TSG-RAN Meeting #18 ***RP-020719***

***New-Orleans, USA, 03* - 06 December 2002**

Title: **CRs (Release '99 and Rel-4/Rel-5 category A) to TS 25.322**

Source: **TSG-RAN WG2**

Agenda item: **7.2.3**

Doc-1st-	Status-	Spec	CR	Rev	Phase	Subject	Cat	Version-	Version
R2-023056	Agreed	25.322	210	-	R99	RB id in ciphering	F	3.12.0	3.13.0
R2-023057	Agreed	25.322	211	-	Rel-4	RB id in ciphering	A	4.6.0	4.7.0
R2-023058	Agreed	25.322	212	-	Rel-5	RB id in ciphering	A	5.2.0	5.3.0

3GPP TSG-RAN2 Meeting #33
Sophia Antipolis, France, 11th-15th November 2002

Tdoc ⌘R2-023056

CR-Form-v7

CHANGE REQUEST

⌘ **25.322** **CR** **210** ⌘ **rev** **-** ⌘ Current version: **3.12.0** ⌘

*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 [X] Radio Access Network [X] Core Network [ ]

Title:	⌘	RB id in ciphering
Source:	⌘	Ericsson
Work item code:	⌘	TEI
Date:	⌘	2002-11-12
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: ⌘ According to 25.331 section 8.6.3.4, 8.6.4.1, 8.6.4.3 and 10.3.4.16 the "RB id" –1 shall be used as the value of BEARER in the ciphering algorithm. in the RLC specification this fact is not reflected (the text in RLC is to a large extent taken from 33.102 which does not go into this level of detail).

Summary of change: ⌘ The value of BEARER is changed from "RB id" to "RB id-1" to align with 25.331

Consequences if not approved: ⌘ Risk for erroneous implementation leading to ciphering failure. However the proposed alignment is considered to be consistent with the general RAN2 understanding.

Backwards compatibility analysis:
If the CR is not implemented in both UE and UTRAN, the UE and UTRAN may potentially use different values of the parameter BEARER in the ciphering algorithm. In this case, the ciphering will fail on all RBs and SRBs.

Impact on T1 specifications:
None. T1 is already aligned with this clarification.

Clauses affected: ⌘ 9.7.8

Other specs affected: ⌘

Y	N	
	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.

9.7.8 Ciphering for acknowledged and unacknowledged mode

The ciphering function is performed in RLC, according to the following rules if a radio bearer is using a non-transparent RLC mode (AM or UM). The data unit that is ciphered, depends on the transmission mode as described below.

- For RLC UM mode, the ciphering unit is the UMD PDU excluding the first octet, i.e. excluding the UMD PDU header. This is shown below in Figure 9.19.

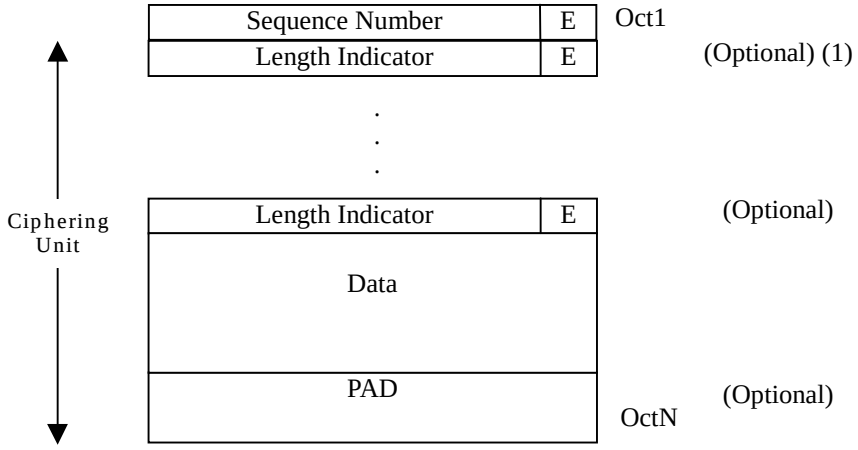

Figure 9.19: Ciphering unit for a UMD PDU

- For RLC AM mode, the ciphering unit is the AMD PDU excluding the first two octets, i.e. excluding the AMD PDU header. This is shown below in Figure 9.20.

