**3GPP TSG-RAN Meeting #18**
**New Orleans, US, 3rd-6th December 2002**

***Tdoc ⌘RP-020874***

*CR-Form-v7*

# CHANGE REQUEST

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ⌘ | **25.321** | **CR** | **156** | ⌘**rev** | **-** | ⌘ Current version: | **3.d.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:*** UICC apps⌘ □ ME ☒ Radio Access Network ☒ Core Network □

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Ciphering of multiple PDUs per TTI | | |
| ***Source:*** | ⌘ | Ericsson, Motorola, Nokia, Nortel | | |
| ***Work item code:*** | ⌘ | TEI | ***Date:*** ⌘ | December 2002 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | R99 |

*Use one of the following categories:*
***F*** *(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 one 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)* |
| *Rel-6* | *(Release 6)* |

***Reason for change:*** ⌘

It is currently not clear from the text in 25.321 how ciphering shall be applied when more than one MAC PDU is transmitted in the same TTI for TM RLC. In 33.105 it is specified that the MAC SDUs are concatenated and ciphered together as one block (Alternative A).
With 4 SDUs in a TTI and a KESYSTREAM BLOCK, K1 this could be expressed as:

CIPHERTEXT = (S1| S2 | S3| S4) xor K1

25.321 specifies that the ciphering unit (the part of the MAC PDU that is ciphered) consists of the MAC SDU (i.e. the MAC PDU excluding the header). 25.321 does not address the case with several MAC PDUs in a TTI.
The text in 25.321 has been interpreted by some as if each SDU shall be ciphered independently with the same ciphering parameters (in particular the same sequence number, CFN). This is denoted Alternative B. It is important to realise that Alternative B means that the same KEYSTREAM BLOCK is used for all SDUs in the TTI. This can be expressed as:

CIPHERTEXT 1 = S1 xor K2
CIPHERTEXT 2 = S2 xor K2
CIPHERTEXT 3 = S3 xor K2
CIPHERTEXT 4 = S4 xor K2

As all the SDUs are X-ored with the same KEYSTREAM BLOCK the transmitted data contains redundancy. The reuse of ciphering parameters in consecutive PDUs is a well known security problem and something that should be avoided.

If different interpretations are implemented in UE and UTRAN it would lead to

| | | |
|---|---|---|
| | | ciphering failure for RABs using TM RLC with more than one TB per TTI. Therefore it is important to clarify this issue in 25.321.<br>We think that Alternative B is not in accordance with the current 3GPP specifications and also not acceptable from a security perspective. Therefore we recommend that the requirement in 33.105 is also captured in 25.321. |
| ***Summary of change:*** | ⌘ | The definition of the PLAINTEXT BLOCK from 33.105 is introduced in 25.321. It is clarified that when several SDUs are transmitted in a TTI, the SDUs are first concatenated and the concatenated SDUs are ciphered together as one block. |
| ***Consequences if not approved:*** | ⌘ | The ambiguity does not affect ciphering of speech (only one TB per TTI per radio bearer). However, several RABs for streaming and conversational services on CS currently defined in 34.108 contains more than one TB per TTI and use TM RLC. This includes “Conversational / unknown / UL:64 DL:64 kbps / CS RAB + UL:3.4 DL:3.4 kbps SRBs for DCCH” which is in GCF Package 1 as high priority and used e.g. for video telephony<br>For the affected RABs:<br>**If no clarification is made:**<br>Different interpretations by different vendors would lead to ciphering failure.<br>**If a clarification is made in a direction where each MAC PDU is ciphered independently:**<br>Consecutive PDUs are ciphered with identical input parameters (in particular the sequence number, CFN will be the same). This gives significant information about the plaintext in the PDUs, i.e. a weakened security level. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 11.5 | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

# 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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 25.301: "Radio Interface Protocol Architecture".

[3] 3GPP TS 25.302: "Services provided by the Physical Layer".

[4] 3GPP TS 25.303: "Interlayer Procedures in Connected Mode".

[5] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[6] 3GPP TS 25.322: "RLC Protocol Specification".

[7] 3GPP TS 25.331: "Radio Resource Control (RRC); protocol specification".

[8] 3GPP TR 25.921: "Guidelines and Principles for Protocol Description and Error Handling".

[9] 3GPP TR 25.990: "Vocabulary for the UTRAN".

[10] 3GPP TS 33.102: "Security architecture".

[11] 3GPP TS 25.425: "UTRAN Iur Interface User Plane Protocols for Common Transport Channel Data Streams".

[12] 3GPP TS 25.133: "Requirements for support of radio resource management (FDD)".

