TSG-RAN Meeting #17 ***RP-020548***
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	A	4.5.0	4.6.0
R2-022321	agreed	25.331	1641		Rel-5	Security clarifications	A	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	agreed	25.331	1655		Rel-5	Nested Cell Updates and SRNS Relocation	A	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	A	4.5.0	4.6.0
R2-022407	agreed	25.331	1670		Rel-5	Corrections to security	A	5.1.0	5.2.0

3GPP TSG-RAN2 Meeting #31
Arlanda, Sweden, 19-23 August, 2002

Tdoc ⌘ R2-022319

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **1639** ⌘ **rev** **-** ⌘ Current version: **3.11.0** ⌘

*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:	⌘	Security clarifications
Source:	⌘	TSG-RAN WG2
Work item code:	⌘	TEI
Date:	⌘	19 August 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:	⌘	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:	⌘	

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.

[…]

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

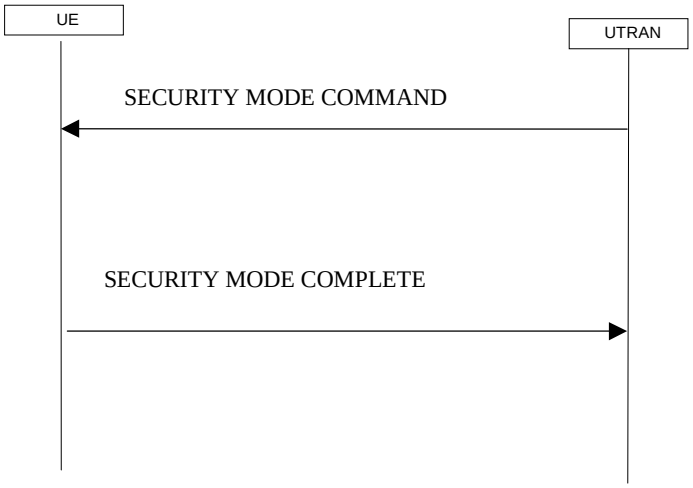

Figure 8.1.12-1: Security mode control procedure

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.

[…]

3GPP TSG-RAN2 Meeting #31
Arlanda, Sweden, 19-23 August, 2002

Tdoc ⌘ R2-022320

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **1640** ⌘ **rev** **-** ⌘ Current version: **4.5.0** ⌘

*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:	⌘	Security clarifications
Source:	⌘	TSG-RAN WG2
Work item code:	⌘	TEI
Date:	⌘	19 August 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:	⌘	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:	⌘	

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.

[…]

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

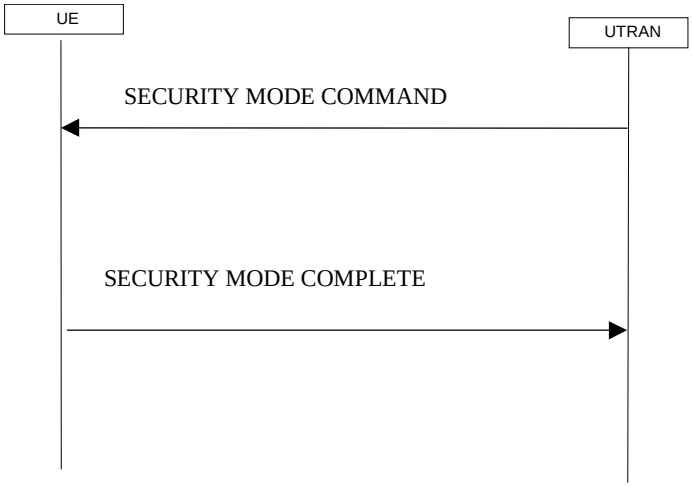

Figure 8.1.12-1: Security mode control procedure

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.

[…]

3GPP TSG-RAN2 Meeting #31
Arlanda, Sweden, 19-23 August, 2002

Tdoc ⌘ R2-022321

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **1641** ⌘ **rev** **-** ⌘ Current version: **5.1.0** ⌘

*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:	⌘	Security clarifications
Source:	⌘	TSG-RAN WG2
Work item code:	⌘	TEI
Date:	⌘	19 August 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:	⌘	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:	⌘	

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.

[…]

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

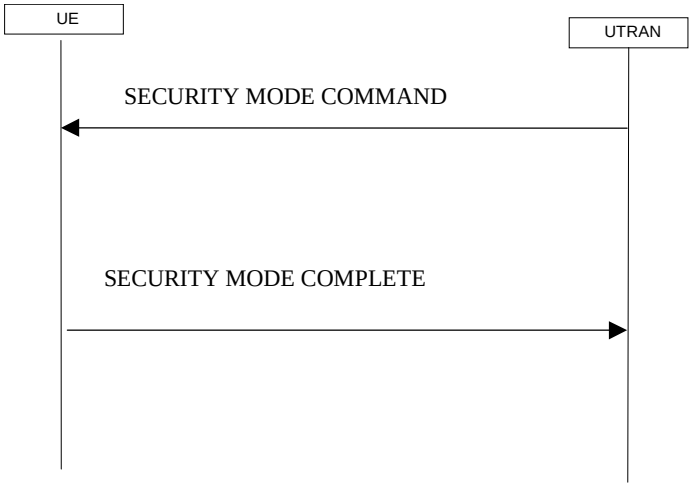

Figure 8.1.12-1: Security mode control procedure

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.

