

**TSG-RAN Meeting #16**  
**Marco Island, FL, USA, 4 - 7 June 2002**

**RP-020336**

**Title:** Agreed CRs (Release '99 and Rel-4/Rel-5 category A) to TS 25.331 (7)

**Source:** TSG-RAN WG2

**Agenda item:** 7.2.3

Doc-1st-	Status-	Spec	CR	Rev	Phase	Subject	Cat	Version	Versio
R2-021440	agreed	25.331	1490		R99	Corrections to Security procedure on Missing integrity protection reset on relocation and counter check response actions for asymmetric bearer configurations	F	3.10.0	3.11.0
R2-021441	agreed	25.331	1491		Rel-4	Corrections to Security procedure on Missing integrity protection reset on relocation and counter check response actions for asymmetric bearer configurations	A	4.4.0	4.5.0
R2-021442	agreed	25.331	1492		Rel-5	Corrections to Security procedure on Missing integrity protection reset on relocation and counter check response actions for asymmetric bearer configurations	A	5.0.0	5.1.0
R2-021446	agreed	25.331	1493		R99	Corrections to cell update interactions with security and SRNS Relocation	F	3.10.0	3.11.0
R2-021447	agreed	25.331	1494		Rel-4	Corrections to cell update interactions with security and SRNS Relocation	A	4.4.0	4.5.0
R2-021448	agreed	25.331	1495		Rel-5	Corrections to cell update interactions with security and SRNS Relocation	A	5.0.0	5.1.0
R2-021449	agreed	25.331	1496		R99	"Out of service" area definition	F	3.10.0	3.11.0
R2-021450	agreed	25.331	1497		Rel-4	"Out of service" area definition	A	4.4.0	4.5.0
R2-021451	agreed	25.331	1498		Rel-5	"Out of service" area definition	A	5.0.0	5.1.0

## CHANGE REQUEST

⌘ **25.331 CR 1490** ⌘ rev **-** ⌘ Current version: **3.10.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

**Title:** ⌘ Corrections to Security procedure on Missing integrity protection reset on relocation and counter check response actions for asymmetric bearer configurations

**Source:** ⌘ TSG-RAN WG2

**Work item code:** ⌘ TEI

**Date:** ⌘ May 13, 2002

**Category:** ⌘ **F**

**Release:** ⌘ R99

Use one of the following categories:

Use one of the following releases:

**F** (correction)

2 (GSM Phase 2)

**A** (corresponds to a correction in an earlier release)

R96 (Release 1996)

**B** (addition of feature),

R97 (Release 1997)

**C** (functional modification of feature)

R98 (Release 1998)

**D** (editorial modification)

R99 (Release 1999)

Detailed explanations of the above categories can be found in 3GPP [TR 21.900](#).

REL-4 (Release 4)

REL-5 (Release 5)

- Reason for change:** ⌘
1. It is not clear if SECURITY MODE COMMAND can change ciphering/integrity protection algorithms.
  2. It is not clear if SECURITY MODE COMMAND can be received with "modify" command for integrity protection for a CN domain for which integrity protection has been already configured, if new keys have not been received.
  3. In the COUNTER CHECK procedure it is not clear how the UE should set the COUNT-C values for a radio bearer which is configured only in one direction or is set to RLC-TM mode in one direction and UM in the other.
  4. ACTIVE SET UPDATE cannot be used to trigger actions at the UE for a SRNS Relocation.
  5. UE actions in case of pending activation times for integrity protection following SRNS Relocation are missing.
  6. UE actions in case of previously received new keys not having yet been activated due to activation times not elapsed at the time of SRNS Relocation are missing.
  7. Mis-alignment between Tabular and ASN.1. ASN.1 does not permit the transfer of START for every domain in the Relocation container between source and target as required..
  8. It is incorrectly stated that a R99 UE shall support any one of UIAx integrity protection algorithms when in fact UIA1 shall be supported.
  9. It is not clear in case of START caculation if "non-ciphered" radio bearers refers also to RBs with ciphering algorithm set to UEA0.
  10. It is incorrectly suggested in Annex a that the USIM stores both the new and old keys as well as the old and new START and KSI values. Only one value - the latest - is stored in the USIM.
  11. The ASN.1 still permits the ciphering mode command to be set to "stop".
  12. It is not stated that the UE shall check to see if a new FRESH value was received

before performing the integrity check on the message.

- 13. 10.3.3.10 is not correctly placed in the Tabular according to alphabetical order.
- 14. In 8.6.4.8 it is stated that if the IE "RB Mapping Info" is included in system information and there is a AM RLC size change the UE shall " *set the HFN values for the corresponding RLC entity equal to the value of the IE "START" for this CN domain that will be included in the CELL UPDATE message that will be sent before the next transmission.* " However since the CELL UPDATE will be sent only in the future it is not possible for the UE to set the START value in advance.

**Summary of change: ☒**

- 1. It is clarified that UTRAN should not change ciphering/integrity protection algorithm using the SECURITY MODE COMMAND procedure.
- 2. It is clarified that UTRAN should not transmit SECURITY MODE COMMAND with "modify" command for integrity protection for a CN domain for which integrity protection has been already configured, if new keys have not been received for that domain.
- 3. It is specified that UE shall set an unspecified value for the COUNT-C for the direction of the radio bearer that is either not configured or is set to RLC-TM.
- 4. All security related procedure text in the ACTIVE SET UPDATE procedure and procedure related to ACTIVE SET UPDATE and security in other procedures is deleted. The tabular and ASN.1 have been appropriately updated.
- 5. It is specified that the UE shall over-write any pending activation times for IP.
- 6. It is specified that UE shall use the pending new keys.
- 7. The ASN.1 is corrected to allow for START value for all domains to be transmitted.
- 8. The NOTE specifying UE support of UEAx and UIAx is deleted. A corresponding correction is made in 25.306.
- 9. It is clarified that "non ciphered" refers to ciphering status set to "not started" and RBs configured with ciphering algorithm UEA0 shall contribute to the START value calculation.
- 10. The suggestion that old values for START, Keys, etc. are stored in the USIM has been deleted.
- 11. The ASN.1 and tabular have been appropriately updated to state that stop is never to be used in any version of the protocol.
- 12. It is stated that if the IE "DL Counter Synchronisation Info" or "New URNTI" in case of RADIO BEARER RECONFIGURATION is present then the UE shall apply the FRESH value in the received message before performing the integrity check.
- 13. RRC State Indicator has been moved in the Tabular per the appropriate alphabetical order.
- 14. The requirement corresponding to the START value transmission in case of AM RLC size change due to system information IE "RB Mapping Info" is deleted since this occurs only in the case of Inter-RAT Handover to UTRAN and in this case there is no AM RLC size change.

**Consequences if not approved:**

- ☒ Incomplete specification related to security procedures causing uncertain UE behavior. Uncertain UE behavior is case of SRNS relocation.

**Isolated Impact Analysis:**

**Corrected Feature: Security**

Both the UE and UTRAN need to implement the changes in this CR for the security feature to function correctly else the two entities will not be synchronised causing loss of connection.

**Impact on T1 test specifications:** Security is in general not well covered in T1 at present and this CR is not foreseen to affect current T1 tests but the corrected functionality will affect future test cases produced by T1 related to security.

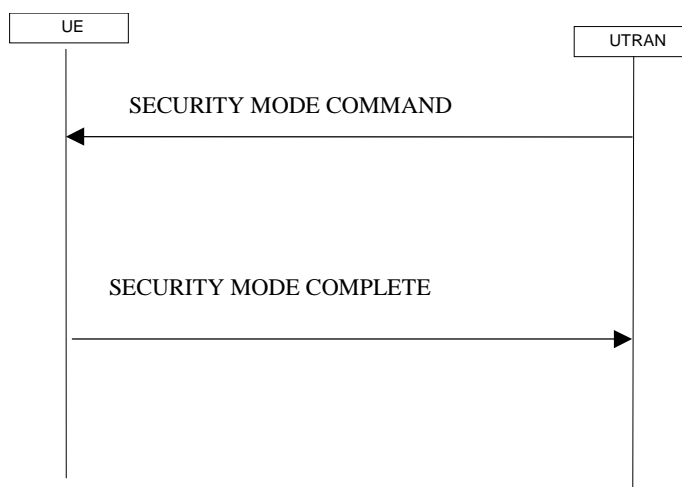
<b>Clauses affected:</b>	⌘	8.1.12.2.1, 8.1.12.2.2, 8.1.15.3, 8.3.4.3, 8.3.4.5a, 8.5.9, 8.5.10, 8.6.3.4, 8.6.3.5, 8.6.4.8, 10.2.1, 10.2.2, 10.3.3.5, 10.3.3.10, 10.3.3.35a (new), 10.3.3.37, 11, A.2	
<b>Other specs</b>	⌘	X Other core specifications	⌘ 25.306, 25.413 25.331 v4.4.0, CR 1491 25.331 v5.0.0, CR 1492
<b>affected:</b>		<input type="checkbox"/> Test specifications	
		<input type="checkbox"/> O&M Specifications	
<b>Other comments:</b>	⌘		

**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.

### 8.1.12 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 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.

### 8.1.12.2.2 Integrity protection configuration change

To start or modify integrity protection, UTRAN sends a SECURITY MODE COMMAND message on the downlink DCCH in AM RLC using the new integrity protection configuration. UTRAN should not "modify" integrity protection for a CN domain to which a SECURITY MODE COMMAND configuring integrity protection has been previously sent for an ongoing signalling connection unless the application of new integrity keys needs to be signalled to the UE. UTRAN should not transmit a SECURITY MODE COMMAND to signal a change in integrity protection algorithm.

When configuring Integrity protection, UTRAN should:

- 1> ensure that the UE needs to store at most three different Integrity protection configurations (keysets) at any given time. This includes the total number of Integrity protection configurations for all signalling radio bearers;
- 1> if Ciphering has already been started for the UE for the CN domain to be set in the IE "CN domain identity" in the SECURITY MODE COMMAND:
  - 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 "Ciphering mode info" in the SECURITY MODE COMMAND.
- 1> if Ciphering has already been configured for the UE for a CN domain different from the CN domain to be set in the IE "CN domain identity" in the SECURITY MODE COMMAND:
  - 2> include the IE "Ciphering mode info" in the SECURITY MODE COMMAND.

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> if this is the first SECURITY MODE COMMAND sent for this RRC connection:
  - 2> if new keys have been received:
    - 3> initialise the hyper frame numbers as follows:
      - 4> set all bits of the hyper frame numbers of the COUNT-I values for all signalling radio bearers to zero.
    - 2> else (if new keys have not been received):
      - 3> use the value "START" in the most recently received IE "START list" or IE "START" that belongs to the CN domain indicated in the IE "CN domain identity" to initialise all hyper frame numbers of COUNT-I for all the signalling radio bearers by:
        - 4> setting the 20 most significant bits of the hyper frame numbers for all signalling radio bearers to the value "START" in the most recently received IE "START list" or IE "START" for that CN domain;
        - 4> setting the remaining bits of the hyper frame numbers equal to zero.
  - 1> else (this is not the first SECURITY MODE COMMAND sent for this RRC connection):
    - 2> if new keys have been received:
      - 3> initialise the hyper frame number for COUNT-I for RB2 as follows:
        - 4> set all bits of the HFN of the COUNT-I value for RB2 to zero.
      - 2> if new keys have not been received:
        - 3> initialise the hyper frame number for COUNT-I for RB2 as follows:
          - 4> set the 20 most significant bits of the HFN of the downlink and uplink COUNT-I to the value of the most recently received IE "START" or IE "START LIST" for the CN domain to be set in the IE "CN Domain Identity";
          - 4> set the remaining bits of the HFN of the downlink and uplink COUNT-I to zero.

- 1> if the IE "Integrity protection mode command" has the value "Start":
  - 2> prohibit the transmission of signalling messages with any RRC SN on all signalling radio bearers, except RB2;
  - 2> set the FRESH value in the IE "Integrity protection initialisation number", included in the IE "Integrity protection mode info".
- 1> if the IE "Integrity protection mode command" has the value "Modify":
  - 2> for each signalling radio bearer RBn, except RB2:
    - 3> prohibit the transmission of signalling messages with RRC SN greater or equal to the RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info".
  - 2> set, for each signalling radio bearer RBn, that has no pending integrity protection activation time set by a previous security mode control procedure, an RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info", at which time the new integrity protection configuration shall be applied;
  - 2> set, for each signalling radio bearer RBn, that has a pending integrity protection activation time set by a previous security mode control procedure, the RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info", to the value used in the previous security mode control procedure, at which time the latest integrity protection configuration shall be applied.
- 1> transmit the SECURITY MODE COMMAND message on RB2 using the new integrity protection configuration.

### 8.1.12.3 Reception of SECURITY MODE COMMAND message by the UE

Upon reception of the SECURITY MODE COMMAND message, the UE shall:

- 1> if neither IE "Ciphering mode info" nor IE "Integrity protection mode info" is included in the SECURITY MODE COMMAND:
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the IE "Security capability" is the same as indicated by variable UE\_CAPABILITY\_TRANSFERRED, and the IE "GSM security capability" (if included in the SECURITY MODE COMMAND) is the same as indicated by the variable UE\_CAPABILITY\_TRANSFERRED:
  - 2> set the variable LATEST\_CONFIGURED\_CN\_DOMAIN equal to the IE "CN domain identity";
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for the CN domain indicated in the IE "CN domain identity" in the received SECURITY MODE COMMAND to the value "Affected";
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all CN domains other than the CN domain indicated in the IE "CN domain identity" to "Not affected";
  - 2> set the IE "RRC transaction identifier" in the SECURITY MODE COMPLETE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE COMMAND message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - 3> perform the actions as specified in subclause 8.6.3.4.
  - 2> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
    - 3> perform the actions as specified in subclause 8.6.3.5.
- 1> prior to sending the SECURITY MODE COMPLETE message:

- 2> use the old ciphering configuration for this message;
- 2> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
  - 3> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 3> for each radio bearer and signalling radio bearer that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN:
    - 4> start or continue incrementing the COUNT-C values for all RLC-AM and RLC-UM signalling radio bearers at the ciphering activation time as specified in the procedure;
    - 4> continue incrementing the COUNT-C values for all RLC-AM and RLC-UM radio bearers.
  - 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN:
    - 4> for ciphering on signalling radio bearers using RLC-AM and RLC-UM in the downlink, at the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info" included in the SECURITY MODE COMMAND, for each signalling radio bearer:
      - 5> set the 20 most significant bits of the HFN component of the downlink COUNT-C to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
      - 5> set the remaining bits of the hyper frame numbers to zero.
  - 3> if new keys have been received:
    - 4> perform the actions in subclause 8.1.12.3.1.
- 2> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
  - 3> include and set the IE "Uplink integrity protection activation info" to the value of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO for each signalling radio bearer;
  - 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN, for RB2:
    - 4> in the downlink, for the received SECURITY MODE COMMAND message:
      - 5> set the 20 most significant bits of the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
      - 5> set the remaining bits of the IE "Downlink RRC HFN" to zero.
    - 4> in the uplink, for the transmitted response message, SECURITY MODE COMPLETE:
      - 5> set the 20 most significant bits of the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
      - 5> set the remaining bits of the IE "Uplink RRC HFN" to zero.
  - 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN, for each signalling radio bearer other than RB2:
    - 4> if the IE "Integrity protection mode command" has the value "start":
      - 5> in the downlink, for this signalling radio bearer:



- 6> set the 20 most significant bits of IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to the value START transmitted in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
- 6> set the remaining bits of the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to zero;
- 4> else:
  - 5> in the downlink, for the first message for which the RRC sequence number in a received RRC message for this signalling radio bearer is equal to or greater than the activation time as indicated in IE "Downlink integrity protection activation info" as included in the IE "Integrity protection mode info", for this signalling radio bearer:
    - 6> set the 20 most significant bits of the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 6> set the remaining bits of the IE "Downlink RRC HFN" to zero.
  - 3> if new keys have been received:
    - 4> perform the actions in subclause 8.1.12.3.1.
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;
  - 2> transmit the SECURITY MODE COMPLETE message on the uplink DCCH in AM RLC;
- 1> when the successful delivery of the SECURITY MODE COMPLETE message has been confirmed by RLC:
  - 2> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN:
      - 4> for ciphering on signalling radio bearers using RLC-AM and RLC-UM in the uplink, at the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info" included in the SECURITY MODE COMPLETE, for each signalling radio bearer:
        - 5> set the HFN component of the uplink COUNT-C to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
        - 5> set the remaining bits of the hyper frame numbers to zero.
    - 3> if new keys have been received:
      - 4> perform the actions in subclause 8.1.12.3.1.
    - 3> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
    - 3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
    - 3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
  - 2> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
    - 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN, for each signalling radio bearer other than RB2:
      - 4> if the IE "Integrity protection mode command" has the value "start":

- 5> in the uplink, for this signalling radio bearer:
  - 6> set the 20 most significant bits of IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to the value START transmitted in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
  - 6> set the remaining bits of the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to zero.
- 4> else:
  - 5> in the uplink, for the first transmitted RRC message for this signalling radio bearer with RRC sequence number equal to the activation time as indicated in IE "Uplink integrity protection activation info" included in the transmitted SECURITY MODE COMPLETE, for this signalling radio bearer:
    - 6> set the 20 most significant bits of the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 6> set the remaining bits of the IE "Uplink RRC HFN" to zero.
- 3> if new keys have been received:
  - 4> perform the actions in subclause 8.1.12.3.1.
- 3> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- 3> set "Uplink RRC Message sequence number" for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO to a value such that next RRC message to be sent on uplink RB0 will use the new integrity protection configuration;
- 3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
- 3> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 2> clear the variable SECURITY\_MODIFICATION;
- 2> notify upper layers upon change of the security configuration;
- 2> and the procedure ends.
- 1> if the IE "Security capability" is not the same as indicated by the variable UE\_CAPABILITY\_TRANSFERRED, or the IE "GSM security capability" (if included in the SECURITY MODE COMMAND) is not the same as indicated by the variable UE\_CAPABILITY\_TRANSFERRED, or if the IE "GSM security capability" is not included in the SECURITY MODE COMMAND and is included in the variable UE\_CAPABILITY\_TRANSFERRED:
  - 2> release all its radio resources;
  - 2> indicate the release 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;
  - 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 2> clear the variable ESTABLISHED\_RABS;
  - 2> clear the variable SECURITY\_MODIFICATION;
  - 2> enter idle mode;
  - 2> perform actions when entering idle mode as specified in subclause 8.5.2;
  - 2> and the procedure ends.

### 8.1.12.3.1 New ciphering and integrity protection keys

If a new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN, the UE shall:

- 1> set the START value for the CN domain indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN to zero;
- 1> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
  - 2> for integrity protection in the downlink on each signalling radio bearer except RB2:
    - 3> if IE "Integrity protection mode command" has the value "start":
      - 4> for the first received message on this signalling radio bearer:
        - 5> start using the new integrity key;
        - 5> for this signalling radio bearer:
          - 6> set the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to zero.
      - 3> else:
        - 4> for the first message for which the RRC sequence number in a received RRC message for this signalling radio bearer is equal to or greater than the activation time as indicated in IE "Downlink integrity protection activation info" as included in the IE "Integrity protection mode info":
          - 5> start using the new integrity key;
          - 5> for this signalling radio bearer:
            - 6> set the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to zero.
      - 2> for integrity protection in the uplink on each signalling radio bearer except RB2:
        - 3> for the first message for which the RRC sequence number in a to be transmitted RRC message for this signalling radio bearer is equal to the activation time as indicated in IE "Uplink integrity protection activation info" included in the transmitted SECURITY MODE COMPLETE message:
          - 4> start using the new integrity key;
          - 4> for this signalling radio bearer:
            - 5> set the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to zero.
      - 2> for integrity protection in the downlink on signalling radio bearer RB2:
        - 3> at the received SECURITY MODECOMMAND:
          - 4> start using the new integrity key;
          - 4> set the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to zero.
      - 2> for integrity protection in the uplink on signalling radio bearer RB2 :
        - 3> at the transmitted SECURITY MODE COMPLETE:
          - 4> start using the new integrity key;
          - 4> set the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to zero.
    - 1> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":

- 2> for each signalling radio bearer and for each radio bearer for the CN domain indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN:
  - 3> if the IE "Status" in the variable CIPHERING\_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers using RLC-TM:
    - 4> at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info":
      - 5> start using the new key in uplink and downlink;
      - 5> set the HFN component of the COUNT-C to zero.
  - 3> if the IE "Status" in the variable CIPHERING\_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers and signalling radio bearers using RLC-AM and RLC-UM:
    - 4> in the downlink, at the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info":
      - 5> start using the new key;
      - 5> set the HFN component of the downlink COUNT-C to zero.
    - 4> in the uplink, at the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info":
      - 5> start using the new key;
      - 5> set the HFN component of the uplink COUNT-C to zero.
- 1> consider the value of the latest transmitted START value to be zero.

#### 8.1.12.4 Void

##### 8.1.12.4a Incompatible simultaneous security reconfiguration

If the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION becomes set to TRUE of the received SECURITY MODE COMMAND message, the UE shall:

- 1> transmit a SECURITY MODE FAILURE message on the uplink DCCH using AM RLC, using the ciphering and integrity protection configurations prior to the reception of this SECURITY MODE COMMAND;
- 1> set the IE "RRC transaction identifier" in the SECURITY MODE FAILURE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE COMMAND message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";
- 1> when the response message has been submitted to lower layers for transmission:
  - 2> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to FALSE;
  - 2> continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - 2> and the procedure ends.

##### 8.1.12.4b Cell update procedure during security reconfiguration

If:

- a cell update procedure according to subclause 8.3.1 is initiated; and
- the received SECURITY MODE COMMAND message causes either,
  - the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE; and/or
  - the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE:

the UE shall:

- 1> abort the ongoing integrity and/or ciphering reconfiguration;
- 1> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
- 1> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- 1> when the response message has been submitted to lower layers for transmission:
  - 2> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - 3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
    - 3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
    - 3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
    - 3> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
  - 2> continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received; and
  - 2> clear the variable SECURITY\_MODIFICATION;
  - 2> the procedure ends.

#### 8.1.12.4c Invalid configuration

If the variable INVALID\_CONFIGURATION is set to TRUE due to the received SECURITY MODE COMMAND message, the UE shall:

- 1> transmit a SECURITY MODE FAILURE message on the DCCH using AM RLC after setting the IEs as specified below:
  - 2> set the IE "RRC transaction identifier" in the SECURITY MODE FAILURE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE COMMAND message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> set the IE "failure cause" to the cause value "invalid configuration".
- 1> when the response message has been submitted to lower layers for transmission:
  - 2> set the variable INVALID\_CONFIGURATION to FALSE;
  - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE;
  - 2> continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - 2> and the procedure ends.

### 8.1.12.5 Reception of SECURITY MODE COMPLETE message by the UTRAN

UTRAN should apply integrity protection on the received SECURITY MODE COMPLETE message and all subsequent messages with the new integrity protection configuration, if changed. When UTRAN has received a SECURITY MODE COMPLETE message and the integrity protection has successfully been applied, UTRAN should:

- 1> if the IE "Ciphering mode info" was included in the SECURITY MODE COMMAND message:
  - 2> if new keys were received for the CN domain set in the IE "CN Domain Identity" in the SECURITY MODE COMMAND:
    - 3> set, at the downlink and uplink activation time, all the bits of the hyper frame numbers of the downlink and uplink COUNT-C values respectively for all radio bearers for this CN domain and all signalling radio bearers to zero.
  - 2> else (if new keys were not received):
    - 3> use, at the downlink and uplink activation time, the value "START" in the most recently received IE "START list" or IE "START" that belongs to the CN domain as indicated in the IE "CN domain identity" to initialise all hyper frame numbers of the downlink and uplink COUNT-C values respectively for all the signalling radio bearers as follows:
      - 4> set the 20 most significant bits of the hyper frame numbers of the COUNT-C for all signalling radio bearers to the value "START" in the most recently received IE "START list" or IE "START" for that CN domain;
      - 4> set the remaining bits of the hyper frame numbers equal to zero.
- 1> if the IE "Integrity protection mode info" was included in the SECURITY MODE COMMAND message:
  - 2> if this was not the first SECURITY MODE COMMAND message for this RRC connection:
    - 3> if new keys have been received for the CN domain set in the IE "CN Domain Identity" included in the transmitted SECURITY MODE COMMAND message:
      - 4> initialise, at the downlink and uplink activation time, all hyper frame numbers of the downlink and uplink COUNT-I values respectively for all the signalling radio bearers other than RB2 as follows:
        - 5> set all bits of the hyper frame numbers of the uplink and downlink COUNT-I to zero.
    - 3> if no new keys have been received for the CN domain set in the IE "CN Domain Identity" included in the transmitted SECURITY MODE COMMAND message:
      - 4> use, at the downlink and uplink activation time, the value "START" in the most recently received IE "START list" or IE "START" that belongs to the CN domain as indicated in the IE "CN domain identity" to initialise all hyper frame numbers of the downlink and uplink COUNT-I values respectively for all the signalling radio bearers other than RB2 as follows:
        - 5> set the 20 most significant bits of the hyper frame numbers of the downlink and uplink COUNT-I respectively for all signalling radio bearers to the value "START" in the most recently received IE "START list" or IE "START" for that CN domain;
        - 5> set the remaining bits of the hyper frame numbers equal to zero.
- 1> send an indication to upper layers that the new security configuration has been activated;
- 1> resume, in the downlink, all suspended radio bearers and all signalling radio bearers;
- 1> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- 1> if the IE "Integrity protection mode command" included in the SECURITY MODE COMMAND had the value "Start":
  - 2> start applying integrity protection in the downlink for all signalling radio bearers.

- 1> if the IE "Integrity protection mode command" included in the SECURITY MODE COMMAND had the value "Modify":
  - 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each signalling radio bearers RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info";
  - 2> continue applying the new integrity configuration for signalling radio bearer RB2;
  - 2> apply the new integrity protection configuration on the received signalling messages with RRC SN greater than or equal to the number associated with the signalling radio bearer in IE "Uplink integrity protection activation info".
- 1> apply the old ciphering configuration for the transmission of RLC PDUs with RLC sequence number less than the number indicated in the IE "Radio bearer downlink ciphering activation time info" included in the IE "Ciphering mode info";
- 1> apply the new ciphering configuration for the transmission of RLC PDUs with RLC sequence number greater than or equal to the number indicated in IE "Radio bearer downlink ciphering activation time info" included in the IE "Ciphering mode info";
- 1> apply the old integrity protection configuration on the received signalling messages with RRC SN smaller than the number associated with the signalling radio bearer in IE "Uplink integrity protection activation info";
- 1> for radio bearers using RLC-AM or RLC-UM:
  - 2> use the old ciphering configuration for received RLC PDUs with RLC sequence number less than the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" sent by the UE;
  - 2> use the new ciphering configuration for received RLC PDUs with RLC sequence number greater than or equal to the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" sent by the UE;
  - 2> if an RLC reset or re-establishment occurs after the SECURITY MODE COMPLETE message has been received by UTRAN before the activation time for the new ciphering configuration has been reached, ignore the activation time and apply the new ciphering configuration immediately after the RLC reset or RLC re-establishment.
- 1> for radio bearers using RLC-TM:
  - 2> use the old ciphering configuration for the received RLC PDUs before the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info" as included in the SECURITY MODE COMMAND;
  - 2> use the new ciphering configuration for the received RLC PDUs at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info" as included in the SECURITY MODE COMMAND.
- 1> and the procedure ends.

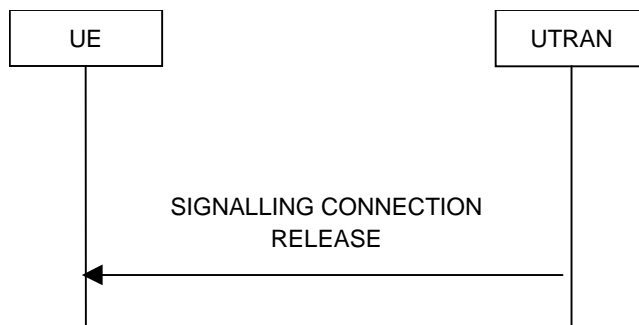
#### 8.1.12.6 Invalid SECURITY MODE COMMAND message

If the SECURITY MODE COMMAND message contains a protocol error causing the variable PROTOCOL\_ERROR\_REJECT to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows:

- 1> transmit a SECURITY MODE FAILURE message on the uplink DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the SECURITY MODE FAILURE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE COMMAND message in the table "Rejected transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;

- 1> set the IE "failure cause" to the cause value "protocol error";
- 1> include the IE "Protocol error information" with contents set to the value of the variable `PROTOCOL_ERROR_INFORMATION`;
- 1> when the response message has been submitted to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - 2> and the procedure ends.

### 8.1.13 Signalling connection release procedure



**Figure 8.1.13-1: Signalling connection release procedure, normal case**

#### 8.1.13.1 General

The signalling connection release procedure is used to notify to the UE that one of its ongoing signalling connections has been released. The procedure does not initiate the release of the RRC connection.

#### 8.1.13.2 Initiation of SIGNALLING CONNECTION RELEASE by the UTRAN

To initiate the procedure, the UTRAN transmits a SIGNALLING CONNECTION RELEASE message on DCCH using AM RLC.

#### 8.1.13.3 Reception of SIGNALLING CONNECTION RELEASE by the UE

Upon reception of a SIGNALLING CONNECTION RELEASE message, the UE shall:

- 1> indicate the release of the signalling connection and pass the value of the IE "CN domain identity" to upper layers;
- 1> remove the signalling connection with the identity indicated by the IE "CN domain identity" from the variable `ESTABLISHED_SIGNALLING_CONNECTIONS`;
- 1> clear the entry for the SIGNALLING CONNECTION RELEASE message in the table "Accepted transactions" in the variable `TRANSACTIONS`;
- 1> the procedure ends.

#### 8.1.13.4 Invalid SIGNALLING CONNECTION RELEASE message

If the UE receives a SIGNALLING CONNECTION RELEASE message, which contains a protocol error causing the variable `PROTOCOL_ERROR_REJECT` to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows:

- 1> include the IE "Identification of received message"; and
- 2> set the IE "Received message type" to SIGNALLING CONNECTION RELEASE;



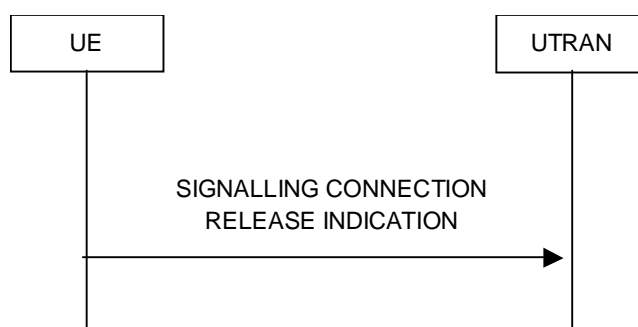
- 2> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the SIGNALLING CONNECTION RELEASE message in the table "Rejected transactions" in the variable TRANSACTIONS; and
- 2> clear that entry.
- 1> include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL\_ERROR\_INFORMATION;
- 1> transmit an RRC STATUS message on the uplink DCCH using AM RLC
- 1> when the RRC STATUS message has been submitted to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the invalid SIGNALLING CONNECTION RELEASE message has not been received.

### 8.1.13.5 Invalid configuration

If radio access bearers for the CN domain indicated by the IE "CN domain identity" exist in the variable ESTABLISHED\_RABS, the UE shall:

- 1> transmit an RRC STATUS message on the uplink DCCH using AM RLC;
- 1> include the IE "Identification of received message"; and
- 1> set the IE "Received message type" to SIGNALLING CONNECTION RELEASE; and
- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the SIGNALLING CONNECTION RELEASE message in the table "Accepted transactions" in the variable TRANSACTIONS and clear that entry;
- 1> include the IE "Protocol error information" with contents set to the value "Message not compatible with receiver state";
- 1> when the RRC STATUS message has been submitted to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the invalid SIGNALLING CONNECTION RELEASE message has not been received.

### 8.1.14 Signalling connection release indication procedure



**Figure 8.1.14-1: Signalling connection release indication procedure, normal case**

#### 8.1.14.1 General

The signalling connection release indication procedure is used by the UE to indicate to the UTRAN that one of its signalling connections has been released. The procedure may in turn initiate the RRC connection release procedure.

### 8.1.14.2 Initiation

The UE shall, on receiving a request to release (abort) the signalling connection from upper layers for a specific CN domain:

- 1> if a signalling connection in the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS for the specific CN domain identified with the IE "CN domain identity" exists:
  - 2> initiate the signalling connection release indication procedure.
- 1> otherwise:
  - 2> abort any ongoing establishment of signalling connection for that specific CN domain as specified in 8.1.3.5a.

Upon initiation of the signalling connection release indication procedure in CELL\_PCH or URA\_PCH state, the UE shall:

- 1> perform a cell update procedure, according to subclause 8.3.1, using the cause "uplink data transmission";
- 1> when the cell update procedure completed successfully:
  - 2> continue with the signalling connection release indication procedure as below.

The UE shall:

- 1> set the IE "CN Domain Identity" to the value indicated by the upper layers. The value of the IE indicates the CN domain whose associated signalling connection the upper layers are indicating to be released;
- 1> remove the signalling connection with the identity indicated by upper layers from the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 1> transmit a SIGNALLING CONNECTION RELEASE INDICATION message on DCCH using AM RLC.

When the SIGNALLING CONNECTION RELEASE INDICATION message has been submitted to lower layers for transmission the procedure ends.

### 8.1.14.3 Reception of SIGNALLING CONNECTION RELEASE INDICATION by the UTRAN

Upon reception of a SIGNALLING CONNECTION RELEASE INDICATION message, the UTRAN requests the release of the signalling connection from upper layers. Upper layers may then initiate the release of the signalling connection.

### 8.1.15 Counter check procedure

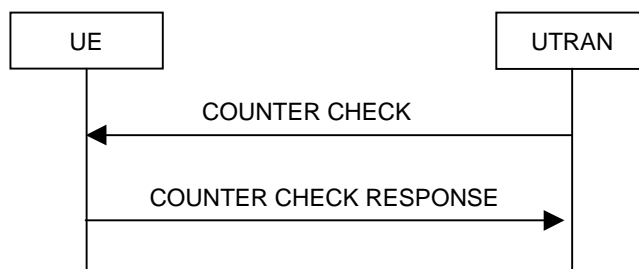


Figure 8.1.15-1: Counter check procedure

#### 8.1.15.1 General

The counter check procedure is used by the UTRAN to perform a local authentication. The purpose of the procedure is to check that the amount of data sent in both directions (uplink and downlink) over the duration of the RRC connection is identical at the UTRAN and at the UE (to detect a possible intruder – a 'man-in-the-middle' – from operating).

This procedure is only applicable to radio bearers, and only to radio bearers using RLC-AM or RLC-UM. It should be noted that this requires that the COUNT-C values for each UL and DL radio bearers using RLC-AM or RLC-UM continue to be incremented even if ciphering is not used. This procedure is not applicable to signalling radio bearers.

### 8.1.15.2 Initiation

The UTRAN monitors the COUNT-C value associated with each radio bearer using UM or AM RLC. The procedure is triggered whenever any of these values reaches a critical checking value. The granularity of these checking values and the values themselves are defined to the UTRAN by the visited network. The UTRAN initiates the procedure by sending a COUNTER CHECK message on the downlink DCCH.

### 8.1.15.3 Reception of a COUNTER CHECK message by the UE

When the UE receives a COUNTER CHECK message it shall compare the COUNT-C MSB values received in the IE "RB COUNT-C MSB information" in the COUNTER CHECK message to the COUNT-C MSB values of the corresponding radio bearers.

The UE shall:

- 1> set the IE "RRC transaction identifier" in the COUNTER CHECK RESPONSE message to the value of "RRC transaction identifier" in the entry for the COUNTER CHECK message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry.

If:

- there is one or more radio bearer(s) using UM or AM RLC mode stored in the variable ESTABLISHED\_RABS, which is (are) not included in the IE "RB COUNT-C MSB information"; or
- there is one or more radio bearer(s) included in the IE "RB COUNT-C MSB information", which is (are) not stored in the variable ESTABLISHED\_RABS; or
- for any radio bearer (excluding signalling radio bearers) using UM or AM RLC mode stored in the variable ESTABLISHED\_RABS and included in the IE "RB COUNT-C MSB information" with COUNT-C MSB values different from the MSB part of the COUNT-C values in the UE:

the UE shall:

- 1> include these radio bearers in the IE "RB COUNT-C information" in the COUNTER CHECK RESPONSE message. For any RB which is included in the IE "RB COUNT-C MSB information" in the COUNTER CHECK message but not stored in the variable ESTABLISHED\_RABS in the UE, the MSB part of COUNT-C values in the COUNTER CHECK RESPONSE message shall be set identical to COUNT-C-MSB values in the COUNTER CHECK message. The LSB part shall be filled with zeroes.

