TSG-RAN Meeting #17 Biarritz, France, 3 - 6 September 2002

Title: Agreed CRs (Release '99 and Rel-4/Rel-5 category A) to TS 25.331

Source: TSG-RAN WG2

Agenda item: 7.2.3

Doc-1st-	Status-	Spec	CR	Rev	Phase	Subject	Cat	Versio	Versio
R2-022319	agreed	25.331	1639		R99	Security clarifications	F	3.11.0	3.12.0
R2-022320	agreed	25.331	1640		Rel-4	Security clarifications	А	4.5.0	4.6.0
R2-022321	agreed	25.331	1641		Rel-5	Security clarifications	А	5.1.0	5.2.0
R2-022322	agreed	25.331	1642		R99	Correction to the actions of Out of service area and In service area	F	3.11.0	3.12.0
R2-022323	agreed	25.331	1643		Rel-4	Correction to the actions of Out of service area and In service area	A	4.5.0	4.6.0
R2-022324	agreed	25.331	1644		Rel-5	Correction to the actions of Out of service area and In service area	A	5.1.0	5.2.0
R2-022325	agreed	25.331	1645		R99	TVM pending time after trigger and initial conditions	F	3.11.0	3.12.0
R2-022326	agreed	25.331	1646		Rel-4	TVM pending time after trigger and initial conditions	A	4.5.0	4.6.0
R2-022327	agreed	25.331	1647		Rel-5	TVM pending time after trigger and initial conditions	A	5.1.0	5.2.0
R2-022442	agreed	25.331	1648	1	R99	Handling of Downlink information for each RL in reconfiguration messages	F	3.11.0	3.12.0
R2-022443	agreed	25.331	1649	1	Rel-4	Handling of Downlink information for each RL in reconfiguration messages	A	4.5.0	4.6.0
R2-022444	agreed	25.331	1650	1	Rel-5	Handling of Downlink information for each RL in reconfiguration messages	A	5.1.0	5.2.0
R2-022369	agreed	25.331	1653		R99	Nested Cell Updates and SRNS Relocation	F	3.11.0	3.12.0
R2-022370	agreed	25.331	1654		Rel-4	Nested Cell Updates and SRNS Relocation	A	4.5.0	4.6.0
R2-022371	-	25.331	1655		Rel-5	Nested Cell Updates and SRNS Relocation	А	5.1.0	5.2.0
R2-022405	agreed	25.331	1668		R99	Corrections to security	F	3.11.0	3.12.0
R2-022406	agreed	25.331	1669		Rel-4	Corrections to security	А	4.5.0	4.6.0
R2-022407	agreed	25.331	1670		Rel-5	Corrections to security	А	5.1.0	5.2.0

Rel-6

(Release 6)

	CHANGE R	EQUEST		CR-Form-v7
ж	<mark>25.331</mark> CR <mark>1639</mark> жг	ev <mark>-</mark> ^{# Cur}	rrent version	3.11.0 *
For <u>HELP</u> on	using this form, see bottom of this pag	e or look at the po	p-up text ove	er the X symbols.
Proposed change	e affects: UICC apps# M	E X Radio Acces	s Network	Core Network
Title: ៖	Security clarifications			
Source: ೫	TSG-RAN WG2			
Work item code: 8	f TEI		Date: ೫ 1	9 August 2002
Category: ទ	 F Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in a B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above cate be found in 3GPP TR 21,900. 	U an earlier release) e)	lse <u>one</u> of the 2 (GS R96 (Re R97 (Re R98 (Re R99 (Re Rel-4 (Re	99 following releases: SM Phase 2) elease 1996) elease 1997) elease 1998) elease 1999) elease 4) elease 5)

Reason for change: ३	Nowhere it is clearly stated that the ciphering is not applicable to signalling radio bearer RB0.
Summary of change: ៖	It is clarified that ciphering is never applied to signalling radio bearer RB0. It is also clarified that signalling radio bearer RB0 is not suspended during security mode control procedure.
	Isolated Impact Change Analysis.
	This change clarifies the ciphering procedure. It is a clarification that captures the common understanding in the industry. It would not affect implementations behaving like indicated in the CR, it would affect implementations supporting the corrected functionality otherwise.
	Impact on test specifications No impact
Consequences if	Some implementations may try to apply ciphering also on signalling radio bearer
not approved:	RB0, making impossible to implement ciphering in CELL_FACH state.
Clauses affected:	6.3, 8.1.12.2.1
	YN
Other specs	
affected:	X Test specifications
	X O&M Specifications
Other comments:	8
•	

Comprehensive information and tips about how to create CRs can be found at <u>http://www.3gpp.org/specs/CR.htm</u>. 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 <u>ftp://ftp.3gpp.org/specs/</u> 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.

[...]