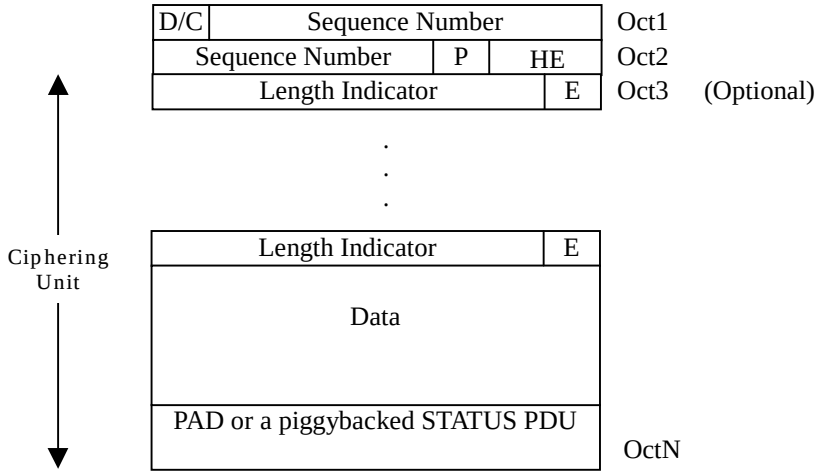

Figure 9.20: Ciphering unit for an AMD PDU

The ciphering algorithm and key to be used are configured by upper layers [8] and the ciphering method shall be applied as specified in [9].

The parameters that are required by RLC for ciphering are defined in [9] and are input to the ciphering algorithm. The parameters required by RLC which are provided by upper layers [8] are listed below:

- RLC AM HFN (Hyper frame number for radio bearers that are mapped onto RLC AM);
- RLC UM HFN (Hyper frame number for radio bearers that are mapped onto RLC UM);
- BEARER (defined as the radio bearer identifier in [9]. It will use the value RB identity –1 as in [8])

(~~Radio Bearer ID -1~~);

- CK (Ciphering Key).

3GPP TSG-RAN2 Meeting #33
Sophia Antipolis, France, 11th-15th November 2002

Tdoc ⌘R2-023057

CR-Form-v7

CHANGE REQUEST

⌘ **25.322** **CR** **211** ⌘ **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 [X] Radio Access Network [X] Core Network [ ]

Title:	⌘	RB id in ciphering
Source:	⌘	Ericsson
Work item code:	⌘	TEI
Date:	⌘	2002-11-12
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:	⌘	According to 25.331 section 8.6.3.4, 8.6.4.1, 8.6.4.3 and 10.3.4.16 the "RB id" –1 shall be used as the value of BEARER in the ciphering algorithm. in the RLC specification this fact is not reflected (the text in RLC is to a large extent taken from 33.102 which does not go into this level of detail).
Summary of change:	⌘	The value of BEARER is changed from "RB id" to "RB id-1" to align with 25.331
Consequences if not approved:	⌘	Risk for erroneous implementation leading to ciphering failure. However the proposed alignment is considered to be consistent with the general RAN2 understanding. **Backwards compatibility analysis:** If the CR is not implemented in both UE and UTRAN, the UE and UTRAN may potentially use different values of the parameter BEARER in the ciphering algorithm. In this case, the ciphering will fail on all RBs and SRBs. **Impact on T1 specifications:** None. T1 is already aligned with this clarification.

Clauses affected:	⌘	9.7.8			
Other specs affected:	⌘	**Y**	**N**		
			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.

9.7.8 Ciphering for acknowledged and unacknowledged mode

The ciphering function is performed in RLC, according to the following rules if a radio bearer is using a non-transparent RLC mode (AM or UM). The data unit that is ciphered, depends on the transmission mode as described below.

- For RLC UM mode, the ciphering unit is the UMD PDU excluding the first octet, i.e. excluding the UMD PDU header. This is shown below in Figure 9.19.