[…]

3GPP TSG-RAN WG2 meeting #31 *R2-022322*
Stockholm, Sweden, 19th - 23th August 2002

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **1642** ⌘ **rev** **-** ⌘ Current version: **3.11.0** ⌘

*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:	⌘	Correction to the actions of "out of service area" and "in service area"
Source:	⌘	TSG-RAN WG2
Work item code:	⌘	TEI
Date:	⌘	20/08/2002
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: ⌘

1. There are three timers i.e. T307, T316, and T317, which may be active when the UE is in “out of service area”. When the UE detects "in service area", these timers should be stopped if they are active. Otherwise, the UE may release all dedicated resources and enter idle mode.

The actions of stopping timers are not completely specified.

~~2.When the UE detects "in service area", T316 should have been stopped. So when T316 expires, the UE should be in “out of service area”. The case of “in service area” is not needed.~~

Summary of change: ⌘

1. Add one action to stop T307 if it is active when the UE re-enters “in service area” in CELL_PCH or URA_PCH state.

Add one action to stop T307 if it is active and no cell update procedure or URA update procedure is ongoing when the UE re-enters “in service area” in CELL_FACH state.

Add one action to stop T317 if a cell update procedure or URA update procedure is ongoing.

~~2.The paragraph in subclause 8.5.5.3 handling the case of “in service area” at T316 expiry is deleted.~~

~~Besides, the actions in subclause 13.1 at T316 expiry are also modified.~~

Isolated Impact Change Analysis.

Impacted functionality: UE re-entry service area.

Correction to a function where specification was 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 not approved:	⌘	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**		
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.

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:

1> stop T317.

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.

3GPP TSG-RAN WG2 meeting #31
Stockholm, Sweden, 19th - 23th August 2002

R2-022323

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **1643** ⌘ **rev** **-** ⌘ Current version: **4.5.0** ⌘

*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 [ ] Core Network [ ]

Title:	⌘	Correction to the actions of "out of service area" and "in service area"
Source:	⌘	TSG-RAN WG2
Work item code:	⌘	TEI
Date:	⌘	20/08/2002
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: ⌘

1. There are three timers i.e. T307, T316, and T317, which may be active when the UE is in “out of service area”. When the UE detects "in service area", these timers should be stopped if they are active. Otherwise, the UE may release all dedicated resources and enter idle mode.

   The actions of stopping timers are not completely specified.

2. ~~When the UE detects "in service area", T316 should have been stopped. So when T316 expires, the UE should be in “out of service area”. The case of “in service area” is not needed.~~

Summary of change: ⌘

1. Add one action to stop T307 if it is active when the UE re-enters “in service area” in CELL_PCH or URA_PCH state.

   Add one action to stop T307 if it is active and no cell update procedure or URA update procedure is ongoing when the UE re-enters “in service area” in CELL_FACH state.

   Add one action to stop T317 if a cell update procedure or URA update procedure is ongoing.

2. ~~The paragraph in subclause 8.5.5.3 handling the case of “in service area” at T316 expiry is deleted.~~

   ~~Besides, the actions in subclause 13.1 at T316 expiry are also modified.~~

Isolated Impact Change Analysis.

Impacted functionality: UE re-entry service area.

Correction to a function where specification was 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 not approved:	⌘	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**		
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.

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:

1> stop T317.

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.

3GPP TSG-RAN WG2 meeting #31 *R2-022324*
Stockholm, Sweden, 19th - 23th August 2002

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **1644** ⌘ **rev** **-** ⌘ Current version: **5.1.0** ⌘

*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:	⌘	Correction to the actions of "out of service area" and "in service area"
Source:	⌘	TSG-RAN WG2
Work item code:	⌘	TEI
Date:	⌘	20/08/2002
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: ⌘

1. There are three timers i.e. T307, T316, and T317, which may be active when the UE is in “out of service area”. When the UE detects "in service area", these timers should be stopped if they are active. Otherwise, the UE may release all dedicated resources and enter idle mode.

   The actions of stopping timers are not completely specified.

~~2.When the UE detects "in service area", T316 should have been stopped. So when T316 expires, the UE should be in “out of service area”. The case of “in service area” is not needed.~~

Summary of change: ⌘

1. Add one action to stop T307 if it is active when the UE re-enters “in service area” in CELL_PCH or URA_PCH state.

   Add one action to stop T307 if it is active and no cell update procedure or URA update procedure is ongoing when the UE re-enters “in service area” in CELL_FACH state.

   Add one action to stop T317 if a cell update procedure or URA update procedure is ongoing.

~~2.The paragraph in subclause 8.5.5.3 handling the case of “in service area” at T316 expiry is deleted.~~

~~Besides, the actions in subclause 13.1 at T316 expiry are also modified.~~

Isolated Impact Change Analysis.

Impacted functionality: UE re-entry service area.

Correction to a function where specification was 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 not approved:	⌘	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**		
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.

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:

1> stop T317.

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.