TSG-RAN Meeting #8 *RP-000214*
Düsseldorf, Germany, 21 – 23 June 2000

Title: **Agreed CRs to TS 25.301**

Source: **TSG-RAN WG2**

Agenda item: **5.2.3**

Doc-1st-	Status-	Spec	CR	Rev	Subject	Cat	Version	Versio
R2-000898	agreed	25.301	036	2	Ciphering related corrections	F	3.4.0	3.5.0
R2-001001	agreed	25.301	037		Clarification of ciphering parameters	F	3.4.0	3.5.0
R2-001145	agreed	25.301	038	1	Signalling radio bearers	D	3.4.0	3.5.0
R2-001185	agreed	25.301	040		Replacement of duplicated information on ciphering description by references	D	3.4.0	3.5.0

3GPP TSG RAN WG2 Meeting #12
Seoul, Korea, 10-13 April 2000

***Document* R2-000898**
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	036r2	Current Version:	3.4.0

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

For submission to:	TSG-RAN #8	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		ME	X	UTRAN / Radio	X	Core Network	

Source: TSG-RAN WG2 **Date:** 11 April 2000

Subject: Ciphering related corrections

Work item:

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change:

Logical channel identity can not be used as BEARER parameter for ciphering algorithm. Radio bearer identity shall be used instead.
If PDCP multiplexing is used always the lowest radio bearer identity of the multiplexed radio bearers shall be used as BEARER parameter.

Clauses affected: 8.2.2

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:

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

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 radio bearer~~logical channel~~ using AM or UM mode plus one for all radio bearers~~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 /~~ non-transparent mode radio bearer~~logical channel~~ is created during a RRC connection, the highest used HFN value (during the lifetime of the current cipher/integrity key set)~~currently in use~~ is incremented, and used as initial value for the ciphering sequence of this new non-transparent mode radio bearer~~logical channel~~. All transparent mode radio bearers have a common hyperframe number (in the MAC layer), which is not incremented due to addition of new transparent mode radio bearer(s). The highest HFN value used during a RRC connection (by any ciphering sequence or any integrity protection 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 24 or 20 MSB are used for the CSN in the RLC modes TM or AM, respectively.

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 radio bearer~~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 radio bearer~~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 radio bearers~~logical channels~~ having the same CK and same COUNT. Each radio bearer~~logical channel~~ is ciphered independently.

In case of multiplexing different radio bearers onto the same RLC entity always the lowest radio bearer identity of the multiplexed radio bearers shall be used as BEARER parameter. This multiplexing is not part of Release 99.

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.

3GPP TSG RAN WG2#13
Oahu, HI, USA, 22nd-26th May, 2000

Document R2-001001
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	037	Current Version:	3.4.0

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

For submission to:	TSG-RAN #8	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		ME	X	UTRAN / Radio	X	Core Network	

Source:	TSG-RAN WG2	**Date:**	2000-05-22

Subject:	Clarification of ciphering parameters

Work item:	

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change:

1) Changed COUNT to COUNT-C, to be consistent with S3 (accompanying CR for TS 25.331)

2) BEARER is the radio bearer ID and 5 bits

3) DIRECTION parameter has been clarified as being 1 bit.

Clauses affected:	8.2.2.1, 8.2.2.3, 8.2.2.4

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:	

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

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-C 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-C 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.