[13] 3GPP TS 25.214: "Physical layer procedures (FDD)".

[14] 3GPP TS 25.123: "Requirements for support of radio resource management (TDD)".

[x] 3GPP TS 33.105: "Cryptographic Algorithm Requirements"

## 11.5 Ciphering

The ciphering function is performed in MAC (i.e. only in MAC-d) if a radio bearer is using the transparent RLC mode. The part of the MAC PDU~~data unit~~ that is ciphered is the MAC SDU and this is shown in Figure 11.5.1 below.

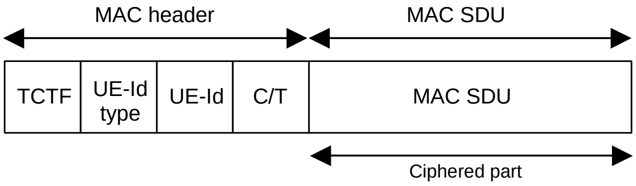

**Figure 11.5.1: Ciphered part~~ing~~ ~~unit~~ for a MAC PDU**

In case a TTI contains multiple MAC PDUs for a given Transparent mode RB, the ciphering unit for this RB  is the bitstring concatenation of all the MAC SDUs, resulting in the PLAINTEXT BLOCK, as defined in [x]. In case there is only one MAC PDU for a given Transparent mode RB, the ciphering unit is the MAC SDU, resulting in the PLAINTEXT BLOCK. The concatenation order is the same as the order of transmission of the Transport Blocks between MAC and Physical layer.

The KEYSTREAM BLOCK as defined in [10] is  applied to the PLAINTEXT BLOCK, and the end result, CIPHERTEXT BLOCK, becomes the ciphered part for the MAC PDU, in case there is only one MAC PDU per RB. In case there is more than one MAC PDU per RB, the CIPHERTEXT BLOCK is split into the corresponding ciphered parts for each MAC PDU. The split order is the same as the order of transmission of the Transport Blocks between MAC and Physical layer.

The ciphering algorithm and key to be used are configured by upper layers [7] and the ciphering method shall be applied as specified in [10].

The parameters that are required by MAC for ciphering are defined in [10] and are input to the ciphering algorithm. The parameters required by MAC which are provided by upper layers [7] are listed below:

- MAC-d HFN (Hyper frame number for radio bearers that are mapped onto transparent mode RLC)
- BEARER (Radio Bearer ID)
- CK (Ciphering Key)

If the TTI consists of more than one 10 ms radio frame, the CFN of the first radio frame in the TTI shall be used as input to the ciphering algorithm for all the data in the TTI.

If the activation time indicated by higher layers for start or stop of ciphering or change of ciphering parameters is not the first CFN in a TTI common to all the transport channels that are multiplexed onto the same CCTrCh, the activation time shall be applied at the first CFN in the following TTI common to all the transport channels that are multiplexed onto the same CCTrCh.

**3GPP TSG-RAN Meeting #18** **Tdoc ⌘RP-020874**
**New Orleans, US, 3rd-6th December 2002**

*CR-Form-v7*

# CHANGE REQUEST

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ⌘ | **25.321** | **CR** | **157** | ⌘**rev** | **-** | ⌘ Current version: | **4.6.0** ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network ☒ Core Network □

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Ciphering of multiple PDUs per TTI | | |
| ***Source:*** | ⌘ | Ericsson, Motorola, Nokia, Nortel | | |
| ***Work item code:*** | ⌘ | TEI | ***Date:*** ⌘ | December 2002 |
| ***Category:*** | ⌘ | **A** | ***Release:*** ⌘ | Rel-4 |

*Use one of the following categories:*
**F** *(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 one 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)* |
| *Rel-6* | *(Release 6)* |

***Reason for change:*** ⌘

It is currently not clear from the text in 25.321 how ciphering shall be applied when more than one MAC PDU is transmitted in the same TTI for TM RLC. In 33.105 it is specified that the MAC SDUs are concatenated and ciphered together as one block (Alternative A).
With 4 SDUs in a TTI and a KESYSTREAM BLOCK, K1 this could be expressed as:

CIPHERTEXT = (S1| S2 | S3| S4) xor K1

25.321 specifies that the ciphering unit (the part of the MAC PDU that is ciphered) consists of the MAC SDU (i.e. the MAC PDU excluding the header). 25.321 does not address the case with several MAC PDUs in a TTI.
The text in 25.321 has been interpreted by some as if each SDU shall be ciphered independently with the same ciphering parameters (in particular the same sequence number, CFN). This is denoted Alternative B. It is important to realise that Alternative B means that the same KEYSTREAM BLOCK is used for all SDUs in the TTI. This can be expressed as:

CIPHERTEXT 1 = S1 xor K2
CIPHERTEXT 2 = S2 xor K2
CIPHERTEXT 3 = S3 xor K2
CIPHERTEXT 4 = S4 xor K2

As all the SDUs are X-ored with the same KEYSTREAM BLOCK the transmitted data contains redundancy. The reuse of ciphering parameters in consecutive PDUs is a well known security problem and something that should be avoided.