6.3 Signalling Radio Bearers

The Radio Bearers (RB) available for transmission of RRC messages are defined as "signalling radio bearers" and are specified in the following. The UE and UTRAN shall select the signalling radio bearers for RRC messages using RLC-TM, RLC-UM or RLC-AM on the DCCH and CCCH, according to the following:

- Signalling radio bearer RB0 shall be used for all messages sent on the CCCH (UL: RLC-TM, DL: RLC-UM).
- Signalling radio bearer RB1 shall be used for all messages sent on the DCCH, when using RLC unacknowledged mode (RLC-UM).
- Signalling radio bearer RB2 shall be used for all messages sent on the DCCH, when using RLC acknowledged mode (RLC-AM), except for the RRC messages carrying higher layer (NAS) signalling.
- Signalling radio bearer RB3 and optionally Signalling radio bearer RB4 shall be used for the RRC messages carrying higher layer (NAS) signalling and sent on the DCCH in RLC acknowledged mode (RLC-AM), as specified in subclauses 8.1.8., 8.1.9 and 8.1.10.
- RRC messages on the SHCCH are mapped either on RACH or on the USCH in the uplink using TM and either on FACH or on the DSCH using RLC-UM. These messages are only specified for TDD mode.

The Radio Bearer configuration for signalling radio bearer RB0, SHCCH, BCCH on FACH and PCCH on PCH are specified in subclauses 13.6, 13.6a, 13.6b and 13.6c.

When an RRC message is transmitted in DL on DCCH or CCCH or SHCCH using RLC UM, RRC may indicate to RLC that a special RLC length indicator indicating that an RLC SDU begins in the beginning of an RLC PDU should be used [16]. The UE shall follow the normal rules for discarding of RLC SDUs when this Length Indicator is not present.

Ciphering is never applied to signalling radio bearer RB0.

[...]

8.1.12 Security mode control

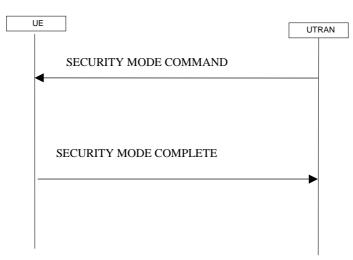


Figure 8.1.12-1: Security mode control procedure

8.1.12.1 General

The purpose of this procedure is to trigger the stop or start of ciphering or to command the restart of the ciphering with a new ciphering configuration, for the radio bearers of one CN domain and for all signalling radio bearers.

It is also used to start integrity protection or to modify the integrity protection configuration for all signalling radio bearers.

8.1.12.2 Initiation

8.1.12.2.1 Ciphering configuration change

To start/restart ciphering, UTRAN sends a SECURITY MODE COMMAND message on the downlink DCCH in AM RLC using the most recent ciphering configuration. If no such ciphering configuration exists then the SECURITY MODE COMMAND is not ciphered. UTRAN should not transmit a SECURITY MODE COMMAND to signal a change in ciphering algorithm.

When configuring ciphering, UTRAN should ensure that the UE needs to store at most two different ciphering configurations (keyset and algorithm) per CN domain, in total over all radio bearers at any given time. For signalling radio bearers the total number of ciphering configurations that need to be stored is at most three. Prior to sending the SECURITY MODE COMMAND, for the CN domain indicated in the IE "CN domain identity" in the SECURITY MODE COMMAND, UTRAN should:

- 1> suspend all radio bearers using RLC-AM or RLC-UM and all signalling radio bearers using RLC-AM or RLC-UM, except the signalling radio bearer used to send the SECURITY MODE COMMAND message on the downlink DCCH in RLC-AM, and except signalling radio bearer RB0, according to the following:
 - 2> not transmit RLC PDUs with sequence number greater than or equal to the number in IE "Radio bearer downlink ciphering activation time info" on all suspended radio bearers and all suspended signalling radio bearers.
- 1> set, for the signalling radio bearer used to send the SECURITY MODE COMMAND, the "RLC send sequence number" in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info", at which time the new ciphering configuration shall be applied;
- 1> if a transparent mode radio bearer for this CN domain exists:
 - 2> include the IE "Ciphering activation time for DPCH" in IE "Ciphering mode info", at which time the new ciphering configuration shall be applied;
- 1> set, for each suspended radio bearer and signalling radio bearer that has no pending ciphering activation time set by a previous security mode control procedure, an "RLC send sequence number" in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info", at which time the new ciphering configuration shall be applied;
- 1> set, for each suspended radio bearer and signalling radio bearer that has a pending ciphering activation time set by a previous security mode control procedure, the "RLC send sequence number" in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info" to the value used in the previous security mode control procedure, at which time the latest ciphering configuration shall be applied;
- 1> if Integrity protection has already been started for the UE:
 - 2> if for the CN domain indicated in the IE "CN domain identity" in the SECURITY MODE COMMAND, a new security key set (new ciphering and integrity protection keys) has been received from upper layers since the transmission of the last SECURITY MODE COMMAND message for that CN domain:
 - 3> include the IE "Integrity protection mode info" in the SECURITY MODE COMMAND.
 - 2> if the IE "CN domain identity" in the SECURITY MODE COMMAND is different from the IE "CN domain identity" that was sent in the previous SECURITY MODE COMMAND message to the UE:

3> include the IE "Integrity protection mode info" in the SECURITY MODE COMMAND.

1> transmit the SECURITY MODE COMMAND message on RB2.

[...]