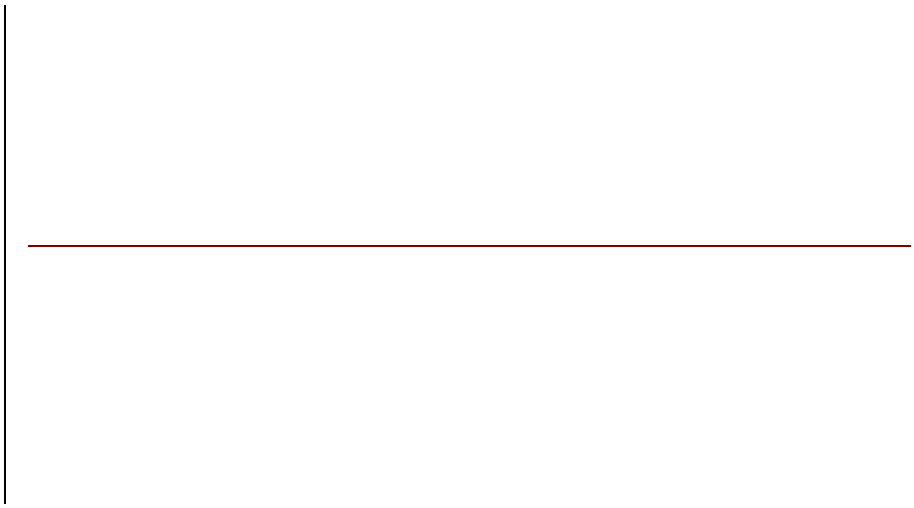

Figure 28: Ciphering algorithm and parameters

~~8.2.2.1 COUNT~~8.2.2.1 COUNT-C

COUNT-C 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-C 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 24 or 20 MSB are used for the CSN in the RLC modes TM or AM, respectively.

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

8.2.2.3 BEARER

This parameter is 5 bits long and 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

The direction identifier DIRECTION is 1 bit long and indicates the transmission direction (uplink/downlink).

The direction identifier ensures that the computed message authentication code of the integrity protection algorithm would not use an identical set of input parameters for the uplink and downlink messages

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

3GPP TSG RAN WG2#13
Oahu, Hawaii, May 22th-26th, 2000

***Document* R2-001145**
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	038r1	Current Version:	3.4.0

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

For submission to:	TSG-RAN #8	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 [ ] ME [X] UTRAN / Radio [X] Core Network [ ]

Source: TSG-RAN WG2 **Date:** May 22, 2000

Subject: Signalling Radio Bearers

Work item:

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification	X		Release 99	X
				Release 00	

Reason for change: Information on establishment and assignment of signalling radio bearers is missing.

Clauses affected: 5.1

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:

5 Radio interface protocol architecture

5.1 Overall protocol structure

The radio interface is layered into three protocol layers:

- the physical layer (L1);
- the data link layer (L2);
- network layer (L3).

Layer 2 is split into following sublayers: Medium Access Control (MAC), Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP) and Broadcast/Multicast Control (BMC).

Layer 3 and RLC are divided into Control (C-) and User (U-) planes. PDCP and BMC exist in the U-plane only.

In the C-plane, Layer 3 is partitioned into sublayers where the lowest sublayer, denoted as Radio Resource Control (RRC), interfaces with layer 2 and terminates in the UTRAN. The next sublayer provides 'Duplication avoidance' functionality as specified in [13]. It terminates in the CN but is part of the Access Stratum; it provides the Access Stratum Services to higher layers. The higher layer signalling such as Mobility Management (MM) and Call Control (CC) are assumed to belong to the non-access stratum, and therefore not in the scope of 3GPP TSG RAN. On the general level, the protocol architecture is similar to the current ITU-R protocol architecture, ITU-R M.1035.

Figure 2 shows the radio interface protocol architecture. Each block in Figure 2 represents an instance of the respective protocol. Service Access Points (SAP) for peer-to-peer communication are marked with circles at the interface between sublayers. The SAP between MAC and the physical layer provides the transport channels (cf. subclause 5.2.1.1). The SAPs between RLC and the MAC sublayer provide the logical channels (cf. subclause 5.3.1.1.1). In the C-plane, the interface between 'Duplication avoidance' and higher L3 sublayers (CC, MM) is defined by the General Control (GC), Notification (Nt) and Dedicated Control (DC) SAPs.

Also shown in the figure are connections between RRC and MAC as well as RRC and L1 providing local inter-layer control services. An equivalent control interface exists between RRC and the RLC sublayer, between RRC and the PDCP sublayer and between RRC and BMC sublayer. These interfaces allow the RRC to control the configuration of the lower layers. For this purpose separate Control SAPs are defined between RRC and each lower layer (PDCP, RLC, MAC, and L1).

The RLC sublayer provides ARQ functionality closely coupled with the radio transmission technique used. There is no difference between RLC instances in C and U planes.

The UTRAN can be requested by the CN to prevent all loss of data (i.e. independently of the handovers on the radio interface), as long as the Iu connection point is not modified. This is a basic requirement to be fulfilled by the UTRAN retransmission functionality as provided by the RLC sublayer.

However, in case of the Iu connection point is changed (e.g. SRNS relocation, streamlining), the prevention of the loss of data may not be guaranteed autonomously by the UTRAN but relies on 'Duplication avoidance' functions in the CN.