The UE shall:

- 1> if no COUNT-C exists for a radio bearer for a given direction (uplink or downlink) because:
  - 2> it is a uni-directional radio bearer configured only for the other direction (downlink or uplink respectively),  
or
  - 2> has been configured to RLC-TM mode in one direction (uplink or downlink) and RLC-UM in the other (downlink or uplink respectively).
- 3> set the COUNT-C in the IE "RB COUNT-C information" in the COUNTER CHECK RESPONSE message, to any value;

- 1> submit a COUNTER CHECK RESPONSE message to lower layers for transmission on the uplink DCCH using AM RLC.

When the COUNTER CHECK RESPONSE message has been submitted to lower layers for transmission the procedure ends.

#### 8.1.15.4 Reception of the COUNTER CHECK RESPONSE message by UTRAN

If the UTRAN receives a COUNTER CHECK RESPONSE message that does not contain any COUNT-C values, the procedure ends.

If the UTRAN receives a COUNTER CHECK RESPONSE message that contains one or several COUNT-C values the UTRAN may release the RRC connection.

#### 8.1.15.5 Cell re-selection

If the UE performs cell re-selection anytime during this procedure it shall, without interrupting the procedure:

- 1> initiate the cell update procedure according to subclause 8.3.1.

#### 8.1.15.6 Invalid COUNTER CHECK message

If the UE receives a COUNTER CHECK message, which contains a protocol error causing the variable `PROTOCOL_ERROR_REJECT` to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows. The UE shall:

- 1> transmit an RRC STATUS message on the uplink DCCH using AM RLC;
- 1> include the IE "Identification of received message"; and
- 1> set the IE "Received message type" to COUNTER CHECK; and
- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the UE COUNTER CHECK message in the table "Rejected transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> include the IE "Protocol error information" with contents set to the value of the variable `PROTOCOL_ERROR_INFORMATION`;
- 1> when the RRC STATUS message has been submitted to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the invalid COUNTER CHECK message has not been received.

#### 8.1.16 Inter RAT handover information transfer



**Figure 8.1.16-1: Inter RAT handover information transfer, normal flow**

##### 8.1.16.1 General

The inter RAT handover information transfer procedure is used by the UE to convey RRC information needed for inter RAT handover to UTRAN.

##### 8.1.16.2 Initiation

If:

- a radio access technology other than UTRA, e.g. GSM, using radio access technology-specific procedures, orders the UE to provide the INTER RAT HANDOVER INFO message; or
- a radio access technology other than UTRA, e.g. GSM, using radio access technology-specific procedures, configures the UE to send the INTER RAT HANDOVER INFO message upon system specific conditions not involving an explicit order e.g. early classmark sending upon entering connected mode; or
- while in connected mode using another radio access technology, the inter RAT handover info changes compared to what has previously been sent via the other radio access technology:

the UE shall:

- 1> initiate the inter RAT handover information transfer procedure.

To determine if the inter RAT handover info has changed compared to what has previously been sent, the UE shall:

- 1> store the information last sent in the variable INTER\_RAT\_HANDOVER\_INFO\_TRANSFERRED;
- 1> if this variable has not yet been set:
  - 2> not initiate the inter RAT handover information transfer procedure due to change of inter RAT handover info.

NOTE: Currently neither the UE security information nor the pre-defined configuration status information change while in connected mode using GSM radio access technology.

### 8.1.16.3 INTER RAT HANDOVER INFO message contents to set

The UE shall:

- 1> include the IE "Pre-defined configuration status information" and the IE "UE security information";
- 1> include the IE "UE radio access capability" and the IE "UE radio access capability extension" in accordance with the following:
  - 2> if the UE supports multiple UTRA FDD Frequency Bands; or
  - 2> if the UE supports a single UTRA FDD Frequency Band different from 2100 MHz:
    - 3> include the IE "UE radio access capability", excluding IEs "RF capability FDD" and "Measurement capability";
    - 3> include the IE "UE radio access capability extension", including the IEs "RF capability FDD extension" and the "Measurement capability extension" associated with each supported UTRA FDD frequency band indicated in the IE "Frequency band".
  - 2> else:
    - 3> include the IE "UE radio access capability", including the IEs "RF capability FDD" and "Measurement capability" associated with the 2100 MHz UTRA FDD frequency band.
- 1> initiate the transfer of the INTER RAT HANDOVER INFO message via the other radio access technology, using radio access technology-specific procedures;
- 1> store the IE "Pre-defined configuration status information", the IE "UE security information", the IE "UE radio access capability" and the IE "UE radio access capability extension", if included in the INTER RAT HANDOVER MESSAGE, in variable INTER\_RAT\_HANDOVER\_INFO\_TRANSFERRED;
- 1> and the procedure ends.

## 8.2 Radio Bearer control procedures

### 8.2.1 Radio bearer establishment

See subclause 8.2.2 Reconfiguration procedures.

## 8.2.2 Reconfiguration procedures

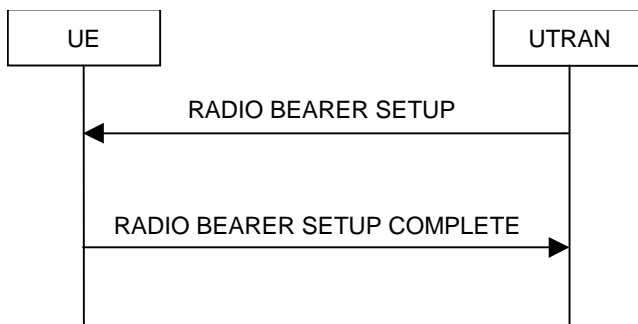


Figure 8.2.2-1: Radio Bearer Establishment, normal case

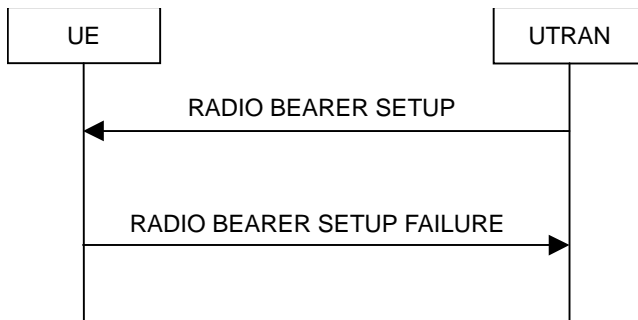


Figure 8.2.2-2: Radio Bearer Establishment, failure case

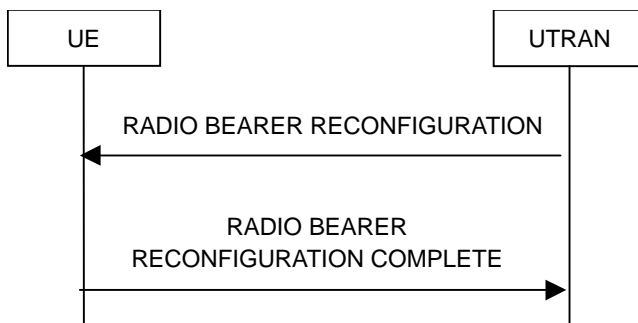


Figure 8.2.2-3: Radio bearer reconfiguration, normal flow

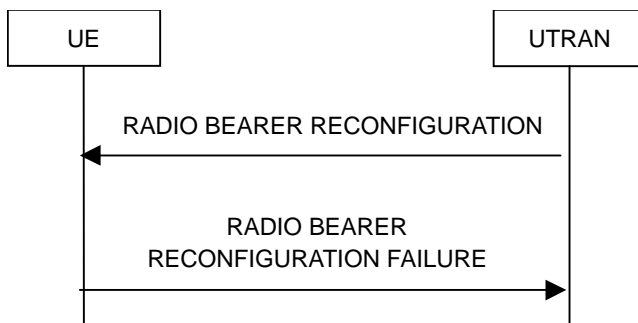


Figure 8.2.2-4: Radio bearer reconfiguration, failure case

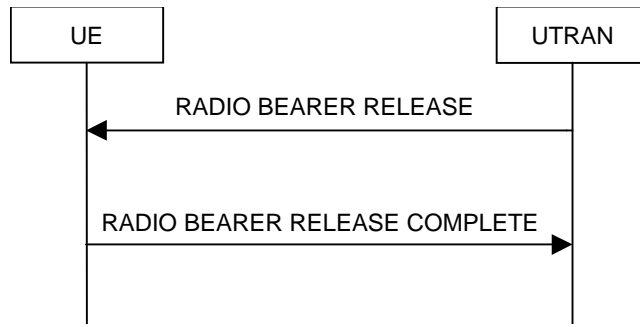


Figure 8.2.2-5: Radio Bearer Release, normal case

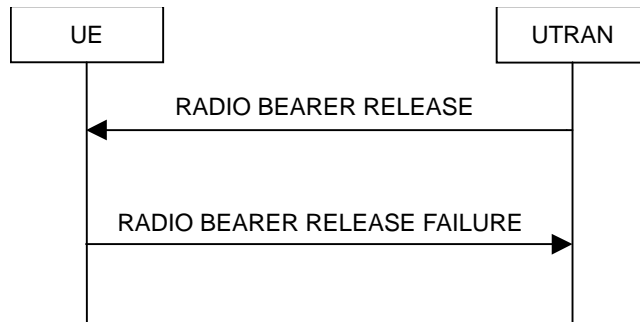


Figure 8.2.2-6: Radio Bearer Release, failure case

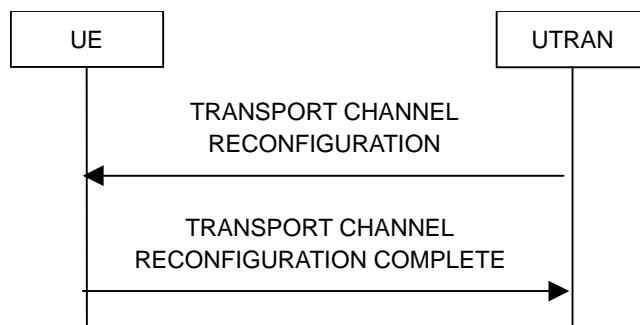


Figure 8.2.2-7: Transport channel reconfiguration, normal flow

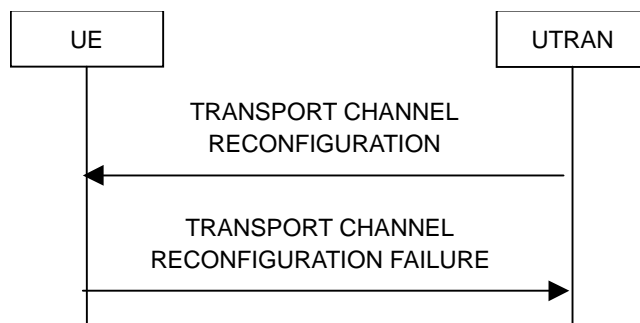


Figure 8.2.2-8: Transport channel reconfiguration, failure case

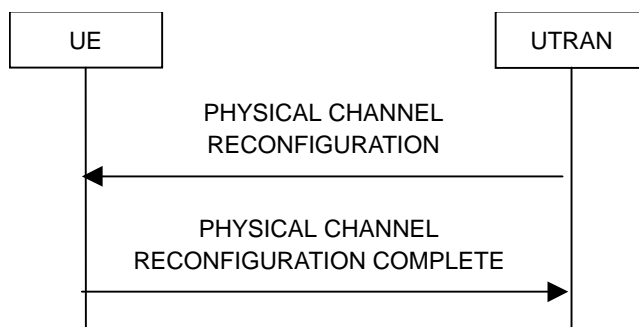


Figure 8.2.2-9: Physical channel reconfiguration, normal flow

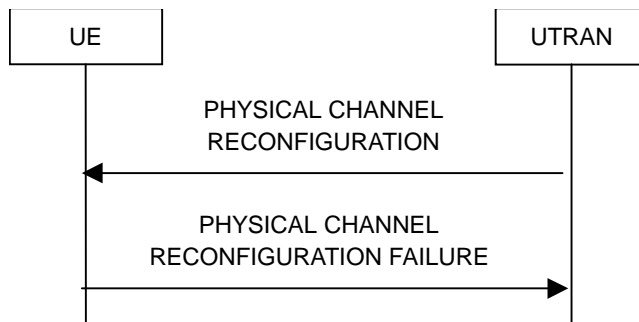


Figure 8.2.2-10: Physical channel reconfiguration, failure case

### 8.2.2.1 General

Reconfiguration procedures include the following procedures:

- the radio bearer establishment procedure;
- radio bearer reconfiguration procedure;
- the radio bearer release procedure;
- the transport channel reconfiguration procedure; and
- the physical channel reconfiguration procedure.

The radio bearer establishment procedure is used to establish new radio bearer(s).

The radio bearer reconfiguration procedure is used to reconfigure parameters for a radio bearer.

The radio bearer release procedure is used to release radio bearer(s).

The transport channel reconfiguration procedure is used to reconfigure transport channel parameters.

The physical channel reconfiguration procedure is used to establish, reconfigure and release physical channels.

While performing any of the above procedures, these procedures may perform a hard handover - see subclause 8.3.5.

### 8.2.2.2 Initiation

To initiate any one of the reconfiguration procedures, UTRAN should:

- 1> configure new radio links in any new physical channel configuration;
- 1> start transmission and reception on the new radio links;
- 1> for a radio bearer establishment procedure:
  - 2> transmit a RADIO BEARER SETUP message on the downlink DCCH using AM or UM RLC;



- 2> if signalling radio bearer RB4 is setup with this procedure and signalling radio bearers RB1-RB3 were already established prior to the procedure:
  - 3> if the variable "LATEST\_CONFIGURED\_CN\_DOMAIN" has been initialised:
    - 4> connect any radio bearers setup by the same message as signalling radio bearer RB4 to the CN domain indicated in the variable "LATEST\_CONFIGURED\_CN\_DOMAIN".
- 1> for a radio bearer reconfiguration procedure:
  - 2> transmit a RADIO BEARER RECONFIGURATION message on the downlink DCCH using AM or UM RLC.
- 1> for a radio bearer release procedure:
  - 2> transmit a RADIO BEARER RELEASE message on the downlink DCCH using AM or UM RLC.
- 1> for a transport channel reconfiguration procedure:
  - 2> transmit a TRANSPORT CHANNEL RECONFIGURATION message on the downlink DCCH using AM or UM RLC.
- 1> for a physical channel reconfiguration procedure:
  - 2> transmit a PHYSICAL CHANNEL RECONFIGURATION message on the downlink DCCH using AM or UM RLC.
- 1> if the reconfiguration procedure is simultaneous with SRNS relocation procedure:
  - 2> if the transmitted message is a RADIO BEARER RECONFIGURATION:
    - 3> include the IE "New U-RNTI".
  - 2> else:
    - 3> include the IE "Downlink counter synchronisation info".
  - 2> if ciphering and/or integrity protection are activated:
    - 3> include new ciphering and/or integrity protection configuration information to be used after reconfiguration.
  - 2> use the downlink DCCH using AM RLC.
- 1> if transport channels are added, reconfigured or deleted in uplink and/or downlink:
  - 2> set TFCS according to the new transport channel(s).
- 1> if transport channels are added or deleted in uplink and/or downlink, and RB Mapping Info applicable to the new configuration has not been previously provided to the UE, the UTRAN should:
  - 2> send the RB Mapping Info for the new configuration.

In the Radio Bearer Reconfiguration procedure UTRAN may indicate that uplink transmission shall be stopped or continued on certain radio bearers. Uplink transmission on a signalling radio bearer used by the RRC signalling (signalling radio bearer RB1 or signalling radio bearer RB2) should not be stopped.

NOTE 1: The RADIO BEARER RECONFIGURATION message always includes the IE "RB information to reconfigure", even if UTRAN does not require the reconfiguration of any RB. In these cases, UTRAN may include only the IE "RB identity" within the IE "RB information to reconfigure".

NOTE 2: The RADIO BEARER RECONFIGURATION message always includes the IE "Downlink information per radio link list", even if UTRAN does not require the reconfiguration of any RL. In these cases, UTRAN may re-send the currently assigned values for the mandatory IEs included within the IE "Downlink information per radio link list ". Moreover, the RADIO BEARER RECONFIGURATION message always includes the IE "Primary CPICH Info" (FDD) or IE "Primary CCPCH Info" (TDD). This implies that in case UTRAN applies the RADIO BEARER RECONFIGURATION message to move the UE to CELL\_FACH state, it has to indicate a cell. However, UTRAN may indicate any cell; the UE anyhow performs cell selection and notifies UTRAN if it selects another cell than indicated by UTRAN.

If the IE "Activation Time" is included, UTRAN should set it to a value taking the UE performance requirements into account.

UTRAN should take the UE capabilities into account when setting the new configuration.

If the message is used to initiate a transition from CELL\_DCH to CELL\_FACH state, the UTRAN may assign a CPCH configuration to be used in that cell by the UE. UTRAN may also assign a C-RNTI to be used in that cell by the UE.

### 8.2.2.3 Reception of RADIO BEARER SETUP or RADIO BEARER RECONFIGURATION or RADIO BEARER RELEASE or TRANSPORT CHANNEL RECONFIGURATION or PHYSICAL CHANNEL RECONFIGURATION message by the UE

The UE shall be able to receive any of the following messages:

- RADIO BEARER SETUP message; or
- RADIO BEARER RECONFIGURATION message; or
- RADIO BEARER RELEASE message; or
- TRANSPORT CHANNEL RECONFIGURATION message; or
- PHYSICAL CHANNEL RECONFIGURATION message;

and perform a hard handover, even if no prior UE measurements have been performed on the target cell and/or frequency.

If the UE receives:

- a RADIO BEARER SETUP message; or
- a RADIO BEARER RECONFIGURATION message; or
- a RADIO BEARER RELEASE message; or
- a TRANSPORT CHANNEL RECONFIGURATION message; or
- a PHYSICAL CHANNEL RECONFIGURATION message:

it shall:

- 1> set the variable ORDERED\_RECONFIGURATION to TRUE;
- 1> perform the physical layer synchronisation procedure as specified in [29];
- 1> act upon all received information elements as specified in subclause 8.6, unless specified in the following and perform the actions below.

The UE may first release the physical channel configuration used at reception of the reconfiguration message. The UE shall then:

- 1> in FDD, if the IE "PDSCH code mapping" is included but the IE "PDSCH with SHO DCH Info" is not included and if the DCH has only one link in its active set:
  - 2> act upon the IE "PDSCH code mapping" as specified in subclause 8.6; and

2> infer that the PDSCH will be transmitted from the cell from which the downlink DPCH is transmitted.

1> enter a state according to subclause 8.6.3.3.

In case the UE receives a RADIO BEARER RECONFIGURATION message including the IE "RB information to reconfigure" that only includes the IE "RB identity", the UE shall:

1> handle the message as if IE "RB information to reconfigure" was absent.

NOTE: The RADIO BEARER RECONFIGURATION message always includes the IE "RB information to reconfigure". UTRAN has to include it even if it does not require the reconfiguration of any RB.

If after state transition the UE enters CELL\_DCH state, the UE shall, after the state transition:

1> remove any C-RNTI from MAC;

1> clear the variable C\_RNTI.

In FDD, if after state transition the UE leaves CELL\_DCH state, the UE shall, after the state transition:

1> remove any DSCH-RNTI from MAC;

1> clear the variable DSCH\_RNTI.

If the UE was in CELL\_DCH state upon reception of the reconfiguration message and remains in CELL\_DCH state, the UE shall:

1> if the IE "Uplink DPCH Info" is absent, not change its current UL Physical channel configuration;

1> if the IE "Downlink information for each radio link" is absent, not change its current DL Physical channel configuration.

If after state transition the UE enters CELL\_FACH state, the UE shall, after the state transition:

1> if the IE "Frequency info" is included in the received reconfiguration message:

2> select a suitable UTRA cell according to [4] on that frequency.

1> if the IE "Frequency info" is not included in the received reconfiguration message:

2> select a suitable UTRA cell according to [4].

1> if the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selects another cell than indicated by this IE or the received reconfiguration message did not include the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD):

2> initiate a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";

2> when the cell update procedure completed successfully:

3> if the UE is in CELL\_PCH or URA\_PCH state:

4> initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";

4> proceed as below.

1> start timer T305 using its initial value if timer T305 is not running and if periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" in system information block type 1;

1> select PRACH according to subclause 8.5.17;

1> select Secondary CCPCH according to subclause 8.5.19;

1> use the transport format set given in system information;

1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:

- 2> ignore that IE and stop using DRX.
- 1> if the contents of the variable C\_RNTI is empty:
  - 2> perform a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";
  - 2> when the cell update procedure completed successfully:
    - 3> if the UE is in CELL\_PCH or URA\_PCH state:
      - 4> initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
      - 4> proceed as below.

If the UE was in CELL\_FACH state upon reception of the reconfiguration message and remains in CELL\_FACH state, the UE shall:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4] on that frequency;
  - 2> if the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE or the received reconfiguration message did not include the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD):
    - 3> initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
    - 3> when the cell update procedure completed successfully:
      - 4> proceed as below.

The UE shall transmit a response message as specified in subclause 8.2.2.4, setting the information elements as specified below. The UE shall:

- 1> if the received reconfiguration message included the IE "Downlink counter synchronisation info"; or
- 1> if the received reconfiguration message is a RADIO BEARER RECONFIGURATION and the IE "New U-RNTI" is included:
  - 2> re-establish RB2;
  - 2> set the new uplink and downlink HFN of RB2 to MAX(uplink HFN of RB2, downlink HFN of RB2);
  - 2> increment by one the downlink and uplink HFN values for RB2;
  - 2> calculate the START value according to subclause 8.5.9;
  - 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message did not include the IE "Downlink counter synchronisation info":
  - 2> if the variable START\_VALUE\_TO\_TRANSMIT is set:
    - 3> include and set the IE "START" to the value of that variable.
  - 2> if the variable START\_VALUE\_TO\_TRANSMIT is not set and the IE "New U-RNTI" is included:
    - 3> calculate the START value according to subclause 8.5.9;
    - 3> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
  - 2> if the received reconfiguration message caused a change in the RLC size for any RB using RLC-AM:
    - 3> calculate the START value according to subclause 8.5.9;

- 3> include the calculated START values for the CN domain associated with the corresponding RB identity in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info":
  - 2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the received reconfiguration message did not contain the IE "Ciphering activation time for DPCH" in IE "Ciphering mode info":
  - 2> if prior to this procedure there exist no transparent mode RLC radio bearers:
    - 3> if, at the conclusion of this procedure, the UE will be in CELL\_DCH state; and
    - 3> if, at the conclusion of this procedure, at least one transparent mode RLC radio bearer exists:
      - 4> include the IE "COUNT-C activation time" and specify a CFN value for this IE.
  - 2> if prior to this procedure there exists at least one transparent mode RLC radio bearer:
    - 3> if, at the conclusion of this procedure, no transparent mode RLC radio bearers exist:
      - 4> include the IE "COUNT-C activation time" and specify a CFN value for this IE.
- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the received message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> if the variable PDCP\_SN\_INFO is not empty:
  - 2> include the IE "RB with PDCP information list" and set it to the value of the variable PDCP\_SN\_INFO.
- 1> in TDD, if the procedure is used to perform a handover to a cell where timing advance is enabled, and the UE can calculate the timing advance value in the new cell (i.e. in a synchronous TDD network):
  - 2> set the IE "Uplink Timing Advance" according to subclause 8.6.6.26.
- 1> if the IE "Integrity protection mode info" was present in the received reconfiguration message:
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.

If after state transition the UE enters CELL\_PCH or URA\_PCH state, the UE shall, after the state transition and transmission of the response message:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4] on that frequency.
- 1> if the IE "Frequency info" is not included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4].
- 1> prohibit periodical status transmission in RLC;
- 1> remove any C-RNTI from MAC;
- 1> clear the variable C\_RNTI;

- 1> start timer T305 using its initial value if timer T305 is not running and if periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" in system information block type 1;
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 2> use the value in the IE "UTRAN DRX Cycle length coefficient" for calculating Paging occasion and PICH Monitoring Occasion as specified in subclause 8.6.3.2.
- 1> if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the UE enters CELL\_PCH state from CELL\_DCH state, and the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE or the received reconfiguration message did not include the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD):
  - 2> initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
  - 2> when the cell update procedure completed successfully:
    - 3> the procedure ends.
- 1> if the UE enters CELL\_PCH state from CELL\_FACH state, and the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE:
  - 2> initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
  - 2> when the cell update procedure is successfully completed:
    - 3> the procedure ends.
- 1> if the UE enters URA\_PCH state, and after cell selection the criteria for URA update caused by "URA reselection" according to subclause 8.3.1 is fulfilled:
  - 2> initiate a URA update procedure according to subclause 8.3.1 using the cause "URA reselection";
  - 2> when the URA update procedure is successfully completed:
    - 3> the procedure ends.

#### 8.2.2.4 Transmission of a response message by the UE, normal case

In case the procedure was triggered by reception of a RADIO BEARER SETUP message, the UE shall:

- 1> transmit a RADIO BEARER SETUP COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a RADIO BEARER RECONFIGURATION message, the UE shall:

- 1> transmit a RADIO BEARER RECONFIGURATION COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a RADIO BEARER RELEASE message, the UE shall:

- 1> transmit a RADIO BEARER RELEASE COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a TRANSPORT CHANNEL RECONFIGURATION message, the UE shall:

- 1> transmit a TRANSPORT CHANNEL RECONFIGURATION COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a PHYSICAL CHANNEL RECONFIGURATION message, the UE shall:

- 1> transmit a PHYSICAL CHANNEL RECONFIGURATION COMPLETE as response message on the uplink DCCH using AM RLC.

If the new state is CELL\_DCH or CELL\_FACH, the response message shall be transmitted using the new configuration after the state transition, and the UE shall:

- 1> if the IE "Downlink counter synchronisation info" was included in the reconfiguration message; or
- 1> if the received reconfiguration message is a RADIO BEARER RECONFIGURATION and the IE "New U-RNTI" is included:
  - 2> when RLC has confirmed the successful transmission of the response message:
    - 3> re-establish all AM and UM RLC entities with RB identities larger than 4 and set the first 20 bits of all their HFN values to the START value included in the response message for the corresponding CN domain;
    - 3> re-establish the RLC entities with RB identities 1, 3 and 4 and set the first 20 bits of all their HFN values to the START value included in the response message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 3> set the remaining bits of the HFN values of all UM RLC entities to zero;
    - 3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].

- 1> if the variable PDCP\_SN\_INFO is empty:

- 2> if the received reconfiguration message contained the IE "Ciphering mode info":
  - 3> when RLC has confirmed the successful transmission of the response message:
    - 4> notify upper layers upon change of the security configuration;
    - 4> perform the actions below.
- 2> if the received reconfiguration message did not contain the IE "Ciphering mode info":
  - 3> when RLC has been requested to transmit the response message:
    - 4> perform the actions below.

- 1> if the variable PDCP\_SN\_INFO is non-empty:

- 2> when RLC has confirmed the successful transmission of the response message:
  - 3> for each radio bearer in the variable PDCP\_SN\_INFO:
    - 4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
      - 5> configure the RLC entity for that radio bearer to "continue".
  - 3> perform the actions below.

If the new state is CELL\_PCH or URA\_PCH, the response message shall be transmitted using the old configuration before the state transition, but the new C-RNTI shall be used if the IE "New C-RNTI" was included in the received reconfiguration message, and the UE shall:

- 1> when RLC has confirmed the successful transmission of the response message:
  - 2> for each radio bearer in the variable PDCP\_SN\_INFO:
    - 3> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
      - 4> configure the RLC entity for that radio bearer to "continue".

2> enter the new state (CELL\_PCH or URA\_PCH, respectively);

2> perform the actions below.

The UE shall:

1> set the variable ORDERED\_RECONFIGURATION to FALSE;

1> if the received reconfiguration message contained the IE "Ciphering mode info":

2> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;

2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and

2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.

1> if the received reconfiguration message contained the IE "Integrity protection mode info":

2> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;

2> set "Uplink RRC Message sequence number" for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO to a value such that next RRC message to be sent on uplink RB0 will use the new integrity protection configuration;

2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and

2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.

1> clear the variable PDCP\_SN\_INFO;

1> clear the variable START\_VALUE\_TO\_TRANSMIT;

1> clear the variable SECURITY\_MODIFICATION.

### 8.2.2.5 Reception of a response message by the UTRAN, normal case

When UTRAN has received

- the RADIO BEARER SETUP COMPLETE message; or
- the RADIO BEARER RECONFIGURATION COMPLETE message; or
- the RADIO BEARER RELEASE COMPLETE message; or
- the TRANSPORT CHANNEL RECONFIGURATION COMPLETE message; or
- the PHYSICAL CHANNEL RECONFIGURATION COMPLETE message.

UTRAN may:

1> delete the old configuration.

If the procedure caused the UE to leave the CELL\_FACH state, UTRAN may:

1> delete the C-RNTI of the UE.

If the IE "UL Timing Advance" is included in TDD, UTRAN should:

1> evaluate the timing advance value that the UE has to use in the new cell after handover.

If the IE "START" or the IE "START list " is included, UTRAN should:

1> set the START value for each CN domain with the corresponding values as received in this response message;

1> consequently, then use the START values to initialise the hyper frame numbers, in the same way as specified for the UE in subclause 8.2.2.3, for any new radio bearers that are established.



If UTRAN has ordered a ciphering reconfiguration by including the IE "Ciphering mode info", UTRAN should:

- 1> for radio bearers using RLC-AM or RLC-UM:
  - 2> use the old ciphering configuration for received RLC PDUs with RLC sequence number less than the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" sent by the UE;
  - 2> use the new ciphering configuration for received RLC PDUs with RLC sequence number greater than or equal to the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" sent by the UE;
  - 2> if an RLC reset or re-establishment occurs after this response message has been received by UTRAN before the activation time for the new ciphering configuration has been reached:
    - 3> ignore the activation time; and
    - 3> apply the new ciphering configuration immediately after the RLC reset or RLC re-establishment.
- 1> for radio bearers using RLC-TM:
  - 2> use the new ciphering configuration and only begin incrementing the COUNT-C at the CFN as indicated in:
    - 3> the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info", if included in the message that triggered the radio bearer control procedure; or
    - 3> the IE "COUNT-C activation time", if included in the response message for this procedure.
- 1> and the procedure ends on the UTRAN side.

#### 8.2.2.6 Unsupported configuration in the UE

If the UTRAN instructs the UE to use a configuration, which it does not support and/or if the received message causes the variable UNSUPPORTED\_CONFIGURATION to be set to TRUE, the UE shall:

- 1> transmit a failure response as specified in subclause 8.2.2.9, setting the information elements as specified below:
  - 2> include the IE "RRC transaction identifier"; and
  - 2> set it to the value of "RRC transaction identifier" in the entry for the received message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> set the IE "failure cause" to "configuration unsupported".
- 1> set the variable UNSUPPORTED\_CONFIGURATION to FALSE;
- 1> continue with any ongoing processes and procedures as if the reconfiguration message was not received.

The procedure ends.

#### 8.2.2.7 Physical channel failure

A physical channel failure occurs in case the criteria defined in subclause 8.5.4 are not fulfilled.

If the received message caused the UE to be in CELL\_DCH state and the UE failed to establish the dedicated physical channel(s) indicated in the received message the UE shall:

- 1> revert to the configuration prior to the reception of the message (old configuration);
- 1> if the old configuration includes dedicated physical channels (CELL\_DCH state) and the UE is unable to revert to the old configuration:
  - 2> initiate a cell update procedure according to subclause 8.3.1, using the cause "radio link failure";

- 2> after the cell update procedure has completed successfully:
  - 3> proceed as below.
- 1> if the old configuration does not include dedicated physical channels (CELL\_FACH state):
  - 2> select a suitable UTRA cell according to [4];
  - 2> if the UE selects another cell than the cell the UE camped on upon reception of the reconfiguration message:
    - 3> initiate a cell update procedure according to subclause 8.3.1, using the cause "Cell reselection";
    - 3> after the cell update procedure has completed successfully:
      - 4> proceed as below.
- 1> transmit a failure response message as specified in subclause 8.2.2.9, setting the information elements as specified below:
  - 2> include the IE "RRC transaction identifier"; and
  - 2> set it to the value of "RRC transaction identifier" in the entry for the received message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> set the IE "failure cause" to "physical channel failure".
- 1> set the variable ORDERED\_RECONFIGURATION to FALSE;
- 1> continue with any ongoing processes and procedures as if the reconfiguration message was not received.

The procedure ends.

### 8.2.2.8 Cell re-selection

If the UE performs cell re-selection during the reconfiguration procedure, the UE shall:

- 1> initiate a cell update procedure, as specified in subclause 8.3.1;
- 1> continue with the reconfiguration procedure.

### 8.2.2.9 Transmission of a response message by the UE, failure case

The UE shall:

- 1> in case of reception of a RADIO BEARER SETUP message:
  - 2> if the radio bearer establishment procedure affects several radio bearers:
    - 3> (may) include the identities of the radio bearers for which the procedure would have been successful into the RADIO BEARER SETUP FAILURE message.
  - 2> transmit a RADIO BEARER SETUP FAILURE as response message on the DCCH using AM RLC.
- 1> in case of reception of a RADIO BEARER RECONFIGURATION message:
  - 2> if the radio bearer reconfiguration procedure affects several radio bearers:
    - 3> (may) include the identities of the radio bearers for which the procedure would have been successful into the RADIO BEARER RECONFIGURATION FAILURE message.
  - 2> transmit a RADIO BEARER RECONFIGURATION FAILURE as response message on the DCCH using AM RLC.
- 1> in case of reception of a RADIO BEARER RELEASE message:

- 2> if the radio bearer release procedure affects several radio bearers:
  - 3> (may) include the identities of the radio bearers for which the procedure would have been successful into the RADIO BEARER RELEASE FAILURE message.
- 2> transmit a RADIO BEARER RELEASE FAILURE as response message on the DCCH using AM RLC.
- 1> in case of reception of a TRANSPORT CHANNEL RECONFIGURATION message:
  - 2> transmit a TRANSPORT CHANNEL RECONFIGURATION FAILURE as response message on the DCCH using AM RLC.
- 1> in case of reception of a PHYSICAL CHANNEL RECONFIGURATION message:
  - 2> transmit a PHYSICAL CHANNEL RECONFIGURATION FAILURE as response message on the DCCH using AM RLC.
- 1> when the response message has been submitted to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if no reconfiguration attempt had occurred.

#### 8.2.2.10 Reception of a response message by the UTRAN, failure case

When the UTRAN has received:

- the RADIO BEARER SETUP FAILURE message; or
- the RADIO BEARER RECONFIGURATION FAILURE message; or
- the RADIO BEARER RELEASE FAILURE message; or
- the TRANSPORT CHANNEL RECONFIGURATION FAILURE message; or
- the PHYSICAL CHANNEL RECONFIGURATION FAILURE message;

the UTRAN may restore the old and delete the new configuration. Upper layers should be notified of the failure.

The procedure ends on the UTRAN side.

#### 8.2.2.11 Invalid configuration

If the variable INVALID\_CONFIGURATION is set to TRUE the UE shall:

- 1> keep the configuration existing before the reception of the message;
- 1> transmit a failure response message as specified in subclause 8.2.2.9, setting the information elements as specified below:
  - 2> include the IE "RRC transaction identifier"; and
    - 3> set it to the value of "RRC transaction identifier" in the entry for the received message in the table "Accepted transactions" in the variable TRANSACTIONS; and
    - 3> clear that entry.
  - 2> set the IE "failure cause" to "invalid configuration".
- 1> set the variable INVALID\_CONFIGURATION to FALSE;
- 1> continue with any ongoing processes and procedures as if the reconfiguration message was not received.

The procedure ends.

### 8.2.2.12 Incompatible simultaneous reconfiguration

If the table "Rejected transactions" in the variable TRANSACTIONS is set due to the received message and the variable PROTOCOL\_ERROR\_REJECT is set to FALSE, the UE shall:

- 1> not apply the configuration contained in the received reconfiguration message;
- 1> transmit a failure response message as specified in subclause 8.2.2.9, setting the information elements as specified below:
  - 2> include the IE "RRC transaction identifier"; and
  - 2> set it to the value of "RRC transaction identifier" in the entry for the received message in the table "Rejected transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> set the IE "failure cause" to "incompatible simultaneous reconfiguration".
- 1> continue with any ongoing processes and procedures as if the reconfiguration message was not received.

The procedure ends.