If different interpretations are implemented in UE and UTRAN it would lead to

|  |  |  |
|---|---|---|
|  |  | ciphering failure for RABs using TM RLC with more than one TB per TTI. Therefore it is important to clarify this issue in 25.321.<br>We think that Alternative B is not in accordance with the current 3GPP specifications and also not acceptable from a security perspective. Therefore we recommend that the requirement in 33.105 is also captured in 25.321. |
| ***Summary of change:*** | ⌘ | The definition of the PLAINTEXT BLOCK from 33.105 is introduced in 25.321. It is clarified that when several SDUs are transmitted in a TTI, the SDUs are first concatenated and the concatenated SDUs are ciphered together as one block. |
| ***Consequences if not approved:*** | ⌘ | The ambiguity does not affect ciphering of speech (only one TB per TTI per radio bearer). However, several RABs for streaming and conversational services on CS currently defined in 34.108 contains more than one TB per TTI and use TM RLC. This includes “Conversational / unknown / UL:64 DL:64 kbps / CS RAB + UL:3.4 DL:3.4 kbps SRBs for DCCH” which is in GCF Package 1 as high priority and used e.g. for video telephony<br>For the affected RABs:<br>**If no clarification is made:**<br>Different interpretations by different vendors would lead to ciphering failure.<br>**If a clarification is made in a direction where each MAC PDU is ciphered independently:**<br>Consecutive PDUs are ciphered with identical input parameters (in particular the sequence number, CFN will be the same). This gives significant information about the plaintext in the PDUs, i.e. a weakened security level. |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 11.5 |  |  |  |  |
|  |  | **Y** | **N** |  |  |  |
| ***Other specs affected:*** | ⌘ |  | **X** | Other core specifications | ⌘ |  |
|  |  |  | **X** | Test specifications |  |  |
|  |  |  | **X** | O&M Specifications |  |  |
| ***Other comments:*** | ⌘ |  |  |  |  |  |

## How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

# 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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 25.301: "Radio Interface Protocol Architecture".

[3] 3GPP TS 25.302: "Services provided by the Physical Layer".

[4] 3GPP TS 25.303: "Interlayer Procedures in Connected Mode".

[5] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[6] 3GPP TS 25.322: "RLC Protocol Specification".

[7] 3GPP TS 25.331: "Radio Resource Control (RRC); protocol specification".

[8] 3GPP TR 25.921: "Guidelines and Principles for Protocol Description and Error Handling".

[9] 3GPP TR 25.990: "Vocabulary for the UTRAN".

[10] 3GPP TS 33.102: "Security architecture".

[11] 3GPP TS 25.425: "UTRAN Iur Interface User Plane Protocols for Common Transport Channel Data Streams".

[12] 3GPP TS 25.133: "Requirements for support of radio resource management (FDD)".

[13] 3GPP TS 25.214: "Physical layer procedures (FDD)".

[14] 3GPP TS 25.123: "Requirements for support of radio resource management (TDD)".

[x] 3GPP TS 33.105: "Cryptographic Algorithm Requirements"

## 11.5 Ciphering

The ciphering function is performed in MAC (i.e. only in MAC-d) if a radio bearer is using the transparent RLC mode. The part of the MAC PDU~~data unit~~ that is ciphered is the MAC SDU and this is shown in Figure 11.5.1 below.

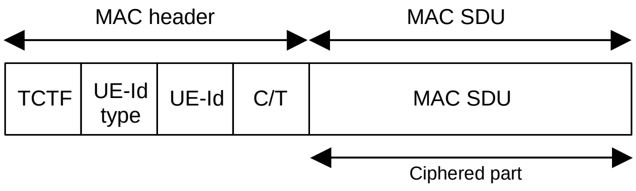

**Figure 11.5.1: Ciphered part~~ing~~ unit for a MAC PDU**

In case a TTI contains multiple MAC PDUs for a given Transparent mode RB, the ciphering unit for this RB is the bitstring concatenation of all the MAC SDUs, resulting in the PLAINTEXT BLOCK, as defined in [x]. In case there is only one MAC PDU for a given Transparent mode RB, the ciphering unit is the MAC SDU, resulting in the PLAINTEXT BLOCK. The concatenation order is the same as the order of transmission of the Transport Blocks between MAC and Physical layer.