There are primarily two kinds of signalling messages transported over the radio interface - RRC generated signalling messages and NAS messages generated in the higher layers. On establishment of the signalling connection between the peer RRC entities three or four signalling radio bearers may be set up. Two of these bearers are set up for transport of RRC generated signalling messages - one for transferring messages through an unacknowledged mode RLC entity [see section 5.3.2. for details on RLC modes] and the other for transferring messages through an acknowledged mode RLC entity. One signalling radio bearer is set up for transferring NAS messages set to "high priority" by the higher layers. An optional signalling radio bearer may be set up for transferring NAS messages set to "low priority" by the higher layers. Subsequent to the establishment of the signalling connection a further signalling radio bearer may be set up for transferring RRC generated signalling messages using transparent mode RLC.

Figure 2: Radio Interface protocol architecture (Service Access Points marked by circles)

3GPP TSP RAN WG 2 Meeting #13
Oahu, Hawaii, USA, 22-26 May 2000

***Document* R2-001185**
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	040	Current Version:	3.4.0

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

For submission to:	TSG-RAN #8	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 [ ] ME [X] UTRAN / Radio [X] Core Network [ ]

Source: TSG-RAN WG2 **Date:** 24 May 2000

Subject: Replacement of duplicated information on ciphering description by references

Work item:

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification	X		Release 99	X
				Release 00	

Reason for change:

Removal of duplicated information between diefferent specifications.

- Section 8 on ciphering is removed.
- References to the Security Architecture specification are included in the MAC, RLC, and RRC functions related to ciphering.

Clauses affected: 5.3.1.2, 5.3.2.2, 5.4.2, 8 (removed)

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:

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

5.3.1.2 MAC functions

The functions of MAC include:

- **Mapping between logical channels and transport channels.** The MAC is responsible for mapping of logical channel(s) onto the appropriate transport channel(s).

- **Selection of appropriate Transport Format for each Transport Channel depending on instantaneous source rate**. Given the Transport Format Combination Set assigned by RRC, MAC selects the appropriate transport format within an assigned transport format set for each active transport channel depending on source rate**.** The control of transport formats ensures efficient use of transport channels.

- **Priority handling between data flows of one UE**. When selecting between the Transport Format Combinations in the given Transport Format Combination Set, priorities of the data flows to be mapped onto the corresponding Transport Channels can be taken into account. Priorities are e.g. given by attributes of Radio Bearer services and RLC buffer status. The priority handling is achieved by selecting a Transport Format Combination for which high priority data is mapped onto L1 with a "high bit rate" Transport Format, at the same time letting lower priority data be mapped with a "low bit rate" (could be zero bit rate) Transport Format. Transport format selection may also take into account transmit power indication from Layer 1.

- **Priority handling between UEs by means of dynamic scheduling**. In order to utilise the spectrum resources efficiently for bursty transfer, a dynamic scheduling function may be applied. MAC realises priority handling on common and shared transport channels. Note that for dedicated transport channels, the equivalent of the dynamic scheduling function is implicitly included as part of the reconfiguration function of the RRC sublayer.

NOTE: In the TDD mode the data to be transported are represented in terms of sets of resource units.

- **Identification of UEs on common transport channels**. When a particular UE is addressed on a common downlink channel, or when a UE is using the RACH, there is a need for inband identification of the UE. Since the MAC layer handles the access to, and multiplexing onto, the transport channels, the identification functionality is naturally also placed in MAC.

- **Multiplexing/demultiplexing of higher layer PDUs into/from transport blocks delivered to/from the physical layer on common transport channels**. MAC should support service multiplexing for common transport channels, since the physical layer does not support multiplexing of these channels.

- **Multiplexing/demultiplexing of higher layer PDUs into/from transport block sets delivered to/from the physical layer on dedicated transport channels**. The MAC allows service multiplexing for dedicated transport channels. This function can be utilised when several upper layer services (e.g. RLC instances) can be mapped efficiently on the same transport channel. In this case the identification of multiplexing is contained in the MAC protocol control information.

- **Traffic volume monitoring**. Measurement of traffic volume on logical channels and reporting to RRC. Based on the reported traffic volume information, RRC performs transport channel switching decisions.

- **Dynamic Transport Channel type switching.** Execution of the switching between common and dedicated transport channels based on a switching decision derived by RRC**.**

- **Ciphering**. This function prevents unauthorised acquisition of data. Ciphering is performed in the MAC layer for transparent RLC mode. Details of the security architecture are specified in [15].