### 8.2.2.12a Incompatible simultaneous security reconfiguration

If the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION is set to TRUE due to the received reconfiguration message, the UE shall:

- 1> transmit a failure response message as specified in subclause 8.2.2.9, setting the information elements as specified below:
  - 2> include the IE "RRC transaction identifier"; and
  - 2> set it to the value of "RRC transaction identifier" in the entry for the received message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration".
- 1> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to FALSE;
- 1> continue with any ongoing processes and procedures as if the reconfiguration message was not received.

The procedure ends.

### 8.2.2.12b Cell update procedure during security reconfiguration

If:

- a cell update procedure according to subclause 8.3.1 is initiated; and
- the received reconfiguration message causes either:
  - the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE; and/or
  - the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE:

the UE shall:

- 1> abort the ongoing integrity and/or ciphering reconfiguration;
- 1> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
- 1> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;

- 1> if the received reconfiguration message contained the IE "Ciphering mode info":
  - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
- 1> if the received reconfiguration message contained the IE "Integrity protection mode info":
  - 2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 1> continue with any ongoing processes and procedures as if the reconfiguration message was not received.

The procedure ends.

### 8.2.2.13 Invalid received message

If the received reconfiguration message contains a protocol error causing the variable PROTOCOL\_ERROR\_REJECT to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows. The UE shall:

- 1> transmit a failure response message as specified in subclause 8.2.2.9, setting the information elements as specified below:
  - 2> include the IE "RRC transaction identifier"; and
  - 2> set it to the value of "RRC transaction identifier" in the entry for the received message in the table "Rejected transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> set the IE "failure cause" to the cause value "protocol error";
  - 2> include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL\_ERROR\_INFORMATION.

The procedure ends.

### 8.2.3 Radio bearer release

See subclause 8.2.2 (Reconfiguration procedures).

### 8.2.4 Transport channel reconfiguration

See subclause 8.2.2 (Reconfiguration procedures).

### 8.3 RRC connection mobility procedures

#### 8.3.1 Cell and URA update procedures

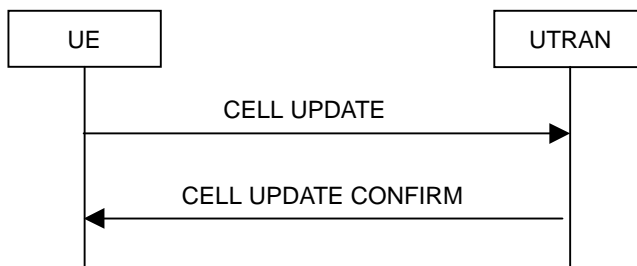


Figure 8.3.1-1: Cell update procedure, basic flow

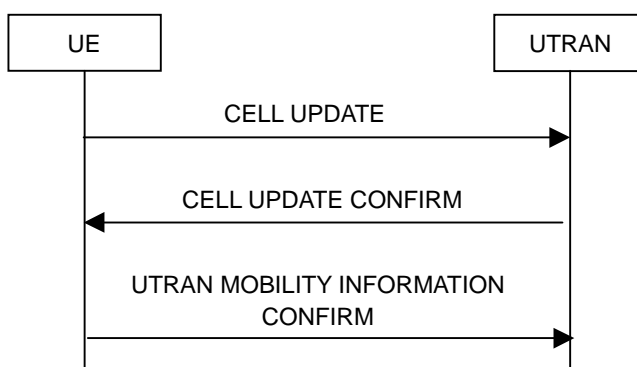


Figure 8.3.1-2: Cell update procedure with update of UTRAN mobility information

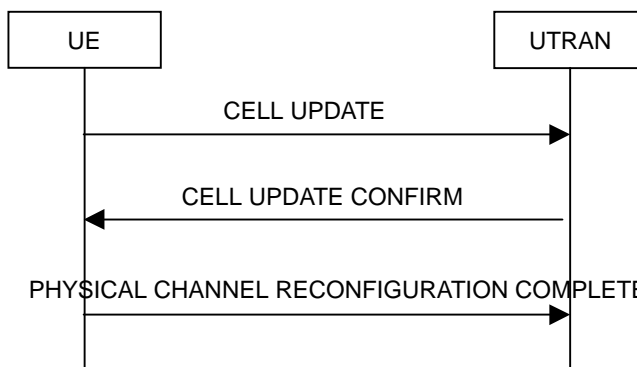


Figure 8.3.1-3: Cell update procedure with physical channel reconfiguration

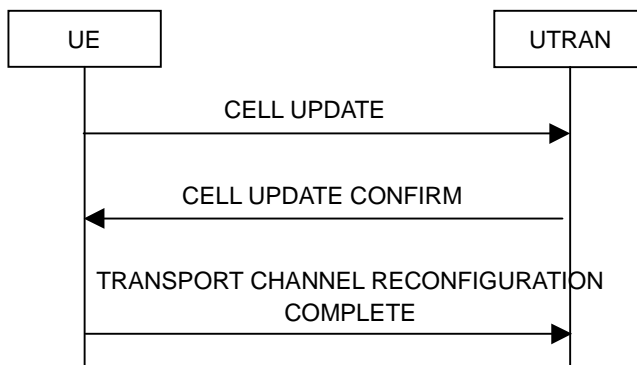


Figure 8.3.1-4: Cell update procedure with transport channel reconfiguration

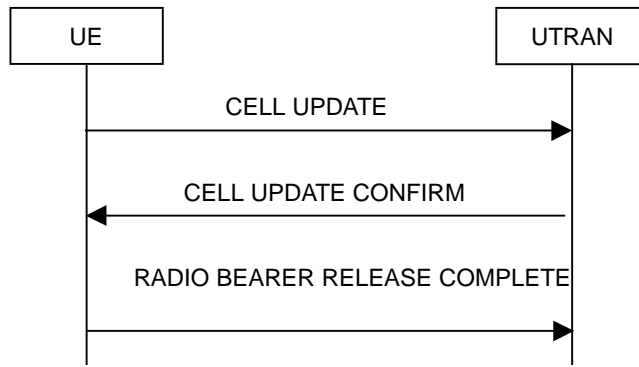


Figure 8.3.1-5: Cell update procedure with radio bearer release

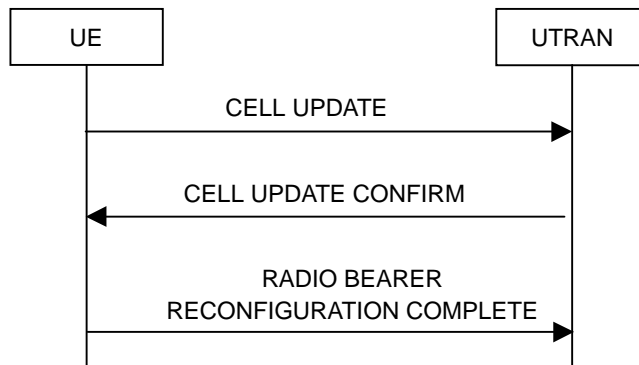


Figure 8.3.1-6: Cell update procedure with radio bearer reconfiguration

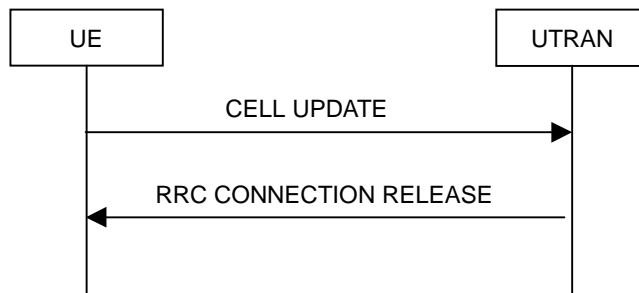


Figure 8.3.1-7: Cell update procedure, failure case

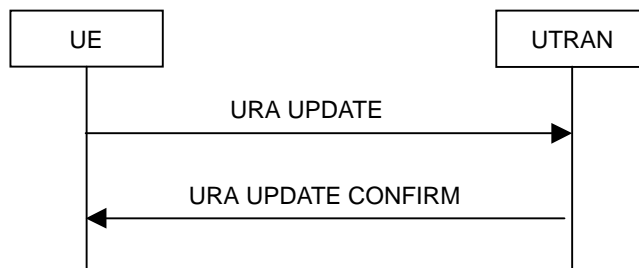
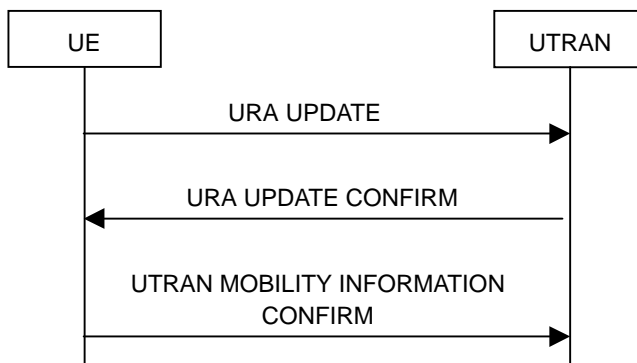
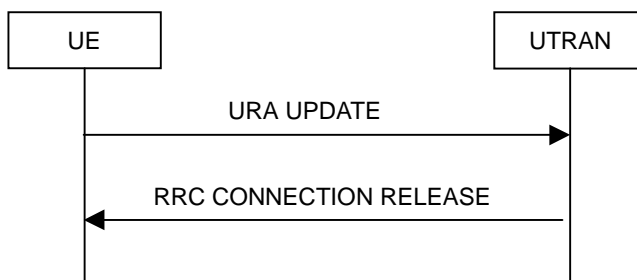


Figure 8.3.1-8: URA update procedure, basic flow



**Figure 8.3.1-9: URA update procedure with update of UTRAN mobility information**



**Figure 8.3.1-10: URA update procedure, failure case**

### 8.3.1.1 General

The URA update and cell update procedures serve several main purposes:

- to notify UTRAN after re-entering service area in the URA\_PCH or CELL\_PCH state;
- to notify UTRAN of an RLC unrecoverable error [16] on an AM RLC entity;
- to be used as a supervision mechanism in the CELL\_FACH, CELL\_PCH, or URA\_PCH state by means of periodical update.

In addition, the URA update procedure also serves the following purpose:

- to retrieve a new URA identity after cell re-selection to a cell not belonging to the current URA assigned to the UE in URA\_PCH state.

In addition, the cell update procedure also serves the following purposes:

- to update UTRAN with the current cell the UE is camping on after cell reselection;
- to act on a radio link failure in the CELL\_DCH state;
- when triggered in the URA\_PCH or CELL\_PCH state, to notify UTRAN of a transition to the CELL\_FACH state due to the reception of UTRAN originated paging or due to a request to transmit uplink data.

The URA update and cell update procedures may:

- 1> include an update of mobility related information in the UE;
- 1> cause a state transition from the CELL\_FACH state to the CELL\_DCH, CELL\_PCH or URA\_PCH states or idle mode.

The cell update procedure may also include:

- a re-establish of AM RLC entities;



- a radio bearer release, radio bearer reconfiguration, transport channel reconfiguration or physical channel reconfiguration.

### 8.3.1.2 Initiation

A UE shall initiate the cell update procedure in the following cases:

1> Uplink data transmission:

- 2> if the UE is in URA\_PCH or CELL\_PCH state; and
- 2> if the UE has uplink RLC data PDU or uplink RLC control PDU on RB1 or upwards to transmit:
  - 3> perform cell update using the cause "uplink data transmission".

1> Paging response:

- 2> if the criteria for performing cell update with the cause specified above in the current subclause is not met; and
- 2> if the UE in URA\_PCH or CELL\_PCH state, receives a PAGING TYPE 1 message fulfilling the conditions for initiating a cell update procedure specified in subclause 8.1.2.3:
  - 3> perform cell update using the cause "paging response".

1> Radio link failure:

- 2> if none of the criteria for performing cell update with the causes specified above in the current subclause is met; and
- 2> if the UE is in CELL\_DCH state; and
- 2> if the criteria for radio link failure is met as specified in subclause 8.5.6:
  - 3> perform cell update using the cause "radio link failure".

1> Re-entering service area:

- 2> if none of the criteria for performing cell update with the causes specified above in the current subclause is met; and
- 2> if the UE is in CELL\_FACH or CELL\_PCH state; and
- 2> if the UE has been out of service area and re-enters service area before T307 or T317 expires:
  - 3> perform cell update using the cause "re-entering service area".

1> RLC unrecoverable error:

- 2> if none of the criteria for performing cell update with the causes specified above in the current subclause is met; and
- 2> if the UE detects RLC unrecoverable error [16] in an AM RLC entity:
  - 3> perform cell update using the cause "RLC unrecoverable error".

1> Cell reselection:

- 2> if none of the criteria for performing cell update with the causes specified above in the current subclause is met:
  - 3> if the UE is in CELL\_FACH or CELL\_PCH state and the UE performs cell re-selection; or
  - 3> if the UE is in CELL\_FACH state and the variable C\_RNTI is empty:
    - 4> perform cell update using the cause "cell reselection".

## 1&gt; Periodical cell update:

- 2> if none of the criteria for performing cell update with the causes specified above in the current subclause is met; and
- 2> if the UE is in CELL\_FACH or CELL\_PCH state; and
- 2> if the timer T305 expires; and
- 2> if the criteria for "in service area" as specified in subclause 8.5.5.2 is fulfilled; and
- 2> if periodic updating has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity":
  - 3> perform cell update using the cause "periodical cell update".

A UE in URA\_PCH state shall initiate the URA update procedure in the following cases:

## 1&gt; URA reselection:

- 2> if the UE detects that the current URA assigned to the UE, stored in the variable URA\_IDENTITY, is not present in the list of URA identities in system information block type 2; or
- 2> if the list of URA identities in system information block type 2 is empty; or
- 2> if the system information block type 2 can not be found:
  - 3> perform URA update using the cause "change of URA".

## 1&gt; Periodic URA update:

- 2> if the criteria for performing URA update with the causes as specified above in the current subclause are not met; and
- 2> if the timer T305 expires while the UE is in the service area; and
- 2> if periodic updating has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity":
  - 3> perform URA update using the cause "periodic URA update".

When initiating the URA update or cell update procedure, the UE shall:

## 1&gt; stop timer T305;

## 1&gt; if the UE is in CELL\_DCH state:

- 2> in the variable RB\_TIMER\_INDICATOR, set the IE "T314 expired" and the IE "T315 expired" to FALSE;
- 2> if the stored values of the timer T314 and timer T315 are both equal to zero:
  - 3> release all its radio resources;
  - 3> 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;
  - 3> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 3> clear the variable ESTABLISHED\_RABS;
  - 3> enter idle mode;
  - 3> perform other actions when entering idle mode from connected mode as specified in subclause 8.5.2;
  - 3> and the procedure ends.

- 2> if the stored value of the timer T314 is equal to zero:
  - 3> release all radio bearers, associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT314";
  - 3> in the variable RB\_TIMER\_INDICATOR set the IE "T314 expired" to TRUE.
- 2> if the stored value of the timer T315 is equal to zero:
  - 3> release all radio bearers associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT315";
  - 3> in the variable RB\_TIMER\_INDICATOR set the IE "T315 expired" to TRUE.
- 2> if the stored value of the timer T314 is greater than zero:
  - 3> if there are radio bearers associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT314":
    - 4> start timer T314.
  - 3> if there are no radio bearers associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT314" or "useT315":
    - 4> start timer T314.
- 2> if the stored value of the timer T315 is greater than zero:
  - 3> if there are radio bearers associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT315":
    - 4> start timer T315.
- 2> for the released radio bearer(s):
  - 3> delete the information about the radio bearer from the variable ESTABLISHED\_RABS;
  - 3> when all radio bearers belonging to the same radio access bearer have been released:
    - 4> indicate local end release of the radio access bearer to upper layers using the CN domain identity together with the RAB identity stored in the variable ESTABLISHED\_RABS;
    - 4> delete all information about the radio access bearer from the variable ESTABLISHED\_RABS.
- 2> select a suitable UTRA cell according to [4];
- 2> set the variable ORDERED\_RECONFIGURATION to FALSE.
- 1> set the variables PROTOCOL\_ERROR\_INDICATOR, FAILURE\_INDICATOR, UNSUPPORTED\_CONFIGURATION and INVALID\_CONFIGURATION to FALSE;
- 1> set the variable CELL\_UPDATE\_STARTED to TRUE;
- 1> move to CELL\_FACH state, if not already in that state;
- 1> if the UE performs cell re-selection:
  - 2> clear the variable C\_RNTI; and
  - 2> stop using that C\_RNTI just cleared from the variable C\_RNTI in MAC.
- 1> set CFN in relation to SFN of current cell according to subclause 8.5.15;
- 1> in case of a cell update procedure:
  - 2> set the contents of the CELL UPDATE message according to subclause 8.3.1.3;
  - 2> submit the CELL UPDATE message for transmission on the uplink CCCH.

- 1> in case of a URA update procedure:
  - 2> set the contents of the URA UPDATE message according to subclause 8.3.1.3;
  - 2> submit the URA UPDATE message for transmission on the uplink CCCH.
- 1> set counter V302 to 1;
- 1> start timer T302 when the MAC layer indicates success or failure in transmitting the message.

### 8.3.1.3 CELL UPDATE / URA UPDATE message contents to set

In case of cell update procedure the UE shall transmit a CELL UPDATE message.

In case of URA update procedure the UE shall transmit a URA UPDATE message.

The UE shall set the IEs in the CELL UPDATE message as follows:

- 1> set the IE "Cell update cause" corresponding to the cause specified in subclause 8.3.1.2 that is valid when the CELL UPDATE message is submitted to lower layers for transmission;

NOTE: During the time period starting from when a cell update procedure is initiated by the UE until when the procedure ends, additional CELL UPDATE messages may be transmitted by the UE with different causes.

- 1> set the IE "U-RNTI" to the value of the variable U\_RNTI;
- 1> if the value of the variable PROTOCOL\_ERROR\_INDICATOR is TRUE:
  - 2> include the IE "RRC transaction identifier"; and
    - 3> set it to the value of "RRC transaction identifier" in the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 2> include and set the IE "failure cause" to the cause value "protocol error";
  - 2> set the IE "Protocol error information" set to the value of the variable PROTOCOL\_ERROR\_INFORMATION.
- 1> if the value of the variable FAILURE\_INDICATOR is TRUE:
  - 2> include the IE "RRC transaction identifier"; and
    - 3> set it to the value of "RRC transaction identifier" in the entry for the CELL UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS.
  - 2> include and set the IE "failure cause" to the value of the variable FAILURE\_CAUSE.
- 1> include the START values for each CN domain, calculated according to subclause 8.5.9;
- 1> if an unrecoverable error [16] in any of the AM RLC entities for the signalling radio bearers RB2, RB3 or RB4 is detected:
  - 2> set the IE "AM\_RLC error indication (RB2, RB3 or RB4)" to TRUE.
- 1> otherwise:
  - 2> set the IE "AM\_RLC error indication (RB2, RB3 or RB4)" to FALSE.
- 1> if an unrecoverable error [16] in any of the AM RLC entities for the RB5 or upward is detected:
  - 2> set the IE "AM\_RLC error indication (RB>4)" to TRUE.
- 1> otherwise:
  - 2> set the IE "AM\_RLC error indication (RB>4)" to FALSE.

- 1> set the IE "RB Timer indicator" to the value of the variable RB\_TIMER\_INDICATOR;
- 1> include an intra-frequency measurement report in the IE "Measured results on RACH", as specified in the IE "Intra-frequency reporting quantity for RACH reporting" and the IE "Maximum number of reported cells on RACH" in system information block type 12 (or System Information Block type 11, if System Information Block type 12 is not being broadcast); and
- 1> include in the IE "Measured results on RACH" all requested reporting quantities for all included measurement objects; and
- 1> take care that the maximum allowed message size is not exceeded when forming the IE "Measured results on RACH".

The UE shall set the IEs in the URA UPDATE message as follows:

- 1> set the IE "U-RNTI" to the value of the variable U\_RNTI;
- 1> set the IE "URA update cause" corresponding to which cause as specified in subclause 8.3.1.2 that is valid when the URA UPDATE message is submitted to lower layers for transmission;

NOTE: During the time period starting from when a URA update procedure is initiated by the UE until when the procedure ends, additional URA UPDATE messages may be transmitted by the UE with different causes, depending on which causes are valid for the respective URA UPDATE message.

- 2> if the value of the variable PROTOCOL\_ERROR\_INDICATOR is TRUE:
  - 3> include the IE "RRC transaction identifier"; and
    - 4> set it to the value of "RRC transaction identifier" in the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS;
  - 3> set the IE "Protocol error indicator" to TRUE;
  - 3> include the IE "Protocol error information" set to the value of the variable PROTOCOL\_ERROR\_INFORMATION.
- 2> if the value of the variable PROTOCOL\_ERROR\_INDICATOR is FALSE:
  - 3> if the value of the variable INVALID\_CONFIGURATION is TRUE:
    - 4> include the IE "RRC transaction identifier"; and
    - 4> set it to the value of "RRC transaction identifier" in the entry for the URA UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS;
    - 4> set the IE "Protocol error indicator" to TRUE;
    - 4> include the IE "Protocol error information" set to "Information element value not comprehended";
  - 3> if the value of the variable INVALID\_CONFIGURATION is FALSE:
    - 4> set the IE "Protocol error indicator" to FALSE.

#### 8.3.1.4 T305 expiry and the UE detects "out of service area"

When the T305 expires and the UE detects that it is "out of service area" as specified in subclause 8.5.5.1, the UE shall

- 1> start timer T307;
- 1> re-select to a new cell, as described in [4].

##### 8.3.1.4.1 Re-entering "in service area"

If the UE detects "in service area" according to subclause 8.5.5.2 and timer T307 or T317 is running, the UE shall:

- 1> check the value of V302; and

- 1> if V302 is equal to or smaller than N302:
  - 2> in case of a cell update procedure:
    - 3> set the contents of the CELL UPDATE message according to subclause 8.3.1.3;
    - 3> submit the CELL UPDATE message for transmission on the uplink CCCH.
  - 2> in case of a URA update procedure:
    - 3> set the contents of the URA UPDATE message according to subclause 8.3.1.3;
    - 3> submit the URA UPDATE message for transmission on the uplink CCCH.
  - 2> increment counter V302;
  - 2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.
- 1> if V302 is greater than N302:
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
  - 2> in case of a cell update procedure:
    - 3> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 2> in case of a URA update procedure:
    - 3> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 2> release all its radio resources;
  - 2> 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;
  - 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 2> clear the variable ESTABLISHED\_RABS;
  - 2> enter idle mode;
  - 2> perform other actions when entering idle mode from connected mode as specified in subclause 8.5.2;
  - 2> and the procedure ends.

#### 8.3.1.4.2 Expiry of timer T307

When the T307 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 other actions when entering idle mode from connected mode as specified in subclause 8.5.2;

1> and the procedure ends.

### 8.3.1.5 Reception of an CELL UPDATE/URA UPDATE message by the UTRAN

When the UTRAN receives a CELL UPDATE/URA UPDATE message, the UTRAN should:

- 1> in case the procedure was triggered by reception of a CELL UPDATE:
  - 2> if SRNS relocation was performed:
    - 3> transmit a CELL UPDATE CONFIRM message on the downlink DCCH.
  - 2> otherwise:
    - 3> update the START value for each CN domain as maintained in UTRAN (refer to subclause 8.5.9) with "START" in the IE "START list" for the CN domain as indicated by "CN domain identity" in the IE "START list";
    - 3> if this procedure was triggered while the UE was not in CELL\_DCH state, then for each CN domain as indicated by "CN domain identity" in the IE "START list":
      - 4> set the 20 MSB of the MAC-d HFN with the corresponding START value in the IE "START list";
      - 4> set the remaining LSB of the MAC-d HFN to zero.
    - 3> transmit a CELL UPDATE CONFIRM message on the downlink DCCH or optionally on the CCCH but only if ciphering is not required; and
    - 3> optionally include the IE "RLC re-establish indicator (RB5 and upwards)" to request a RLC re-establishment in the UE, in which case the corresponding RLC entities should also be re-established in UTRAN; or
- 1> in case the procedure was triggered by reception of a URA UPDATE:
  - 2> if SRNS relocation was performed:
    - 3> transmit a URA UPDATE CONFIRM message on the downlink DCCH.
  - 2> otherwise:
    - 3> transmit a URA UPDATE CONFIRM message on the downlink CCCH or DCCH.
  - 2> include the IE "URA identity" in the URA UPDATE CONFIRM message in a cell where multiple URA identifiers are broadcast; or
- 1> initiate an RRC connection release procedure (see subclause 8.1.4) by transmitting an RRC CONNECTION RELEASE message on the downlink CCCH. In particular UTRAN should:
  - 2> if the CELL UPDATE message was sent because of an unrecoverable error in RB2, RB3 or RB4:
    - 3> initiate an RRC connection release procedure (subclause 8.1.4) by transmitting an RRC CONNECTION RELEASE message on the downlink CCCH.

### 8.3.1.6 Reception of the CELL UPDATE CONFIRM/URA UPDATE CONFIRM message by the UE

When the UE receives a CELL UPDATE CONFIRM/URA UPDATE CONFIRM message; and

- if the message is received on the CCCH, and IE "U-RNTI" is present and has the same value as the variable U\_RNTI; or
- if the message is received on DCCH:

the UE shall:

- 1> stop timer T302;

- 1> in case of a cell update procedure and the CELL UPDATE CONFIRM message:
  - 2> includes "RB information elements"; and/or
  - 2> includes "Transport channel information elements"; and/or
  - 2> includes "Physical channel information elements"; and
  - 2> if the variable ORDERED\_RECONFIGURATION is set to FALSE:
    - 3> set the variable ORDERED\_RECONFIGURATION to TRUE.
- 1> act upon all received information elements as specified in subclause 8.6, unless specified otherwise in the following:
  - 2> if the IE "Frequency info" is included in the message:
    - 3> if the IE "RRC State Indicator" is set to the value "CELL\_FACH" or "CELL\_PCH" or "URA\_PCH":
      - 4> select a suitable UTRA cell according to [4] on that frequency;
      - 4> act as specified in subclause 8.3.1.12.
    - 3> if the IE "RRC State Indicator" is set to the value "CELL\_DCH":
      - 4> act on the IE "Frequency info" as specified in subclause 8.6.6.1.
  - 2> use the transport channel(s) applicable for the physical channel types that is used; and
  - 2> if the IE "TFS" is neither included nor previously stored in the UE for that transport channel(s):
    - 3> use the TFS given in system information.
  - 2> if none of the TFS stored is compatible with the physical channel:
    - 3> delete the stored TFS;
    - 3> use the TFS given in system information.
  - 2> perform the physical layer synchronisation procedure as specified in [29];
  - 2> if the CELL UPDATE CONFIRM message includes the IE "RLC re-establish indicator (RB2, RB3 and RB4)":
    - 3> re-establish the RLC entities for signalling radio bearer RB2, signalling radio bearer RB3 and signalling radio bearer RB4 (if established);
    - 3> if the value of the IE "Status" in the variable CIPHERING\_STATUS of the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN is set to "Started":
      - 4> set the HFN values for AM RLC entities with RB identity 2, RB identity 3 and RB identity 4 (if established) equal to the START value included in the latest transmitted CELL UPDATE message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN.
  - 2> if the CELL UPDATE CONFIRM message includes the IE "RLC re-establish indicator (RB5 and upwards)":
    - 3> for radio bearers with RB identity 5 and upwards:
      - 4> re-establish the AM RLC entities;
      - 4> if the value of the IE "Status" in the variable CIPHERING\_STATUS of the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS is set to "Started":
        - 5> set the HFN values for AM RLC entities equal to the START value included in this CELL UPDATE message for the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS.



- 1> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected".
- 1> enter a state according to subclause 8.6.3.3 applied on the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message.

If the UE after state transition enters CELL\_DCH state, it shall:

- 1> not prohibit periodical status transmission in RLC;
- 1> for each CN domain for which a transparent mode radio bearer exists and for which the IE "Status" in the variable CIPHERING\_STATUS is set to "Started" for that CN domain:
  - 2> choose an activation time for the ciphering on transparent mode radio bearers and include it in the response message in the IE "COUNT-C activation time";
  - 2> set the 20 MSB of the MAC-d HFN with the corresponding START value in the most recently sent IE "START list";
  - 2> set the remaining LSB of the MAC-d HFN to zero;
  - 2> apply ciphering on the transparent mode radio bearers;
  - 2> start incrementing the COUNT-C value from the CFN that has been included in the IE "COUNT-C activation time".

If the UE after state transition remains in CELL\_FACH state, it shall

- 1> start the timer T305 using its initial value if timer T305 is not running and periodical cell update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity";
- 1> select PRACH according to subclause 8.5.17;
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> not prohibit periodical status transmission in RLC;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 2> ignore that IE and stop using DRX.

If the UE after state transition enters URA\_PCH or CELL\_PCH state, it shall:

- 1> prohibit periodical status transmission in RLC;
- 1> clear the variable C\_RNTI;
- 1> stop using that C\_RNTI just cleared from the variable C\_RNTI in MAC;
- 1> start the timer T305 using its initial value if timer T305 is not running 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";
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 2> use the value in the IE "UTRAN DRX Cycle length coefficient" for calculating Paging Occasion and PICH Monitoring Occasion as specified in subclause 8.6.3.2 in CELL\_PCH state.
- 1> if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.

If the UE after the state transition remains in CELL\_FACH state; and

1> the contents of the variable C\_RNTI are empty:

it shall check the value of V302; and:

1> if V302 is equal to or smaller than N302:

2> if, caused by the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:

3> the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE; and/or

3> the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE:

4> abort the ongoing integrity and/or ciphering reconfiguration;

4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":

5> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and

5> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.

4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":

5> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and

5> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.

2> in case of a URA update procedure:

3> stop the URA update procedure; and

3> continue with a cell update procedure.

2> set the contents of the CELL UPDATE message according to subclause 8.3.1.3, except for the IE "Cell update cause" which shall be set to "cell reselection";

2> submit the CELL UPDATE message for transmission on the uplink CCCH;

2> increment counter V302;

2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.

1> if V302 is greater than N302:

2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;

2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;

2> in case of a cell update procedure:

3> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.

2> in case of a URA update procedure:

3> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.

2> release all its radio resources;

2> 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;

2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;

2> clear the variable ESTABLISHED\_RABS;

2> enter idle mode;

2> other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;

2> and the procedure ends.

If the UE after the state transition remains in CELL\_FACH state; and

- a C-RNTI is stored in the variable C\_RNTI;

or

- the UE after the state transition moves to another state than the CELL\_FACH state:

the UE shall:

1> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info":

2> include and set the IE "Radio bearer uplink ciphering activation time info" in any response message transmitted below to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.

1> in case of a cell update procedure:

2> set the IE "RRC transaction identifier" in any response message transmitted below to the value of "RRC transaction identifier" in the entry for the CELL UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS; and

2> clear that entry.

1> in case of a URA update procedure:

2> set the IE "RRC transaction identifier" in any response message transmitted below to the value of "RRC transaction identifier" in the entry for the URA UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS; and

2> clear that entry;

1> if the variable PDCP\_SN\_INFO is non-empty:

2> include the IE "RB with PDCP information list" in any response message transmitted below and set it to the value of the variable PDCP\_SN\_INFO.

1> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message included the IE "Downlink counter synchronisation info":

2> re-establish RB2;

2> set the new uplink and downlink HFN of RB2 to MAX(uplink HFN of RB2, downlink HFN of RB2);

2> increment by one the downlink and uplink HFN values for RB2;

2> calculate the START value according to subclause 8.5.9;

2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in any response message transmitted below.

1> transmit a response message as specified in subclause 8.3.1.7;

1> if the IE "Integrity protection mode info" was present in the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:

2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.

1> if the variable ORDERED\_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:

- 2> set the variable ORDERED\_RECONFIGURATION to FALSE.
- 1> clear the variable PDCP\_SN\_INFO;
- 1> when the response message transmitted per subclause 8.3.1.7 to the UTRAN has been confirmed by RLC:
  - 2> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
    - 3> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
    - 3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
    - 3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
  - 2> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
    - 3> set "Uplink RRC Message sequence number" for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO to a value such that next RRC message to be sent on uplink RB0 will use the new integrity protection configuration;
    - 3> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
    - 3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE.
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 1> in case of a cell update procedure:
  - 2> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- 1> in case of a URA update procedure:
  - 2> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- 1> set the variable CELL\_UPDATE\_STARTED to FALSE;
- 1> clear the variable SECURITY\_MODIFICATION.

The procedure ends.

### 8.3.1.7 Transmission of a response message to UTRAN

If the CELL UPDATE CONFIRM message:

- includes the IE "RB information to release list":

the UE shall:

- 1> transmit a RADIO BEARER RELEASE COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include the IE "RB information to release list"; and
- includes the IE "RB information to reconfigure list"; or
- includes the IE "RB information to be affected list":

the UE shall:

- 1> transmit a RADIO BEARER RECONFIGURATION COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- includes "Transport channel information elements":

the UE shall:

- 1> transmit a TRANSPORT CHANNEL RECONFIGURATION COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- does not include "Transport channel information elements"; and
- includes "Physical channel information elements":

the UE shall:

- 1> transmit a PHYSICAL CHANNEL RECONFIGURATION COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- does not include "Transport channel information elements"; and
- does not include "Physical channel information elements"; and
- includes "CN information elements"; or
- includes the IE "Ciphering mode info"; or
- includes the IE "Integrity protection mode info"; or
- includes the IE "New C-RNTI"; or
- includes the IE "New U-RNTI":

the UE shall:

- 1> transmit a UTRAN MOBILITY INFORMATION CONFIRM as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- does not include "Transport channel information elements"; and
- does not include "Physical channel information elements"; and
- does not include "CN information elements"; and
- does not include the IE "Ciphering mode info"; and
- does not include the IE "Integrity protection mode info"; and
- does not include the IE "New C-RNTI"; and
- does not include the IE "New U-RNTI":

the UE shall:

- 1> transmit no response message.

If the URA UPDATE CONFIRM message:

- includes "CN information elements"; or
- includes the IE "Ciphering mode info"; or
- includes the IE "Integrity protection mode info"; or
- includes any one or both of the IEs "New C-RNTI" and "New U-RNTI":

the UE shall:

- 1> transmit a UTRAN MOBILITY INFORMATION CONFIRM as response message using AM RLC.

If the URA UPDATE CONFIRM message:

- does not include "CN information elements"; and
- does not include the IE "Ciphering mode info"; and
- does not include the IE "Integrity protection mode info"; and
- does not include the IE "New U-RNTI"; and
- does not include the IE "New C-RNTI":

the UE shall:

- 1> transmit no response message.

If the new state is CELL\_DCH or CELL\_FACH, the response message shall be transmitted using the new configuration after the state transition., and the UE shall:

- 1> if the IE "Downlink counter synchronisation info" was included in the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:
  - 2> when RLC has confirmed the successful transmission of the response message:
    - 3> re-establish all AM and UM RLC entities with RB identities larger than 4 and set the first 20 bits of all their HFN values to the START value included in the response message for the corresponding CN domain;
    - 3> re-establish the RLC entities with RB identities 1, 3 and 4 and set the first 20 bits of all their HFN values to the START value included in the response message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 3> set the remaining bits of the HFN values of all UM RLC entities to zero;
    - 3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].

- 1> if the variable PDCP\_SN\_INFO is empty:

- 2> if the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
  - 3> when RLC has confirmed the successful transmission of the response message:
    - 4> continue with the remainder of the procedure.
- 2> if the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message did not contain the IE "Ciphering mode info":
  - 3> when RLC has been requested to transmit the response message,
    - 4> continue with the remainder of the procedure.

- 1> if the variable PDCP\_SN\_INFO non-empty:

- 2> when RLC has confirmed the successful transmission of the response message:
  - 3> for each radio bearer in the variable PDCP\_SN\_INFO:
    - 4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
      - 5> configure the RLC entity for that radio bearer to "continue".
  - 3> continue with the remainder of the procedure.

If the new state is CELL\_PCH or URA\_PCH, the response message shall be transmitted in CELL\_FACH state, and the UE shall:

- 1> when RLC has confirmed the successful transmission of the response message:
  - 2> for each radio bearer in the variable PDCP\_SN\_INFO:
    - 3> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
      - 4> configure the RLC entity for that radio bearer to "continue".
  - 2> enter the new state (CELL\_PCH or URA\_PCH, respectively).
- 1> continue with the remainder of the procedure.

