalling radio bearers are data integrity protected by the IK of the service domain for which the most recent security mode negotiation took place. This may require that the integrity key of an (already integrity protected) ongoing signalling connection has to be changed, when a new connection is established with another service domain, or when a security mode negotiation follow a re-authentication during an ongoing connection. This change should be completed by the RNC within five seconds after receiving the security mode command from the VLR/SGSN.

   NOTE: For the behaviour of the terminal regarding key changes see section 6.4.5.

6.5.6   UIA identification

Each UMTS Integrity Algorithm (UIA) will be assigned a 4-bit identifier. Currently, the following values have been defined:

     "0001_2"   :   UIA1, Kasumi.

The remaining values are not defined.

The use of Kasumi for the integrity protection function f9 is specified in TS 35.201 [11] and TS 35.202 [12]. Implementers' test data and design conformance data is provided in TS 35.203 [13] and TS 35.202 [14].

6.6 Access link data confidentiality for UTRAN

6.6.1 General

User data and some signalling information elements are considered sensitive and must be confidentiality protected. To ensure identity confidentiality (see section 6.1), the temporary user indentity (P-)TMSI must be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it.

These needs for a protected mode of transmission are fulfilled by a confidentiality function which is applied on dedicated channels between the ME and the RNC.

6.6.2 Layer of ciphering

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

- If a radio bearer is using a non-transparent RLC mode (AM or UM), ciphering is performed in the RLC sub-layer.

- If a radio bearer is using the transparent RLC mode, ciphering is performed in the MAC sub-layer (MAC-d entity).

Ciphering when applied is performed in the S-RNC and the ME and the context needed for ciphering (CK, HFN, etc.) is only known in S-RNC and the ME.

6.6.3 Ciphering method

Figure 16b illustrates the use of the ciphering algorithm f8 to encrypt plaintext by applying a keystream using a bit per bit binary addition of the plaintext and the keystream. The plaintext may be recovered by generating the same keystream using the same input parameters and applying a bit per bit binary addition with the ciphertext.
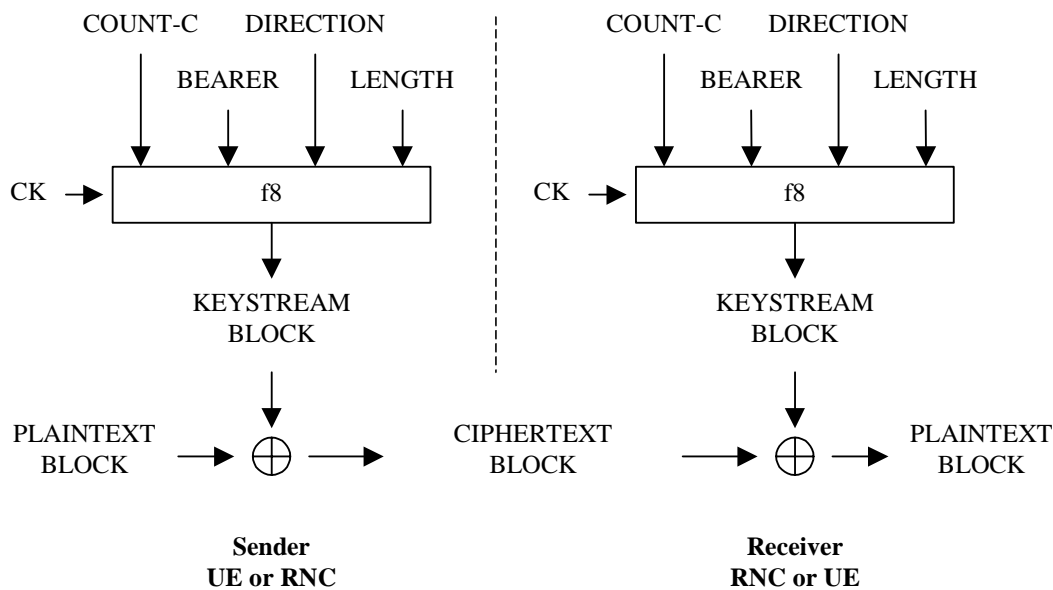
Figure 16b: Ciphering of user and signalling data transmitted over the radio access link

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.

6.6.4 Input parameters to the cipher algorithm

6.6.4.1 COUNT-C

The ciphering sequence number COUNT-C is 32 bits long.

There is one COUNT-C value per up-link radio bearer and one COUNT-C value per down-link radio bearer using RLC AM or RLC UM. There is one up-link COUNT-C value and one down-link COUNT-C value for all radio bearers using the transparent RLC mode that are connected to the same CN domain (and mapped onto DCH).