Rel-6

(Release 6)

CHANGE REQUEST										
ж	25.331 CR 1640 #re	🖌 🗕 🕷 Curre	ent version	4.5.0	ж					
For <u>HELP</u> on	using this form, see bottom of this page	or look at the pop-	up text ove	er the ¥ syn	nbols.					
	_		_	_						
Proposed change	e affects: UICC apps೫ ME	X Radio Access	Network	Core Net	twork					
Title:	Security clarifications									
Source:	# TSG-RAN WG2									
Work item code:	H TEI	D	Date: ೫ 1	9 August 20	02					
Category:	ж <mark>А</mark>	Polo	ase: ೫ R	ol_/						
category.	Use <u>one</u> of the following categories:			following relea	ases:					
	<i>F</i> (correction)			SM Phase 2)						
	A (corresponds to a correction in an	earlier release) I	R96 (Re	elease 1996)						
	B (addition of feature), R97									
	C (functional modification of feature)			elease 1998)						
	D (editorial modification)			elease 1999)						
	Detailed explanations of the above categor be found in 3GPP TR 21.900.			elease 4) elease 5)						

Reason for change: ೫	Nowhere it is clearly stated that the ciphering is not applicable to signalling radio bearer RB0.						
Summary of change: #	It is clarified that ciphering is never applied to signalling radio bearer RB0. It is also clarified that signalling radio bearer RB0 is not suspended during security mode control procedure.						
	Isolated Impact Change Analysis.						
	This change clarifies the ciphering procedure. It is a clarification that captures the common understanding in the industry. It would not affect implementations behaving like indicated in the CR, it would affect implementations supporting the corrected functionality otherwise.						
	Impact on test specifications No impact						
Consequences if # not approved:	Some implementations may try to apply ciphering also on signalling radio bearer RB0, making impossible to implement ciphering in CELL_FACH state.						
••							
Clauses affected: #	6.3, 8.1.12.2.1						
Other specs % affected:	Y N X Other core specifications # X Test specifications # X O&M Specifications #						
Other comments: #							

Comprehensive information and tips about how to create CRs can be found at <u>http://www.3gpp.org/specs/CR.htm</u>. 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 <u>ftp://ftp.3gpp.org/specs/</u> 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.

[...]

6.3 Signalling Radio Bearers

The Radio Bearers (RB) available for transmission of RRC messages are defined as "signalling radio bearers" and are specified in the following. The UE and UTRAN shall select the signalling radio bearers for RRC messages using RLC-TM, RLC-UM or RLC-AM on the DCCH and CCCH, according to the following:

- Signalling radio bearer RB0 shall be used for all messages sent on the CCCH (UL: RLC-TM, DL: RLC-UM).
- Signalling radio bearer RB1 shall be used for all messages sent on the DCCH, when using RLC unacknowledged mode (RLC-UM).
- Signalling radio bearer RB2 shall be used for all messages sent on the DCCH, when using RLC acknowledged mode (RLC-AM), except for the RRC messages carrying higher layer (NAS) signalling.
- Signalling radio bearer RB3 and optionally Signalling radio bearer RB4 shall be used for the RRC messages carrying higher layer (NAS) signalling and sent on the DCCH in RLC acknowledged mode (RLC-AM), as specified in subclauses 8.1.8., 8.1.9 and 8.1.10.
- RRC messages on the SHCCH are mapped either on RACH or on the USCH in the uplink using TM and either on FACH or on the DSCH using RLC-UM. These messages are only specified for TDD mode.

The Radio Bearer configuration for signalling radio bearer RB0, SHCCH, BCCH on FACH and PCCH on PCH are specified in subclauses 13.6, 13.6a, 13.6b and 13.6c.

Ciphering is never applied to signalling radio bearer RB0.

[...]

8.1.12 Security mode control

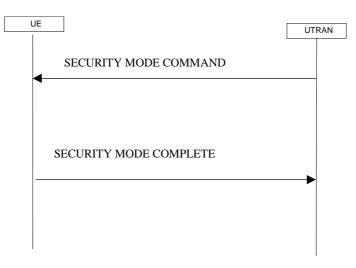


Figure 8.1.12-1: Security mode control procedure

8.1.12.1 General

The purpose of this procedure is to trigger the stop or start of ciphering or to command the restart of the ciphering with a new ciphering configuration, for the radio bearers of one CN domain and for all signalling radio bearers.

It is also used to start integrity protection or to modify the integrity protection configuration for all signalling radio bearers.

8.1.12.2 Initiation

8.1.12.2.1 Ciphering configuration change

To start/restart ciphering, UTRAN sends a SECURITY MODE COMMAND message on the downlink DCCH in AM RLC using the most recent ciphering configuration. If no such ciphering configuration exists then the SECURITY MODE COMMAND is not ciphered. UTRAN should not transmit a SECURITY MODE COMMAND to signal a change in ciphering algorithm.

When configuring ciphering, UTRAN should ensure that the UE needs to store at most two different ciphering configurations (keyset and algorithm) per CN domain, in total over all radio bearers at any given time. For signalling radio bearers the total number of ciphering configurations that need to be stored is at most three. Prior to sending the SECURITY MODE COMMAND, for the CN domain indicated in the IE "CN domain identity" in the SECURITY MODE COMMAND, UTRAN should:

- 1> suspend all radio bearers using RLC-AM or RLC-UM and all signalling radio bearers using RLC-AM or RLC-UM, except the signalling radio bearer used to send the SECURITY MODE COMMAND message on the downlink DCCH in RLC-AM, and except signalling radio bearer RB0, according to the following:
 - 2> not transmit RLC PDUs with sequence number greater than or equal to the number in IE "Radio bearer downlink ciphering activation time info" on all suspended radio bearers and all suspended signalling radio bearers.
- 1> set, for the signalling radio bearer used to send the SECURITY MODE COMMAND, the "RLC send sequence number" in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info", at which time the new ciphering configuration shall be applied;
- 1> if a transparent mode radio bearer for this CN domain exists:
 - 2> include the IE "Ciphering activation time for DPCH" in IE "Ciphering mode info", at which time the new ciphering configuration shall be applied;
- 1> set, for each suspended radio bearer and signalling radio bearer that has no pending ciphering activation time set by a previous security mode control procedure, an "RLC send sequence number" in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info", at which time the new ciphering configuration shall be applied;
- 1> set, for each suspended radio bearer and signalling radio bearer that has a pending ciphering activation time set by a previous security mode control procedure, the "RLC send sequence number" in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info" to the value used in the previous security mode control procedure, at which time the latest ciphering configuration shall be applied;
- 1> if Integrity protection has already been started for the UE:
 - 2> if for the CN domain indicated in the IE "CN domain identity" in the SECURITY MODE COMMAND, a new security key set (new ciphering and integrity protection keys) has been received from upper layers since the transmission of the last SECURITY MODE COMMAND message for that CN domain:

3> include the IE "Integrity protection mode info" in the SECURITY MODE COMMAND.

2> if the IE "CN domain identity" in the SECURITY MODE COMMAND is different from the IE "CN domain identity" that was sent in the previous SECURITY MODE COMMAND message to the UE:

3> include the IE "Integrity protection mode info" in the SECURITY MODE COMMAND.

1> transmit the SECURITY MODE COMMAND message on RB2.

[...]

CHANGE REQUEST										CR-Form-v7	
ж	2	<mark>5.331</mark>	CR	1641	жrev	-	ж	Current vers	ion:	5.1.0	ж
For <u>HELP</u> or	n usin	ng this for	m, see	bottom of this	s page oi	r look	at the	e pop-up text	over th	he	nbols.
Proposed chang	ie aff	ects: l	JICC a	ррѕж	ME	Rad	dio A	ccess Networ	k X	Core Ne	twork
Title:	ж 5	Security o	larifica	tions							
Source:	ж <mark>г</mark>	rsg-ran	<mark>I WG2</mark>								
Work item code:	ж Т	ΓEI						<i>Date:</i>	19 A	ugust 20	02
Category:	De	F (con F (con A (con B (add C (fun D (edi etailed exp	rection) respond lition of ctional i torial mo planatio	wing categories ds to a correctio feature), modification of f odification) ns of the above <u>TR 21.900</u> .	n in an ea feature)			Release: % Use <u>one</u> of 2 9) R96 R97 R98 R99 Rel-4 Rel-5 Rel-6	the follo (GSM) (Relea (Relea (Relea	owing relé Phase 2) se 1996) se 1997) se 1998) se 1999) se 4) se 5)	eases:

Reason for change: ೫	Nowhere it is clearly stated that the ciphering is not applicable to signalling radio bearer RB0.
Summary of change: ℜ	It is clarified that ciphering is never applied to signalling radio bearer RB0. It is also clarified that signalling radio bearer RB0 is not suspended during security mode control procedure.
	Isolated Impact Change Analysis.
	This change clarifies the ciphering procedure. It is a clarification that captures the common understanding in the industry. It would not affect implementations behaving like indicated in the CR, it would affect implementations supporting the corrected functionality otherwise.
	Impact on test specifications No impact
Consequences if % not approved:	Some implementations may try to apply ciphering also on signalling radio bearer RB0, making impossible to implement ciphering in CELL_FACH state.
Clauses affected: %	6.3, 8.1.12.2.1
	YN
Other specs ℜ affected:	X Other core specifications # X Test specifications # X O&M Specifications #
Other comments: ೫	

Comprehensive information and tips about how to create CRs can be found at <u>http://www.3gpp.org/specs/CR.htm</u>. 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 <u>ftp://ftp.3gpp.org/specs/</u> 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.

[...]

6.3 Signalling Radio Bearers

The Radio Bearers (RB) available for transmission of RRC messages are defined as "signalling radio bearers" and are specified in the following. The UE and UTRAN shall select the signalling radio bearers for RRC messages using RLC-TM, RLC-UM or RLC-AM on the DCCH and CCCH, according to the following:

- Signalling radio bearer RB0 shall be used for all messages sent on the CCCH (UL: RLC-TM, DL: RLC-UM).
- Signalling radio bearer RB1 shall be used for all messages sent on the DCCH, when using RLC unacknowledged mode (RLC-UM).
- Signalling radio bearer RB2 shall be used for all messages sent on the DCCH, when using RLC acknowledged mode (RLC-AM), except for the RRC messages carrying higher layer (NAS) signalling.
- Signalling radio bearer RB3 and optionally Signalling radio bearer RB4 shall be used for the RRC messages carrying higher layer (NAS) signalling and sent on the DCCH in RLC acknowledged mode (RLC-AM), as specified in subclauses 8.1.8., 8.1.9 and 8.1.10.
- RRC messages on the SHCCH are mapped either on RACH or on the USCH in the uplink using TM and either on FACH or on the DSCH using RLC-UM. These messages are only specified for TDD mode.