#### 8.3.1.7a Physical channel failure

If the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message would cause the UE to transit to CELL\_DCH state; and

- 1> in case of a received CELL UPDATE CONFIRM message:
  - 2> if the UE failed to establish the physical channel(s) indicated in the received CELL UPDATE CONFIRM message according to the criteria defined in subclause 8.5.4 are not fulfilled; or
  - 2> the received CELL UPDATE CONFIRM message does not contain dedicated physical channels;
- 1> in case of the UE received a URA UPDATE CONFIRM message:

the UE shall:

- 1> if, caused by the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message
  - 2> the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE; and/or
  - 2> the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE:
    - 3> abort the ongoing integrity and/or ciphering reconfiguration;
    - 3> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
      - 4> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
      - 4> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
    - 3> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
      - 4> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
      - 4> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 1> if the variable ORDERED\_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:
  - 2> set the variable ORDERED\_RECONFIGURATION to FALSE.

- 1> if V302 is equal to or smaller than N302:
  - 2> in case of a URA update procedure:
    - stop the URA update procedure; and
    - 3> continue with a cell update procedure.
  - 2> select a suitable UTRA cell according to [4];
  - 2> set the contents of the CELL UPDATE message according to subclause 8.3.1.3, except for the IE "Cell update cause" which shall be set to "Radio link failure";
  - 2> submit the CELL UPDATE message for transmission on the uplink CCCH;
  - 2> increment counter V302;
  - 2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.
- 1> if V302 is greater than N302:
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
  - 2> in case of a cell update procedure:
    - 3> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 2> in case of a URA update procedure:
    - 3> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 2> release all its radio resources;
  - 2> 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;
  - 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 2> clear the variable ESTABLISHED\_RABS;
  - 2> set the variable CELL\_UPDATE\_STARTED to FALSE;
  - 2> enter idle mode.

### 8.3.1.8 Unsupported configuration by the UE

If the UE does not support the configuration in the CELL UPDATE CONFIRM message and/or the variable UNSUPPORTED\_CONFIGURATION is set to TRUE, the UE shall:

- 1> if V302 is equal to or smaller than N302, the UE shall:
  - 2> if, caused by the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message
    - 3> the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE; and/or
    - 3> the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE:
      - 4> abort the ongoing integrity and/or ciphering reconfiguration;
    - 4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":



- 5> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
- 5> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
  - 5> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
  - 5> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 2> if the variable ORDERED\_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:
  - 3> set the variable ORDERED\_RECONFIGURATION to FALSE.
  - 2> set the variable FAILURE\_INDICATOR to TRUE;
  - 2> set the variable FAILURE\_CAUSE to "Unsupported configuration";
  - 2> set the content of the CELL UPDATE message according to subclause 8.3.1.3;
  - 2> submit the CELL UPDATE message for transmission on the uplink CCCH;
  - 2> increment counter V302;
  - 2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.
- 1> if V302 is greater than N302, the UE shall:
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
  - 2> clear the variable PDCP\_SN\_INFO;
  - 2> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS;
  - 2> release all its radio resources;
  - 2> 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;
  - 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 2> clear the variable ESTABLISHED\_RABS;
  - 2> set the variable CELL\_UPDATE\_STARTED to FALSE;
  - 2> enter idle mode;
  - 2> Other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
  - 2> and the procedure ends.

### 8.3.1.9 Invalid configuration

If the variable INVALID\_CONFIGURATION is set to TRUE, the UE shall:

- 1> if V302 is equal to or smaller than N302:
  - 2> if, caused by the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message
  - 3> the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE; and/or

- 3> the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE:
  - 4> abort the ongoing integrity and/or ciphering reconfiguration;
  - 4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
    - 5> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
    - 5> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
  - 4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info";
    - 5> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
    - 5> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 3> if the variable ORDERED\_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:
  - 4> set the variable ORDERED\_RECONFIGURATION to FALSE.
- 2> in case of a cell update procedure:
  - 3> set the variable FAILURE\_INDICATOR to TRUE;
  - 3> set the variable FAILURE\_CAUSE to "Invalid configuration";
  - 3> set the contents of the CELL UPDATE message according to subclause 8.3.1.3;
  - 3> submit the CELL UPDATE message for transmission on the uplink CCCH.
- 2> in case of a URA update procedure:
  - 3> set the contents of the URA UPDATE message according to subclause 8.3.1.3;
  - 3> submit the URA UPDATE message for transmission on the uplink CCCH.
- 2> increment counter V302;
- 2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.
- 1> if V302 is greater than N302:
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
  - 2> clear the variable PDCP\_SN\_INFO;
  - 2> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS;
  - 2> release all its radio resources;
  - 2> 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;
  - 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 2> clear the variable ESTABLISHED\_RABS;
  - 2> set the variable CELL\_UPDATE\_STARTED to FALSE;
  - 2> enter idle mode;

- 2> Other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
- 2> the procedure ends.

### 8.3.1.9a Incompatible simultaneous reconfiguration

In case of a cell update procedure and if the received CELL UPDATE CONFIRM message

- includes "RB information elements"; and/or
- includes "Transport channel information elements"; and/or
- includes "Physical channel information elements"; and
- the variable ORDERED\_RECONFIGURATION is set to TRUE because of an ongoing Reconfiguration procedure;

and/or

- if the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION becomes set to TRUE of the received CELL UPDATE CONFIRM message:

the UE shall:

- 1> if V302 is equal to or smaller than N302:
  - 2> if, caused by the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message
    - 3> the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE; and/or
    - 3> the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE:
      - 4> abort the ongoing integrity and/or ciphering reconfiguration;
      - 4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
        - 5> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
        - 5> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
      - 4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
        - 5> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
        - 5> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
    - 3> if the variable ORDERED\_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:
      - 4> set the variable ORDERED\_RECONFIGURATION to FALSE.
  - 2> set the variable FAILURE\_INDICATOR to TRUE;
  - 2> set the variable FAILURE\_CAUSE to "Incompatible simultaneous reconfiguration";
  - 2> set the content of the CELL UPDATE message according to subclause 8.3.1.3;
  - 2> submit the CELL UPDATE message for transmission on the uplink CCCH;
  - 2> increment counter V302;
  - 2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.
- 1> if V302 is greater than N302:

- 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
- 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
- 2> clear the variable PDCP\_SN\_INFO;
- 2> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to FALSE;
- 2> clear the entry for the CELL\_UPDATE\_CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS;
- 2> release all its radio resources;
- 2> 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;
- 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 2> clear the variable ESTABLISHED\_RABS;
- 2> set the variable CELL\_UPDATE\_STARTED to FALSE;
- 2> enter idle mode;
- 2> Other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
- 2> the procedure ends.

#### 8.3.1.10 Confirmation error of URA ID list

If the URA\_UPDATE\_CONFIRM message causes a confirmation error of URA identity list as specified in subclause 8.6.2.1 the UE shall:

- 1> check the value of V302; and
- 1> if V302 is smaller or equal than N302:
  - 2> if, caused by the received URA\_UPDATE\_CONFIRM message
    - 3> the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE; and/or
    - 3> the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE:
      - 4> abort the ongoing integrity and/or ciphering reconfiguration;
      - 4> if the received URA\_UPDATE\_CONFIRM message contained the IE "Ciphering mode info":
        - 5> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
        - 5> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
      - 4> if the received URA\_UPDATE\_CONFIRM message contained the IE "Integrity protection mode info"
        - 5> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
        - 5> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
  - 2> set the IEs in the URA\_UPDATE message according to subclause 8.3.1.3;
  - 2> submit the URA\_UPDATE message for transmission on the uplink CCCH;
  - 2> increment counter V302;
  - 2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.
- 1> if V302 is greater than N302:

- 2> release all its radio resources;
- 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
- 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
- 2> clear the variable PDCP\_SN\_INFO;
- 2> 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;
- 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 2> clear the variable ESTABLISHED\_RABS;
- 2> set the variable CELL\_UPDATE\_STARTED to FALSE;
- 2> enter idle mode;
- 2> perform the actions specified in subclause 8.5.2 when entering idle mode from connected mode;
- 2> the procedure ends.

#### 8.3.1.11 Invalid CELL UPDATE CONFIRM/URA UPDATE CONFIRM message

If the UE receives an CELL UPDATE CONFIRM/URA UPDATE CONFIRM message, which contains a protocol error causing the variable PROTOCOL\_ERROR\_REJECT to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows:

- 1> If V302 is equal to or smaller than N302, the UE shall:
  - 2> set the variable PROTOCOL\_ERROR\_INDICATOR to TRUE;
  - 2> in case of a cell update procedure:
    - 3> set the contents of the CELL UPDATE message according to subclause 8.3.1.3;
    - 3> submit the CELL UPDATE message for transmission on the uplink CCCH.
  - 2> in case of a URA update procedure:
    - 3> set the contents of the URA UPDATE message according to subclause 8.3.1.3;
    - 3> submit the URA UPDATE message for transmission on the uplink CCCH.
  - 2> increment counter V302;
  - 2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.
- 1> if V302 is greater than N302, the UE shall:
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> in case of a cell update procedure:
    - 3> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 2> in case of a URA update procedure:
    - 3> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 2> 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;

- 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 2> clear the variable ESTABLISHED\_RABS;
- 2> set the variable CELL\_UPDATE\_STARTED to FALSE;
- 2> release all its radio resources;
- 2> enter idle mode;
- 2> Other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
- 2> the procedure ends.

### 8.3.1.12 T302 expiry or cell reselection

If any or several of the following conditions are true:

- expiry of timer T302;
- reselection to another UTRA cell (including the previously serving cell) before completion of the cell update or URA update procedure;

the UE shall:

- 1> stop T302 if it is running;
- 1> if the UE was in CELL\_DCH state prior to the initiation of the procedure; and
  - 2> if timers T314 and T315 have elapsed while T302 was running:
    - 3> enter idle mode.
    - 3> 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. Other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2.
    - 3> and the procedure ends.
  - 2> if timer T314 has elapsed while T302 was running and,
    - 3> if "T314 expired" in the variable RB\_TIMER\_INDICATOR is set to FALSE and
    - 3> if T315 is still running:
      - 4> release locally all radio bearers which are associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT314";
      - 4> indicate release of those radio access bearers to upper layers;
      - 4> delete all information about those radio access bearers from the variable ESTABLISHED\_RABS;
      - 4> set "T314 expired" in the variable RB\_TIMER\_INDICATOR to TRUE.
  - 2> if timer T315 has elapsed while T302 was running and,
    - 3> if "T315 expired" in the variable RB\_TIMER\_INDICATOR is set to FALSE and,
    - 3> if T314 is still running:
      - 4> release locally all radio bearers which are associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT315";
      - 4> indicate release of those radio access bearers to upper layers;

- 4> delete all information about those radio access bearers from the variable ESTABLISHED\_RABS;
  - 4> set "T315 expired" in the variable RB\_TIMER\_INDICATOR to TRUE.
- 1> check whether it is still in "in service area" (see subclause 8.5.5.2);
  - 1> if, caused by the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE:
    - 2> abort the ongoing integrity and/or ciphering reconfiguration;
    - 2> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
      - 3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
      - 3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
    - 2> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
      - 3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
      - 3> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
  - 1> if the variable ORDERED\_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:
    - 2> set the variable ORDERED\_RECONFIGURATION to FALSE.
  - 1> in case of a cell update procedure:
    - 2> clear any entry for the CELL UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS.
  - 1> in case of a URA update procedure:
    - 2> clear any entry for the URA UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS.

If the UE detects "in service area" if it has not entered idle mode, and:

- 1> if V302 is equal to or smaller than N302, the UE shall:
  - 2> if the UE performed cell re-selection:
    - 3> delete its C-RNTI
    - 3> set the contents of the CELL UPDATE message according to subclause 8.3.1.3;
    - 3> submit the CELL UPDATE message for transmission on the uplink CCCH.
  - 2> in case of a URA update procedure:
    - 3> set the contents of the URA UPDATE message according to subclause 8.3.1.3;
    - 3> submit the URA UPDATE message for transmission on the uplink CCCH.
  - 2> increment counter V302;
  - 2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.
- 1> if V302 is greater than N302, the UE shall:
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;

- 2> clear the variable PDCP\_SN\_INFO;
- 2> in case of a cell update procedure:
  - 3> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- 2> in case of a URA update procedure:
  - 3> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- 2> release all its radio resources;
- 2> 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;
- 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 2> clear the variable ESTABLISHED\_RABS;
- 2> set the variable CELL\_UPDATE\_STARTED to FALSE;
- 2> enter idle mode;
- 2> other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
- 2> and the procedure ends.

If the UE does not detect "in service area", it shall:

- 1> continue searching for "in service area".

### 8.3.1.13 T314 expiry

Upon expiry of timer T314 the UE shall:

- 1> if timer T302 is running:
  - 2> continue awaiting response message from UTRAN.
- 1> if timer T302 is not running and timer T315 is running:
  - 2> set IE "T314 expired" in variable RB\_TIMER\_INDICATOR to TRUE;
  - 2> release locally all radio bearers which are associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT314";
  - 2> indicate release of those radio access bearers to upper layers;
  - 2> delete all information about those radio access bearers from the variable ESTABLISHED\_RABS.
- 1> if timers T302 and T315 are not running:
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
  - 2> clear the variable PDCP\_SN\_INFO;
  - 2> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS;
  - 2> release all its radio resources;



- 2> 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;
- 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 2> clear the variable ESTABLISHED\_RABS;
- 2> set the variable CELL\_UPDATE\_STARTED to FALSE;
- 2> enter idle mode;
- 2> other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
- 2> and the procedure ends.

#### 8.3.1.14 T315 expiry

Upon expiry of timer T315 the UE shall:

- 1> if timer T302 is running:
  - 2> continue awaiting response message from UTRAN.
- 1> if timer T302 is not running and timer T314 is running:
  - 2> set IE "T315 expired" in variable RB\_TIMER\_INDICATOR to TRUE;
  - 2> release locally all radio bearers which are associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "use T315";
  - 2> indicate release of those radio access bearers to upper layers;
  - 2> delete all information about those radio access bearers from the variable ESTABLISHED\_RABS.
- 1> if timers T302 and T314 are not running:
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
  - 2> clear the variable PDCP\_SN\_INFO;
  - 2> clear the entry for the CELL\_UPDATE\_CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS;
  - 2> release all its radio resources;
  - 2> 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;
  - 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 2> clear the variable ESTABLISHED\_RABS;
  - 2> set the variable CELL\_UPDATE\_STARTED to FALSE;
  - 2> enter idle mode;
  - 2> other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
  - 2> and the procedure ends.

### 8.3.1.15 Reception of the UTRAN MOBILITY INFORMATION CONFIRM message by the UTRAN

See subclause 8.3.3.4.

## 8.3.2 URA update

See subclause 8.3.1.

## 8.3.3 UTRAN mobility information

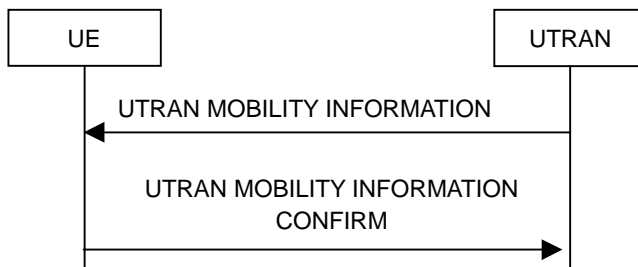


Figure 8.3.3-1: UTRAN mobility information procedure, normal flow

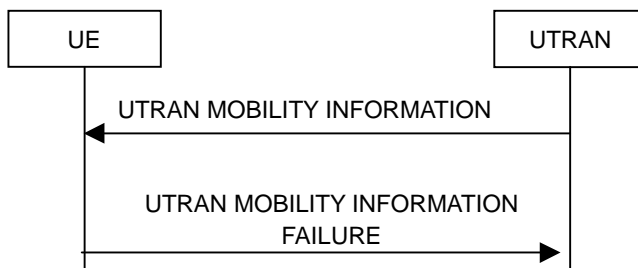


Figure 8.3.3-2: UTRAN mobility information procedure, failure case

### 8.3.3.1 General

The purpose of this procedure is to allocate any one or a combination of the following to a UE in connected mode:

- a new C-RNTI;
- a new U-RNTI;
- other mobility related information.

### 8.3.3.2 Initiation

To initiate the procedure UTRAN transmits a UTRAN MOBILITY INFORMATION message to the UE on the downlink DCCH using AM or UM RLC. In case of SRNS relocation, the message is sent using UM RLC only.

### 8.3.3.3 Reception of UTRAN MOBILITY INFORMATION message by the UE

When the UE receives a UTRAN MOBILITY INFORMATION message, it shall:

- 1> act on received information elements as specified in subclause 8.6;
- 1> if the IE "UE Timers and constants in connected mode" is present:
  - 2> store the values of the IE "UE Timers and constants in connected mode" in the variable TIMERS\_AND\_CONSTANTS, replacing any previously stored value for each timer and constant; and

- 2> for each updated timer value:
  - 3> start using the new value next time the timer is started;
- 2> for each updated constant value:
  - 3> start using the new value directly;
- 1> if the IE "CN domain specific DRX cycle length coefficient" is present:
  - 2> store the value of the IE "CN domain specific DRX cycle length coefficient" for that CN domain, replacing any previously stored value; and
  - 2> use the value to determine the connected mode paging occasions according to [4].
- 1> set the IE "RRC transaction identifier" in the UTRAN MOBILITY INFORMATION CONFIRM message to the value of "RRC transaction identifier" in the entry for the UTRAN MOBILITY INFORMATION message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected";
- 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
  - 2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the variable PDCP\_SN\_INFO is non-empty:
  - 2> include the IE "RB with PDCP information list" in the UTRAN MOBILITY INFORMATION CONFIRM message and set it to the value of the variable PDCP\_SN\_INFO.
- 1> if the received UTRAN MOBILITY INFORMATION message included the IE "Downlink counter synchronisation info":
  - 2> re-establish RB2;
  - 2> set the new uplink and downlink HFN of RB2 to MAX(uplink HFN of RB2, downlink HFN of RB2);
  - 2> increment by one the downlink and uplink HFN values for RB2;
  - 2> calculate the START value according to subclause 8.5.9;
  - 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the UTRAN MOBILITY INFORMATION CONFIRM message.
- 1> transmit a UTRAN MOBILITY INFORMATION CONFIRM message on the uplink DCCH using AM RLC;
- 1> if the IE "Integrity protection mode info" was present in the UTRAN MOBILITY INFORMATION message:
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted UTRAN MOBILITY INFORMATION CONFIRM message.
- 1> if the IE "Downlink counter synchronisation info" was included in the received UTRAN MOBILITY INFORMATION message:
  - 2> when RLC has confirmed the successful transmission of the response message:
    - 3> re-establish all AM and UM RLC entities with RB identities larger than 4 and set the first 20 bits of all their HFN values to the START value included in the response message for the corresponding CN domain;

- 3> re-establish the RLC entities with RB identities 1, 3 and 4 and set the first 20 bits of all their HFN values to the START value included in the response message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
  - 3> set the remaining bits of the HFN values of all UM RLC entities to zero;
  - 3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].
- 1> if the variable PDCP\_SN\_INFO is empty; and
- 2> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
    - 3> when RLC has confirmed the successful transmission of the UTRAN MOBILITY INFORMATION CONFIRM message, perform the actions below.
  - 2> if the UTRAN MOBILITY INFORMATION message did not contain the IE "Ciphering mode info":
    - 3> when RLC has been requested to transmit the UTRAN MOBILITY INFORMATION CONFIRM message, perform the actions below.
- 1> if the variable PDCP\_SN\_INFO is non-empty:
- 2> when RLC has confirmed the successful transmission of the UTRAN MOBILITY INFORMATION CONFIRM message:
    - 3> for each radio bearer in the variable PDCP\_SN\_INFO:
      - 4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
        - 5> configure the RLC entity for that radio bearer to "continue".
    - 3> clear the variable PDCP\_SN\_INFO.
- 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
- 2> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
  - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Integrity protection mode info":
- 2> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
  - 2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 1> clear the variable SECURITY\_MODIFICATION.

The procedure ends.

#### 8.3.3.4 Reception of an UTRAN MOBILITY INFORMATION CONFIRM message by the UTRAN

When the network receives UTRAN MOBILITY INFORMATION CONFIRM message, UTRAN may delete any old U-RNTI. The procedure ends.

#### 8.3.3.5 Cell re-selection

If the UE performs cell re-selection, the UE shall:

- 1> initiate a cell update procedure according to subclause 8.3.1;

- 1> if the UTRAN MOBILITY INFORMATION message contains the IE "New C-RNTI"; and
- 1> if the UE has not yet submitted the UTRAN MOBILITY INFORMATION CONFIRM message to lower layers for transmission;
  - 2> transmit a UTRAN MOBILITY INFORMATION FAILURE message on the uplink DCCH using AM RLC;
  - 2> set the IE "RRC transaction identifier" in the UTRAN MOBILITY INFORMATION FAILURE message to the value of "RRC transaction identifier" in the entry for the UTRAN MOBILITY INFORMATION message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry.
  - 2> set the IE "failure cause" to the cause value "cell update occurred";
  - 2> when the UTRAN MOBILITY INFORMATION FAILURE message has been submitted to lower layers for transmission:
    - 3> continue with any ongoing processes and procedures as if the invalid UTRAN MOBILITY INFORMATION message has not been received and the procedure ends.
- 1> otherwise:
  - 2> continue the procedure normally.

### 8.3.3.5a Incompatible simultaneous security reconfiguration

If the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION becomes set to TRUE of the received UTRAN MOBILITY INFORMATION message, the UE shall:

- 1> transmit a UTRAN MOBILITY INFORMATION FAILURE message on the uplink DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the UTRAN MOBILITY INFORMATION FAILURE message to the value of "RRC transaction identifier" in the entry for the UTRAN MOBILITY INFORMATION message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";
- 1> when the UTRAN MOBILITY INFORMATION FAILURE message has been delivered to lower layers for transmission:
  - 2> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to FALSE;
  - 2> continue with any ongoing processes and procedures as if the UTRAN MOBILITY INFORMATION message has not been received;
  - 2> and the procedure ends.

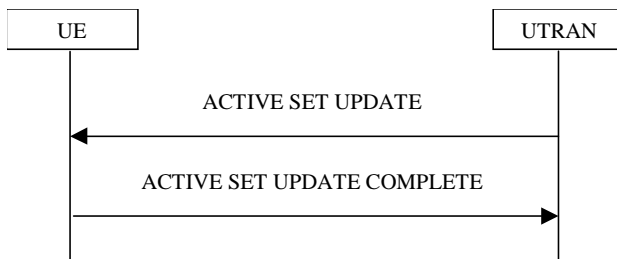
### 8.3.3.6 Invalid UTRAN MOBILITY INFORMATION message

If the UTRAN MOBILITY INFORMATION message contains a protocol error causing the variable PROTOCOL\_ERROR\_REJECT to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows. The UE shall:

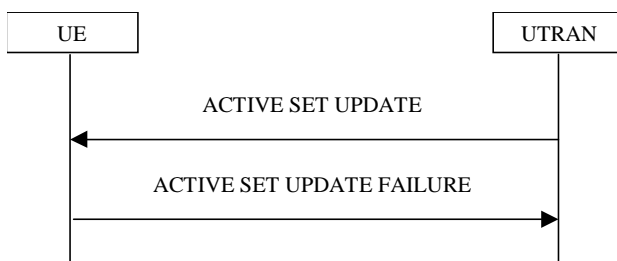
- 1> transmit a UTRAN MOBILITY INFORMATION FAILURE message on the uplink DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the UTRAN MOBILITY INFORMATION FAILURE message to the value of "RRC transaction identifier" in the entry for the UTRAN MOBILITY INFORMATION message in the table "Rejected transactions" in the variable TRANSACTIONS, and;
- 1> clear that entry.
- 1> set the IE "failure cause" to the cause value "protocol error";

- 1> include the IE "Protocol error information" with contents set to the value of the variable `PROTOCOL_ERROR_INFORMATION`;
- 1> when the UTRAN MOBILITY INFORMATION FAILURE message has been submitted to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the invalid UTRAN MOBILITY INFORMATION message has not been received;
  - 2> and the procedure ends.

### 8.3.4 Active set update



**Figure 8.3.4-1: Active Set Update procedure, successful case**



**Figure 8.3.4-2: Active Set Update procedure, failure case**

#### 8.3.4.1 General

The purpose of the active set update procedure is to update the active set of the connection between the UE and UTRAN. This procedure shall be used in CELL\_DCH state. The UE should keep on using the old RLs while configuring the new RLs. Also the UE should keep the transmitter turned on during the procedure. This procedure is only used in FDD mode.

#### 8.3.4.2 Initiation

The procedure is initiated when UTRAN orders a UE in CELL\_DCH state, to make the following modifications of the active set of the connection:

- a) Radio link addition;
- b) Radio link removal;
- c) Combined radio link addition and removal.

In case a) and c), UTRAN should:

- 1> prepare new additional radio link(s) in the UTRAN prior to the command to the UE.

In all cases, UTRAN should:

- 1> send an ACTIVE SET UPDATE message on downlink DCCH using AM or UM RLC.

UTRAN should include the following information:

- 1> IE "Radio Link Addition Information": Downlink DPCH information and other optional parameters relevant for the radio links to be added along with the IE "Primary CPICH info" used for the reference ID to indicate which radio link to add. This IE is needed in cases a) and c) listed above;
- 1> IE "Radio Link Removal Information": IE "Primary CPICH info" used for the reference ID to indicate which radio link to remove. This IE is needed in cases b) and c) listed above.

### 8.3.4.3 Reception of an ACTIVE SET UPDATE message by the UE

Upon reception of an ACTIVE SET UPDATE message the UE shall act upon all received information elements as specified in 8.6, unless specified otherwise in the following. The UE shall:

- 1> first add the RLs indicated in the IE "Radio Link Addition Information";
- 1> remove the RLs indicated in the IE "Radio Link Removal Information". If the UE active set is full or becomes full, an RL, which is included in the IE "Radio Link Removal Information" for removal, shall be removed before adding RL, which is included in the IE "Radio Link Addition Information" for addition;
- 1> perform the physical layer synchronisation procedure as specified in [29];
- ~~1> if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
 
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected".~~
- ~~1> if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":
 
  - 2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.~~
- ~~1> if the variable PDCP\_SN\_INFO is non-empty:
 
  - 2> include the IE "RB with PDCP information list" in the ACTIVE SET UPDATE COMPLETE message; and
  - 2> set it to the value of the variable PDCP\_SN\_INFO.~~
- 1> if the IE "TFCI combining indicator" associated with a radio link to be added is set to TRUE:
  - 2> if a DSCH transport channel is assigned and there is a 'hard' split in the TFCI field:
    - 3> configure Layer 1 to soft-combine TFCI (field 2) of this new link with those links already in the TFCI (field 2) combining set.
- ~~1> if the received ACTIVE SET UPDATE message included the IE "Downlink counter synchronisation info":
 
  - 2> calculate the START value according to subclause 8.5.9;
  - 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the ACTIVE SET UPDATE COMPLETE message.~~
- 1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE COMPLETE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> transmit an ACTIVE SET UPDATE COMPLETE message on the uplink DCCH using AM RLC without waiting for the Physical Layer synchronization;
- ~~1> if the IE "Integrity protection mode info" was present in the ACTIVE SET UPDATE message:
 
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted ACTIVE SET UPDATE COMPLETE message.~~

- 1> if the IE "Downlink counter synchronisation info" was included in the received ACTIVE SET UPDATE message:
    - 2> when RLC has confirmed the successful transmission of the response message:
      - 3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].
  - 1> if the variable PDCP\_SN\_INFO is empty:
    - 2> if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":
      - 3> when RLC has confirmed the successful transmission of the ACTIVE SET UPDATE COMPLETE message:
        - 4> perform the actions below.
    - 2> if the ACTIVE SET UPDATE message did not contain the IE "Ciphering mode info":
      - 3> when RLC has been requested to transmit the ACTIVE SET UPDATE COMPLETE message:
        - 4> perform the actions below.
  - 1> if the variable PDCP\_SN\_INFO is non-empty:
    - 2> when RLC has confirmed the successful transmission of the ACTIVE SET UPDATE COMPLETE message:
      - 3> for each radio bearer in the variable PDCP\_SN\_INFO:
        - 4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
          - 5> configure the RLC entity for that radio bearer to "continue".
      - 3> clear the variable PDCP\_SN\_INFO.
  - 1> if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":
    - 2> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
    - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
    - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
  - 1> if the ACTIVE SET UPDATE message contained the IE "Integrity protection mode info":
    - 2> allow the transmission of RRC messages on all signalling bearers with any RRC SN;
    - 2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
    - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
  - 1> clear the variable SECURITY\_MODIFICATION;
- 1> the procedure ends on the UE side.

#### 8.3.4.4 Unsupported configuration in the UE

If UTRAN instructs the UE to use a configuration that it does not support, the UE shall:

- 1> keep the active set as it was before the ACTIVE SET UPDATE message was received;
- 1> transmit an ACTIVE SET UPDATE FAILURE message on the DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and



- 1> clear that entry;
- 1> set the IE "failure cause" to "configuration unsupported";
- 1> when the ACTIVE SET UPDATE FAILURE message has been submitted to lower layers for transmission:
  - 2> the procedure ends on the UE side.

### 8.3.4.5 Invalid configuration

If any of the following conditions are valid:

- a radio link indicated by the IE "Downlink DPCH info for each RL" in the IE "Radio link addition information" has a different spreading factor than the spreading factor for the radio links in the active set that will be established at the time indicated by the IE "Activation time"; and/or
- a radio link in the IE "Radio link addition information" is also present in the IE "Radio Link Removal Information"; and/or
- the IE "Radio Link Removal Information" contains all the radio links which are part of or will be part of the active set at the time indicated by the IE "Activation time"; and/or
- the IE "TX Diversity Mode" is not set to "none" and it indicates a diversity mode that is different from the one currently used in all or part of the active set; and/or
- a radio link indicated by the IE "Radio Link Removal Information" does not exist in the active set; and/or
- after the removal of all radio links indicated by the IE "Radio Link Removal Information" and the addition of all radio links indicated by the IE "Radio Link Addition Information" the active set would contain more than the maximum allowed number of radio links; and/or
- the variable INVALID\_CONFIGURATION is set to TRUE:

the UE shall:

- 1> keep the active set as it was before the ACTIVE SET UPDATE message was received;
- 1> transmit an ACTIVE SET UPDATE FAILURE message on the DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to "Invalid configuration";
- 1> When the ACTIVE SET UPDATE FAILURE message has been submitted to lower layers for transmission:
  - 2> the procedure ends on the UE side.

#### 8.3.4.5a ~~Incompatible simultaneous reconfiguration~~ Void

~~If the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION becomes set to TRUE due to the received ACTIVE SET UPDATE message, the UE shall:~~

- ~~1> transmit a ACTIVE SET UPDATE FAILURE message on the uplink DCCH using AM RLC;~~
- ~~1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and~~
- ~~1> clear that entry;~~
- ~~1> set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";~~

- ~~1> when the ACTIVE SET UPDATE FAILURE message has been delivered to lower layers for transmission:~~
- ~~2> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to FALSE;~~
- ~~2> continue with any ongoing processes and procedures as if the ACTIVE SET UPDATE message has not been received;~~
- ~~2> and the procedure ends.~~

~~If the variable ORDERED\_RECONFIGURATION is set to TRUE; and~~

- ~~1> if the activation time for the procedure that has set variable ORDERED\_RECONFIGURATION and the activation time for the Active Set Update procedure are within a time window of 5 frames, the UE may:~~
- ~~2> transmit a ACTIVE SET UPDATE FAILURE message on the uplink DCCH using AM RLC;~~
- ~~2> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and~~
- ~~2> clear that entry;~~
- ~~2> set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";~~
- ~~2> when the ACTIVE SET UPDATE FAILURE message has been delivered to lower layers for transmission:~~
  - ~~3> continue with any ongoing processes and procedures as if the ACTIVE SET UPDATE message has not been received;~~
  - ~~3> and the procedure ends.~~

#### 8.3.4.6 Reception of the ACTIVE SET UPDATE COMPLETE message by the UTRAN

When the UTRAN has received the ACTIVE SET UPDATE COMPLETE message,

- 1> the UTRAN may remove radio link(s) that are indicated to remove to the UE in case b) and c); and
- 1> the procedure ends on the UTRAN side.

#### 8.3.4.7 Reception of the ACTIVE SET UPDATE FAILURE message by the UTRAN

When the UTRAN has received the ACTIVE SET UPDATE FAILURE message, the UTRAN may delete radio links that were included in the IE "Radio Link Addition Information" for addition. The procedure ends on the UTRAN side.

#### 8.3.4.8 Invalid ACTIVE SET UPDATE message

If the ACTIVE SET UPDATE message contains a protocol error causing the variable PROTOCOL\_ERROR\_REJECT to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows. The UE shall:

- 1> transmit a ACTIVE SET UPDATE FAILURE message on the uplink DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Rejected transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to the cause value "protocol error";
- 1> include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL\_ERROR\_INFORMATION;
- 1> when the ACTIVE SET UPDATE FAILURE message has been delivered to lower layers for transmission:

- 2> continue with any ongoing processes and procedures as if the invalid ACTIVE SET UPDATE message has not been received;
- 2> and the procedure ends.

#### 8.3.4.9 Reception of an ACTIVE SET UPDATE message in wrong state

If the UE is in another state than CELL\_DCH state upon reception of the ACTIVE SET UPDATE message, the UE shall perform procedure specific error handling as follows. The UE shall:

- 1> transmit a ACTIVE SET UPDATE FAILURE message on the uplink DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to the cause value "protocol error";
- 1> include the IE "Protocol error information" with the IE "Protocol error cause" set to "Message not compatible with receiver state";
- 1> when the ACTIVE SET UPDATE FAILURE message has been delivered to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the ACTIVE SET UPDATE message has not been received;
  - 2> and the procedure ends.

### 8.3.5 Hard handover

When performing hard handover with change of frequency, the UE shall:

- 1> stop all intra-frequency and inter-frequency measurements on the cells listed in the variable CELL\_INFO\_LIST until a MEASUREMENT CONTROL message is received from UTRAN.

#### 8.3.5.1 Timing re-initialised hard handover

##### 8.3.5.1.1 General

The purpose of the timing re-initialised hard handover procedure is to remove all the RL(s) in the active set and establish new RL(s) along with a change in the UL transmission timing and the CFN in the UE according to the SFN of the target cell.(see subclause 8.5.15).

This procedure is initiated when UTRAN does not know the target SFN timing before hard handover.

##### 8.3.5.1.2 Initiation

Timing re-initialised hard handover initiated by the UTRAN is normally performed by using the procedure "Physical channel reconfiguration" (subclause 8.2.6), but may also be performed by using either one of the following procedures:

- "radio bearer establishment" (subclause 8.2.1);
- "Radio bearer reconfiguration" (subclause 8.2.2);
- "Radio bearer release" (subclause 8.2.3); or
- "Transport channel reconfiguration" (subclause 8.2.4).

If IE "Timing indication" has the value "initialise", UE shall:

- 1> execute the Timing Re-initialised hard handover procedure by following the procedure indicated in the subclause relevant to the procedure chosen by the UTRAN.

In this case of a timing re-initialised hard handover, UTRAN should include the IE "Default DPCH Offset Value" and:

1> in FDD mode:

2> set "Default DPCH Offset Value" and "DPCH frame offset" respecting the following relation

$$(\text{Default DPCH Offset Value}) \bmod 38400 = \text{DPCH frame offset}_j$$

3> where  $j$  indicates the first radio link listed in the message and the IE values used are the Actual Values of the IEs as defined in clause 11.

If the IE "Default DPCH Offset Value" is included, the UE shall:

1> in FDD mode:

2> if the above relation between "Default DPCH Offset Value" and "DPCH frame offset" is not respected:

3> set the variable INVALID\_CONFIGURATION to true.

If the IE "Default DPCH Offset Value" is not included, the UE shall:

1> set the variable INVALID\_CONFIGURATION to true.

### 8.3.5.2 Timing-maintained hard handover

#### 8.3.5.2.1 General

The purpose of the Timing-maintained hard handover procedure is to remove all the RL(s) in the active set and establish new RL(s) while maintaining the UL transmission timing and the CFN in the UE.

This procedure can be initiated only if UTRAN knows the target SFN timing before hard handover. The target SFN timing can be known by UTRAN in the following 2 cases:

- UE reads SFN when measuring "Cell synchronisation information" and sends it to the UTRAN in MEASUREMENT REPORT message.
- UTRAN internally knows the time difference between the cells.