COUNT-C is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number forms the least significant bits of COUNT-C while the "long" sequence number forms the most significant bits of COUNT-C. The update of COUNT-C depends on the transmission mode as described below (see figure 16c).
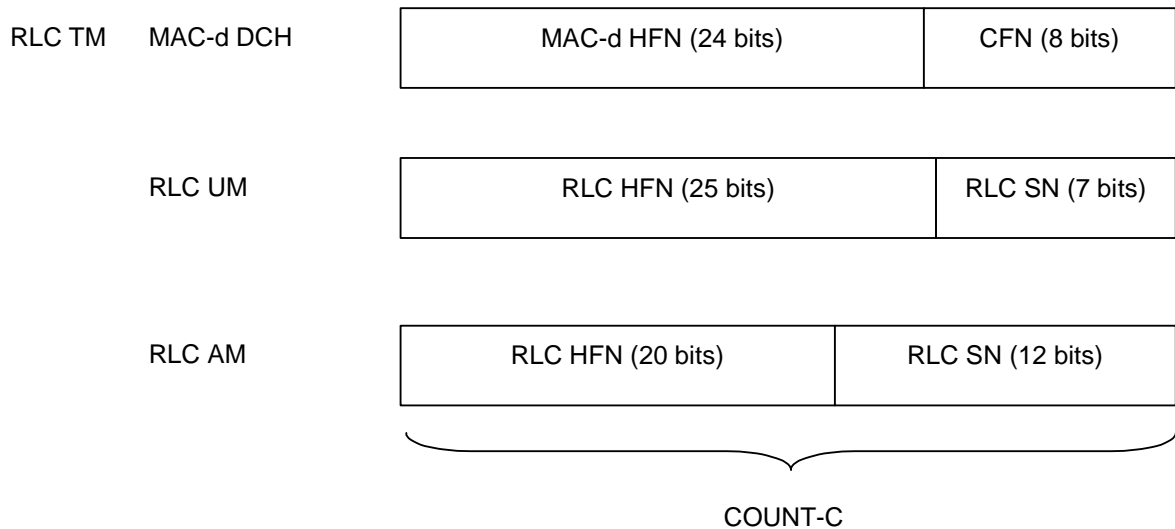
RLC TM	MAC-d DCH	MAC-d HFN (24 bits)	CFN (8 bits)

	RLC UM	RLC HFN (25 bits)	RLC SN (7 bits)

	RLC AM	RLC HFN (20 bits)	RLC SN (12 bits)

COUNT-C

Figure 16c: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 8-bit connection frame number CFN of COUNT-C. It is independently maintained in the ME MAC-d entity and the SRNC MAC-d entity. The "long" sequence number is the 24-bit MAC-d HFN, which is incremented at each CFN cycle.

- For RLC UM mode, the "short" sequence number is the 7-bit RLC sequence number (RLC SN) and this is part of the RLC UM PDU header. The "long" sequence number is the 25-bit RLC UM HFN which is incremented at each RLC SN cycle.

- For RLC AM mode, the "short" sequence number is the 12-bit RLC sequence number (RLC SN) and this is part of the RLC AM PDU header. The "long" sequence number is the 20-bit RLC AM HFN which is incremented at each RLC SN cycle.

The hyperframe number HFN is initialised by means of the parameter START, which is described in subclause 6.4.8. The ME and the RNC then initialise the 20 most significant bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN to START. The remaining bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN are initialised to zero.

When a new radio bearer is created during a RRC connection in ciphered mode, the HFN is initialised by the current START value (see subclause 6.4.8).

6.6.4.2   CK

The cipher key CK is 128 bits long.

There may be one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user. The CK to use for a particular radio bearer is described in 6.6.5. For UMTS subscribers, CK is established during UMTS AKA, as the output of the cipher key derivation function f3, available in the USIM and in HLR/AuC. For GSM subscribers that access the UTRAN, CK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 8.2.

CK is stored in the USIM and a copy is stored in the ME. CK is sent from the USIM to the ME upon request of the ME. The USIM shall send CK under the condition that a valid CK is available. The ME shall trigger a new authentication procedure if the current value of $START_{CS}$ or $START_{PS}$ in the USIM have reached THRESHOLD. The ME shall delete CK from memory after power-off as well as after removal of the USIM.

CK is sent from the HLR/AuC to the VLR/SGSN and stored in the VLR/SGSN as part of the quintet. It is sent from the VLR/SGSN to the RNC in the (RANAP) security mode command.

At handover, the CK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed. The cipher CK remains unchanged at handover.

6.6.4.3 BEARER

The radio bearer identifier BEARER is 5 bits long.

There is one BEARER parameter per radio bearer associated with the same user and multiplexed on a single 10ms physical layer frame. The radio bearer identifier is input to avoid that for different keystream an identical set of input parameter values is used.

6.6.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the keystreams for the up-link and for the down-link would use the an identical set of input parameter values. The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

6.6.4.5 LENGTH

The length indicator LENGTH is 16 bits long.

The length indicator determines the length of the required keystream block. LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

6.6.5 Cipher key selection

There is one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user.

The radio bearers for CS user data are ciphered with CK_{CS}.

The radio bearers for PS user data are ciphered with CK_{PS}.

The signalling radio bearers are used for transfer of signalling data for services delivered by both CS and PS service domains. These signalling radio bearers are ciphered by the CK of the service domain for which the most recent security mode negotiation took place. This may require that the cipher key of an (already ciphered) ongoing signalling connection has to be changed, when a new connection is established with another service domain, or when a security mode negotiation follows a re-authentication during an ongoing connection. This change should be completed by the RNC within five seconds after recieving the security mode command from the VLR/SGSN.

NOTE: For the behaviour of the terminal regarding key changes see section 6.4.5.

6.6.6 UEA identification

Each UEA will be assigned a 4-bit identifier. Currently the following values have been defined:

"0000_2" : UEA0, no encryption.

"0001_2" : UEA1, Kasumi.

The remaining values are not defined.

The use of Kasumi for the ciphering function f8 is specified in TS 35.201 [11] and TS 35.202 [12]. Implementers' test data and design conformance data is provided in TS 35.203 [13] and TS 35.202 [14].

6.7 ~~6.7~~ Access link data integrity for GERAN~~Void~~

The stage 2 specification for GERAN access link data integrity is included in 3GPP TS 43.051[22].

6.8 Access link data confidentiality for GERAN

The stage 2 specification for GERAN access link data confidentiality is included in 3GPP TS 43.051[22].