The Radio Bearer configuration for signalling radio bearer RB0, SHCCH, BCCH on FACH and PCCH on PCH are specified in subclauses 13.6, 13.6a, 13.6b and 13.6c.

Ciphering is never applied to signalling radio bearer RB0.

[...]

8.1.12 Security mode control

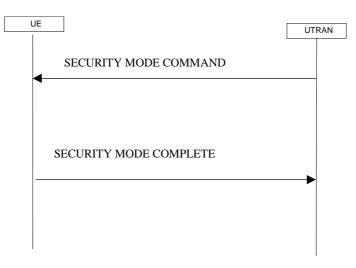


Figure 8.1.12-1: Security mode control procedure

8.1.12.1 General

The purpose of this procedure is to trigger the stop or start of ciphering or to command the restart of the ciphering with a new ciphering configuration, for the radio bearers of one CN domain and for all signalling radio bearers.

It is also used to start integrity protection or to modify the integrity protection configuration for all signalling radio bearers.

8.1.12.2 Initiation

8.1.12.2.1 Ciphering configuration change

To start/restart ciphering, UTRAN sends a SECURITY MODE COMMAND message on the downlink DCCH in AM RLC using the most recent ciphering configuration. If no such ciphering configuration exists then the SECURITY MODE COMMAND is not ciphered. UTRAN should not transmit a SECURITY MODE COMMAND to signal a change in ciphering algorithm.

When configuring ciphering, UTRAN should ensure that the UE needs to store at most two different ciphering configurations (keyset and algorithm) per CN domain, in total over all radio bearers at any given time. For signalling radio bearers the total number of ciphering configurations that need to be stored is at most three. Prior to sending the SECURITY MODE COMMAND, for the CN domain indicated in the IE "CN domain identity" in the SECURITY MODE COMMAND, UTRAN should:

- 1> suspend all radio bearers using RLC-AM or RLC-UM and all signalling radio bearers using RLC-AM or RLC-UM, except the signalling radio bearer used to send the SECURITY MODE COMMAND message on the downlink DCCH in RLC-AM, and except signalling radio bearer RB0, according to the following:
 - 2> not transmit RLC PDUs with sequence number greater than or equal to the number in IE "Radio bearer downlink ciphering activation time info" on all suspended radio bearers and all suspended signalling radio bearers.
- 1> set, for the signalling radio bearer used to send the SECURITY MODE COMMAND, the "RLC send sequence number" in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info", at which time the new ciphering configuration shall be applied;
- 1> if a transparent mode radio bearer for this CN domain exists:
 - 2> include the IE "Ciphering activation time for DPCH" in IE "Ciphering mode info", at which time the new ciphering configuration shall be applied;
- 1> set, for each suspended radio bearer and signalling radio bearer that has no pending ciphering activation time set by a previous security mode control procedure, an "RLC send sequence number" in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info", at which time the new ciphering configuration shall be applied;
- 1> set, for each suspended radio bearer and signalling radio bearer that has a pending ciphering activation time set by a previous security mode control procedure, the "RLC send sequence number" in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info" to the value used in the previous security mode control procedure, at which time the latest ciphering configuration shall be applied;
- 1> if Integrity protection has already been started for the UE:
 - 2> if for the CN domain indicated in the IE "CN domain identity" in the SECURITY MODE COMMAND, a new security key set (new ciphering and integrity protection keys) has been received from upper layers since the transmission of the last SECURITY MODE COMMAND message for that CN domain:

3> include the IE "Integrity protection mode info" in the SECURITY MODE COMMAND.

2> if the IE "CN domain identity" in the SECURITY MODE COMMAND is different from the IE "CN domain identity" that was sent in the previous SECURITY MODE COMMAND message to the UE:

3> include the IE "Integrity protection mode info" in the SECURITY MODE COMMAND.

1> transmit the SECURITY MODE COMMAND message on RB2.

[...]

	C	HANGE	REQ	UES	ST		CR-Form-v7
^ж 25	.331 CR	1642	жrev	- 9	ff (Current version:	<mark>3.11.0</mark> [⋇]
For <u>HELP</u> on using	this form, see	bottom of this	page or	look at	t the	pop-up text ove	er the X symbols.
Proposed change affec	<i>ts:</i> UICC ap	ps#	ME X	Radic	o Ac	cess Network	Core Network
Title: ೫ Co	rrection to the	actions of "ou	It of servi	ce area	a" ar	nd "in service are	ea"
Source: ೫ TS	G-RAN WG2						
Work item code: ೫ <mark>⊤</mark> Е	l					<i>Date:</i>	0/08/2002
Deta	one of the follow F (correction) A (correspond. B (addition of the functional of the functional of the functional of the functional of the function o	s to a correctior eature), nodification of fe dification) s of the above	n in an ear eature)			2 (GS R96 (Rei R97 (Rei R98 (Rei R99 (Rei Rei-4 (Rei Rei-5 (Rei	99 following releases: SM Phase 2) lease 1996) lease 1997) lease 1998) lease 1999) lease 4) lease 5) lease 6)
Reason for change: ೫	the UE is timers sho dedicated The action 2.When the when T316 (in "out of serv ould be stoppe resources an s of stopping UE detects "ir	vice area" ad if they ad enter ic timers ar a service E should	. Wher are ac dle mod e not c area",	n the tive. de. comp T31	• UE detects "in Otherwise, the oletely specified. 6 should have b	ay be active when service area", these UE may release all
Summary of change: ೫	area" in C Add one a update pro CELL_FA Add one a procedure 2.The parag T316 exp	ELL_PCH or ction to stop T ocedure is ong CH state. ction to stop T is ongoing. raph <u>in subcla</u> ry is deleted.	URA_PC T307 if it going whe T317 if a ause 8.5.{	H state is activ en the cell up <u>5.3 har</u>	e. ve ar UE i idate	nd no cell update re-enters "in ser e procedure or U	IRA update) service area" at
	Isolated Im	oact Change	Analysis	5.			
	Impacted fur	nctionality: UE	re-entry	servic	e ar	ea.	
	Correction to	a function w	here spea	cificatio	on w	as not sufficient	. The change has