#### 8.3.5.2.2 Initiation

Timing-maintained hard handover initiated by the network is normally performed by using the procedure "Physical channel reconfiguration" (subclause 8.2.6), but may also be performed by using either one of the following procedures:

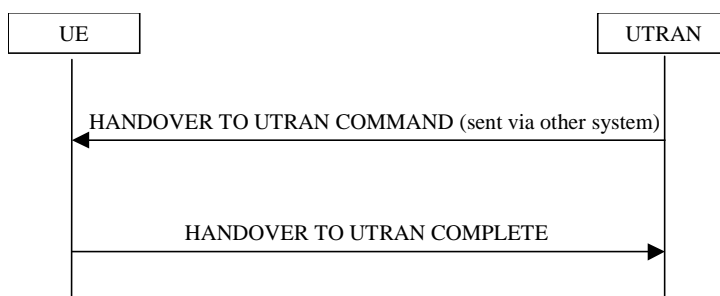
- "radio bearer establishment" (subclause 8.2.1);
- "Radio bearer reconfiguration" (subclause 8.2.2);
- "Radio bearer release" (subclause 8.2.3); or
- "Transport channel reconfiguration" (subclause 8.2.4).

If IE "Timing indication" has the value "maintain", UE shall initiate the Timing-maintained hard handover procedure by following the procedure indicated in the subclause relevant to the procedure chosen by the UTRAN. In this case UTRAN should not include the IE "Default DPCH Offset Value".

If the IE "Default DPCH Offset Value" is included, the UE shall:

1> ignore the IE "Default DPCH Offset Value".

## 8.3.6 Inter-RAT handover to UTRAN



**Figure 8.3.6-1: Inter-RAT handover to UTRAN, successful case**

### 8.3.6.1 General

The purpose of the inter-RAT handover procedure is to, under the control of the network, transfer a connection between the UE and another radio access technology (e.g. GSM) to UTRAN.

### 8.3.6.2 Initiation

The procedure is initiated when a radio access technology other than UTRAN, e.g. GSM, using radio access technology-specific procedures, orders the UE to make a handover to UTRAN.

A **HANDOVER TO UTRAN COMMAND** message is sent to the UE via the radio access technology from which inter-RAT handover is performed.

In case UTRAN decides to use a predefined or default radio configuration that is stored in the UE, it should include the following information in the **HANDOVER TO UTRAN COMMAND** message.

- the IE "New U-RNTI" to be assigned;
- the IE "Predefined configuration identity", to indicate which pre-defined configuration of RB, transport channel and physical channel parameters shall be used; or
- the IE "Default configuration mode" and IE "Default configuration identity", to indicate which default configuration of RB, transport channel and physical channel parameters shall be used;
- PhyCH information elements.

**NOTE 1:** When using a predefined or default configuration during handover to UTRAN, UTRAN can only assign values of IEs "New U-RNTI" and "scrambling code" that are within the special subranges defined exclusively for this procedure. UTRAN may re-assign other values after completion of the handover procedure.

**NOTE 2:** When using a predefined or default configuration during handover to UTRAN, fewer IEs are signalled; when using this signalling option some parameters e.g. concerning compressed mode, DSCH, SSdT can not be configured. In this case, the corresponding functionality can not be activated immediately.

In case UTRAN does not use a predefined radio configuration that is stored in the UE, it should include the following information in the **HANDOVER TO UTRAN COMMAND** message.

- the IE "New U-RNTI" to be assigned;
- the complete set of RB, TrCH and PhyCH information elements to be used.

### 8.3.6.3 Reception of **HANDOVER TO UTRAN COMMAND** message by the UE

The UE shall be able to receive a **HANDOVER TO UTRAN COMMAND** message and perform an inter-RAT handover, even if no prior UE measurements have been performed on the target UTRAN cell and/or frequency.

The UE shall act upon all received information elements as specified in subclause 8.6, unless specified otherwise in the following. The UE shall:

- 1> store a U-RNTI value (32 bits), which is derived by the IEs "SRNC identity" (12 bits) and "S-RNTI 2" (10 bits) included in IE "U-RNTI-short". In order to produce a full size U-RNTI value, a full size "S-RNTI" (20 bits) shall be derived by padding the IE "S-RNTI 2" with 10 zero bits in the most significant positions; and
- 1> initialise the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS with the signalling connections that remains after the handover according to the specifications of the source RAT;
- 1> initialise the variable UE\_CAPABILITIES\_TRANSFERRED with the UE capabilities that have been transferred to the network up to the point prior to the handover, if any;
- 1> initialise the variable TIMERS\_AND\_CONSTANTS to the default values and start to use those timer and constants values;
- 1> if IE "Specification mode" is set to "Preconfiguration" and IE "Preconfiguration mode" is set to "Predefined configuration":
  - 2> initiate the radio bearer and transport channel configuration in accordance with the predefined parameters identified by the IE "Predefined configuration identity";
  - 2> initiate the physical channels in accordance with the predefined parameters identified by the IE "Predefined radio configuration identity" and the received physical channel information elements;
  - 2> store information about the established radio access bearers and radio bearers according to the IE "Predefined configuration identity"; and
  - 2> set the IE "RAB Info Post" in the variable ESTABLISHED\_RABS and the IE "Re-establishment timer" in the IE "RAB Info" in the variable ESTABLISHED\_RABS to "useT314".
- 1> if IE "Specification mode" is set to "Preconfiguration" and IE "Preconfiguration mode" is set to "Default configuration":
  - 2> initiate the radio bearer and transport channel configuration in accordance with the default parameters identified by the IE "Default configuration mode" and IE "Default configuration identity";
  - 2> initiate the physical channels in accordance with the default parameters identified by the IE "Default configuration mode" and IE "Default configuration identity" and the received physical channel information elements;

NOTE IE "Default configuration mode" specifies whether the FDD or TDD version of the default configuration shall be used

- 2> set the IE "RAB Info Post" in the variable ESTABLISHED\_RABS and the IE "Re-establishment timer" in the IE "RAB Info" in the variable ESTABLISHED\_RABS to "useT314".
- 1> if IE "Specification mode" is set to "Preconfiguration":
  - 2> use the following values for parameters that are neither signalled within the HANDOVER TO UTRAN COMMAND message nor included within pre-defined or default configuration:
    - 3> 0 dB for the power offset  $P_{\text{Pilot-DPCH}}$  bearer in FDD;
    - 3> calculate the Default DPCH Offset Value using the following formula:
      - 3> in FDD:
 
$$\text{Default DPCH Offset Value} = (\text{SRNTI 2 mod } 600) * 512$$
      - 3> in TDD:
 
$$\text{Default DPCH Offset Value} = (\text{SRNTI 2 mod } 7)$$
    - 3> handle the above Default DPCH Offset Value as if an IE with that value was included in the message, as specified in subclause 8.6.6.21.

- 1> if IE "Specification mode" is set to "Complete specification":
  - 2> initiate the radio bearer, transport channel and physical channel configuration in accordance with the received radio bearer, transport channel and physical channel information elements.
- 1> perform an open loop estimation to determine the UL transmission power according to subclause 8.5.3;
- 1> set the IE "START" for each CN domain, in the IE "START list" in the HANDOVER TO UTRAN COMPLETE message equal to the START value for each CN domain stored in the USIM if the USIM is present, or as stored in the UE for each CN domain if the SIM is present;
- 1> if ciphering has been activated and ongoing in the radio access technology from which inter- RAT handover is performed:
  - 2> for the CN domain as in the IE "CN domain identity" which is included in the IE "RAB info" of the IE "RAB information to setup":
    - 3> set the 20 MSB of the HFN component of the COUNT-C variable for all radio bearers using RLC-TM and all signalling radio bearers to the "START" value included in the IE "UE security information" in the variable "INTER\_RAT\_HANDOVER\_INFO\_TRANSFERRED";
    - 3> set the remaining LSBs of the HFN component of COUNT-C for all radio bearers using RLC-TM and all signalling radio bearers to zero;
    - 3> not increment the HFN component of COUNT-C for radio bearers using RLC-TM, i.e. keep the HFN value fixed without incrementing every CFN cycle;
    - 3> set the CFN component of the COUNT-C variable to the value of the CFN as calculated in subclause 8.5.15;
    - 3> set the IE "Status" in the variable CIPHERING\_STATUS to "Started";
    - 3> apply the algorithm according to IE "Ciphering Algorithm" and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND.
- 1> if ciphering has not been activated and ongoing in the radio access technology from which inter-RAT handover is performed:
  - 2> for the CN domain as in the IE "CN domain identity" which is included in the IE "RAB info" of the IE "RAB information to setup":
    - 3> set the IE "Status" in the variable CIPHERING\_STATUS to "Not Started".

If the UE succeeds in establishing the connection to UTRAN, it shall:

- 1> if the IE "Status" in the variable CIPHERING\_STATUS of a CN domain is set to "Started" and transparent mode radio bearers have been established by this procedure for that CN domain:
  - 2> include the IE "COUNT-C activation time" in the response message and specify a CFN value other than the default, "Now" for this IE;
  - 2> at the CFN value as indicated in the response message in the IE "COUNT-C activation time" for radio bearers using RLC-TM:
    - 3> set the 20 MSB of the HFN component of the COUNT-C variable to the START value as indicated in the IE "START list" of the response message for the relevant CN domain; and
    - 3> set the remaining LSBs of the HFN component of COUNT-C to zero;
    - 3> increment the HFN component of the COUNT-C variable by one;
    - 3> set the CFN component of the COUNT-C to the value of the IE "COUNT-C activation time" of the response message. The HFN component and the CFN component completely initialise the COUNT-C variable;
    - 3> step the COUNT-C variable, as normal, at each CFN value. The HFN component is no longer fixed in value but incremented at each CFN cycle.

- 1> transmit a HANOVER TO UTRAN COMPLETE message on the uplink DCCH, using, if ciphering has been started, the new ciphering configuration;
- 1> when the HANOVER TO UTRAN COMPLETE message has been submitted to lower layers for transmission:
  - 2> enter UTRA RRC connected mode in state CELL\_DCH;
  - 2> initialise variables upon entering UTRA RRC connected mode as specified in subclause 13.4;
  - 2> for all radio bearers using RLC-AM or RLC-UM:
    - 3> set the 20 MSB of the HFN component of the uplink and downlink COUNT-C variable to the START value indicated in the IE "START list" of the response message for the relevant CN domain; and
    - 3> set the remaining LSBs of the HFN component of COUNT-C to zero;
    - 3> increment the HFN component of the COUNT-C variable by one;
    - 3> start incrementing the COUNT-C values.
- 1> and the procedure ends.

#### 8.3.6.4 Invalid Handover to UTRAN command message

If the UE receives a HANOVER TO UTRAN COMMAND message, which contains a protocol error causing the variable `PROTOCOL_ERROR_REJECT` to be set to `TRUE` according to clause 9, the UE shall perform procedure specific error handling according to the source radio access technology. The UE shall:

- 1> if allowed by the source RAT:
  - 2> transmit an RRC FAILURE INFO message to the source radio access technology; and
  - 2> include the IE "Protocol error information" with contents set to the value of the variable `PROTOCOL_ERROR_INFORMATION`;
- 1> Other details may be provided in the specifications related to the source radio access technology.

NOTE: The other RAT may include the above diagnostics information in a subsequent handover request towards the same RNC.

#### 8.3.6.4a Unsupported configuration in HANOVER TO UTRAN COMMAND message

If the UE does not support the configuration included in the HANOVER TO UTRAN COMMAND message, e.g., the message includes a pre-defined configuration that the UE has not stored, the UE shall:

- 1> continue the connection using the other radio access technology; and
- 1> indicate the failure to the other radio access technology.

#### 8.3.6.5 UE fails to perform handover

If the UE does not succeed in establishing the connection to UTRAN, it shall:

- 1> terminate the procedure including release of the associated resources;
- 1> resume the connection used before the handover; and
- 1> indicate the failure to the other radio access technology.

Upon receiving an indication about the failure from the other radio access technology, UTRAN should release the associated resources and the context information concerning this UE.



### 8.3.6.6 Reception of message HANDOVER TO UTRAN COMPLETE by the UTRAN

Upon receiving a HANDOVER TO UTRAN COMPLETE message, UTRAN should consider the inter-RAT handover procedure as having been completed successfully and indicate this to the Core Network.

### 8.3.7 Inter-RAT handover from UTRAN

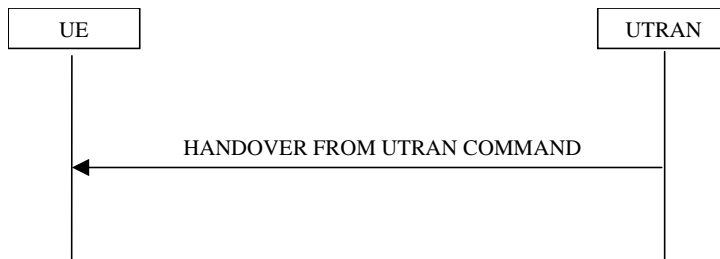


Figure 8.3.7-1: Inter-RAT handover from UTRAN, successful case

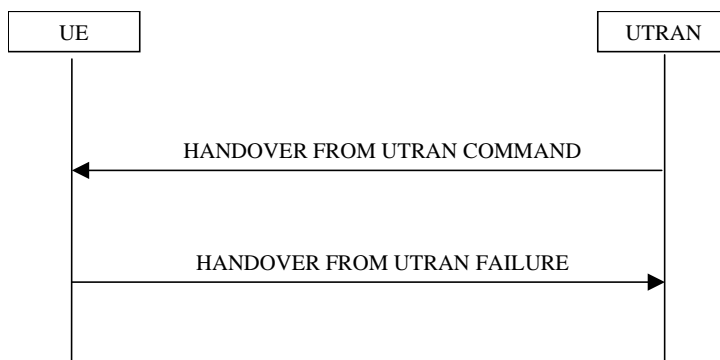


Figure 8.3.7-2: Inter-RAT handover from UTRAN, failure case

#### 8.3.7.1 General

The purpose of the inter-RAT handover procedure is to, under the control of the network, transfer a connection between the UE and UTRAN to another radio access technology (e.g. GSM). This procedure may be used in CELL\_DCH state.

NOTE: This procedure is applicable to CS domain service.

#### 8.3.7.2 Initiation

The procedure is initiated when UTRAN orders a UE in CELL\_DCH state, to make a handover to a radio access technology other than UTRAN, e.g. GSM.

To initiate the procedure, UTRAN sends a HANDOVER FROM UTRAN COMMAND message.

### 8.3.7.3 Reception of a HANDOVER FROM UTRAN COMMAND message by the UE

The UE shall be able to receive a HANDOVER FROM UTRAN COMMAND message and perform an inter-RAT handover, even if no prior UE measurements have been performed on the target cell.

The UE shall:

- 1> establish the connection to the target radio access technology, by using the contents of the IE "Inter-RAT message". This IE contains a message specified in another standard, as indicated by the IE "System type", and carries information about the candidate/ target cell identifier(s) and radio parameters relevant for the target radio access technology. The correspondence between the value of the IE "System type", the standard to apply and the message contained within IE "Inter RAT message" is shown in the following:

Value of the IE "System type"	Standard to apply	Inter RAT Message
GSM	GSM TS 04.18, version 8.5.0 or later	HANDOVER COMMAND
cdma2000	TIA/EIA/IS-2000 or later, TIA/EIA/IS-833 or later, TIA/EIQ/IS-834 or later	

- 1> if the IE "System type" has the value "GSM":
  - 2> if the IE "Frequency band" has the value "GSM /DCS 1800 band used":
    - 3> set the BAND\_INDICATOR [45] to "ARFCN indicates 1800 band".
  - 2> if the IE "Frequency band" has the value " GSM /PCS 1900 band used":
    - 3> set the BAND\_INDICATOR [45] to "ARFCN indicates 1900 band".
- 1> apply the "Inter RAT Message" according to the "standard to apply" in the table above.
- 1> in case one or more IEs "RAB info" is included in the HANDOVER FROM UTRAN COMMAND message:
  - 2> connect upper layer entities corresponding to indicated RABs to the radio resources indicated in the inter-RAT message.

NOTE: Requirements concerning the establishment of the radio connection towards the other radio access technology and the signalling procedure are outside the scope of this specification.

### 8.3.7.4 Successful completion of the inter-RAT handover

Upon successfully completing the handover, UTRAN should:

- 1> release the radio connection; and
- 1> remove all context information for the concerned UE.

Upon successfully completing the handover, the UE shall:

- 1> if the USIM is present:
  - 2> store the current START value for every CN domain in the USIM [50];
  - 2> if the "START" stored in the USIM [50] for a CN domain is greater than or equal to the value "THRESHOLD" of the variable START\_THRESHOLD:
    - 3> delete the ciphering and integrity keys that are stored in the USIM for that CN domain;
    - 3> inform the deletion of these keys to upper layers.
- 1> if the SIM is present:
  - 2> store the current START value for every CN domain in the UE;

- 2> if the "START" stored in the UE for a CN domain is greater than or equal to the value "THRESHOLD" of the variable START\_THRESHOLD:
- 3> delete the ciphering and integrity keys that are stored in the SIM for that CN domain;
- 3> inform the deletion of these keys to upper layers.
- 1> if there are any NAS messages with the IE "CN domain identity" set to "CS domain" for which the successful delivery of the INITIAL DIRECT TRANSFER message or UPLINK DIRECT TRANSFER message on signalling radio bearer RB3 or signalling radio bearer RB4 that have not yet been confirmed by RLC:
  - 2> retransmit those NAS messages to the network on the newly established radio connection to the target radio access technology.
- 1> clear or set variables upon leaving UTRA RRC connected mode as specified in subclause 13.4.

NOTE: The release of the UMTS radio resources is initiated from the target RAT.

### 8.3.7.5 UE fails to complete requested handover

If the UE does not succeed in establishing the connection to the target radio access technology, it shall:

- 1> revert back to the UTRA configuration;
- 1> establish the UTRA physical channel(s) used at the time for reception of HANDOVER FROM UTRAN COMMAND;
- 1> if the UE does not succeed to establish the UTRA physical channel(s):
  - 2> perform a cell update procedure according to subclause 8.3.1 with cause "Radio link failure";
  - 2> when the cell update procedure has completed successfully:
    - 3> proceed as below.
- 1> transmit the HANDOVER FROM UTRAN FAILURE message setting the information elements as specified below:
  - 2> include the IE "RRC transaction identifier"; and
  - 2> set it to the value of "RRC transaction identifier" in the entry for the HANDOVER FROM UTRAN COMMAND message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> set the IE "Inter-RAT handover failure" to "physical channel failure".
- 1> When the HANDOVER FROM UTRAN FAILURE message has been submitted to lower layer for transmission:
  - 2> the procedure ends.

### 8.3.7.6 Invalid HANDOVER FROM UTRAN COMMAND message

If the IE "Inter-RAT message" received within the HANDOVER FROM UTRAN COMMAND message does not include a valid inter RAT handover message in accordance with the protocol specifications for the target RAT, the UE shall perform procedure specific error handling as follows. The UE shall:

- 1> set the IE "failure cause" to the cause value "Inter-RAT protocol error";
- 1> include the IE "Inter-RAT message" in case the target RAT provides further details about the inter RAT protocol error;
- 1> transmit a HANDOVER FROM UTRAN FAILURE message on the uplink DCCH using AM RLC;
- 1> when the transmission of the HANDOVER FROM UTRAN FAILURE message has been confirmed by RLC:

- 2> continue with any ongoing processes and procedures as if the invalid HANDOVER FROM UTRAN COMMAND message has not been received;
- 2> and the procedure ends.

If the HANDOVER FROM UTRAN COMMAND message contains a protocol error causing the variable `PROTOCOL_ERROR_REJECT` to be set to `TRUE` according to clause 9, the UE shall perform procedure specific error handling as follows. The UE shall:

- 1> set the IE "RRC transaction identifier" in the HANDOVER FROM UTRAN FAILURE message to the value of "RRC transaction identifier" in the entry for the HANDOVER FROM UTRAN COMMAND message in the table "Rejected transactions" in the variable `TRANSACTIONS`; and
- 1> clear that entry;
- 1> set the IE "failure cause" to the cause value "protocol error";
- 1> include the IE "Protocol error information" with contents set to the value of the variable `PROTOCOL_ERROR_INFORMATION`;
- 1> transmit a HANDOVER FROM UTRAN FAILURE message on the uplink DCCH using AM RLC;
- 1> when the HANDOVER FROM UTRAN FAILURE message has been submitted to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the invalid HANDOVER FROM UTRAN COMMAND message has not been received;
  - 2> and the procedure ends.

#### 8.3.7.7 Reception of an HANDOVER FROM UTRAN FAILURE message by UTRAN

Upon receiving an HANDOVER FROM UTRAN FAILURE message, UTRAN may initiate the release the resources in the target radio access technology.

#### 8.3.7.8 Unsupported configuration in HANDOVER FROM UTRAN COMMAND message

If the UTRAN instructs the UE to perform a non-supported handover scenario, e.g. multiple RAB or to use a non-supported configuration, the UE shall:

- 1> transmit a HANDOVER FROM UTRAN FAILURE message, setting the information elements as specified below:
  - 2> include the IE "RRC transaction identifier"; and
  - 2> set it to the value of "RRC transaction identifier" in the entry for the HANDOVER FROM UTRAN COMMAND message in the table "Accepted transactions" in the variable `TRANSACTIONS`; and
  - 2> clear that entry;
  - 2> set the IE "Inter-RAT handover failure" to "configuration unacceptable";
  - 2> when the HANDOVER FROM UTRAN FAILURE message has been submitted to lower layers for transmission:
    - 3> resume normal operation as if the invalid HANDOVER FROM UTRAN COMMAND message has not been received;
    - 3> and the procedure ends.

### 8.3.7.8a Reception of HANDOVER FROM UTRAN COMMAND message by UE in CELL\_FACH

If the UE receives HANDOVER FROM UTRAN COMMAND while in CELL\_FACH, the UE shall:

- 1> transmit a HANDOVER FROM UTRAN FAILURE message, setting the information elements as specified below:
  - 2> include the IE "RRC transaction identifier"; and
  - 2> set it to the value of "RRC transaction identifier" in the entry for the HANDOVER FROM UTRAN COMMAND message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> set the IE "Inter-RAT handover failure" to "protocol error", include IE "Protocol error information"; and
  - 2> set the value of IE "Protocol error cause" to "Message not compatible with receiver state";
  - 2> when the HANDOVER FROM UTRAN FAILURE message has been submitted to lower layers for transmission:
    - 3> resume normal operation as if the invalid HANDOVER FROM UTRAN COMMAND message has not been received;
    - 3> and the procedure ends.

## 8.5.9 START value calculation

In connected mode, the START value for CN domain 'X' is calculated as

Let  $START_X$  = the START value for CN domain 'X' prior to the calculation below:

$START_X' = MSB_{20} ( MAX \{ COUNT-C, COUNT-I \mid \text{radio bearers and signalling radio bearers using the most recently configured } CK_X \text{ and } IK_X \}) + 2.$

- if  $START_X' =$  the maximum value = 1048575 then  $START_X = START_X'$ ;
- if the current  $START_X < START_X'$  then  $START_X = START_X'$ , otherwise  $START_X$  is unchanged.

NOTE: Here, "most recently configured" means that if there is more than one key in use for a CN domain, due to non-expiry of the ciphering and/or integrity protection activation time for any signalling radio bearers and/or radio bearers, do not include the COUNT-I/COUNT-C for these signalling radio bearers and/or radio bearers in the calculation of the  $START_X'$ .

COUNT-C corresponding to non-ciphered radio bearers ([i.e. RBs with ciphering status set to "not started"](#)) shall not be included in the calculation of the  $START_X'$ . If a radio bearer is released and the radio bearer was ciphered, the values of the COUNT-C at the time the radio bearer is released shall be taken into account in the calculation of the  $START_X'$ .

## 8.5.10 Integrity protection

If the "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" then the UE shall:

- 1> perform integrity protection (and integrity checking) on all RRC messages, with the following exceptions:
  - HANDOVER TO UTRAN COMPLETE
  - PAGING TYPE 1
  - PUSCH CAPACITY REQUEST
  - PHYSICAL SHARED CHANNEL ALLOCATION

RRC CONNECTION REQUEST

RRC CONNECTION SETUP

RRC CONNECTION SETUP COMPLETE

RRC CONNECTION REJECT

RRC CONNECTION RELEASE (CCCH only)

SYSTEM INFORMATION

SYSTEM INFORMATION CHANGE INDICATION

If the "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started" then integrity protection (and integrity checking) shall not be performed on any RRC message.

For each signalling radio bearer, the UE shall use two RRC hyper frame numbers:

- "Uplink RRC HFN";
- "Downlink RRC HFN".

and two message sequence numbers:

- "Uplink RRC Message sequence number";
- "Downlink RRC Message sequence number".

The above information is stored in the variable INTEGRITY\_PROTECTION\_INFO per signalling radio bearer (RB0-RB4).

Upon the first activation of integrity protection for an RRC connection, UE and UTRAN initialise the "Uplink RRC Message sequence number" and "Downlink RRC Message sequence number" for all signalling radio bearers as specified in subclauses 8.6.3.5 and 8.5.10.1.

The RRC message sequence number (RRC SN) is incremented for every integrity protected RRC message.

If the IE "Integrity Protection Mode Info" is present in a received message, the UE shall:

- 1> perform the actions in subclause 8.6.3.5 before proceeding with the integrity check of the received message.

### 8.5.10.1 Integrity protection in downlink

If the UE receives an RRC message on signalling radio bearer with RB identity n, the "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and the IE 'Integrity check info' is present the UE shall:

- 1> check the value of the IE "RRC message sequence number" included in the IE "Integrity check info";
- 2> if the "Downlink RRC Message sequence number" is not present in the variable INTEGRITY\_PROTECTION\_INFO:
  - 3> initialise the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO with the value of the IE "RRC message sequence number" included in the IE "Integrity check info" of the received message.
- 2> if the "Downlink RRC Message sequence number" is present in the variable INTEGRITY\_PROTECTION\_INFO:
  - 3> if the RRC message sequence number is lower than the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO:
    - 4> increment "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO with one.
  - 3> if the RRC message sequence number is equal to the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO:

- 4> discard the message.
- 1> calculate an expected message authentication code in accordance with subclause 8.5.10.3;
- 1> compare the expected message authentication code with the value of the received IE "message authentication code" contained in the IE "Integrity check info";
  - 2> if the expected message authentication code and the received message authentication code are the same, the integrity check is successful:
    - 3> update the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO with the value of the IE "RRC message sequence number" included in the IE "Integrity check info" of the received RRC message.
  - 2> if the calculated expected message authentication code and the received message authentication code differ:
    - 3> if the IE "RRC message sequence number" included in the IE "Integrity check info" is lower than the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO (in this case the "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO was incremented by one, as stated above):
      - 4> decrement "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO by one.
    - 3> discard the message.

If the UE receives an RRC message on signalling radio bearer with identity n, the "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and the IE 'Integrity check info' is not present the UE shall:

- 1> discard the message.

#### 8.6.3.4 Cipherng mode info

The IE "Cipherng mode info" defines the new cipherng configuration. At any given time, the UE needs to store at most two different cipherng configurations (keyset and algorithm) per CN domain at any given time in total for all radio bearers and three configurations in total for all signalling radio bearers.

If the IE "Cipherng mode info" is present and if the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE, the UE shall:

- 1> ignore this second attempt to change the cipherng configuration; and
- 1> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to TRUE.

If the IE "Cipherng mode info" is present and if the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to FALSE, the UE shall:

- 1> if the IE "Status" in the variable CIPHERING STATUS has the value "Not started", and this IE was included in a message that is not the message SECURITY MODE COMMAND; or
- 1> if there does not exist exactly one cipherng activation time in the IE "Radio bearer downlink cipherng activation time info" for each established RLC-AM and RLC-UM radio bearers included in the IE "RB information" in the IE "ESTABLISHED\_RABS" for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN; or
- 1> if the IE "Cipherng activation time for DPCH" is not included in message ACTIVE SET UPDATE or SECURITY MODE COMMAND, and there exist radio bearers using RLC-TM according to the IE "RB information" in the IE "ESTABLISHED\_RABS" for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN; or
- 1> if there does not exist exactly one cipherng activation time in the IE "Radio bearer downlink cipherng activation time info" for each established signalling radio bearer included in the IE "Signalling radio bearer information" in the IE "ESTABLISHED\_RABS":
  - 2> ignore this attempt to change the cipherng configuration;

- 2> set the variable INVALID\_CONFIGURATION to TRUE;
- 2> perform the actions as specified in subclause 8.1.12.4c.
- 1> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to TRUE;
- 1> set the IE "Status" in the variable CIPHERING\_STATUS of the CN domains for which the IE "Status" of the variable SECURITY\_MODIFICATION is set to "Affected" to "Started";
- 1> apply the new ciphering configuration in the lower layers for all RBs that belong to a CN domain for which the IE "Status" of the variable SECURITY\_MODIFICATION is set to "Affected" and all signalling radio bearers:
  - 2> using the ciphering algorithm (UEA [40]) indicated by the IE "Ciphering algorithm" as part of the new ciphering configuration;
  - 2> for each radio bearer that belongs to a CN domain for which the IE "Status" of the variable SECURITY\_MODIFICATION is set to "Affected" and all signalling radio bearers:
    - 3> using the value of the IE "RB identity" in the variable ESTABLISHED\_RABS minus one as the value of BEARER [40] in the ciphering algorithm.
- 1> apply the new ciphering configuration as follows:
  - 2> consider an activation time in downlink to be pending:
    - 3> for UM-RLC until an UMD PDU with sequence number equal to or larger than activation time –1 has been received;
    - 3> for AM-RLC until all AMD PDUs with sequence numbers up to and including activation time –1 have been received;
    - 3> for TM-RLC until the CFN indicated in the activation time has been reached.
  - 2> if there are pending activation times in downlink set for ciphering by a previous procedure changing the ciphering configuration:
    - 3> apply the ciphering configuration included in the current message at this pending activation time;
    - 3> [consider the ciphering keys that were to be applied following a previous procedure changing the ciphering configuration and which have not yet been applied due to the activation time not having elapsed for a given radio bearer, as part of the ciphering configuration received in the current message.](#)
  - 2> if the IE "Ciphering activation time for DPCH" is present in the IE "Ciphering mode info" and the UE was in CELL\_DCH state prior to this procedure:
    - 3> for radio bearers using RLC-TM:
      - 4> apply the old ciphering configuration for CFN less than the number indicated in the IE "Ciphering activation time for DPCH";
      - 4> apply the new ciphering configuration for CFN greater than or equal to the number indicated in IE "Ciphering activation time for DPCH".
  - 2> if the UE was in CELL\_FACH state prior to this procedure and at completion of this procedure a transparent mode radio bearer exists and the IE "Ciphering activation time for DPCH" is not present in the IE "Ciphering mode info":
    - 3> for radio bearers using RLC-TM:
      - 4> apply the old ciphering configuration for CFN less than the number as indicated [by the IE "COUNT-C activation time"](#) in the transmitted uplink response message for the ciphering activation time for this radio bearer;
      - 4> apply the new ciphering configuration for CFN greater than or equal to the number ~~as~~ indicated in the transmitted uplink response message for the ciphering activation time for this radio bearer.

~~NOTE:—This is indicated by the IE "COUNT-C activation time" in the transmitted uplink response message.~~



- 2> if the IE "Radio bearer downlink ciphering activation time info" is present:
  - 3> apply the following procedure for each radio bearer and signalling radio bearers using RLC-AM or RLC-UM indicated by the IE "RB identity":
    - 4> suspend uplink transmission on the radio bearer or the signalling radio bearer (except for the SRB where the response message is transmitted) according to the following:
      - 5> do not transmit RLC PDUs with sequence number greater than or equal to the uplink activation time, where the uplink activation time is selected according to the rules below.
    - 4> select an "RLC send sequence number" at which (activation) time the new ciphering configuration shall be applied in uplink for that radio bearer according to the following:
      - 5> for each radio bearer and signalling radio bearer that has no pending ciphering activation time in uplink as set by a previous procedure changing the security configuration:
        - 6> set a suitable value that would ensure a minimised delay in the change to the latest security configuration.
      - 5> for each radio bearer and signalling radio bearer that has a pending ciphering activation time in uplink as set by a previous procedure changing the security configuration:
        - 6> set the same value as the pending ciphering activation time.
    - 5> consider this activation time in uplink to be elapsed when the selected activation time (as above) is equal to the "RLC send sequence number";
  - 4> store the selected "RLC send sequence number" for that radio bearer in the entry for the radio bearer in the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 4> switch to the new ciphering configuration according to the following:
    - 5> use the old ciphering configuration for the transmitted and received RLC PDUs with RLC sequence numbers smaller than the corresponding RLC sequence numbers indicated in the IE "Radio bearer uplink ciphering activation time info" sent to UTRAN and in the received IE "Radio bearer downlink ciphering activation time info" received from UTRAN, respectively;
    - 5> use the new ciphering configuration for the transmitted and received RLC PDUs with RLC sequence numbers greater than or equal to the corresponding RLC sequence numbers indicated in the IE "Radio bearer uplink ciphering activation time info" sent to UTRAN and in the received IE "Radio bearer downlink ciphering activation time info" received from UTRAN, respectively;
    - 5> for a radio bearer using RLC-AM, when the RLC sequence number indicated in the IE "Radio bearer downlink ciphering activation time info" falls below the RLC receiving window and the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" falls below the RLC transmission window, the UE may release the old ciphering configuration for that radio bearer;
    - 5> if an RLC reset or re-establishment occurs before the activation time for the new ciphering configuration has been reached, ignore the activation time and apply the new ciphering configuration immediately after the RLC reset or RLC re-establishment.

If the IE "Ciphering mode info" is not present, the UE shall:

- 1> not change the ciphering configuration.

### 8.6.3.5 Integrity protection mode info

The IE "Integrity protection mode info" defines the new integrity protection configuration. At any given time, the UE needs to store at most three different integrity protection configurations (keysets) in total for all signalling radio bearers for all CN domains.

If the IE "Integrity protection mode info" is present and if the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE, the UE shall:

1> ignore this second attempt to change the integrity protection configuration; and

1> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to TRUE.

If the IE "Integrity protection mode info" is present and if the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to FALSE, the UE shall:

1> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to TRUE;

1> if IE "Integrity protection mode command" has the value "start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and this IE was included in the message SECURITY MODE COMMAND:

2> initialise the information for all signalling radio bearers in the variable INTEGRITY\_PROTECTION\_INFO according to the following:

3> set the IE "Uplink RRC Message sequence number" in the variable INTEGRITY\_PROTECTION\_INFO to zero;

3> do not set the IE "Downlink RRC Message sequence number" in the variable INTEGRITY\_PROTECTION\_INFO;

3> set the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO to zero for each signalling radio bearer in the IE "ESTABLISHED\_RABS".

2> set the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO to the value "Started";

2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:

3> using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";

3> using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].

2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer in the IE "ESTABLISHED\_RABS" except RB2 at the next received RRC message;

2> start applying the new integrity protection configuration in the downlink for signalling radio bearer RB2 from and including the received SECURITY MODE COMMAND message;

2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;

2> start applying the new integrity protection configuration in the uplink for signalling radio bearers other than RB2 at the uplink activation time included in the IE "Uplink integrity protection activation info".

1> if IE "Integrity protection mode command" has the value "start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and this IE was not included SECURITY MODE COMMAND:

NOTE: This case is used in SRNS relocation

2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:

3> using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";

3> using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].

2> let RB<sub>m</sub> be the signalling radio bearer where the reconfiguration message was received and let RB<sub>n</sub> be the signalling radio bearer where the response message is transmitted;

- 2> prohibit transmission of RRC messages on all signalling radio bearers in the IE "ESTABLISHED\_RABS" except the radio bearer where the response message is transmitted;
- 2> consider the new integrity protection configuration to include any new keys that were activated through a security procedure received prior to the current message but not applied for the signalling radio bearer, due to the activation time for the corresponding signalling radio bearer not having elapsed;
- 2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer in the IE "ESTABLISHED\_RABS" except RB<sub>m</sub> at the next received RRC message disregarding any pending activation times for the corresponding signalling radio bearer;
- 2> start applying the new integrity protection configuration in the downlink for signalling radio bearer RB<sub>m</sub> from and including the received configuration message;
- 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB<sub>n</sub> from and including the transmitted response message;
- 2> start applying the new integrity protection configuration in the uplink for signalling radio bearers other than RB<sub>n</sub> ~~at the uplink activation time included in the IE "Uplink integrity protection activation info"~~ from the first message onwards.

NOTE : The UTRAN should ignore the information included in the IE "Uplink integrity protection info".