The KEYSTREAM BLOCK as defined in [10] is applied to the PLAINTEXT BLOCK, and the end result, CIPHERTEXT BLOCK, becomes the ciphered part for the MAC PDU, in case there is only one MAC PDU per RB. In case there is more than one MAC PDU per RB, the CIPHERTEXT BLOCK is split into the corresponding ciphered parts for each MAC PDU. The split order is the same as the order of transmission of the Transport Blocks between MAC and Physical layer.

The ciphering algorithm and key to be used are configured by upper layers [7] and the ciphering method shall be applied as specified in [10].

The parameters that are required by MAC for ciphering are defined in [10] and are input to the ciphering algorithm. The parameters required by MAC which are provided by upper layers [7] are listed below:

- MAC-d HFN (Hyper frame number for radio bearers that are mapped onto transparent mode RLC)
- BEARER (Radio Bearer ID)
- CK (Ciphering Key)

If the TTI consists of more than one 10 ms radio frame, the CFN of the first radio frame in the TTI shall be used as input to the ciphering algorithm for all the data in the TTI.

If the activation time indicated by higher layers for start or stop of ciphering or change of ciphering parameters is not the first CFN in a TTI common to all the transport channels that are multiplexed onto the same CCTrCh, the activation time shall be applied at the first CFN in the following TTI common to all the transport channels that are multiplexed onto the same CCTrCh.

**3GPP TSG-RAN Meeting #18**
**New Orleans, US, 3rd-6th December 2002**

***Tdoc ⌘RP-020874***

*CR-Form-v7*

# CHANGE REQUEST

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ⌘ | **25.321** | **CR** | **158** | ⌘**rev** | **-** | ⌘ | Current version: | **5.2.0** ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network ☒ Core Network □

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Ciphering of multiple PDUs per TTI | | |
| ***Source:*** | ⌘ | Ericsson, Motorola, Nokia, Nortel | | |
| ***Work item code:*** | ⌘ | TEI | ***Date:*** ⌘ | December 2002 |
| ***Category:*** | ⌘ | **A** | ***Release:*** ⌘ | Rel-5 |

*Use one of the following categories:*
**F** *(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 one 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)* |
| *Rel-6* | *(Release 6)* |

***Reason for change:*** ⌘ It is currently not clear from the text in 25.321 how ciphering shall be applied when more than one MAC PDU is transmitted in the same TTI for TM RLC. In 33.105 it is specified that the MAC SDUs are concatenated and ciphered together as one block (Alternative A).
With 4 SDUs in a TTI and a KESYSTREAM BLOCK, K1 this could be expressed as:

CIPHERTEXT = (S1| S2 | S3| S4) xor K1

25.321 specifies that the ciphering unit (the part of the MAC PDU that is ciphered) consists of the MAC SDU (i.e. the MAC PDU excluding the header). 25.321 does not address the case with several MAC PDUs in a TTI.
The text in 25.321 has been interpreted by some as if each SDU shall be ciphered independently with the same ciphering parameters (in particular the same sequence number, CFN). This is denoted Alternative B. It is important to realise that Alternative B means that the same KEYSTREAM BLOCK is used for all SDUs in the TTI. This can be expressed as:

CIPHERTEXT 1 = S1 xor K2
CIPHERTEXT 2 = S2 xor K2
CIPHERTEXT 3 = S3 xor K2
CIPHERTEXT 4 = S4 xor K2

As all the SDUs are X-ored with the same KEYSTREAM BLOCK the transmitted data contains redundancy. The reuse of ciphering parameters in consecutive PDUs is a well known security problem and something that should be avoided.