	isolated impact to the UE. It would not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.
Consequences if solution to the sequences of the sequence	Failing to stop either timer T307 or T317 will result in the release of all dedicated resources.
Clauses affected:	\$ 8.5.5.2.1, 8.5.5.2.2
	Y N X Other core specifications X Test specifications X O&M Specifications
Other comments:	£

Comprehensive information and tips about how to create CRs can be found at <u>http://www.3gpp.org/specs/CR.htm</u>. 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 <u>ftp://ftp.3gpp.org/specs/</u> 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.

8.5.5 Actions in "out of service area" and "in service area"

This subclause specifies the general actions the UE shall perform when it detects "out of service" or "in service" area. The specific UE behaviour when it detects "out of service" or "in service area" and periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" is specified in subclause 8.3.1.

8.5.5.1 Detection of "out of service" area

The UE shall detect "out of service" area as defined in [19].

8.5.5.1.1 Actions following detection of "out of service" area in URA_PCH or CELL_PCH state

If the UE detects the "out of service area" and the UE is in URA_PCH or CELL_PCH state it shall perform the following actions:

1> start timer T316;

1> perform processes described in subclause 7.2.2.

8.5.5.1.2 Actions following detection of "out of service" area in CELL_FACH state

If the UE detects the "out of service area" and the UE is in CELL_FACH state it shall perform the following actions. The UE shall:

1> start timer T317 if not already running;

1> perform processes described in subclause 7.2.2.

8.5.5.2 Detection of "in service" area

When a suitable cell is found based on the description in [4], the UE considers it as having detected "in service area".

8.5.5.2.1 Actions following Re-entry into "in service area" in URA_PCH or CELL_PCH state

If the UE re-enters "in service area" before T316 expiry the UE shall perform the following actions. The UE shall:

1> stop T316;

1> stop T307 if it is active.

1> perform processes described in subclause 7.2.2.

8.5.5.2.2 Actions following re-entry into "in service area" in CELL_FACH state

If the UE detects "in service area" before T317 expiry the UE shall perform the following actions. If no cell update procedure or URA update procedure is ongoing, the UE shall:

1> stop T317;

1> stop T307 if it is active.

1> initiate the cell update procedure using as cause "Re-entering service area" as specified in subclause 8.3.1;

1> perform processes described in subclause 7.2.2.

If an cell update procedure or URA update procedure is ongoing, the UE shall:

<u>1> stop T317.</u>

1> perform the actions as specified in 8.3.1.

8.5.5.3 T316 expiry

On T316 expiry the UE shall perform the following actions. The UE shall:

1> if "out of service area" is detected:

- 2> start timer T317;
- 2> move to CELL_FACH state;
- 2> perform processes described in subclause 7.2.2.
- 1> if "in service area" is detected:
 - 2> initiate the cell update procedure using as cause "Re-entering service area" as specified in subclause 8.3.1;
 - 2> perform processes described in subclause 7.2.2.

8.5.5.4 T317 expiry

When the T317 expires, the UE shall:

- 1> move to idle mode;
- 1> release all dedicated resources;
- 1> indicate release (abort) of the established signalling connections (as stored in the variable ESTABLISHED_SIGNALLING_CONNECTIONS) and established radio access bearers (as stored in the variable ESTABLISHED_RABS) to upper layers;
- 1> clear the variable ESTABLISHED_SIGNALLING_CONNECTIONS;
- 1> clear the variable ESTABLISHED_RABS;
- 1> perform actions specified in subclause 8.5.2 when entering idle mode from connected mode.