- 1> if IE "Integrity protection mode command" has the value "modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and this IE was included in SECURITY MODE COMMAND:
  - 2> store the (oldest currently used) integrity protection configuration until activation times have elapsed for the new integrity protection configuration to be applied on all signalling radio bearers;
  - 2> if there are pending activation times set for integrity protection by a previous procedure changing the integrity protection configuration:
    - 3> apply the integrity protection configuration at this pending activation time as indicated in this procedure.
  - 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each signalling radio bearer n, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info";
  - 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1;
    - 3> if present, use the algorithm indicated by the IE "Integrity protection algorithm" (UIA [40]);
  - 2> set the content of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO according to the following:
    - 3> for each established signalling radio bearer, stored in the variable ESTABLISHED\_RABS:
      - 4> select a value of the RRC sequence number at which (activation) time the new integrity protection configuration shall be applied in uplink for that signalling radio bearer according to the following:
        - 5> for each signalling radio bearer that has no pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
          - 6> set a suitable value that would ensure a minimised delay in the change to the latest integrity protection configuration.
        - 5> for signalling radio bearer that has a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
          - 6> set the same value as the pending activation time for integrity protection;

5> consider this (pending) activation time to be elapsed when the selected activation time (as above) is equal to the next RRC sequence number to be used, which means that the last RRC message using the old integrity protection configuration has been submitted to lower layers.

4> for signalling radio bearer RB0:

5> set the value of the included RRC sequence number to greater than or equal to the current value of the RRC sequence number for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO, plus the value of the constant N302 plus one.

4> prohibit the transmission of RRC messages on all signalling radio bearers, except for RB2, with RRC SN greater than or equal to the value in the "RRC message sequence number list" for the signalling radio bearer in the IE "Uplink integrity protection activation info" of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.

2> start applying the new integrity protection configuration in the uplink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Uplink integrity protection activation info", included in the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;

2> start applying the new integrity protection configuration in the uplink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration;

2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info";

NOTE: For signalling radio bearers that have a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration, UTRAN should set this value in IE "Downlink integrity protection activation info".

2> start applying the new integrity protection configuration in the downlink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration.

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and the IE "Integrity protection mode command info" was not included in the message SECURITY MODE COMMAND; or

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and the IE "Integrity protection mode info" was included in the message SECURITY MODE COMMAND, and the IE "Integrity protection algorithm" is not included; or

If the IE "Integrity protection mode command" has the value "Modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not Started"; or

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started", and the IE "Integrity protection mode command info" was included in the message SECURITY MODE COMMAND; or

If there does not exist exactly one integrity protection activation time in the IE "Downlink integrity protection activation info" for each established signalling radio bearer included in the IE "Signalling radio bearer information" in the IE "ESTABLISHED\_RABS"; or

If IE "Integrity protection mode command" has the value "Modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started", and the IE "Integrity protection mode info" was not included in the message SECURITY MODE COMMAND:

the UE shall:

1> ignore this attempt to change the integrity protection configuration; and

1> set the variable INVALID\_CONFIGURATION to TRUE.

If the IE "Integrity protection mode info" is not present, the UE shall:

- 1> not change the integrity protection configuration.

#### 8.6.3.6 Void

#### 8.6.3.7 Void

#### 8.6.3.8 Integrity check info

If the IE "Integrity check info" is present the UE shall:

- 1> act as described in subclause 8.5.10.1.

#### 8.6.3.9 New C-RNTI

If the IE "New C-RNTI" is included, the UE shall:

- 1> store the value in the variable C\_RNTI, replacing any old stored value;
- 1> use that C-RNTI when using common transport channels of type RACH, FACH and CPCH in the current cell.

#### 8.6.3.9a New DSCH-RNTI

If the IE "New DSCH-RNTI" is included, the UE shall:

- 1> in FDD:
  - 2> if the UE will be in CELL\_DCH at the end of the procedure where the received message included this IE:
    - 3> if the UE supports DSCH as indicated in the IE "Physical Channel Capability" included in the IE "UE Radio Access Capability":
      - 4> store the value in the variable DSCH\_RNTI, replacing any old stored value;
      - 4> use that DSCH-RNTI when using common transport channels of type DSCH in the current cell.
- 1> in TDD:
  - 2> if the UE will be in CELL\_DCH or CELL\_FACH at the end of the procedure where the received message included this IE:
    - 3> if the UE supports DSCH or USCH as indicated in the IE "Physical Channel Capability" included in the IE "UE Radio Access Capability":
      - 4> store the value in the variable DSCH\_RNTI, replacing any old stored value;
      - 4> use that DSCH-RNTI when using SHCCH signalling in the current cell.

#### 8.6.3.10 New U-RNTI

If the IE "New U-RNTI" is included in a received message, the UE shall:

- 1> store the value in the variable U\_RNTI, replacing any old stored value.

### 8.6.4.8 RB mapping info

If the IE "RB mapping info" is included, the UE shall:

- 1> for each multiplexing option of the RB:
  - 2> if a transport channel that would not exist as a result of the message (i.e. removed in the same message in IE "Deleted DL TrCH information" and IE "Deleted UL TrCH information") is referred to:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if a multiplexing option that maps a logical channel corresponding to a TM-RLC entity onto RACH, CPCH, FACH or DSCH is included:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if the multiplexing option realises the radio bearer on the uplink (resp. on the downlink) using two logical channels with different values of the IE "Uplink transport channel type" (resp. of the IE "Downlink transport channel type"):
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if that RB is using TM and the IE "Segmentation indication" is set to TRUE and, based on the multiplexing configuration resulting from this message, the logical channel corresponding to it is mapped onto the same transport channel as another logical channel:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if the transport channel considered in that multiplexing option is different from RACH and if that RB is using AM and the set of RLC sizes applicable to the logical channel transferring data PDUs has more than one element:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if that RB is using UM or TM and the multiplexing option realises it using two logical channels:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
- 2> for each logical channel in that multiplexing option:
  - 3> if the value of the IE "RLC size list" is set to "Explicit list":
    - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is included in the same message, and the value (index) of any IE "RLC size index" in the IE "Explicit list" does not correspond to an "RLC size" in the IE transport format set of that transport channel given in the message; or
    - 4> if the transport channel this logical channel is mapped on in this multiplexing option is different from RACH, and if a "Transport format set" for that transport channel is not included in the same message, and the value (index) of any IE "RLC size index" in the IE "Explicit list" does not correspond to an "RLC size" in the stored transport format set of that transport channel; or
    - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is included in the same message, and the value of any IE "Logical channel list" in the transport format set is not set to "Configured"; or
    - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is not included in the same message, and the value of any IE "Logical channel list" in the stored transport format set of that transport channel is not set to "Configured":
      - 5> set the variable INVALID\_CONFIGURATION to TRUE.

- 3> if the value of the IE "RLC size list" is set to "All":
  - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is included in the same message, and the value of any IE "Logical channel list" in the transport format set is not set to "Configured"; or
  - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is not included in the same message, and the value of any IE "Logical channel list" in the stored transport format set of that transport channel is not set to "Configured":
    - 5> set the variable INVALID\_CONFIGURATION to TRUE.
- 3> if the value of the IE "RLC size list" is set to "Configured":
  - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is included in the same message, and for none of the RLC sizes defined for that transport channel in the "Transport format set", the "Logical Channel List" is set to "All" or given as an "Explicit List" which contains this logical channel; or
  - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is not included in the same message, and for none of the RLC sizes defined in the transport format set stored for that transport channel, the "Logical Channel List" is set to "All" or given as an "Explicit List" which contains this logical channel:
    - 5> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if, as a result of the message this IE is included in, several radio bearers can be mapped onto the same transport channel, and the IE "Logical Channel Identity" was not included in the RB mapping info of any of those radio bearers for a multiplexing option on that transport channel or the same "Logical Channel Identity" was used more than once in the RB mapping info of those radio bearers for the multiplexing options on that transport channel:
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> delete all previously stored multiplexing options for that radio bearer;
- 1> store each new multiplexing option for that radio bearer;
- 1> select and configure the multiplexing options applicable for the transport channels to be used;
- 1> if the IE "Uplink transport channel type" is set to the value "RACH":
  - 2> refer the IE "RLC size index" to the RACH Transport Format Set of the first PRACH received in the IE "PRACH system information list" received in SIB5 or SIB6.
- 1> determine the sets of RLC sizes that apply to the logical channels used by that RB, based on the IEs "RLC size list" and/or the IEs "Logical Channel List" included in the applicable "Transport format set" (either the ones received in the same message or the ones stored if none were received); and
- 1> in case the selected multiplexing option is a multiplexing option on RACH:
  - 2> ignore the RLC size indexes that do not correspond to any RLC size within the Transport Format Set stored for RACH.
- 1> if RACH is the transport channel to be used on the uplink, if that RB has a multiplexing option on RACH and if it is using AM:
  - 2> apply the largest size amongst the ones derived according to the previous bullet for the RLC size (or RLC sizes in case the RB is realised using two logical channels) for the corresponding RLC entity.

Note: The IE "RB mapping info" is only included in IE "Predefined RB configurations" in system information; which is when used for Inter-RAT handover to UTRAN and there is no AM RLC size change involved in this case.

- 1> if that RB is using AM and the RLC size applicable to the logical channel transporting data PDUs is different from the one derived from the previously stored configuration:

- 2> re-establish the corresponding RLC entity;
- 2> configure the corresponding RLC entity with the new RLC size;
- 2> for each AM RLC radio bearer in the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS whose RLC size is changed; and
- 2> for each AM RLC signalling radio bearer in the CN domain as indicated in the IE "CN domain identity" in the variable LATEST\_CONFIGURED\_CN\_DOMAIN whose RLC size is changed:
- 3> if the IE "Status" in the variable CIPHERING\_STATUS of this CN domain is set to "Started":
  - ~~4> if this IE was included in system information:~~
    - ~~5> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" for this CN domain that will be included in the CELL\_UPDATE message that will be sent before the next transmission.~~
  - 4> if this IE was included in CELL UPDATE CONFIRM:
    - 5> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" included in the latest transmitted CELL UPDATE message for this CN domain.
  - 4> if this IE was included in a reconfiguration message:
    - 5> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" that will be included in the reconfiguration complete message for this CN domain.
- 1> if that RB is using UM:
  - 2> indicate the largest applicable RLC size to the corresponding RLC entity.
- 1> configure MAC multiplexing according to the selected multiplexing option (MAC multiplexing shall only be configured for a logical channel if the transport channel it is mapped on according to the selected multiplexing option is the same as the transport channel another logical channel is mapped on according to the multiplexing option selected for it);
  - 1> configure the MAC with the logical channel priorities according to selected multiplexing option;
  - 1> configure the MAC with the set of applicable RLC Sizes for each of the logical channels used for that RB;
  - 1> if there is no multiplexing option applicable for the transport channels to be used:
    - 2> set the variable INVALID\_CONFIGURATION to TRUE.
  - 1> if there is more than one multiplexing option applicable for the transport channels to be used:
    - 2> set the variable INVALID\_CONFIGURATION to TRUE.

In case IE "RLC info" includes IE "Downlink RLC mode " ("DL RLC logical channel info" is mandatory present) but IE "Number of downlink RLC logical channels" is absent in the corresponding IE "RB mapping info", the parameter values are exactly the same as for the corresponding UL logical channels. In case two multiplexing options are specified for the UL, the first options shall be used as default for the DL. As regards the IE "Channel type", the following rule should be applied to derive the DL channel type from the UL channel included in the IE:

Channel used in UL	DL channel type implied by "same as"
DCH	DCH
RACH	FACH
CPCH	FACH
USCH	DSCH

### 8.6.5.1 Transport Format Set

If the IE "Transport format set" is included, the UE shall:



- 1> if the transport format set is a RACH TFS received in System Information Block type 5 or 6, and CHOICE "Logical Channel List" has the value "Explicit List":
  - 2> ignore that System Information Block.
- 1> if the transport format set for a downlink transport channel is received in a System Information Block, and CHOICE "Logical Channel List" has a value different from 'ALL':
  - 2> ignore that System Information Block.
- 1> if the transport format set for a downlink transport channel is received in a message on a DCCH, and CHOICE "Logical Channel List" has a value different from 'ALL':
  - 2> keep the transport format set if this exists for that transport channel;
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the value of any IE "RB identity" (and "Logical Channel" for RBs using two UL logical channels) in the IE "Logical channel list" does not correspond to a logical channel indicated to be mapped onto this transport channel in any RB multiplexing option (either included in the same message or previously stored and not changed by this message); or
- 1> if the "Logical Channel List" for any of the RLC sizes defined for that transport channel is set to "Configured" while it is set to "All" or given as an "Explicit List" for any other RLC size; or
- 1> if the "Logical Channel List" for any of the RLC sizes defined for that transport channel is set to "All" and for any logical channel mapped to this transport channel, the value of the "RLC size list" (either provided in the IE "RB mapping info" if included in the same message, or stored) is not set to "Configured"; or
- 1> if the "Logical Channel List" for any of the RLC sizes defined for that transport channel is given as an "Explicit List" that contains a logical channel for which the value of the "RLC size list" (either provided in the IE "RB mapping info" if included in the same message, or stored) is not set to "Configured"; or
- 1> if the "Logical Channel List" for all the RLC sizes defined for that transport channel are given as "Explicit List" and if one of the logical channels mapped onto this transport channel is not included in any of those lists; or
- 1> if the "Logical Channel List" for the RLC sizes defined for that transport channel is set to "Configured" and for any logical channel mapped onto that transport channel, the value of the "RLC size list" (either provided in the IE "RB mapping info" if included in the same message, or stored) is also set to "Configured"; or
- 1> if the IE "Transport Format Set" was not received within the IE "PRACH system information list" and if the "Logical Channel List" for the RLC sizes defined for that transport channel is set to "Configured" and for any logical channel mapped onto that transport channel, the "RLC size list" (either provided in the IE "RB mapping info" if included in the same message, or stored) is given as an "Explicit List" that includes an "RLC size index" that does not correspond to any RLC size in this "Transport Format Set":
  - 2> keep the transport format set if this exists for that transport channel;
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the total number of configured transport formats for the transport channel exceeds maxTF:
  - 2> keep the transport format set if this exists for that transport channel;
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the IE "Transport format set" is considered as valid according to the rules above:
  - 2> remove a previously stored transport format set if this exists for that transport channel;
  - 2> store the transport format set for that transport channel;
  - 2> consider the first instance of the parameter *Number of TBs and TTI List* within the *Dynamic transport format information* to correspond to transport format 0 for this transport channel, the second to transport format 1 and so on;
  - 2> if the IE "Transport format Set" has the choice "Transport channel type" set to "Dedicated transport channel":

3> calculate the transport block size for all transport formats in the TFS using the following

$$\text{TB size} = \text{RLC size} + \text{MAC header size},$$

where:

- MAC header size is calculated according to [15] if MAC multiplexing is used. Otherwise it is 0 bits;
- 'RLC size' reflects the RLC PDU size.

2> if the IE "Transport format Set" has the choice "Transport channel type" set to "Common transport channel":

3> calculate the transport block size for all transport formats in the TFS using the following:

$$\text{TB size} = \text{RLC size}.$$

2> if the IE "Number of Transport blocks"  $\neq$  0 and IE "RLC size" = 0, no RLC PDU data exists but only parity bits exist for that transport format;

2> if the IE "Number of Transport blocks" = 0, neither RLC PDU neither data nor parity bits exist for that transport format;

2> configure the MAC with the new transport format set (with computed transport block sizes) for that transport channel;

2> if the RB multiplexing option for a RB mapped onto that transport channel (based on the stored RB multiplexing option) is not modified by this message:

3> determine the sets of RLC sizes that apply to the logical channels used by that RB, based on the IE "Logical Channel List" and/or the IE "RLC Size List" from the previously stored RB multiplexing option.

3> if the IE "Transport Format Set" was received within the IE "PRACH system information list":

4> ignore the RLC size indexes in the stored RB multiplexing option that do not correspond to any RLC size in the received Transport Format Set.

3> if the IE "Transport Format Set" was received within the IE "PRACH system information list", if that RB is using AM and if RACH is the transport channel to be used on the uplink:

4> apply the largest size amongst the ones derived according to the previous bullet for the RLC size (or RLC sizes in case the RB is realised using two logical channels) for the corresponding RLC entity.

3> if the IE "Transport Format Set" was not received within the IE "PRACH system information list", and if that RB is using AM and the set of RLC sizes applicable to the logical channel transferring data PDUs has more than one element:

4> set the variable INVALID\_CONFIGURATION to true.

3> if that RB is using AM and the RLC size applicable to the logical channel transporting data PDUs is different from the one derived from the previously stored configuration:

4> re-establish the corresponding RLC entity;

4> configure the corresponding RLC entity with the new RLC size;

4> for each AM RLC radio bearer in the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS whose RLC size is changed; and

4> for each AM RLC signalling radio bearer in the CN domain as indicated in the IE "CN domain identity" in the variable LATEST\_CONFIGURED\_CN\_DOMAIN whose RLC size is changed:

5> if this IE was included in system information and if the IE "Status" in variable CIPHERING\_STATUS of this CN domain is set to "Started":

6> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" for this CN domain that will be included in the CELL UPDATE message that will be sent before the next transmission.

- 5> if this IE was included in CELL UPDATE CONFIRM and if the IE "Status" in the variable CIPHERING\_STATUS of this CN domain is set to "Started":
- 6> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" included in the latest transmitted CELL UPDATE message for this CN domain.
- 5> if this IE was included in a reconfiguration message and if the IE "Status" in the variable CIPHERING\_STATUS of this CN domain is set to "Started":
- 6> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" that will be included in the reconfiguration complete message for this CN domain.
- 5> if this IE was included in ACTIVE SET UPDATE and if the IE "Status" in the variable CIPHERING\_STATUS of this CN domain is set to "Started":
- 6> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" that will be included in the ACTIVE SET UPDATE COMPLETE message for this CN domain.
- 3> if that RB is using UM:
- 4> indicate the largest applicable RLC size to the corresponding RLC entity.
- 3> configure MAC with the set of applicable RLC Sizes for each of the logical channels used for that RB.

For configuration restrictions on Blind Transport Format Detection, see [27].

## 10.2.1 ACTIVE SET UPDATE

NOTE: Only for FDD.

This message is used by UTRAN to add, replace or delete radio links in the active set of the UE.

RLC-SAP: AM or UM

Logical channel: DCCCH

Direction: UTRAN → UE

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message Type	MP		Message Type	
<b>UE information elements</b>				
RRC transaction identifier	MP		RRC transaction identifier 10.3.3.36	
Integrity check info	CH		Integrity check info 10.3.3.16	
<del>Integrity protection mode info</del>	<del>OP</del>		<del>Integrity protection mode info 10.3.3.19</del>	
<del>Ciphering mode info</del>	<del>OP</del>		<del>Ciphering mode info 10.3.3.5</del>	
Activation time	MD		Activation time 10.3.3.1	Default value is "now".
New U-RNTI	OP		U-RNTI 10.3.3.47	
<b>CN information elements</b>				
CN Information info	OP		CN	

Information Element/Group name	Need	Multi	Type and reference	Semantics description
			Information info 10.3.1.3	
<b>RB information elements</b>				
<del>Downlink counter synchronisation info</del>	OP			
<del>&gt;RB with PDCP information list</del>	OP	1 to <maxRBall RABs>		<del>This IE is needed for each RB having PDCP in the case of lossless SRNS relocation</del>
<del>&gt;&gt;RB with PDCP information</del>	MP		<del>RB with PDCP information 10.3.4.22</del>	
<b>Phy CH information elements</b>				
<b>Uplink radio resources</b>				
Maximum allowed UL TX power	MD		Maximum allowed UL TX power 10.3.6.39	Default value is the existing "maximum UL TX power.
<b>Downlink radio resources</b>				
Radio link addition information	OP	1 to <maxRL-1>		Radio link addition information required for each RL to add
>Radio link addition information	MP		Radio link addition information 10.3.6.68	
Radio link removal information	OP	1 to <maxRL>		Radio link removal information required for each RL to remove
>Radio link removal information	MP		Radio link removal information 10.3.6.69	
TX Diversity Mode	MD		TX Diversity Mode 10.3.6.86	Default value is the existing TX diversity mode.
SSDT information	OP		SSDT information 10.3.6.77	

## 10.2.2 ACTIVE SET UPDATE COMPLETE

NOTE: For FDD only.

This message is sent by UE when active set update has been completed.

RLC-SAP: AM

Logical channel: DCCH

Direction: UE→UTRAN

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message Type	MP		Message Type	
<b>UE information elements</b>				
RRC transaction identifier	MP		RRC transaction identifier 10.3.3.36	
Integrity check info	CH		Integrity check info	

Information Element/Group name	Need	Multi	Type and reference	Semantics description
<del>Uplink integrity protection activation-info</del>	<del>OP</del>		<del>10.3.3.16</del> <del>Integrity protection activation info</del> <del>10.3.3.17</del>	
<b>RB Information elements</b>				
<del>Radio bearer uplink ciphering activation time-info</del>	<del>OP</del>		<del>RB activation time info</del> <del>10.3.4.13</del>	
<del>Uplink counter synchronisation info</del>	<del>OP</del>			
<del>&gt;RB-with-PDCP-information-list</del>	<del>OP</del>	<del>1 to &lt;maxRBall RABs&gt;</del>		<del>This IE is needed for each RB having PDCP in the case of lossless SRNS relocation</del>
<del>&gt;&gt;RB-with-PDCP-information</del>	<del>MP</del>		<del>RB-with PDCP information</del> <del>10.3.4.22</del>	
<del>&gt;START-list</del>	<del>MP</del>	<del>1 to &lt;maxCNdomains&gt;</del>		<del>START [40] values for all CN domains.</del>
<del>&gt;&gt;CN-domain-identity</del>	<del>MP</del>		<del>CN domain identity</del> <del>10.3.1.1</del>	
<del>&gt;&gt;&gt;START</del>	<del>MP</del>		<del>START</del> <del>10.3.3.38</del>	<del>START value to be used in this CN domain.</del>

### 10.2.3 ACTIVE SET UPDATE FAILURE

NOTE: Only for FDD.

This message is sent by UE if the update of the active set has failed, e.g. because the radio link is not a part of the active set.

RLC-SAP: AM

Logical channel: DCCH

Direction: UE→UTRAN

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message Type	MP		Message Type	
<b>UE information elements</b>				
RRC transaction identifier	MP		RRC transaction identifier 10.3.3.36	
Integrity check info	CH		Integrity check info 10.3.3.16	
Failure cause	MP		Failure cause and error information 10.3.3.14	

### 10.3.3.5 Cipherng mode info

This information element contains the cipherng specific security mode control information.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Cipherng mode command	MP		Enumerated (start/restart, stop)	<del>The command "stop" is not used in this version of the protocol.</del>
Cipherng algorithm	<del>CV-</del> <del>notStop</del> MP		Cipherng algorithm 10.3.3.4	
Cipherng activation time for DPCH	OP		Activation time 10.3.3.1	Used for radio bearers mapped on RLC-TM. Only applicable if the UE is already in CELL_DCH state
Radio bearer downlink cipherng activation time info	OP		RB activation time info, 10.3.4.13	Used for radio bearers mapped on RLC-AM or RLC-UM

Condition	Explanation
<del>notStop</del>	<del>The IE is mandatory present if the IE "Cipherng mode command" has the value "start/restart", otherwise the IE is not needed in the message.</del>

### 10.3.3.10 RRC State Indicator

~~Indicates to a UE the RRC state to be entered.~~

Information Element/Group name	Need	Multi	Type and reference	Semantics description
RRC State indicator	MP		Enumerated( CELL_DCH, CELL_FACH ; CELL_PCH, URA_PCH)	

### 10.3.3.35a RRC State Indicator

Indicates to a UE the RRC state to be entered.

<u>Information Element/Group name</u>	<u>Need</u>	<u>Multi</u>	<u>Type and reference</u>	<u>Semantics description</u>
<u>RRC State indicator</u>	<u>MP</u>		<u>Enumerated(CELL_DCH, CELL_FACH, CELL_PCH, URA_PCH)</u>	

### 10.3.3.36 RRC transaction identifier

This IE contains an identification of the RRC procedure transaction local for the type of the message this IE was included within.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
RRC transaction identifier	MP		Integer (0..3)	

### 10.3.3.37 Security capability

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Ciphering algorithm capability	MP			
>UEA0	MP		Boolean	<del>The value TRUE means that an unciphered connection after the Security mode control procedure is accepted by the UE.</del>
>UEA1	MP		Boolean	<del>The value TRUE means that UEA1, Kasumi, is supported</del>
>Spare	MP	14	Boolean	Shall be set to FALSE by UEs complying with this version of the protocol.
Integrity protection algorithm capability	MP			
>UIA1	MP		Boolean	The value TRUE means that UIA1, Kasumi, is supported
>Spare	MP	15	Boolean	Shall be set to FALSE by UEs complying with this version of the protocol.

~~NOTE: The UE shall support at least one UEAx other than UEA0 and one UIAx.~~

### 10.3.3.38 START

There is a START value per CN domain. The START is used to initialise the 20 MSBs of all hyper frame numbers (MAC-d HFN, RLC UM HFN, RLC AM HFN, RRC HFN) for a CN domain.

Information Element/Group name	Need	Multi	Type and Reference	Semantics description
START	MP		Bit string (20)	The START [40] bits are numbered b0-b19, where b0 is the least significant bit.

```

-----
*****
--
-- ACTIVE SET UPDATE (FDD only)
--
*****

```

```
ActiveSetUpdate ::= CHOICE {
```

```

r3
  activeSetUpdate-r3      SEQUENCE {
    nonCriticalExtensions  ActiveSetUpdate-r3-IEs,
                          SEQUENCE {} OPTIONAL
  },
  later-than-r3          SEQUENCE {
    rrc-TransactionIdentifier  RRC-TransactionIdentifier,
    criticalExtensions          SEQUENCE {}
  }
}

ActiveSetUpdate-r3-IEs ::= SEQUENCE {
  -- User equipment IEs
  rrc-TransactionIdentifier  RRC-TransactionIdentifier,
  -- dummy and dummy2 are not used in this version of the specification, they should
  -- not be sent and if received they should be ignored.
  integrityProtectionModeInfodummy  IntegrityProtectionModeInfo  OPTIONAL,
  dummy2cipheringModeInfo          CipheringModeInfo  OPTIONAL,
  activationTime            ActivationTime  OPTIONAL,
  newU-RNTI                 U-RNTI  OPTIONAL,
  -- Core network IEs
  cn-InformationInfo        CN-InformationInfo  OPTIONAL,
  -- Radio bearer IEs
  -- dummy3 is not used in this version of the specification, it should
  -- not be sent and if received it should be ignored.
  dummy3dl-CounterSynchronisationInfo DL-CounterSynchronisationInfo  OPTIONAL,
  -- Physical channel IEs
  maxAllowedUL-TX-Power     MaxAllowedUL-TX-Power  OPTIONAL,
  rl-AdditionInformationList  RL-AdditionInformationList  OPTIONAL,
  rl-RemovalInformationList  RL-RemovalInformationList  OPTIONAL,
  tx-DiversityMode          TX-DiversityMode  OPTIONAL,
  ssdt-Information          SSDT-Information  OPTIONAL
}

-- *****
--
-- ACTIVE SET UPDATE COMPLETE (FDD only)
--
-- *****

ActiveSetUpdateComplete ::= SEQUENCE {
  -- User equipment IEs
  rrc-TransactionIdentifier  RRC-TransactionIdentifier,
  -- dummy is not used in this version of the specification, it should
  -- not be sent and if received it should be ignored.
  ul-IntegProtActivationInfodummy  IntegrityProtActivationInfo  OPTIONAL,
  -- Radio bearer IEs
  -- dummy2 and dummy3 are not used in this version of the specification, they should
  -- not be sent and if received they should be ignored.
  dummy2rb-UL-CiphActivationTimeInfo RB-ActivationTimeInfoList  OPTIONAL,
  dummy3ul-CounterSynchronisationInfo UL-CounterSynchronisationInfo  OPTIONAL,
  -- Extension mechanism for non- release99 information
  nonCriticalExtensions      SEQUENCE {} OPTIONAL
}

-- *****
--
-- ACTIVE SET UPDATE FAILURE (FDD only)
--
-- *****

ActiveSetUpdateFailure ::= SEQUENCE {
  -- User equipment IEs
  rrc-TransactionIdentifier  RRC-TransactionIdentifier,
  failureCause               FailureCauseWithProtErr,
  -- Extension mechanism for non- release99 information
  nonCriticalExtensions      SEQUENCE {} OPTIONAL
}

-- *****
--
-- *****
--
-- USER EQUIPMENT INFORMATION ELEMENTS (10.3.3)
--
-- *****

```



```

-- TABULAR : for ActivationTime, value 'now' always appears as default, and is encoded
-- by absence of the field
ActivationTime ::=                               INTEGER (0..255)

BackoffControlParams ::=                       SEQUENCE {
    n-AP-RetransMax                             N-AP-RetransMax,
    n-AccessFails                             N-AccessFails,
    nf-BO-NoAICH                             NF-BO-NoAICH,
    ns-BO-Busy                             NS-BO-Busy,
    nf-BO-AllBusy                             NF-BO-AllBusy,
    nf-BO-Mismatch                             NF-BO-Mismatch,
    t-CPCH                                     T-CPCH
}

C-RNTI ::=                                     BIT STRING (SIZE (16))

CapabilityUpdateRequirement ::=                SEQUENCE {
    ue-RadioCapabilityFDDUpdateRequirement     BOOLEAN,
    ue-RadioCapabilityTDDUpdateRequirement     BOOLEAN,
    systemSpecificCapUpdateReqList            SystemSpecificCapUpdateReqList     OPTIONAL
}

CellUpdateCause ::=                           ENUMERATED {
    cellReselection,
    periodicalCellUpdate,
    uplinkDataTransmission,
    utran-pagingResponse,
    re-enteredServiceArea,
    radiolinkFailure,
    rlc-unrecoverableError,
    spare1 }

ChipRateCapability ::=                        ENUMERATED {
    mcps3-84, mcps1-28 }

CipheringAlgorithm ::=                       ENUMERATED {
    uea0, uea1 }

CipheringModeCommand ::=                    CHOICE {
    startRestart                               CipheringAlgorithm,
    dummystopCiphering                         NULL
}

CipheringModeInfo ::=                       SEQUENCE {
    -- TABULAR: The ciphering algorithm is included in the CipheringModeCommand.
    cipheringModeCommand                       CipheringModeCommand,
    activationTimeForDPCH                       ActivationTime                               OPTIONAL,
    rb-DL-CiphActivationTimeInfo                RB-ActivationTimeInfoList                   OPTIONAL
}

CN-DRX-CycleLengthCoefficient ::=           INTEGER (6..9)

```

## 11.5 RRC information between network nodes

```
Internode-definitions DEFINITIONS AUTOMATIC TAGS ::=
```

```
BEGIN
```

```
IMPORTS
```

```

    HandoverToUTRANCommand,
    MeasurementReport,
    PhysicalChannelReconfiguration,
    RadioBearerReconfiguration,
    RadioBearerRelease,
    RadioBearerSetup,
    RRC-FailureInfo,
    TransportChannelReconfiguration

```

```
FROM PDU-definitions
```

```
-- Core Network IEs :
```

```

    CN-DomainIdentity,
    CN-DomainInformationList,
    CN-DRX-CycleLengthCoefficient,
    NAS-SystemInformationGSM-MAP,

```

```

-- UTRAN Mobility IEs :
  CellIdentity,
  URA-Identity,
-- User Equipment IEs :
  C-RNTI,
  DL-PhysChCapabilityFDD-v380ext,
  FailureCauseWithProtErr,
  RRC-MessageSequenceNumber,
  STARTList,
  STARTSingle,
  START-Value,
  U-RNTI,
  UE-RadioAccessCapability,
  UE-RadioAccessCapability-v370ext,
  UE-RadioAccessCapability-v380ext,
  UE-RadioAccessCapability-v3a0ext,
-- Radio Bearer IEs :
  PredefinedConfigStatusList,
  PredefinedConfigValueTag,
  RAB-InformationSetupList,
  RB-Identity,
  SRB-InformationSetupList,
-- Transport Channel IEs :
  CPCH-SetID,
  DL-CommonTransChInfo,
  DL-AddReconfTransChInfoList,
  DRAC-StaticInformationList,
  UL-CommonTransChInfo,
  UL-AddReconfTransChInfoList,
-- Measurement IEs :
  MeasurementIdentity,
  MeasurementReportingMode,
  MeasurementType,
  AdditionalMeasurementID-List,
  PositionEstimate,
-- Other IEs :
  InterRAT-UE-RadioAccessCapabilityList
FROM InformationElements

```

```

  maxCNdomains,
  maxNoOfMeas,
  maxRB,
  maxSRBsetup
FROM Constant-definitions;

```

<Cut until the next modified version>

```

-- *****
--
-- SRNC Relocation information
--
-- *****

```

```

SRNC-RelocationInfo ::= CHOICE {
  r3 SEQUENCE {
    sRNC-RelocationInfo-r3 SRNC-RelocationInfo-r3-IEs,
    v380NonCriticalExtensions SEQUENCE {
      sRNC-RelocationInfo-v380ext SRNC-RelocationInfo-v380ext-IEs,
      -- Reserved for future non critical extension
      v390NonCriticalExtensions SEQUENCE {
        sRNC-RelocationInfo-v390ext SRNC-RelocationInfo-v390ext-IEs,
        v3a0NonCriticalExtensions SEQUENCE {
          sRNC-RelocationInfo-v3a0ext SRNC-RelocationInfo-v3a0ext-IEs,
          v3b0NonCriticalExtensions SEQUENCE {
            sRNC-RelocationInfo-v3b0ext SRNC-RelocationInfo-v3b0ext-IEs,
            -- Reserved for future non critical extension
            nonCriticalExtensions SEQUENCE {} OPTIONAL
          }
          Reserved for future non critical extension
          nonCriticalExtensions SEQUENCE {} OPTIONAL
        }
      }
    }
  }
  criticalExtensions SEQUENCE {}
}

```

```

SRNC-RelocationInfo-r3-IEs ::= SEQUENCE {
  -- Non-RRC IEs
  stateOfRRC                StateOfRRC,
  stateOfRRC-Procedure      StateOfRRC-Procedure,
  -- Ciphering related information IEs
  -- If the extension v380 is included use the extension for the ciphering status per CN domain
  cipheringStatus           CipheringStatus,
  calculationTimeForCiphering CalculationTimeForCiphering OPTIONAL,
  cipheringInfoPerRB-List  CipheringInfoPerRB-List   OPTIONAL,
  count-C-List             COUNT-C-List           OPTIONAL,
  integrityProtectionStatus IntegrityProtectionStatus,
  srb-SpecificIntegrityProtInfo SRB-SpecificIntegrityProtInfoList,
  implementationSpecificParams ImplementationSpecificParams OPTIONAL,
  -- User equipment IEs
  u-RNTI                   U-RNTI,
  c-RNTI                   C-RNTI           OPTIONAL,
  ue-RadioAccessCapability UE-RadioAccessCapability,
  ue-Positioning-LastKnownPos UE-Positioning-LastKnownPos OPTIONAL,
  -- Other IEs
  ue-RATSpecificCapability InterRAT-UE-RadioAccessCapabilityList OPTIONAL,
  -- UTRAN mobility IEs
  ura-Identity             URA-Identity           OPTIONAL,
  -- Core network IEs
  cn-CommonGSM-MAP-NAS-SysInfo NAS-SystemInformationGSM-MAP,
  cn-DomainInformationList  CN-DomainInformationList   OPTIONAL,
  -- Measurement IEs
  ongoingMeasRepList       OngoingMeasRepList     OPTIONAL,
  -- Radio bearer IEs
  predefinedConfigStatusList PredefinedConfigStatusList,
  srb-InformationList      SRB-InformationSetupList,
  rab-InformationList      RAB-InformationSetupList   OPTIONAL,
  -- Transport channel IEs
  ul-CommonTransChInfo    UL-CommonTransChInfo     OPTIONAL,
  ul-TransChInfoList      UL-AddReconfTransChInfoList   OPTIONAL,
  modeSpecificInfo        CHOICE {
    fdd                    SEQUENCE {
      cpch-SetID           CPCH-SetID           OPTIONAL,
      transChDRAC-Info     DRAC-StaticInformationList OPTIONAL
    },
    tdd                    NULL
  },
  dl-CommonTransChInfo    DL-CommonTransChInfo     OPTIONAL,
  dl-TransChInfoList      DL-AddReconfTransChInfoList   OPTIONAL,
  -- Measurement report
  measurementReport       MeasurementReport     OPTIONAL
}

SRNC-RelocationInfo-v380ext-IEs ::= SEQUENCE {
  -- Ciphering related information IEs
  cn-DomainIdentity       CN-DomainIdentity,
  cipheringStatusList     CipheringStatusList
}

SRNC-RelocationInfo-v390ext-IEs ::= SEQUENCE {
  cn-DomainInformationList-v390ext CN-DomainInformationList-v390ext OPTIONAL,
  ue-RadioAccessCapability-v370ext UE-RadioAccessCapability-v370ext OPTIONAL,
  ue-RadioAccessCapability-v380ext UE-RadioAccessCapability-v380ext OPTIONAL,
  dl-PhysChCapabilityFDD-v380ext   DL-PhysChCapabilityFDD-v380ext,
  failureCauseWithProtErr         FailureCauseWithProtErr     OPTIONAL
}

SRNC-RelocationInfo-v3a0ext-IEs ::= SEQUENCE {
  cipheringInfoForSRB1-v3a0ext CipheringInfoPerRB-List-v3a0ext,
  ue-RadioAccessCapability-v3a0ext UE-RadioAccessCapability-v3a0ext OPTIONAL,
  -- cn-domain identity for IE startValueForCiphering-v3a0ext is specified
  -- in subsequent extension (SRNC-RelocationInfo-v3b0ext-IEs)
  startValueForCiphering-v3a0ext START-Value
}

SRNC-RelocationInfo-v3b0ext-IEs ::= SEQUENCE {
  -- cn-domain identity for IE startValueForCiphering-v3a0ext included in previous extension
  cn-DomainIdentity CN-DomainIdentity,
  -- the remaining start values are contained in IE startValueForCiphering-v3b0ext
  startValueForCiphering-v3b0ext STARTList2 OPTIONAL
}

STARTList2 ::= SEQUENCE (SIZE (2..maxCNdomains)) OF

```

STARTSingle

```

CipheringInfoPerRB-List-v3a0ext ::= SEQUENCE {
    dl-UM-SN                BIT STRING (SIZE (7))
}

CipheringStatusList ::=
    SEQUENCE (SIZE (1..maxCNdomains)) OF
        CipheringStatusCNdomain

CipheringStatusCNdomain ::=
    SEQUENCE {
        cn-DomainIdentity    CN-DomainIdentity,
        cipheringStatus      CipheringStatus
    }

-- IE definitions

CalculationTimeForCiphering ::=
    SEQUENCE {
        cell-Id              CellIdentity,
        sfn                  INTEGER (0..4095)
    }

CipheringInfoPerRB ::=
    SEQUENCE {
        dl-HFN                BIT STRING (SIZE (20..25)),
        ul-HFN                BIT STRING (SIZE (20..25))
    }

-- TABULAR: CipheringInfoPerRB-List, multiplicity value numberOfRadioBearers
-- has been replaced with maxRB.
CipheringInfoPerRB-List ::=
    SEQUENCE (SIZE (1..maxRB)) OF
        CipheringInfoPerRB

CipheringStatus ::=
    ENUMERATED {
        started, notStarted }

CN-DomainInformation-v390ext ::=
    SEQUENCE {
        cn-DRX-CycleLengthCoeff    CN-DRX-CycleLengthCoefficient
    }

CN-DomainInformationList-v390ext ::=
    SEQUENCE (SIZE (1..maxCNdomains)) OF
        CN-DomainInformation-v390ext

COUNT-C-List ::=
    SEQUENCE (SIZE (1..maxCNdomains)) OF
        COUNT-CSingle

COUNT-CSingle ::=
    SEQUENCE {
        cn-DomainIdentity    CN-DomainIdentity,
        count-C              BIT STRING (SIZE (32))
    }

ImplementationSpecificParams ::=
    BIT STRING (SIZE (1..512))

IntegrityProtectionStatus ::=
    ENUMERATED {
        started, notStarted }

MeasurementCommandWithType ::=
    CHOICE {
        setup                MeasurementType,
        modify               NULL,
        release               NULL
    }

OngoingMeasRep ::=
    SEQUENCE {
        measurementIdentity    MeasurementIdentity,
        -- TABULAR: The CHOICE Measurement in the tabular description is included
        -- in MeasurementCommandWithType
        measurementCommandWithType    MeasurementCommandWithType,
        measurementReportingMode      MeasurementReportingMode                OPTIONAL,
        additionalMeasurementID-List   AdditionalMeasurementID-List          OPTIONAL
    }

OngoingMeasRepList ::=
    SEQUENCE (SIZE (1..maxNoOfMeas)) OF
        OngoingMeasRep

SRB-SpecificIntegrityProtInfo ::=
    SEQUENCE {
        ul-RRC-HFN            BIT STRING (SIZE (28)),
        dl-RRC-HFN            BIT STRING (SIZE (28)),
        ul-RRC-SequenceNumber RRC-MessageSequenceNumber,
        dl-RRC-SequenceNumber RRC-MessageSequenceNumber
    }

```

```

}

SRB-SpecificIntegrityProtInfoList ::= SEQUENCE (SIZE (4..maxSRBsetup)) OF
    SRB-SpecificIntegrityProtInfo

StateOfRRC ::=
    ENUMERATED {
        cell-DCH, cell-FACH,
        cell-PCH, ura-PCH }

StateOfRRC-Procedure ::=
    ENUMERATED {
        awaitNoRRC-Message,
        awaitRRC-ConnectionRe-establishmentComplete,
        awaitRB-SetupComplete,
        awaitRB-ReconfigurationComplete,
        awaitTransportCH-ReconfigurationComplete,
        awaitPhysicalCH-ReconfigurationComplete,
        awaitActiveSetUpdateComplete,
        awaitHandoverComplete,
        sendCellUpdateConfirm,
        sendUraUpdateConfirm,
        sendRrcConnectionReestablishment,
        otherStates
    }

UE-Positioning-LastKnownPos ::=
    SEQUENCE {
        sfn                INTEGER (0..4095),
        cell-id            CellIdentity,
        positionEstimate   PositionEstimate
    }

END
    
```

### 14.12.4.2 SRNS RELOCATION INFO

This RRC message is sent between network nodes when preparing for an SRNS relocation.