- **Access Service Class selection for RACH transmission**. The RACH resources (i.e. access slots and preamble signatures for FDD, timeslot and channelisation code for TDD) may be divided between different Access Service Classes in order to provide different priorities of RACH usage. In addition it is possible for more than one ASC or for all ASCs to be assigned to the same access slot/signature space. Each access service class will also have a set of back-off parameters associated with it, some or all of which may be broadcast by the network. The MAC function applies the appropriate back-off and indicates to the PHY layer the RACH partition associated to a given MAC PDU transfer.

Next modifed Section

5.3.2.2 RLC Functions

- **Segmentation and reassembly.** This function performs segmentation/reassembly of variable-length higher layer PDUs into/from smaller RLC Payload Units (PUs). The RLC PDU size is adjustable to the actual set of transport formats.

NOTE: Multiple PUs in a RLC PDU is not supported in Release 99. For Release 99 an RLC PDU will include only a single RLC PU.

- **Concatenation.** If the contents of an RLC SDU do not fill an integer number of RLC PUs, the first segment of the next RLC SDU may be put into the RLC PU in concatenation with the last segment of the previous RLC SDU.

- **Padding.** When concatenation is not applicable and the remaining data to be transmitted does not fill an entire RLC PDU of given size, the remainder of the data field shall be filled with padding bits.

- **Transfer of user data.** This function is used for conveyance of data between users of RLC services. RLC supports acknowledged, unacknowledged and transparent data transfer. QoS setting controls transfer of user data.

- **Error correction.** This function provides error correction by retransmission (e.g. Selective Repeat, Go Back N, or a Stop-and-Wait ARQ) in acknowledged data transfer mode.

- **In-sequence delivery of higher layer PDUs**. This function preserves the order of higher layer PDUs that were submitted for transfer by RLC using the acknowledged data transfer service. If this function is not used, out-of-sequence delivery is provided.

- **Duplicate Detection.** This function detects duplicated received RLC PDUs and ensures that the resultant higher Layer PDU is delivered only once to the upper layer.

- **Flow control**. This function allows an RLC receiver to control the rate at which the peer RLC transmitting entity may send information.

- **Sequence number check (Unacknowledged data transfer mode).** This function guarantees the integrity of reassembled PDUs and provides a mechanism for the detection of corrupted RLC SDUs through checking sequence number in RLC PDUs when they are reassembled into a RLC SDU. A corrupted RLC SDU will be discarded.

- **Protocol error detection and recovery**. This function detects and recovers from errors in the operation of the RLC protocol.

- **Ciphering**. This function prevents unauthorised acquisition of data. Ciphering is performed in RLC layer for non-transparent RLC mode. Details of the security architecture are specified in [15].

- **Suspend/resume function**. Suspension and resumption of data transfer as in e.g. LAPDm (cf. GSM 04.05).

Next modifed Section

5.4.2 RRC functions

The Radio Resource Control (RRC) layer handles the control plane signalling of Layer 3 between the UEs and UTRAN. The RRC performs the following functions:

- **Broadcast of information provided by the non-access stratum (Core Network).** The RRC layer performs system information broadcasting from the network to all UEs. The system information is normally repeated on a regular basis. The RRC layer performs the scheduling, segmentation and repetition. This function supports

broadcast of higher layer (above RRC) information. This information may be cell specific or not. As an example RRC may broadcast Core Network location service area information related to some specific cells.

- **Broadcast of information related to the access stratum.** The RRC layer performs system information broadcasting from the network to all UEs. The system information is normally repeated on a regular basis. The RRC layer performs the scheduling, segmentation and repetition. This function supports broadcast of typically cell-specific information.

- **Broadcast of ODMA relay node neighbour information.** The RRC layer performs probe information broadcasting to allow ODMA routeing information to be collected.

- **Establishment, re-establishment, maintenance and release of an RRC connection between the UE and UTRAN.** The establishment of an RRC connection is initiated by a request from higher layers at the UE side to establish the first Signalling Connection for the UE. The establishment of an RRC connection includes an optional cell re-selection, an admission control, and a layer 2 signalling link establishment. The release of an RRC connection can be initiated by a request from higher layers to release the last Signalling Connection for the UE or by the RRC layer itself in case of RRC connection failure. In case of connection loss, the UE requests re-establishment of the RRC connection. In case of RRC connection failure, RRC releases resources associated with the RRC connection.