	(CHANGE	EREQ	UES	т		CR-Form-v7
^ж 25	<mark>.331</mark> CR	1643	ж rev	- *	Current ver	sion: 4.5.0	ж
For <u>HELP</u> on using	this form, see	bottom of thi	s page or	look at	the pop-up tex	t over the X sy	mbols.
Proposed change affec	<i>ts:</i> UICC a	pps# 📃	ME X	Radio	Access Netwo	ork Core Ne	etwork
Title: % Co	rrection to the	actions of "o	ut of servi	<mark>ce area</mark>	and "in servio	ce area"	
Source: ೫ TS	<mark>G-RAN WG2</mark>						
Work item code: ೫ <mark>⊺</mark> Е	I				Date: ଖ	£ 20/08/2002	
Deta	one of the follo F (correction) A (correspond B (addition of C (functional in D (editorial me illed explanatio pund in 3GPP <u>1</u>	ls to a correction feature), modification of podification) ms of the above	on in an ear feature)		2	Rel-4 f the following rel (GSM Phase 2) (Release 1996) (Release 1997) (Release 1998) (Release 1999) (Release 4) (Release 5) (Release 6)	
Reason for change: ೫	the UE is timers sh dedicated The action 2. When the when T3	in "out of ser ould be stopp d resources a ons of stoppin the UE detects	vice area" bed if they nd enter io g timers a "in service e UE shou	. When are act dle mod re not c area",	the UE detect ive. Otherwise e. ompletely spe T316 should h	ch may be activ s "in service are , the UE may re cified. ave been stopp e area". The cas	ea", these lease all ed. So
Summary of change: ₩	 Add one action to stop T307 if it is active when the UE re-enters "in searea" in CELL_PCH or URA_PCH state. Add one action to stop T307 if it is active and no cell update procedur update procedure is ongoing when the UE re-enters "in service area" CELL_FACH state. Add one action to stop T317 if a cell update procedure or URA update procedure is ongoing. The paragraph in subclause 8.5.5.3 handling the case of "in service area" T316 expiry is deleted. Besides, the actions in subclause 13.1 at T316 expiry are also modified 						e or URA in ca" at
	Isolated Im	pact Change	e Analysis	6.			
	Impacted fu	nctionality: U	E re-entry	service	e area.		
	Correction t	o a function v	where spe	cificatio	<mark>n was not suff</mark> i	<mark>cient. The chan</mark>	ge has

	isolated impact to the UE. It would not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.
Consequences if solution to the sequences of the sequence	Failing to stop either timer T307 or T317 will result in the release of all dedicated resources.
Clauses affected:	₩ 8.5.5.2.1, 8.5.5.2.2
	Y N X Other core specifications X Test specifications X O&M Specifications
Other comments:	¥

Comprehensive information and tips about how to create CRs can be found at <u>http://www.3gpp.org/specs/CR.htm</u>. 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 <u>ftp://ftp.3gpp.org/specs/</u> 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.

8.5.5 Actions in "out of service area" and "in service area"

This subclause specifies the general actions the UE shall perform when it detects "out of service" or "in service" area. The specific UE behaviour when it detects "out of service" or "in service area" and periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" is specified in subclause 8.3.1.

8.5.5.1 Detection of "out of service" area

The UE shall detect "out of service" area as defined in [19].

8.5.5.1.1 Actions following detection of "out of service" area in URA_PCH or CELL_PCH state

If the UE detects the "out of service area" and the UE is in URA_PCH or CELL_PCH state it shall perform the following actions:

1> start timer T316;

1> perform processes described in subclause 7.2.2.

8.5.5.1.2 Actions following detection of "out of service" area in CELL_FACH state

If the UE detects the "out of service area" and the UE is in CELL_FACH state it shall perform the following actions. The UE shall:

1> start timer T317 if not already running;

1> perform processes described in subclause 7.2.2.

8.5.5.2 Detection of "in service" area

When a suitable cell is found based on the description in [4], the UE considers it as having detected "in service area".

8.5.5.2.1 Actions following Re-entry into "in service area" in URA_PCH or CELL_PCH state

If the UE re-enters "in service area" before T316 expiry the UE shall perform the following actions. The UE shall:

1> stop T316;

1> stop T307 if it is active.

1> perform processes described in subclause 7.2.2.

8.5.5.2.2 Actions following re-entry into "in service area" in CELL_FACH state

If the UE detects "in service area" before T317 expiry the UE shall perform the following actions. If no cell update procedure or URA update procedure is ongoing, the UE shall:

1> stop T317;

1> stop T307 if it is active.

1> initiate the cell update procedure using as cause "Re-entering service area" as specified in subclause 8.3.1;

1> perform processes described in subclause 7.2.2.

If an cell update procedure or URA update procedure is ongoing, the UE shall:

<u>1> stop T317.</u>

1> perform the actions as specified in 8.3.1.

8.5.5.3 T316 expiry

On T316 expiry the UE shall perform the following actions. The UE shall:

1> if "out of service area" is detected:

- 2> start timer T317;
- 2> move to CELL_FACH state;
- 2> perform processes described in subclause 7.2.2.
- 1> if "in service area" is detected:
 - 2> initiate the cell update procedure using as cause "Re-entering service area" as specified in subclause 8.3.1;
 - 2> perform processes described in subclause 7.2.2.

8.5.5.4 T317 expiry

When the T317 expires, the UE shall:

- 1> move to idle mode;
- 1> release all dedicated resources;
- 1> indicate release (abort) of the established signalling connections (as stored in the variable ESTABLISHED_SIGNALLING_CONNECTIONS) and established radio access bearers (as stored in the variable ESTABLISHED_RABS) to upper layers;
- 1> clear the variable ESTABLISHED_SIGNALLING_CONNECTIONS;
- 1> clear the variable ESTABLISHED_RABS;
- 1> perform actions specified in subclause 8.5.2 when entering idle mode from connected mode.