Direction: source RAT→target RNC

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
<b>Non RRC IEs</b>				
>State of RRC	MP		RRC state indicator, 10.3.3.10	
>State of RRC procedure	MP		Enumerated (await no RRC message, Complete, await RB Setup Complete, await RB Reconfiguration Complete, await RB Release Complete, await Transport CH Reconfiguration Complete, await Physical CH Reconfiguration	

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
			ion Complete, await Active Set Update Complete, await Handover Complete, send Cell Update Confirm, send URA Update Confirm, , others)	
<b>Ciphering related information</b>				
>Ciphering status for each CN domain	MP	<1 to maxCNDo mains>		
>>CN domain identity	MP		CN domain identity 10.3.1.1	
>>Ciphering status	MP		Enumerated( Not started, Started)	
>>START	MP		START 10.3.3.38	START value to be used in this CN domain.
>Latest configured CN domain	MP		CN domain identity 10.3.1.1	Value contained in the variable of the same name.
>Calculation time for ciphering related information	CV- <i>Ciphering</i>			Time when the ciphering information of the message were calculated, relative to a cell of the target RNC
>>Cell Identity	MP		Cell Identity 10.3.2.2	Identity of one of the cells under the target RNC and included in the active set of the current call
>>SFN	MP		Integer(0..4095)	
>COUNT-C list	CV- <i>Ciphering</i>	1 to <maxCNdo mains>		COUNT-C values for radio bearers using transparent mode RLC
>>CN domain identity	MP		CN domain identity 10.3.1.1	
>>COUNT-C	MP		Bit string(32)	
>Ciphering info per radio bearer	OP	1 to <maxRB>		For signalling radio bearers this IE is mandatory.
>>RB identity	MP		RB identity 10.3.4.16	
>>Downlink HFN	MP		Bit string(20..25)	This IE is either RLC AM HFN (20 bits) or RLC UM HFN (25 bits)
>>Downlink SN	CV- <i>SRB1</i>		Bit String(7)	VT(US) of RLC UM
>>Uplink HFN	MP		Bit string(20..25)	This IE is either RLC AM HFN (20 bits) or RLC UM HFN (25 bits)
<b>Integrity protection related information</b>				
>Integrity protection status	MP		Enumerated( Not started, Started)	
>Signalling radio bearer specific integrity protection information	CV- <i>IP</i>	4 to <maxSRBs		

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
		etup>		
>>Uplink RRC HFN	MP		Bit string (28)	
>>Downlink RRC HFN	MP		Bit string (28)	
>>Uplink RRC Message sequence number	MP		Integer (0..15)	
>>Downlink RRC Message sequence number	MP		Integer (0..15)	
>Implementation specific parameters	OP		Bit string (1..512)	
<b>RRC IEs</b>				
<b>UE Information elements</b>				
>U-RNTI	MP		U-RNTI 10.3.3.47	
>C-RNTI	OP		C-RNTI 10.3.3.8	
>UE radio access Capability	MP		UE radio access capability 10.3.3.42	
>UE radio access capability extension	OP		UE radio access capability extension 10.3.3.42a	
>Last known UE position	OP			
>>SFN	MP		Integer (0..4095)	Time when position was estimated
>>Cell ID	MP		Cell identity; 10.3.2.2	Indicates the cell, the SFN is valid for.
>>CHOICE <i>Position estimate</i>	MP			
>>>Ellipsoid Point			Ellipsoid Point; 10.3.8.4a	
>>>Ellipsoid point with uncertainty circle			Ellipsoid point with uncertainty circle 10.3.8.4d	
>>>Ellipsoid point with uncertainty ellipse			Ellipsoid point with uncertainty ellipse 10.3.8.4e	
>>>Ellipsoid point with altitude			Ellipsoid point with altitude 10.3.8.4b	
>>>Ellipsoid point with altitude and uncertainty ellipsoid			Ellipsoid point with altitude and uncertainty ellipsoid 10.3.8.4c	
<b>Other Information elements</b>				
>UE system specific capability	OP	1 to <maxSystemCapability>		
>>Inter-RAT UE radio access capability	MP		Inter-RAT UE radio access capability 10.3.8.7	

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
<b>UTRAN Mobility Information elements</b>				
>URA Identifier	OP		URA identity 10.3.2.6	
<b>CN Information Elements</b>				
>CN common GSM-MAP NAS system information	MP		NAS system information (GSM-MAP) 10.3.1.9	
>CN domain related information	OP	1 to <MaxCNdomains>		CN related information to be provided for each CN domain
>>CN domain identity	MP			
>>CN domain specific GSM-MAP NAS system info	MP		NAS system information (GSM-MAP) 10.3.1.9	
>>CN domain specific DRX cycle length coefficient	MP		CN domain specific DRX cycle length coefficient, 10.3.3.6	
<b>Measurement Related Information elements</b>				
>For each ongoing measurement reporting	OP	1 to <MaxNoOf Meas>		
>>Measurement Identity	MP		Measurement identity 10.3.7.48	
>>Measurement Command	MP		Measurement command 10.3.7.46	
>>Measurement Type	<i>CV-Setup</i>		Measurement type 10.3.7.50	
>>Measurement Reporting Mode	OP		Measurement reporting mode 10.3.7.49	
>>Additional Measurements list	OP		Additional measurements list 10.3.7.1	
>>CHOICE <i>Measurement</i>	OP			
>>>Intra-frequency				
>>>>Intra-frequency cell info	OP		Intra-frequency cell info list 10.3.7.33	
>>>>Intra-frequency measurement quantity	OP		Intra-frequency measurement quantity 10.3.7.38	
>>>>Intra-frequency reporting quantity	OP		Intra-frequency reporting quantity 10.3.7.41	
>>>>Reporting cell status	OP		Reporting cell status 10.3.7.61	
>>>>Measurement validity	OP		Measurement validity	



Information Element/Group Name	Need	Multi	Type and reference	Semantics description
>>>>CHOICE <i>report criteria</i>	OP		10.3.7.51	
>>>>>Intra-frequency measurement reporting criteria			Intra-frequency measurement reporting criteria 10.3.7.39	
>>>>>Periodical reporting			Periodical reporting criteria 10.3.7.53	
>>>>>No reporting			NULL	
>>>Inter-frequency				
>>>>Inter-frequency cell info	OP		Inter-frequency cell info list 10.3.7.13	
>>>>Inter-frequency measurement quantity	OP		Inter-frequency measurement quantity 10.3.7.18	
>>>>Inter-frequency reporting quantity	OP		Inter-frequency reporting quantity 10.3.7.21	
>>>>Reporting cell status	OP		Reporting cell status 10.3.7.61	
>>>>Measurement validity	OP		Measurement validity 10.3.7.51	
>>>>CHOICE <i>report criteria</i>	OP			
>>>>>Inter-frequency measurement reporting criteria			Inter-frequency measurement reporting criteria 10.3.7.19	
>>>>>Periodical reporting			Periodical reporting criteria 10.3.7.53	
>>>>>No reporting			NULL	
>>>Inter-RAT				
>>>>Inter-RAT cell info	OP		Inter-RAT cell info list 10.3.7.23	
>>>>Inter-RAT measurement quantity	OP		Inter-RAT measurement quantity 10.3.7.29	
>>>>Inter-RAT reporting quantity	OP		Inter-RAT reporting quantity 10.3.7.32	
>>>>Reporting cell status	OP		Reporting cell status 10.3.7.61	
>>>>Measurement validity	OP		Measurement validity 10.3.7.51	
>>>>CHOICE <i>report criteria</i>	OP			

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
>>>>Inter-RAT measurement reporting criteria			Inter-RAT measurement reporting criteria 10.3.7.30	
>>>>Periodical reporting			Periodical reporting criteria 10.3.7.53	
>>>>No reporting			NULL	
>>>Traffic Volume				
>>>>Traffic volume measurement Object	OP		Traffic volume measurement object 10.3.7.70	
>>>>Traffic volume measurement quantity	OP		Traffic volume measurement quantity 10.3.7.71	
>>>>Traffic volume reporting quantity	OP		Traffic volume reporting quantity 10.3.7.74	
>>>>CHOICE <i>report criteria</i>	OP			
>>>>>Traffic volume measurement reporting criteria			Traffic volume measurement reporting criteria 10.3.7.72	
>>>>>Periodical reporting			Periodical reporting criteria 10.3.7.53	
>>>>>No reporting			NULL	
>>>Quality				
>>>>Quality measurement Object	OP		Quality measurement object	
>>>>CHOICE <i>report criteria</i>	OP			
>>>>>Quality measurement reporting criteria			Quality measurement reporting criteria 10.3.7.58	
>>>>>Periodical reporting			Periodical reporting criteria 10.3.7.53	
>>>>>No reporting			NULL	
>>>UE internal				
>>>>UE internal measurement quantity	OP		UE internal measurement quantity 10.3.7.79	
>>>>UE internal reporting quantity	OP		UE internal reporting quantity 10.3.7.82	
>>>>CHOICE <i>report criteria</i>	OP			
>>>>>UE internal measurement reporting criteria			UE internal measurement	

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
			t reporting criteria 10.3.7.80	
>>>>Periodical reporting			Periodical reporting criteria 10.3.7.53	
>>>>No reporting			NULL	
>>>UE positioning				
>>>>LCS reporting quantity	OP		LCS reporting quantity 10.3.7.111	
>>>>CHOICE <i>report criteria</i>	OP			
>>>>>LCS reporting criteria			LCS reporting criteria 10.3.7.110	
>>>>>Periodical reporting			Periodical reporting criteria 10.3.7.53	
>>>>>No reporting				
<b>Radio Bearer Information Elements</b>				
>Pre-defined configuration status information	OP		Pre-defined configuration status information 14.13.2.3	
>Signalling RB information list	MP	1 to <maxSRBs etup>		For each signalling radio bearer
>>Signalling RB information	MP		Signalling RB information to setup 10.3.4.24	
>RAB information list	OP	1 to <maxRABs etup>		Information for each RAB
>>RAB information	MP		RAB information to setup 10.3.4.10	
<b>Transport Channel Information Elements</b>				
<b>Uplink transport channels</b>				
>UL Transport channel information common for all transport channels	OP		UL Transport channel information common for all transport channels 10.3.5.24	
>UL transport channel information list	OP	1 to <MaxTrCH >		
>>UL transport channel information	MP		Added or reconfigured UL TrCH information 10.3.5.2	
>CHOICE <i>mode</i>	OP			
>>FDD				

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
>>>CPCH set ID	OP		CPCH set ID 10.3.5.5	
>>>Transport channel information for DRAC list	OP	1 to <MaxTrCH >		
>>>>DRAC static information	MP		DRAC static information 10.3.5.7	
>>TDD				(no data)
<b>Downlink transport channels</b>				
>DL Transport channel information common for all transport channels	OP		DL Transport channel information common for all transport channels 10.3.5.6	
>DL transport channel information list	OP	1 to <MaxTrCH >		
>>DL transport channel information	MP		Added or reconfigured DL TrCH information 10.3.5.1	
>Measurement report	OP		MEASUREMENT REPORT 10.2.17	
<b>Other Information elements</b>				
Failure cause	OP		Failure cause 10.3.3.13	Diagnostics information related to an earlier SRNC Relocation request (see NOTE 2 in 14.12.0a)
Protocol error information	CV-ProtErr		Protocol error information 10.3.8.12	

Multi Bound	Explanation
MaxNoOfMeas	Maximum number of active measurements, upper limit 16

Condition	Explanation
<i>Setup</i>	The IE is mandatory present when the IE Measurement command has the value "Setup", otherwise the IE is not needed.
<i>Ciphering</i>	The IE is mandatory present when the IE Ciphering Status has the value "started" and the ciphering counters need not be reinitialised, otherwise the IE is not needed.
<i>IP</i>	The IE is mandatory present when the IE Integrity protection status has the value "started" and the integrity protection counters need not be reinitialised, otherwise the IE is not needed.
<i>ProtErr</i>	This IE is mandatory present if the IE "Protocol error indicator" is included and has the value "TRUE". Otherwise it is not needed.
<i>SRB1</i>	The IE is mandatory present for RB1. Otherwise it is not needed.

## Annex A (informative): USIM parameters

### A.1 Introduction

This annex contains recommendations about the RRC parameters to be stored in the USIM.

### A.2 Ciphering information

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Cipher key for each CN domain	MP	<1 to maxCNDomain>		Cipher key is described in [40].
>Old CK	MP		Bit string (128)	
>New CK	MP		Bit string (128)	
Integrity key for each CN domain	MP	<1 to maxCNDomain>		Integrity key is described in [40].
>Old IK	MP		Bit string (128)	
>New IK	MP		Bit string (128)	
THRESHOLD	MP		Bit string (20)	
START value for each CN domain	MP	<1 to maxCNDomain>		START value is described in [40].
>Old START	MP		Bit string (20)	
>New START	MP		Bit string (20)	
KSI, Key set identifier for each CN domain	MP	<1 to maxCNDomain>		Key set identifier is described in [40].
>Old KSI	MP		Bit string (3)	
>New KSI	MP		Bit string (3)	

## A.3 Frequency information

Neighbour cell list.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
FDD cell list	OP	<1 to maxFDDFr eqList>		
>UARFCN uplink (Nu)	OP		Integer(0..16383)	[21] If IE not present, default duplex distance of 190 MHz shall be used.
>UARFCN downlink (Nd)	MP		Integer(0 .. 16383)	[21]
>Primary scrambling code	OP	<1 to maxFDDFr eqCellList>	Primary CPICH info 10.3.6.60	
TDD cell list	OP	<1 to maxTDDFr eqList>		
>UARFCN (Nt)	MP		Integer(0 .. 16383)	[22]
>Cell parameters ID	OP	<1 to maxTDDFr eqCellList>	Integer (0..127)	The Cell parameters ID is described in [32].
GSM Neighbour cell list	OP			
>GSM neighbour cell info	MP	<1 to maxGSMCellList>		
>>BSIC	MP			
>>BCCH ARFCN	MP			

## A.4 Multiplicity values and type constraint values

Constant	Explanation	Value
<b>Ciphering information</b>		
maxCNDomains	Maximum number of CN domains	4
<b>Frequency information</b>		
maxFDDFr eqList	Maximum number of FDD carrier frequencies to be stored in USIM	4
maxTDDFr eqList	Maximum number of TDD carrier frequencies to be stored in USIM	4
maxFDDFr eqCellList	Maximum number of neighbouring FDD cells on one carrier to be stored in USIM	32
maxTDDFr eqCellList	Maximum number of neighbouring TDD cells on one carrier to be stored in USIM	32
maxGSMCellList	Maximum number of GSM cells to be stored in USIM	32

## CHANGE REQUEST

⌘ **25.331 CR 1491** ⌘ rev **-** ⌘ Current version: **4.4.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

**Title:** ⌘ Corrections to Security procedure on Missing integrity protection reset on relocation and counter check response actions for asymmetric bearer configurations

**Source:** ⌘ TSG-RAN WG2

**Work item code:** ⌘ TEI

**Date:** ⌘ May 13, 2002

**Category:** ⌘ **A**

**Release:** ⌘ REL-4

Use one of the following categories:

Use one of the following releases:

- F** (correction)
- A** (corresponds to a correction in an earlier release)
- B** (addition of feature),
- C** (functional modification of feature)
- D** (editorial modification)

- 2** (GSM Phase 2)
- R96** (Release 1996)
- R97** (Release 1997)
- R98** (Release 1998)
- R99** (Release 1999)
- REL-4** (Release 4)
- REL-5** (Release 5)

Detailed explanations of the above categories can be found in 3GPP [TR 21.900](#).

- Reason for change:** ⌘
1. It is not clear if SECURITY MODE COMMAND can change ciphering/integrity protection algorithms.
  2. It is not clear if SECURITY MODE COMMAND can be received with "modify" command for integrity protection for a CN domain for which integrity protection has been already configured, if new keys have not been received.
  3. In the COUNTER CHECK procedure it is not clear how the UE should set the COUNT-C values for a radio bearer which is configured only in one direction or is set to RLC-TM mode in one direction and UM in the other.
  4. ACTIVE SET UPDATE cannot be used to trigger actions at the UE for a SRNS Relocation.
  5. UE actions in case of pending activation times for integrity protection following SRNS Relocation are missing.
  6. UE actions in case of previously received new keys not having yet been activated due to activation times not elapsed at the time of SRNS Relocation are missing.
  7. Mis-alignment between Tabular and ASN.1. ASN.1 does not permit the transfer of START for every domain in the Relocation container between source and target as required..
  8. It is incorrectly stated that a R99 UE shall support any one of UIAx integrity protection algorithms when in fact UIA1 shall be supported.
  9. It is not clear in case of START calculation if "non-ciphered" radio bearers refers also to RBs with ciphering algorithm set to UEA0.
  10. It is incorrectly suggested in Annex a that the USIM stores both the new and old keys as well as the old and new START and KSI values. Only one value - the latest - is stored in the USIM.
  11. The ASN.1 still permits the ciphering mode command to be set to "stop".
  12. It is not stated that the UE shall check to see if a new FRESH value was received

before performing the integrity check on the message.

- 13. 10.3.3.10 is not correctly placed in the Tabular according to alphabetical order.
- 14. In 8.6.4.8 it is stated that if the IE "RB Mapping Info" is included in system information and there is a AM RLC size change the UE shall " *set the HFN values for the corresponding RLC entity equal to the value of the IE "START" for this CN domain that will be included in the CELL UPDATE message that will be sent before the next transmission.* " However since the CELL UPDATE will be sent only in the future it is not possible for the UE to set the START value in advance.

**Summary of change: ☞**

- 1. It is clarified that UTRAN should not change ciphering/integrity protection algorithm using the SECURITY MODE COMMAND procedure.
- 2. It is clarified that UTRAN should not transmit SECURITY MODE COMMAND with "modify" command for integrity protection for a CN domain for which integrity protection has been already configured, if new keys have not been received for that domain.
- 3. It is specified that UE shall set an unspecified value for the COUNT-C for the direction of the radio bearer that is either not configured or is set to RLC-TM.
- 4. All security related procedure text in the ACTIVE SET UPDATE procedure and procedure related to ACTIVE SET UPDATE and security in other procedures is deleted. The tabular and ASN.1 have been appropriately updated.
- 5. It is specified that the UE shall over-write any pending activation times for IP.
- 6. It is specified that UE shall use the pending new keys.
- 7. The ASN.1 is corrected to allow for START value for all domains to be transmitted.
- 8. The NOTE specifying UE support of UEAX and UIAX is deleted. A corresponding correction is made in 25.306.
- 9. It is clarified that "non ciphered" refers to ciphering status set to "not started" and RBs configured with ciphering algorithm UEA0 shall contribute to the START value calculation.
- 10. The suggestion that old values for START, Keys, etc. are stored in the USIM has been deleted.
- 11. The ASN.1 and tabular have been appropriately updated to state that stop is never to be used in any version of the protocol.
- 12. It is stated that if the IE "DL Counter Synchronisation Info" or "New URNTI" in case of RADIO BEARER RECONFIGURATION is present then the UE shall apply the FRESH value in the received message before performing the integrity check.
- 13. RRC State Indicator has been moved in the Tabular per the appropriate alphabetical order.
- 14. The requirement corresponding to the START value transmission in case of AM RLC size change due to system information IE "RB Mapping Info" is deleted since this occurs only in the case of Inter-RAT Handover to UTRAN and in this case there is no AM RLC size change.

**Consequences if not approved:**

- ☞ Incomplete specification related to security procedures causing uncertain UE behavior. Uncertain UE behavior in case of SRNS relocation.



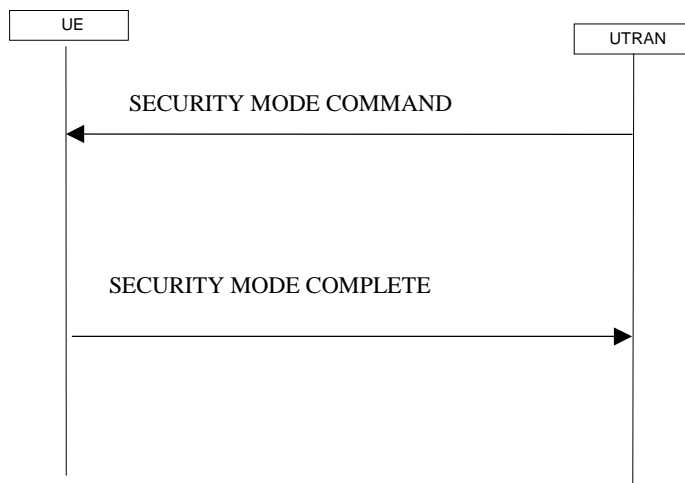
<b>Clauses affected:</b>	⌘	8.1.12.2.1, 8.1.12.2.2, 8.1.15.3, 8.3.4.3, 8.3.4.5a, 8.5.9, 8.5.10, 8.6.3.4, 8.6.3.5, 8.6.4.8, 10.2.1, 10.2.2, 10.3.3.5, 10.3.3.10, 10.3.3.35a (new), 10.3.3.37, 11, A.2	
<b>Other specs</b>	⌘	<input checked="" type="checkbox"/>	Other core specifications
<b>affected:</b>		<input type="checkbox"/>	Test specifications
		<input type="checkbox"/>	O&M Specifications
<b>Other comments:</b>	⌘		

**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.

## 8.1.12 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 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.

#### 8.1.12.2.2 Integrity protection configuration change

To start or modify integrity protection, UTRAN sends a SECURITY MODE COMMAND message on the downlink DCCH in AM RLC using the new integrity protection configuration. [UTRAN should not "modify" integrity protection for a CN domain to which a SECURITY MODE COMMAND configuring integrity protection has been previously sent for an ongoing signalling connection unless the application of new integrity keys needs to be signalled to the UE. UTRAN should not transmit a SECURITY MODE COMMAND to signal a change in integrity protection algorithm.](#)

When configuring Integrity protection, UTRAN should:

- 1> ensure that the UE needs to store at most three different Integrity protection configurations (keysets) at any given time. This includes the total number of Integrity protection configurations for all signalling radio bearers;
- 1> if Ciphering has already been started for the UE for the CN domain to be set in the IE "CN domain identity" in the SECURITY MODE COMMAND:
  - 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 "Ciphering mode info" in the SECURITY MODE COMMAND.
- 1> if Ciphering has already been configured for the UE for a CN domain different from the CN domain to be set in the IE "CN domain identity" in the SECURITY MODE COMMAND:
  - 2> include the IE "Ciphering mode info" in the SECURITY MODE COMMAND.

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> if this is the first SECURITY MODE COMMAND sent for this RRC connection:
  - 2> if new keys have been received:
    - 3> initialise the hyper frame numbers as follows:
      - 4> set all bits of the hyper frame numbers of the COUNT-I values for all signalling radio bearers to zero.

- 2> else (if new keys have not been received):
  - 3> use the value "START" in the most recently received IE "START list" or IE "START" that belongs to the CN domain indicated in the IE "CN domain identity" to initialise all hyper frame numbers of COUNT-I for all the signalling radio bearers by:
    - 4> setting the 20 most significant bits of the hyper frame numbers for all signalling radio bearers to the value "START" in the most recently received IE "START list" or IE "START" for that CN domain;
    - 4> setting the remaining bits of the hyper frame numbers equal to zero.
- 1> else (this is not the first SECURITY MODE COMMAND sent for this RRC connection):
  - 2> if new keys have been received:
    - 3> initialise the hyper frame number for COUNT-I for RB2 as follows:
      - 4> set all bits of the HFN of the COUNT-I value for RB2 to zero.
  - 2> if new keys have not been received:
    - 3> initialise the hyper frame number for COUNT-I for RB2 as follows:
      - 4> set the 20 most significant bits of the HFN of the downlink and uplink COUNT-I to the value of the most recently received IE "START" or IE "START LIST" for the CN domain to be set in the IE "CN Domain Identity";
      - 4> set the remaining bits of the HFN of the downlink and uplink COUNT-I to zero.
- 1> if the IE "Integrity protection mode command" has the value "Start":
  - 2> prohibit the transmission of signalling messages with any RRC SN on all signalling radio bearers, except RB2;
  - 2> set the FRESH value in the IE "Integrity protection initialisation number", included in the IE "Integrity protection mode info".
- 1> if the IE "Integrity protection mode command" has the value "Modify":
  - 2> for each signalling radio bearer RBn, except RB2:
    - 3> prohibit the transmission of signalling messages with RRC SN greater or equal to the RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info".
    - 2> set, for each signalling radio bearer RBn, that has no pending integrity protection activation time set by a previous security mode control procedure, an RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info", at which time the new integrity protection configuration shall be applied;
    - 2> set, for each signalling radio bearer RBn, that has a pending integrity protection activation time set by a previous security mode control procedure, the RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info", to the value used in the previous security mode control procedure, at which time the latest integrity protection configuration shall be applied.
- 1> transmit the SECURITY MODE COMMAND message on RB2 using the new integrity protection configuration.

### 8.1.12.3 Reception of SECURITY MODE COMMAND message by the UE

Upon reception of the SECURITY MODE COMMAND message, the UE shall:

- 1> if neither IE "Ciphering mode info" nor IE "Integrity protection mode info" is included in the SECURITY MODE COMMAND:

- 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the IE "Security capability" is the same as indicated by variable UE\_CAPABILITY\_TRANSFERRED, and the IE "GSM security capability" (if included in the SECURITY MODE COMMAND) is the same as indicated by the variable UE\_CAPABILITY\_TRANSFERRED:
  - 2> set the variable LATEST\_CONFIGURED\_CN\_DOMAIN equal to the IE "CN domain identity";
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for the CN domain indicated in the IE "CN domain identity" in the received SECURITY MODE COMMAND to the value "Affected";
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all CN domains other than the CN domain indicated in the IE "CN domain identity" to "Not affected";
  - 2> set the IE "RRC transaction identifier" in the SECURITY MODE COMPLETE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE COMMAND message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - 3> perform the actions as specified in subclause 8.6.3.4.
  - 2> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
    - 3> perform the actions as specified in subclause 8.6.3.5.
- 1> prior to sending the SECURITY MODE COMPLETE message:
  - 2> use the old ciphering configuration for this message;
  - 2> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - 3> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
    - 3> for each radio bearer and signalling radio bearer that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN:
      - 4> start or continue incrementing the COUNT-C values for all RLC-AM and RLC-UM signalling radio bearers at the ciphering activation time as specified in the procedure;
      - 4> continue incrementing the COUNT-C values for all RLC-AM and RLC-UM radio bearers.
    - 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN:
      - 4> for ciphering on signalling radio bearers using RLC-AM and RLC-UM in the downlink, at the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info" included in the SECURITY MODE COMMAND, for each signalling radio bearer:
        - 5> set the 20 most significant bits of the HFN component of the downlink COUNT-C to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
        - 5> set the remaining bits of the hyper frame numbers to zero.
    - 3> if new keys have been received:
      - 4> perform the actions in subclause 8.1.12.3.1.
  - 2> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
    - 3> include and set the IE "Uplink integrity protection activation info" to the value of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO for each signalling radio bearer;

- 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN, for RB2:
  - 4> in the downlink, for the received SECURITY MODE COMMAND message:
    - 5> set the 20 most significant bits of the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 5> set the remaining bits of the IE "Downlink RRC HFN" to zero.
  - 4> in the uplink, for the transmitted response message, SECURITY MODE COMPLETE:
    - 5> set the 20 most significant bits of the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 5> set the remaining bits of the IE "Uplink RRC HFN" to zero.
- 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN, for each signalling radio bearer other than RB2:
  - 4> if the IE "Integrity protection mode command" has the value "start":
    - 5> in the downlink, for this signalling radio bearer:
      - 6> set the 20 most significant bits of IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to the value START transmitted in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
      - 6> set the remaining bits of the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to zero;
    - 4> else:
      - 5> in the downlink, for the first message for which the RRC sequence number in a received RRC message for this signalling radio bearer is equal to or greater than the activation time as indicated in IE "Downlink integrity protection activation info" as included in the IE "Integrity protection mode info", for this signalling radio bearer:
        - 6> set the 20 most significant bits of the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
        - 6> set the remaining bits of the IE "Downlink RRC HFN" to zero.
  - 3> if new keys have been received:
    - 4> perform the actions in subclause 8.1.12.3.1.
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;
  - 2> transmit the SECURITY MODE COMPLETE message on the uplink DCCH in AM RLC;

1> when the successful delivery of the SECURITY MODE COMPLETE message has been confirmed by RLC:

  - 2> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":

- 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN:
    - 4> for ciphering on signalling radio bearers using RLC-AM and RLC-UM in the uplink, at the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info" included in the SECURITY MODE COMPLETE, for each signalling radio bearer:
      - 5> set the HFN component of the uplink COUNT-C to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
      - 5> set the remaining bits of the hyper frame numbers to zero.
  - 3> if new keys have been received:
    - 4> perform the actions in subclause 8.1.12.3.1.
  - 3> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
  - 3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
  - 3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 2> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
- 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN, for each signalling radio bearer other than RB2:
    - 4> if the IE "Integrity protection mode command" has the value "start":
      - 5> in the uplink, for this signalling radio bearer:
        - 6> set the 20 most significant bits of IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to the value START transmitted in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
        - 6> set the remaining bits of the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to zero.
    - 4> else:
      - 5> in the uplink, for the first transmitted RRC message for this signalling radio bearer with RRC sequence number equal to the activation time as indicated in IE "Uplink integrity protection activation info" included in the transmitted SECURITY MODE COMPLETE, for this signalling radio bearer:
        - 6> set the 20 most significant bits of the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
        - 6> set the remaining bits of the IE "Uplink RRC HFN" to zero.
  - 3> if new keys have been received:
    - 4> perform the actions in subclause 8.1.12.3.1.
  - 3> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
  - 3> set "Uplink RRC Message sequence number" for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO to a value such that next RRC message to be sent on uplink RB0 will use the new integrity protection configuration;
  - 3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and

- 3> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 2> clear the variable SECURITY\_MODIFICATION;
- 2> notify upper layers upon change of the security configuration;
- 2> and the procedure ends.
- 1> if the IE "Security capability" is not the same as indicated by the variable UE\_CAPABILITY\_TRANSFERRED, or the IE "GSM security capability" (if included in the SECURITY MODE COMMAND) is not the same as indicated by the variable UE\_CAPABILITY\_TRANSFERRED, or if the IE "GSM security capability" is not included in the SECURITY MODE COMMAND and is included in the variable UE\_CAPABILITY\_TRANSFERRED:
  - 2> release all its radio resources;
  - 2> indicate the release 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;
  - 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 2> clear the variable ESTABLISHED\_RABS;
  - 2> clear the variable SECURITY\_MODIFICATION;
  - 2> enter idle mode;
  - 2> perform actions when entering idle mode as specified in subclause 8.5.2;
  - 2> and the procedure ends.

#### 8.1.12.3.1 New ciphering and integrity protection keys

If a new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN, the UE shall:

- 1> set the START value for the CN domain indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN to zero;
- 1> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
  - 2> for integrity protection in the downlink on each signalling radio bearer except RB2:
    - 3> if IE "Integrity protection mode command" has the value "start":
      - 4> for the first received message on this signalling radio bearer:
        - 5> start using the new integrity key;
        - 5> for this signalling radio bearer:
          - 6> set the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to zero.
      - 3> else:
        - 4> for the first message for which the RRC sequence number in a received RRC message for this signalling radio bearer is equal to or greater than the activation time as indicated in IE "Downlink integrity protection activation info" as included in the IE "Integrity protection mode info":
          - 5> start using the new integrity key;
          - 5> for this signalling radio bearer:
            - 6> set the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to zero.