- **Collating ODMA neighbour list and gradient information.** The ODMA relay node neighbour lists and their respective gradient information will be maintaining by the RRC.

- **Maintenance of number of ODMA relay node neighbours.** The RRC will adjust the broadcast powers used for probing messages to maintain the desired number of neighbours.

- **Establishment, maintenance and release of a route between ODMA relay nodes.** The establishment of an ODMA route and RRC connection based upon the routeing algorithm.

- **Interworking between the Gateway ODMA relay node and the UTRAN.** The RRC layer will control the interworking with the standard TDD or FDD communication link between the Gateway ODMA relay node and the UTRAN.

- **Establishment, reconfiguration and release of Radio Bearers.** The RRC layer can, on request from higher layers, perform the establishment, reconfiguration and release of Radio Bearers in the user plane. A number of Radio Bearers can be established to an UE at the same time. At establishment and reconfiguration, the RRC layer performs admission control and selects parameters describing the Radio Bearer processing in layer 2 and layer 1, based on information from higher layers.

- **Assignment, reconfiguration and release of radio resources for the RRC connection.** The RRC layer handles the assignment of radio resources (e.g. codes, CPCH channels) needed for the RRC connection including needs from both the control and user plane. The RRC layer may reconfigure radio resources during an established RRC connection. This function includes coordination of the radio resource allocation between multiple radio bearers related to the same RRC connection. RRC controls the radio resources in the uplink and downlink such that UE and UTRAN can communicate using unbalanced radio resources (asymmetric uplink and downlink). RRC signals to the UE to indicate resource allocations for purposes of handover to GSM or other radio systems.

- **RRC connection mobility functions.** The RRC layer performs evaluation, decision and execution related to RRC connection mobility during an established RRC connection, such as handover, preparation of handover to GSM or other systems, cell re-selection and cell/paging area update procedures, based on e.g. measurements done by the UE**.**

- **Paging/notification.** The RRC layer can broadcast paging information from the network to selected UEs. Higher layers on the network side can request paging and notification. The RRC layer can also initiate paging during an established RRC connection.

- **Routing of higher layer PDUs.** This function performs at the UE side routing of higher layer PDUs to the correct higher layer entity, at the UTRAN side to the correct RANAP entity.

- **Control of requested QoS**. This function shall ensure that the QoS requested for the Radio Bearers can be met. This includes the allocation of a sufficient number of radio resources.

- **UE measurement reporting and control of the reporting.** The measurements performed by the UE are controlled by the RRC layer, in terms of what to measure, when to measure and how to report, including both

UMTS air interface and other systems. The RRC layer also performs the reporting of the measurements from the UE to the network.

- **Outer loop power control.** The RRC layer controls setting of the target of the closed loop power control.
- **Control of ciphering.** The RRC layer provides procedures for setting of ciphering (on/off) between the UE and UTRAN. Details of the security architecture are specified in [15].
- **Slow DCA**. Allocation of preferred radio resources based on long-term decision criteria. It is applicable only in TDD mode.
- **Arbitration of radio resources on uplink DCH**. This function controls the allocation of radio resources on uplink DCH on a fast basis, using a broadcast channel to send control information to all involved users.

NOTE: This function is implemented in the CRNC.

- **Initial cell selection and re-selection in idle mode.** Selection of the most suitable cell based on idle mode measurements and cell selection criteria.
- **Integrity protection.** This function adds a Message Authentication Code (MAC-I) to those RRC messages that are considered sensitive and/or contain sensitive information. The mechanism how the MAC-I is calculated is described in TS 33.105 [14].
- **Initial Configuration for CBS**
  This function performs the initial configuration of the BMC sublayer.
- **Allocation of radio resources for CBS**
  This function allocates radio resources for CBS based on traffic volume requirements indicated by BMC. The radio resource allocation set by RRC (i.e. the schedule for mapping of CTCH onto FACH/S-CCPCH) is indicated to BMC to enable generation of schedule messages. The resource allocation for CBS shall be broadcast as system information.
- **Configuration for CBS discontinuous reception**
  This function configures the lower layers (L1, L2) of the UE when it shall listen to the resources allocated for CBS based on scheduling information received from BMC.
- **Timing advance control.** The RRC controls the operation of timing advance. It is applicable only in TDD mode.

~~8 Ciphering~~

~~The ciphering architecture is specified in TS 33.102 [15].~~

~~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 24 or 20 MSB are used for the CSN in the RLC modes TM or AM, respectively.

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.