	(CHANGE	REQ	UES	т			CR-Form-v7
[#] 25	.331 CR	1644	жrev	- #	Current	version:	5.1.0	ж
For <u>HELP</u> on using	this form, see	bottom of this	s page or	look at	the pop-up	text ovei	r the ೫ syr	nbols.
Proposed change affec		pps# 📃		-	Access Net		_	etwork
Title: ೫ Co	prrection to the	actions of "o	ut of servi	<mark>ce area</mark>	<mark>and "in se"</mark>	rvice are	ea"	
Source: ೫ TS	G-RAN WG2							
Work item code: 🕷 🛛 TE	:1				Date	e:	/08/2002	
Deta	B (addition of	Is to a correction feature), modification of to polification) ns of the above	on in an ear feature)		2	e of the f (GS) (Rel (Rel (Rel 4 (Rel 5 (Rel	el-5 ollowing rele M Phase 2) ease 1996) ease 1997) ease 1998) ease 1999) ease 4) ease 5) ease 6)	eases:
Reason for change: ೫	the UE is timers sh dedicate The action 2.When the when T316	e three timers in "out of ser ould be stopp d resources a ons of stopping UE detects "i expires, the L a" is not need	vice area" bed if they nd enter io g timers a In service JE should	. When are act dle mod re not c area", 1	the UE deto ive. Otherwi e. ompletely s 5316 should	ects "in s ise, the l pecified. I have b e	service are UE may re	a", these lease all ed. So
Summary of change: ¥	area" in (Add one update p CELL_F/ Add one procedur 2.The parag T316 exp Besides,	action to stop CELL_PCH or action to stop ocedure is or ACH state. action to stop e is ongoing. graph <u>in subel</u> piry is deleted. the actions in	URA_PC T307 if it ngoing who T317 if a <u>ause 8.5.6</u>	H state is active en the U cell upo <u>5.3 hane</u> e 13.1 c	JE re-enters date procedu	ll update s "in serv ure or Ul se of "in	e procedure vice area" i RA update service are	e or URA n ca" at
	Impacted fu	Inctionality: U	E re-entry	service	e area.			
	Correction	o a function v	where spea	cificatio	n was not s	ufficient.	The chan	ge has

	isolated impact to the UE. It would not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.
Consequences if solution to the sequences of the sequence	Failing to stop either timer T307 or T317 will result in the release of all dedicated resources.
Clauses affected:	£ 8.5.5.2.1, 8.5.5.2.2
	Y N X Other core specifications X Test specifications X O&M Specifications
Other comments:	fe and the second se

Comprehensive information and tips about how to create CRs can be found at <u>http://www.3gpp.org/specs/CR.htm</u>. 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 <u>ftp://ftp.3gpp.org/specs/</u> 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.

8.5.5 Actions in "out of service area" and "in service area"

This subclause specifies the general actions the UE shall perform when it detects "out of service" or "in service" area. The specific UE behaviour when it detects "out of service" or "in service area" and periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" is specified in subclause 8.3.1.

8.5.5.1 Detection of "out of service" area

The UE shall detect "out of service" area as defined in [19].

8.5.5.1.1 Actions following detection of "out of service" area in URA_PCH or CELL_PCH state

If the UE detects the "out of service area" and the UE is in URA_PCH or CELL_PCH state it shall perform the following actions:

1> start timer T316;

1> perform processes described in subclause 7.2.2.

8.5.5.1.2 Actions following detection of "out of service" area in CELL_FACH state

If the UE detects the "out of service area" and the UE is in CELL_FACH state it shall perform the following actions. The UE shall:

1> start timer T317 if not already running;

1> perform processes described in subclause 7.2.2.

8.5.5.2 Detection of "in service" area

When a suitable cell is found based on the description in [4], the UE considers it as having detected "in service area".

8.5.5.2.1 Actions following Re-entry into "in service area" in URA_PCH or CELL_PCH state

If the UE re-enters "in service area" before T316 expiry the UE shall perform the following actions. The UE shall:

1> stop T316;

1> stop T307 if it is active.

1> perform processes described in subclause 7.2.2.

8.5.5.2.2 Actions following re-entry into "in service area" in CELL_FACH state

If the UE detects "in service area" before T317 expiry the UE shall perform the following actions. If no cell update procedure or URA update procedure is ongoing, the UE shall:

1> stop T317;

1> stop T307 if it is active.

1> initiate the cell update procedure using as cause "Re-entering service area" as specified in subclause 8.3.1;

1> perform processes described in subclause 7.2.2.

If an cell update procedure or URA update procedure is ongoing, the UE shall:

<u>1> stop T317.</u>

1> perform the actions as specified in 8.3.1.

8.5.5.3 T316 expiry

On T316 expiry the UE shall perform the following actions. The UE shall:

1> if "out of service area" is detected:

- 2> start timer T317;
- 2> move to CELL_FACH state;
- 2> perform processes described in subclause 7.2.2.
- 1> if "in service area" is detected:
 - 2> initiate the cell update procedure using as cause "Re-entering service area" as specified in subclause 8.3.1;
 - 2> perform processes described in subclause 7.2.2.

8.5.5.4 T317 expiry

When the T317 expires, the UE shall:

- 1> move to idle mode;
- 1> release all dedicated resources;
- 1> indicate release (abort) of the established signalling connections (as stored in the variable ESTABLISHED_SIGNALLING_CONNECTIONS) and established radio access bearers (as stored in the variable ESTABLISHED_RABS) to upper layers;
- 1> clear the variable ESTABLISHED_SIGNALLING_CONNECTIONS;
- 1> clear the variable ESTABLISHED_RABS;
- 1> perform actions specified in subclause 8.5.2 when entering idle mode from connected mode.