If different interpretations are implemented in UE and UTRAN it would lead to

| | | |
|---|---|---|
| | | ciphering failure for RABs using TM RLC with more than one TB per TTI. Therefore it is important to clarify this issue in 25.321.<br>We think that Alternative B is not in accordance with the current 3GPP specifications and also not acceptable from a security perspective. Therefore we recommend that the requirement in 33.105 is also captured in 25.321. |
| ***Summary of change:*** | ⌘ | The definition of the PLAINTEXT BLOCK from 33.105 is introduced in 25.321. It is clarified that when several SDUs are transmitted in a TTI, the SDUs are first concatenated and the concatenated SDUs are ciphered together as one block. |
| ***Consequences if not approved:*** | ⌘ | The ambiguity does not affect ciphering of speech (only one TB per TTI per radio bearer). However, several RABs for streaming and conversational services on CS currently defined in 34.108 contains more than one TB per TTI and use TM RLC. This includes “Conversational / unknown / UL:64 DL:64 kbps / CS RAB + UL:3.4 DL:3.4 kbps SRBs for DCCH” which is in GCF Package 1 as high priority and used e.g. for video telephony<br>For the affected RABs:<br>**If no clarification is made:**<br>Different interpretations by different vendors would lead to ciphering failure.<br>**If a clarification is made in a direction where each MAC PDU is ciphered independently:**<br>Consecutive PDUs are ciphered with identical input parameters (in particular the sequence number, CFN will be the same). This gives significant information about the plaintext in the PDUs, i.e. a weakened security level. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 11.5 | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

# 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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 25.301: "Radio Interface Protocol Architecture".

[3] 3GPP TS 25.302: "Services provided by the Physical Layer".

[4] 3GPP TS 25.303: "Interlayer Procedures in Connected Mode".

[5] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[6] 3GPP TS 25.322: "RLC Protocol Specification".

[7] 3GPP TS 25.331: "Radio Resource Control (RRC); protocol specification".

[8] 3GPP TR 25.921: "Guidelines and Principles for Protocol Description and Error Handling".

[9] 3GPP TR 25.990: "Vocabulary for the UTRAN".

[10] 3GPP TS 33.102: "Security architecture".

[11] 3GPP TS 25.425: "UTRAN Iur Interface User Plane Protocols for Common Transport Channel Data Streams".

[12] 3GPP TS 25.133: "Requirements for support of radio resource management (FDD)".

[13] 3GPP TS 25.214: "Physical layer procedures (FDD)".

[14] 3GPP TS 25.123: "Requirements for support of radio resource management (TDD)".

[x] 3GPP TS 33.105: "Cryptographic Algorithm Requirements"

## 11.5 Ciphering

The ciphering function is performed in MAC (i.e. only in MAC-d) if a radio bearer is using the transparent RLC mode. The part of the MAC PDU~~data unit~~ that is ciphered is the MAC SDU and this is shown in Figure 11.5.1 below.

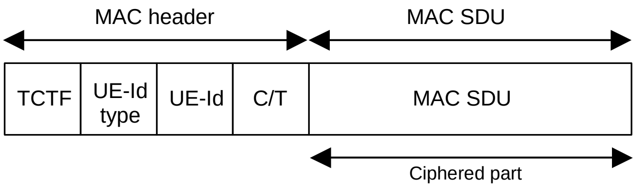

**Figure 11.5.1: Ciphered part~~ing~~ unit for a MAC PDU**

In case a TTI contains multiple MAC PDUs for a given Transparent mode RB, the ciphering unit for this RB is the bitstring concatenation of all the MAC SDUs, resulting in the PLAINTEXT BLOCK, as defined in [x]. In case there is only one MAC PDU for a given Transparent mode RB, the ciphering unit is the MAC SDU, resulting in the PLAINTEXT BLOCK. The concatenation order is the same as the order of transmission of the Transport Blocks between MAC and Physical layer.

The KEYSTREAM BLOCK as defined in [10] is applied to the PLAINTEXT BLOCK, and the end result, CIPHERTEXT BLOCK, becomes the ciphered part for the MAC PDU, in case there is only one MAC PDU per RB. In case there is more than one MAC PDU per RB, the CIPHERTEXT BLOCK is split into the corresponding ciphered parts for each MAC PDU. The split order is the same as the order of transmission of the Transport Blocks between MAC and Physical layer.

The ciphering algorithm and key to be used are configured by upper layers [7] and the ciphering method shall be applied as specified in [10].

The parameters that are required by MAC for ciphering are defined in [10] and are input to the ciphering algorithm. The parameters required by MAC which are provided by upper layers [7] are listed below:

- MAC-d HFN (Hyper frame number for radio bearers that are mapped onto transparent mode RLC)
- BEARER (Radio Bearer ID)
- CK (Ciphering Key)

If the TTI consists of more than one 10 ms radio frame, the CFN of the first radio frame in the TTI shall be used as input to the ciphering algorithm for all the data in the TTI.

If the activation time indicated by higher layers for start or stop of ciphering or change of ciphering parameters is not the first CFN in a TTI common to all the transport channels that are multiplexed onto the same CCTrCh, the activation time shall be applied at the first CFN in the following TTI common to all the transport channels that are multiplexed onto the same CCTrCh.