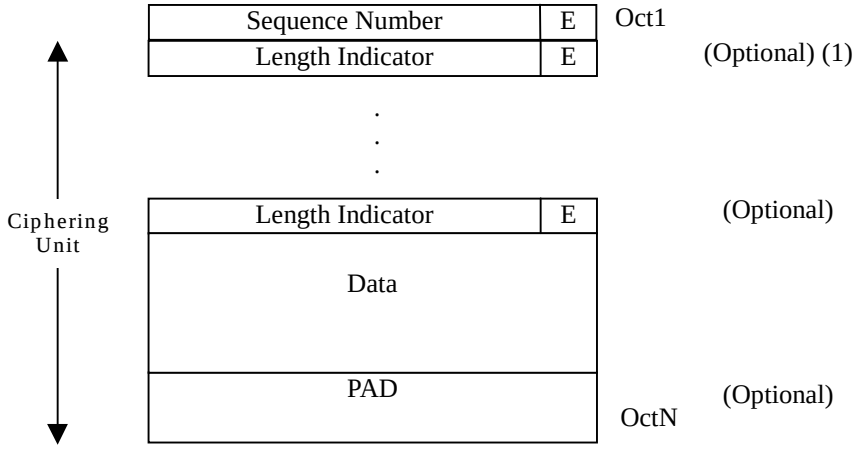

Figure 9.19: Ciphering unit for a UMD PDU

- For RLC AM mode, the ciphering unit is the AMD PDU excluding the first two octets, i.e. excluding the AMD PDU header. This is shown below in Figure 9.20.

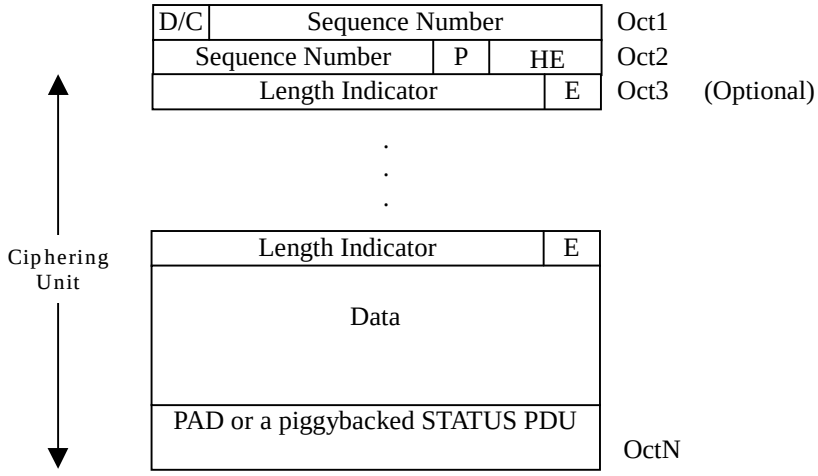

Figure 9.20: Ciphering unit for an AMD PDU

The ciphering algorithm and key to be used are configured by upper layers [8] and the ciphering method shall be applied as specified in [9].

The parameters that are required by RLC for ciphering are defined in [9] and are input to the ciphering algorithm. The parameters required by RLC which are provided by upper layers [8] are listed below:

- RLC AM HFN (Hyper frame number for radio bearers that are mapped onto RLC AM);
- RLC UM HFN (Hyper frame number for radio bearers that are mapped onto RLC UM);
- BEARER (defined as the radio bearer identifier in [9]. It will use the value RB identity –1 as in [8])

(~~Radio Bearer ID -1~~);

- CK (Ciphering Key).

3GPP TSG-RAN2 Meeting #33
Sophia Antipolis, France, 11th-15th November 2002

Tdoc ⌘R2-023058

CR-Form-v7

CHANGE REQUEST

⌘ **25.322** **CR** **212** ⌘ **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 [X] Radio Access Network [X] Core Network [ ]

Title:	⌘	RB id in ciphering
Source:	⌘	Ericsson
Work item code:	⌘	TEI
Date:	⌘	2002-11-12
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: ⌘ According to 25.331 section 8.6.3.4, 8.6.4.1, 8.6.4.3 and 10.3.4.16 the "RB id" –1 shall be used as the value of BEARER in the ciphering algorithm. in the RLC specification this fact is not reflected (the text in RLC is to a large extent taken from 33.102 which does not go into this level of detail).

Summary of change: ⌘ The value of BEARER is changed from "RB id" to "RB id-1" to align with 25.331

Consequences if not approved: ⌘ Risk for erroneous implementation leading to ciphering failure. However the proposed alignment is considered to be consistent with the general RAN2 understanding.

Backwards compatibility analysis:
If the CR is not implemented in both UE and UTRAN, the UE and UTRAN may potentially use different values of the parameter BEARER in the ciphering algorithm. In this case, the ciphering will fail on all RBs and SRBs.

Impact on T1 specifications:
None. T1 is already aligned with this clarification.

Clauses affected: ⌘ 9.7.8

Other specs affected: ⌘

Y	N	
	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.

9.7.8 Ciphering for acknowledged and unacknowledged mode

The ciphering function is performed in RLC, according to the following rules if a radio bearer is using a non-transparent RLC mode (AM or UM). The data unit that is ciphered, depends on the transmission mode as described below.

- For RLC UM mode, the ciphering unit is the UMD PDU excluding the first octet, i.e. excluding the UMD PDU header. This is shown below in Figure 9.19.

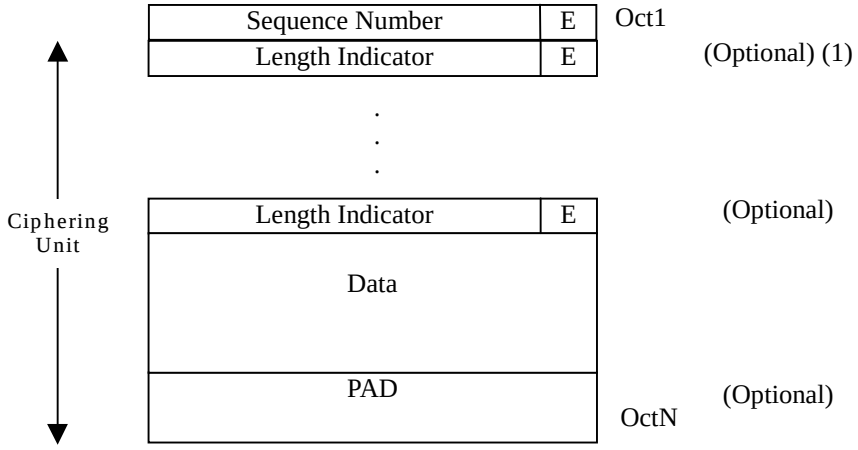

Figure 9.19: Ciphering unit for a UMD PDU

- For RLC AM mode, the ciphering unit is the AMD PDU excluding the first two octets, i.e. excluding the AMD PDU header. This is shown below in Figure 9.20.

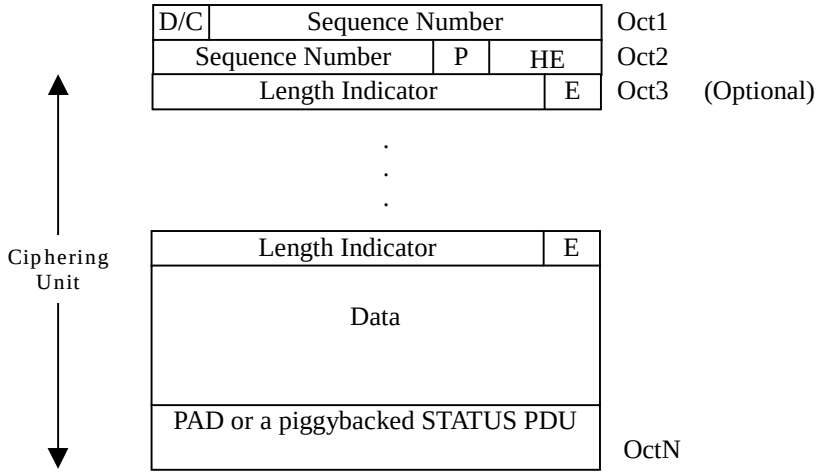

Figure 9.20: Ciphering unit for an AMD PDU

The ciphering algorithm and key to be used are configured by upper layers [8] and the ciphering method shall be applied as specified in [9].

The parameters that are required by RLC for ciphering are defined in [9] and are input to the ciphering algorithm. The parameters required by RLC which are provided by upper layers [8] are listed below:

- RLC AM HFN (Hyper frame number for radio bearers that are mapped onto RLC AM);
- RLC UM HFN (Hyper frame number for radio bearers that are mapped onto RLC UM);
- BEARER (defined as the radio bearer identifier in [9]. It will use the value RB identity –1 as in [8])

(~~Radio Bearer ID -1~~);

- CK (Ciphering Key).