- 2> for integrity protection in the uplink on each signalling radio bearer except RB2:
  - 3> for the first message for which the RRC sequence number in a to be transmitted RRC message for this signalling radio bearer is equal to the activation time as indicated in IE "Uplink integrity protection activation info" included in the transmitted SECURITY MODE COMPLETE message:
    - 4> start using the new integrity key;
    - 4> for this signalling radio bearer:
      - 5> set the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to zero.
- 2> for integrity protection in the downlink on signalling radio bearer RB2:
  - 3> at the received SECURITY MODECOMMAND:
    - 4> start using the new integrity key;
    - 4> set the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to zero.
- 2> for integrity protection in the uplink on signalling radio bearer RB2 :
  - 3> at the transmitted SECURITY MODE COMPLETE:
    - 4> start using the new integrity key;
    - 4> set the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to zero.
- 1> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
  - 2> for each signalling radio bearer and for each radio bearer for the CN domain indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN:
    - 3> if the IE "Status" in the variable CIPHERING\_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers using RLC-TM:
      - 4> at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info":
        - 5> start using the new key in uplink and downlink;
        - 5> set the HFN component of the COUNT-C to zero.
    - 3> if the IE "Status" in the variable CIPHERING\_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers and signalling radio bearers using RLC-AM and RLC-UM:
      - 4> in the downlink, at the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info":
        - 5> start using the new key;
        - 5> set the HFN component of the downlink COUNT-C to zero.
      - 4> in the uplink, at the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info":
        - 5> start using the new key;
        - 5> set the HFN component of the uplink COUNT-C to zero.
- 1> consider the value of the latest transmitted START value to be zero.

#### 8.1.12.4 Void

##### 8.1.12.4a Incompatible simultaneous security reconfiguration

If the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION becomes set to TRUE of the received SECURITY MODE COMMAND message, the UE shall:

- 1> transmit a SECURITY MODE FAILURE message on the uplink DCCH using AM RLC, using the ciphering and integrity protection configurations prior to the reception of this SECURITY MODE COMMAND;
- 1> set the IE "RRC transaction identifier" in the SECURITY MODE FAILURE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE COMMAND message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";
- 1> when the response message has been submitted to lower layers for transmission:
  - 2> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to FALSE;
  - 2> continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - 2> and the procedure ends.

##### 8.1.12.4b Cell update procedure during security reconfiguration

If:

- a cell update procedure according to subclause 8.3.1 is initiated; and
- the received SECURITY MODE COMMAND message causes either,
  - the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE; and/or
  - the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE;

the UE shall:

- 1> abort the ongoing integrity and/or ciphering reconfiguration;
- 1> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
- 1> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- 1> when the response message has been submitted to lower layers for transmission:
  - 2> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - 3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
    - 3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
    - 3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
    - 3> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
  - 2> continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received; and

- 2> clear the variable SECURITY\_MODIFICATION;
- 2> the procedure ends.

#### 8.1.12.4c Invalid configuration

If the variable INVALID\_CONFIGURATION is set to TRUE due to the received SECURITY MODE COMMAND message, the UE shall:

- 1> transmit a SECURITY MODE FAILURE message on the DCCH using AM RLC after setting the IEs as specified below:
  - 2> set the IE "RRC transaction identifier" in the SECURITY MODE FAILURE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE COMMAND message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> set the IE "failure cause" to the cause value "invalid configuration".
- 1> when the response message has been submitted to lower layers for transmission:
  - 2> set the variable INVALID\_CONFIGURATION to FALSE;
  - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE;
  - 2> continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - 2> and the procedure ends.

#### 8.1.12.5 Reception of SECURITY MODE COMPLETE message by the UTRAN

UTRAN should apply integrity protection on the received SECURITY MODE COMPLETE message and all subsequent messages with the new integrity protection configuration, if changed. When UTRAN has received a SECURITY MODE COMPLETE message and the integrity protection has successfully been applied, UTRAN should:

- 1> if the IE "Ciphering mode info" was included in the SECURITY MODE COMMAND message:
  - 2> if new keys were received for the CN domain set in the IE "CN Domain Identity" in the SECURITY MODE COMMAND:
    - 3> set, at the downlink and uplink activation time, all the bits of the hyper frame numbers of the downlink and uplink COUNT-C values respectively for all radio bearers for this CN domain and all signalling radio bearers to zero.
  - 2> else (if new keys were not received):
    - 3> use, at the downlink and uplink activation time, the value "START" in the most recently received IE "START list" or IE "START" that belongs to the CN domain as indicated in the IE "CN domain identity" to initialise all hyper frame numbers of the downlink and uplink COUNT-C values respectively for all the signalling radio bearers as follows:
      - 4> set the 20 most significant bits of the hyper frame numbers of the COUNT-C for all signalling radio bearers to the value "START" in the most recently received IE "START list" or IE "START" for that CN domain;
      - 4> set the remaining bits of the hyper frame numbers equal to zero.
- 1> if the IE "Integrity protection mode info" was included in the SECURITY MODE COMMAND message:
  - 2> if this was not the first SECURITY MODE COMMAND message for this RRC connection:
    - 3> if new keys have been received for the CN domain set in the IE "CN Domain Identity" included in the transmitted SECURITY MODE COMMAND message:

- 4> initialise, at the downlink and uplink activation time, all hyper frame numbers of the downlink and uplink COUNT-I values respectively for all the signalling radio bearers other than RB2 as follows:
  - 5> set all bits of the hyper frame numbers of the uplink and downlink COUNT-I to zero.
- 3> if no new keys have been received for the CN domain set in the IE "CN Domain Identity" included in the transmitted SECURITY MODE COMMAND message:
  - 4> use, at the downlink and uplink activation time, the value "START" in the most recently received IE "START list" or IE "START" that belongs to the CN domain as indicated in the IE "CN domain identity" to initialise all hyper frame numbers of the downlink and uplink COUNT-I values respectively for all the signalling radio bearers other than RB2 as follows:
    - 5> set the 20 most significant bits of the hyper frame numbers of the downlink and uplink COUNT-I respectively for all signalling radio bearers to the value "START" in the most recently received IE "START list" or IE "START" for that CN domain;
    - 5> set the remaining bits of the hyper frame numbers equal to zero.
- 1> send an indication to upper layers that the new security configuration has been activated;
- 1> resume, in the downlink, all suspended radio bearers and all signalling radio bearers;
- 1> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- 1> if the IE "Integrity protection mode command" included in the SECURITY MODE COMMAND had the value "Start":
  - 2> start applying integrity protection in the downlink for all signalling radio bearers.
- 1> if the IE "Integrity protection mode command" included in the SECURITY MODE COMMAND had the value "Modify":
  - 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each signalling radio bearers RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info";
  - 2> continue applying the new integrity configuration for signalling radio bearer RB2;
  - 2> apply the new integrity protection configuration on the received signalling messages with RRC SN greater than or equal to the number associated with the signalling radio bearer in IE "Uplink integrity protection activation info".
- 1> apply the old ciphering configuration for the transmission of RLC PDUs with RLC sequence number less than the number indicated in the IE "Radio bearer downlink ciphering activation time info" included in the IE "Ciphering mode info";
- 1> apply the new ciphering configuration for the transmission of RLC PDUs with RLC sequence number greater than or equal to the number indicated in IE "Radio bearer downlink ciphering activation time info" included in the IE "Ciphering mode info";
- 1> apply the old integrity protection configuration on the received signalling messages with RRC SN smaller than the number associated with the signalling radio bearer in IE "Uplink integrity protection activation info";
- 1> for radio bearers using RLC-AM or RLC-UM:
  - 2> use the old ciphering configuration for received RLC PDUs with RLC sequence number less than the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" sent by the UE;
  - 2> use the new ciphering configuration for received RLC PDUs with RLC sequence number greater than or equal to the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" sent by the UE;
  - 2> if an RLC reset or re-establishment occurs after the SECURITY MODE COMPLETE message has been received by UTRAN before the activation time for the new ciphering configuration has been reached, ignore

the activation time and apply the new ciphering configuration immediately after the RLC reset or RLC re-establishment.

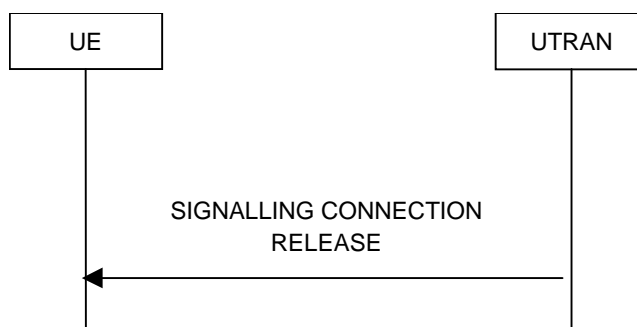
- 1> for radio bearers using RLC-TM:
  - 2> use the old ciphering configuration for the received RLC PDUs before the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info" as included in the SECURITY MODE COMMAND;
  - 2> use the new ciphering configuration for the received RLC PDUs at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info" as included in the SECURITY MODE COMMAND.
- 1> and the procedure ends.

### 8.1.12.6 Invalid SECURITY MODE COMMAND message

If the SECURITY MODE COMMAND message contains a protocol error causing the variable PROTOCOL\_ERROR\_REJECT to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows:

- 1> transmit a SECURITY MODE FAILURE message on the uplink DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the SECURITY MODE FAILURE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE COMMAND message in the table "Rejected transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to the cause value "protocol error";
- 1> include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL\_ERROR\_INFORMATION;
- 1> when the response message has been submitted to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - 2> and the procedure ends.

### 8.1.13 Signalling connection release procedure



**Figure 8.1.13-1: Signalling connection release procedure, normal case**

#### 8.1.13.1 General

The signalling connection release procedure is used to notify to the UE that one of its ongoing signalling connections has been released. The procedure does not initiate the release of the RRC connection.

### 8.1.13.2 Initiation of SIGNALLING CONNECTION RELEASE by the UTRAN

To initiate the procedure, the UTRAN transmits a SIGNALLING CONNECTION RELEASE message on DCCH using AM RLC.

### 8.1.13.3 Reception of SIGNALLING CONNECTION RELEASE by the UE

Upon reception of a SIGNALLING CONNECTION RELEASE message, the UE shall:

- 1> indicate the release of the signalling connection and pass the value of the IE "CN domain identity" to upper layers;
- 1> remove the signalling connection with the identity indicated by the IE "CN domain identity" from the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 1> clear the entry for the SIGNALLING CONNECTION RELEASE message in the table "Accepted transactions" in the variable TRANSACTIONS;
- 1> the procedure ends.

### 8.1.13.4 Invalid SIGNALLING CONNECTION RELEASE message

If the UE receives a SIGNALLING CONNECTION RELEASE message, which contains a protocol error causing the variable `PROTOCOL_ERROR_REJECT` to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows:

- 1> include the IE "Identification of received message"; and
  - 2> set the IE "Received message type" to SIGNALLING CONNECTION RELEASE;
  - 2> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the SIGNALLING CONNECTION RELEASE message in the table "Rejected transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry.
- 1> include the IE "Protocol error information" with contents set to the value of the variable `PROTOCOL_ERROR_INFORMATION`;
- 1> transmit an RRC STATUS message on the uplink DCCH using AM RLC
- 1> when the RRC STATUS message has been submitted to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the invalid SIGNALLING CONNECTION RELEASE message has not been received.

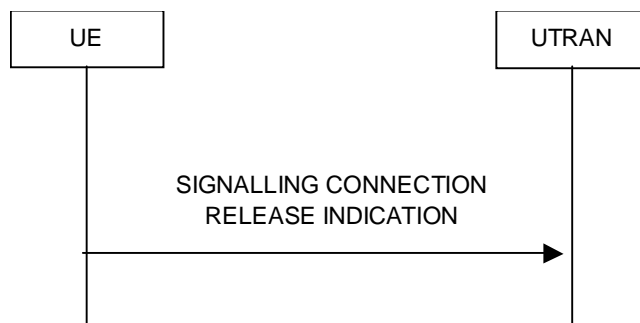
### 8.1.13.5 Invalid configuration

If radio access bearers for the CN domain indicated by the IE "CN domain identity" exist in the variable `ESTABLISHED_RABS`, the UE shall:

- 1> transmit an RRC STATUS message on the uplink DCCH using AM RLC;
- 1> include the IE "Identification of received message"; and
- 1> set the IE "Received message type" to SIGNALLING CONNECTION RELEASE; and
- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the SIGNALLING CONNECTION RELEASE message in the table "Accepted transactions" in the variable TRANSACTIONS and clear that entry;
- 1> include the IE "Protocol error information" with contents set to the value "Message not compatible with receiver state";
- 1> when the RRC STATUS message has been submitted to lower layers for transmission:

- 2> continue with any ongoing processes and procedures as if the invalid SIGNALLING CONNECTION RELEASE message has not been received.

### 8.1.14 Signalling connection release indication procedure



**Figure 8.1.14-1: Signalling connection release indication procedure, normal case**

#### 8.1.14.1 General

The signalling connection release indication procedure is used by the UE to indicate to the UTRAN that one of its signalling connections has been released. The procedure may in turn initiate the RRC connection release procedure.

#### 8.1.14.2 Initiation

The UE shall, on receiving a request to release (abort) the signalling connection from upper layers for a specific CN domain:

- 1> if a signalling connection in the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS for the specific CN domain identified with the IE "CN domain identity" exists:
  - 2> initiate the signalling connection release indication procedure.
- 1> otherwise:
  - 2> abort any ongoing establishment of signalling connection for that specific CN domain as specified in 8.1.3.5a.

Upon initiation of the signalling connection release indication procedure in CELL\_PCH or URA\_PCH state, the UE shall:

- 1> perform a cell update procedure, according to subclause 8.3.1, using the cause "uplink data transmission";
- 1> when the cell update procedure completed successfully:
  - 2> continue with the signalling connection release indication procedure as below.

The UE shall:

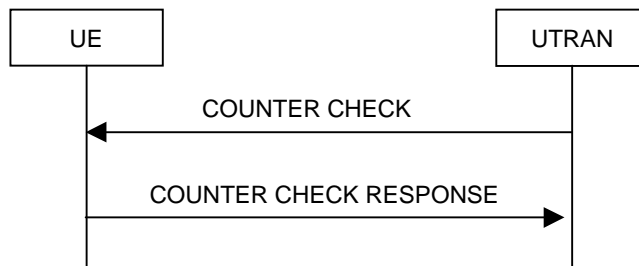
- 1> set the IE "CN Domain Identity" to the value indicated by the upper layers. The value of the IE indicates the CN domain whose associated signalling connection the upper layers are indicating to be released;
- 1> remove the signalling connection with the identity indicated by upper layers from the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 1> transmit a SIGNALLING CONNECTION RELEASE INDICATION message on DCCH using AM RLC.

When the SIGNALLING CONNECTION RELEASE INDICATION message has been submitted to lower layers for transmission the procedure ends.

### 8.1.14.3 Reception of SIGNALLING CONNECTION RELEASE INDICATION by the UTRAN

Upon reception of a SIGNALLING CONNECTION RELEASE INDICATION message, the UTRAN requests the release of the signalling connection from upper layers. Upper layers may then initiate the release of the signalling connection.

### 8.1.15 Counter check procedure



**Figure 8.1.15-1: Counter check procedure**

#### 8.1.15.1 General

The counter check procedure is used by the UTRAN to perform a local authentication. The purpose of the procedure is to check that the amount of data sent in both directions (uplink and downlink) over the duration of the RRC connection is identical at the UTRAN and at the UE (to detect a possible intruder – a 'man-in-the-middle' – from operating).

This procedure is only applicable to radio bearers, and only to radio bearers using RLC-AM or RLC-UM. It should be noted that this requires that the COUNT-C values for each UL and DL radio bearers using RLC-AM or RLC-UM continue to be incremented even if ciphering is not used. This procedure is not applicable to signalling radio bearers.

#### 8.1.15.2 Initiation

The UTRAN monitors the COUNT-C value associated with each radio bearer using UM or AM RLC. The procedure is triggered whenever any of these values reaches a critical checking value. The granularity of these checking values and the values themselves are defined to the UTRAN by the visited network. The UTRAN initiates the procedure by sending a COUNTER CHECK message on the downlink DCCH.

#### 8.1.15.3 Reception of a COUNTER CHECK message by the UE

When the UE receives a COUNTER CHECK message it shall compare the COUNT-C MSB values received in the IE "RB COUNT-C MSB information" in the COUNTER CHECK message to the COUNT-C MSB values of the corresponding radio bearers.

The UE shall:

- 1> set the IE "RRC transaction identifier" in the COUNTER CHECK RESPONSE message to the value of "RRC transaction identifier" in the entry for the COUNTER CHECK message in the table "Accepted transactions" in the variable TRANSACTIONS; and

- 1> clear that entry.

If:

- there is one or more radio bearer(s) using UM or AM RLC mode stored in the variable ESTABLISHED\_RABS, which is (are) not included in the IE "RB COUNT-C MSB information"; or
- there is one or more radio bearer(s) included in the IE "RB COUNT-C MSB information", which is (are) not stored in the variable ESTABLISHED\_RABS; or



- for any radio bearer (excluding signalling radio bearers) using UM or AM RLC mode stored in the variable ESTABLISHED\_RABS and included in the IE "RB COUNT-C MSB information" with COUNT-C MSB values different from the MSB part of the COUNT-C values in the UE:

the UE shall:

- 1> include these radio bearers in the IE "RB COUNT-C information" in the COUNTER CHECK RESPONSE message. For any RB which is included in the IE "RB COUNT-C MSB information" in the COUNTER CHECK message but not stored in the variable ESTABLISHED\_RABS in the UE, the MSB part of COUNT-C values in the COUNTER CHECK RESPONSE message shall be set identical to COUNT-C-MSB values in the COUNTER CHECK message. The LSB part shall be filled with zeroes.

The UE shall:

- 1> if no COUNT-C exists for a radio bearer for a given direction (uplink or downlink) because:
  - 2> it is a uni-directional radio bearer configured only for the other direction (downlink or uplink respectively),  
or
  - 2> has been configured to RLC-TM mode in one direction (uplink or downlink) and RLC-UM in the other (downlink or uplink respectively),
  - 3> set the COUNT-C in the IE "RB COUNT-C information" in the COUNTER CHECK RESPONSE message, to any value;

- 1> submit a COUNTER CHECK RESPONSE message to lower layers for transmission on the uplink DCCH using AM RLC.

When the COUNTER CHECK RESPONSE message has been submitted to lower layers for transmission the procedure ends.

#### 8.1.15.4 Reception of the COUNTER CHECK RESPONSE message by UTRAN

If the UTRAN receives a COUNTER CHECK RESPONSE message that does not contain any COUNT-C values, the procedure ends.

If the UTRAN receives a COUNTER CHECK RESPONSE message that contains one or several COUNT-C values the UTRAN may release the RRC connection.

#### 8.1.15.5 Cell re-selection

If the UE performs cell re-selection anytime during this procedure it shall, without interrupting the procedure:

- 1> initiate the cell update procedure according to subclause 8.3.1.

#### 8.1.15.6 Invalid COUNTER CHECK message

If the UE receives a COUNTER CHECK message, which contains a protocol error causing the variable PROTOCOL\_ERROR\_REJECT to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows. The UE shall:

- 1> transmit an RRC STATUS message on the uplink DCCH using AM RLC;
- 1> include the IE "Identification of received message"; and
- 1> set the IE "Received message type" to COUNTER CHECK; and
- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the UE COUNTER CHECK message in the table "Rejected transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL\_ERROR\_INFORMATION;

- 1> when the RRC STATUS message has been submitted to lower layers for transmission:
- 2> continue with any ongoing processes and procedures as if the invalid COUNTER CHECK message has not been received.

-----

### 8.3.4 Active set update

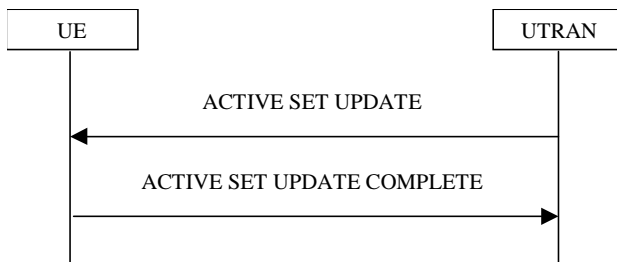


Figure 8.3.4-1: Active Set Update procedure, successful case

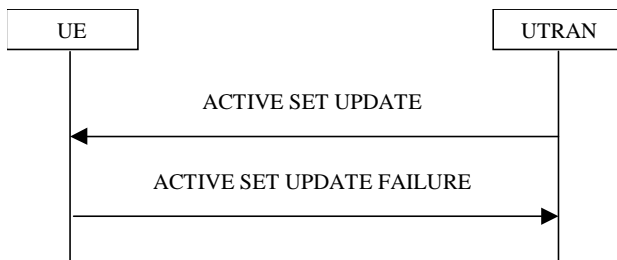


Figure 8.3.4-2: Active Set Update procedure, failure case

#### 8.3.4.1 General

The purpose of the active set update procedure is to update the active set of the connection between the UE and UTRAN. This procedure shall be used in CELL\_DCH state. The UE should keep on using the old RLs while configuring the new RLs. Also the UE should keep the transmitter turned on during the procedure. This procedure is only used in FDD mode.

#### 8.3.4.2 Initiation

The procedure is initiated when UTRAN orders a UE in CELL\_DCH state, to make the following modifications of the active set of the connection:

- a) Radio link addition;
- b) Radio link removal;
- c) Combined radio link addition and removal.

In case a) and c), UTRAN should:

- 1> prepare new additional radio link(s) in the UTRAN prior to the command to the UE.

In all cases, UTRAN should:

- 1> send an ACTIVE SET UPDATE message on downlink DCCH using AM or UM RLC.

UTRAN should include the following information:

- 1> IE "Radio Link Addition Information": Downlink DPCH information and other optional parameters relevant for the radio links to be added along with the IE "Primary CPICH info" used for the reference ID to indicate which radio link to add. This IE is needed in cases a) and c) listed above;
- 1> IE "Radio Link Removal Information": IE "Primary CPICH info" used for the reference ID to indicate which radio link to remove. This IE is needed in cases b) and c) listed above.

### 8.3.4.3 Reception of an ACTIVE SET UPDATE message by the UE

Upon reception of an ACTIVE SET UPDATE message the UE shall act upon all received information elements as specified in 8.6, unless specified otherwise in the following.

The UE may:

- 1> maintain a list of the set of cells to which the UE has Radio Links if the IE "Cell ID" is present.

The UE shall:

- 1> first add the RLs indicated in the IE "Radio Link Addition Information";
- 1> remove the RLs indicated in the IE "Radio Link Removal Information". If the UE active set is full or becomes full, an RL, which is included in the IE "Radio Link Removal Information" for removal, shall be removed before adding RL, which is included in the IE "Radio Link Addition Information" for addition;
- 1> perform the physical layer synchronisation procedure as specified in [29];

~~1> if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":~~

~~2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected".~~

~~1> if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":~~

~~2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.~~

~~1> if the variable PDCP\_SN\_INFO is non-empty:~~

~~2> include the IE "RB with PDCP information list" in the ACTIVE SET UPDATE COMPLETE message; and~~

~~2> set it to the value of the variable PDCP\_SN\_INFO.~~

1> if the IE "TFCI combining indicator" associated with a radio link to be added is set to TRUE:

2> if a DSCH transport channel is assigned and there is a 'hard' split in the TFCI field:

3> configure Layer 1 to soft-combine TFCI (field 2) of this new link with those links already in the TFCI (field 2) combining set.

~~1> if the received ACTIVE SET UPDATE message included the IE "Downlink counter synchronisation info":~~

~~2> calculate the START value according to subclause 8.5.9;~~

~~2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the ACTIVE SET UPDATE COMPLETE message.~~

1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE COMPLETE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and

1> clear that entry;

1> transmit an ACTIVE SET UPDATE COMPLETE message on the uplink DCCH using AM RLC without waiting for the Physical Layer synchronization;

~~1> if the IE "Integrity protection mode info" was present in the ACTIVE SET UPDATE message:~~

- 2> ~~start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted ACTIVE SET UPDATE COMPLETE message.~~
  - 1> ~~if the IE "Downlink counter synchronisation info" was included in the received ACTIVE SET UPDATE message:~~
    - 2> ~~when RLC has confirmed the successful transmission of the response message:~~
      - 3> ~~re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].~~
  - 1> ~~if the variable PDCP\_SN\_INFO is empty:~~
    - 2> ~~if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":~~
      - 3> ~~when RLC has confirmed the successful transmission of the ACTIVE SET UPDATE COMPLETE message:~~
        - 4> ~~perform the actions below.~~
    - 2> ~~if the ACTIVE SET UPDATE message did not contain the IE "Ciphering mode info":~~
      - 3> ~~when RLC has been requested to transmit the ACTIVE SET UPDATE COMPLETE message:~~
        - 4> ~~perform the actions below.~~
  - 1> ~~if the variable PDCP\_SN\_INFO is non-empty:~~
    - 2> ~~when RLC has confirmed the successful transmission of the ACTIVE SET UPDATE COMPLETE message:~~
      - 3> ~~for each radio bearer in the variable PDCP\_SN\_INFO:~~
        - 4> ~~if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":~~
          - 5> ~~configure the RLC entity for that radio bearer to "continue".~~
      - 3> ~~clear the variable PDCP\_SN\_INFO.~~
  - 1> ~~if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":~~
    - 2> ~~resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;~~
    - 2> ~~set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and~~
    - 2> ~~clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.~~
  - 1> ~~if the ACTIVE SET UPDATE message contained the IE "Integrity protection mode info":~~
    - 2> ~~allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;~~
    - 2> ~~set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and~~
    - 2> ~~clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.~~
  - 1> ~~clear the variable SECURITY\_MODIFICATION;~~
- 1> the procedure ends on the UE side.

#### 8.3.4.4 Unsupported configuration in the UE

If UTRAN instructs the UE to use a configuration that it does not support, the UE shall:

- 1> keep the active set as it was before the ACTIVE SET UPDATE message was received;
- 1> transmit an ACTIVE SET UPDATE FAILURE message on the DCCH using AM RLC;

- 1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to "configuration unsupported";
- 1> when the ACTIVE SET UPDATE FAILURE message has been submitted to lower layers for transmission:
  - 2> the procedure ends on the UE side.

### 8.3.4.5 Invalid configuration

If any of the following conditions are valid:

- a radio link indicated by the IE "Downlink DPCH info for each RL" in the IE "Radio link addition information" has a different spreading factor than the spreading factor for the radio links in the active set that will be established at the time indicated by the IE "Activation time"; and/or
- a radio link in the IE "Radio link addition information" is also present in the IE "Radio Link Removal Information"; and/or
- the IE "Radio Link Removal Information" contains all the radio links which are part of or will be part of the active set at the time indicated by the IE "Activation time"; and/or
- the IE "TX Diversity Mode" is not set to "none" and it indicates a diversity mode that is different from the one currently used in all or part of the active set; and/or
- a radio link indicated by the IE "Radio Link Removal Information" does not exist in the active set; and/or
- after the removal of all radio links indicated by the IE "Radio Link Removal Information" and the addition of all radio links indicated by the IE "Radio Link Addition Information" the active set would contain more than the maximum allowed number of radio links; and/or
- the variable INVALID\_CONFIGURATION is set to TRUE:

the UE shall:

- 1> keep the active set as it was before the ACTIVE SET UPDATE message was received;
- 1> transmit an ACTIVE SET UPDATE FAILURE message on the DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to "Invalid configuration";
- 1> When the ACTIVE SET UPDATE FAILURE message has been submitted to lower layers for transmission:
  - 2> the procedure ends on the UE side.

#### ~~8.3.4.5a Incompatible simultaneous reconfiguration~~

~~If the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION becomes set to TRUE due to the received ACTIVE SET UPDATE message, the UE shall:~~

- ~~1> transmit a ACTIVE SET UPDATE FAILURE message on the uplink DCCH using AM RLC;~~
- ~~1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and~~

~~1> clear that entry;~~

~~1> set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";~~

~~1> when the ACTIVE SET UPDATE FAILURE message has been delivered to lower layers for transmission:~~

~~2> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to FALSE;~~

~~2> continue with any ongoing processes and procedures as if the ACTIVE SET UPDATE message has not been received;~~

~~2> and the procedure ends.~~

~~If the variable ORDERED\_RECONFIGURATION is set to TRUE; and~~

~~1> if the activation time for the procedure that has set variable ORDERED\_RECONFIGURATION and the activation time for the Active Set Update procedure are within a time window of 5 frames, the UE may:~~

~~2> transmit a ACTIVE SET UPDATE FAILURE message on the uplink DCCH using AM RLC;~~

~~2> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and~~

~~2> clear that entry;~~

~~2> set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";~~

~~2> when the ACTIVE SET UPDATE FAILURE message has been delivered to lower layers for transmission:~~

~~3> continue with any ongoing processes and procedures as if the ACTIVE SET UPDATE message has not been received;~~

~~3> and the procedure ends.~~

#### 8.3.4.6 Reception of the ACTIVE SET UPDATE COMPLETE message by the UTRAN

When the UTRAN has received the ACTIVE SET UPDATE COMPLETE message,

1> the UTRAN may remove radio link(s) that are indicated to remove to the UE in case b) and c); and

1> the procedure ends on the UTRAN side.

#### 8.3.4.7 Reception of the ACTIVE SET UPDATE FAILURE message by the UTRAN

When the UTRAN has received the ACTIVE SET UPDATE FAILURE message, the UTRAN may delete radio links that were included in the IE "Radio Link Addition Information" for addition. The procedure ends on the UTRAN side.

#### 8.3.4.8 Invalid ACTIVE SET UPDATE message

If the ACTIVE SET UPDATE message contains a protocol error causing the variable PROTOCOL\_ERROR\_REJECT to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows. The UE shall:

1> transmit a ACTIVE SET UPDATE FAILURE message on the uplink DCCH using AM RLC;

1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Rejected transactions" in the variable TRANSACTIONS; and

1> clear that entry;

1> set the IE "failure cause" to the cause value "protocol error";

- 1> include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL\_ERROR\_INFORMATION;
- 1> when the ACTIVE SET UPDATE FAILURE message has been delivered to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the invalid ACTIVE SET UPDATE message has not been received;
  - 2> and the procedure ends.

#### 8.3.4.9 Reception of an ACTIVE SET UPDATE message in wrong state

If the UE is in another state than CELL\_DCH state upon reception of the ACTIVE SET UPDATE message, the UE shall perform procedure specific error handling as follows. The UE shall:

- 1> transmit a ACTIVE SET UPDATE FAILURE message on the uplink DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to the cause value "protocol error";
- 1> include the IE "Protocol error information" with the IE "Protocol error cause" set to "Message not compatible with receiver state";
- 1> when the ACTIVE SET UPDATE FAILURE message has been delivered to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the ACTIVE SET UPDATE message has not been received;
  - 2> and the procedure ends.

#### 8.5.9 START value calculation

In connected mode, the START value for CN domain 'X' is calculated as

Let  $START_X$  = the START value for CN domain 'X' prior to the calculation below:

$START_X' = MSB_{20} ( MAX \{ COUNT-C, COUNT-I \mid \text{radio bearers and signalling radio bearers using the most recently configured } CK_X \text{ and } IK_X \}) + 2.$

- if  $START_X' = \text{the maximum value} = 1048575$  then  $START_X = START_X'$ ;
- if the current  $START_X < START_X'$  then  $START_X = START_X'$ , otherwise  $START_X$  is unchanged.

NOTE: Here, "most recently configured" means that if there is more than one key in use for a CN domain, due to non-expiry of the ciphering and/or integrity protection activation time for any signalling radio bearers and/or radio bearers, do not include the COUNT-I/COUNT-C for these signalling radio bearers and/or radio bearers in the calculation of the  $START_X'$ .

COUNT-C corresponding to non-ciphered radio bearers ([i.e. RBs with ciphering status set to "not started"](#)) shall not be included in the calculation of the  $START_X'$ . If a radio bearer is released and the radio bearer was ciphered, the values of the COUNT-C at the time the radio bearer is released shall be taken into account in the calculation of the  $START_X'$ .

#### 8.5.10 Integrity protection

If the "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" then the UE shall:

- 1> perform integrity protection (and integrity checking) on all RRC messages, with the following exceptions:  
HANDOVER TO UTRAN COMPLETE

PAGING TYPE 1

PUSCH CAPACITY REQUEST

PHYSICAL SHARED CHANNEL ALLOCATION

RRC CONNECTION REQUEST

RRC CONNECTION SETUP

RRC CONNECTION SETUP COMPLETE

RRC CONNECTION REJECT

RRC CONNECTION RELEASE (CCCH only)

SYSTEM INFORMATION

SYSTEM INFORMATION CHANGE INDICATION

TRANSPORT FORMAT COMBINATION CONTROL (TM DCCH only)

If the "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started" then integrity protection (and integrity checking) shall not be performed on any RRC message.

For each signalling radio bearer, the UE shall use two RRC hyper frame numbers:

- "Uplink RRC HFN";
- "Downlink RRC HFN".

and two message sequence numbers:

- "Uplink RRC Message sequence number";
- "Downlink RRC Message sequence number".

The above information is stored in the variable INTEGRITY\_PROTECTION\_INFO per signalling radio bearer (RB0-RB4).

Upon the first activation of integrity protection for an RRC connection, UE and UTRAN initialise the "Uplink RRC Message sequence number" and "Downlink RRC Message sequence number" for all signalling radio bearers as specified in subclauses 8.6.3.5 and 8.5.10.1.

The RRC message sequence number (RRC SN) is incremented for every integrity protected RRC message.

If the IE "Integrity Protection Mode Info" is present in a received message, the UE shall:

1> perform the actions in subclause 8.6.3.5 before proceeding with the integrity check of the received message.

### 8.5.10.1 Integrity protection in downlink

If the UE receives an RRC message on signalling radio bearer with RB identity n, the "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and the IE 'Integrity check info' is present the UE shall:

- 1> check the value of the IE "RRC message sequence number" included in the IE "Integrity check info";
- 2> if the "Downlink RRC Message sequence number" is not present in the variable INTEGRITY\_PROTECTION\_INFO:
  - 3> initialise the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO with the value of the IE "RRC message sequence number" included in the IE "Integrity check info" of the received message.
- 2> if the "Downlink RRC Message sequence number" is present in the variable INTEGRITY\_PROTECTION\_INFO:



- 3> if the RRC message sequence number is lower than the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO:
  - 4> increment "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO with one.
- 3> if the RRC message sequence number is equal to the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO:
  - 4> discard the message.
- 1> calculate an expected message authentication code in accordance with subclause 8.5.10.3;
- 1> compare the expected message authentication code with the value of the received IE "message authentication code" contained in the IE "Integrity check info";
  - 2> if the expected message authentication code and the received message authentication code are the same, the integrity check is successful:
    - 3> update the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO with the value of the IE "RRC message sequence number" included in the IE "Integrity check info" of the received RRC message.
  - 2> if the calculated expected message authentication code and the received message authentication code differ:
    - 3> if the IE "RRC message sequence number" included in the IE "Integrity check info" is lower than the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO (in this case the "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO was incremented by one, as stated above):
      - 4> decrement "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO by one.
    - 3> discard the message.

If the UE receives an RRC message on signalling radio bearer with identity n, the "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and the IE 'Integrity check info' is not present the UE shall:

- 1> discard the message.

#### 8.6.3.4 Cipherng mode info

The IE "Cipherng mode info" defines the new cipherng configuration. At any given time, the UE needs to store at most two different cipherng configurations (keyset and algorithm) per CN domain at any given time in total for all radio bearers and three configurations in total for all signalling radio bearers.

If the IE "Cipherng mode info" is present and if the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE, the UE shall:

- 1> ignore this second attempt to change the cipherng configuration; and
- 1> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to TRUE.

If the IE "Cipherng mode info" is present and if the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to FALSE, the UE shall:

- 1> if the IE "Status" in the variable CIPHERING STATUS has the value "Not started", and this IE was included in a message that is not the message SECURITY MODE COMMAND; or
- 1> if there does not exist exactly one cipherng activation time in the IE "Radio bearer downlink cipherng activation time info" for each established RLC-AM and RLC-UM radio bearers included in the IE "RB information" in the IE "ESTABLISHED\_RABS" for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN; or

- 1> if the IE "Ciphering activation time for DPCH" is not included in message ACTIVE SET UPDATE or SECURITY MODE COMMAND, and there exist radio bearers using RLC-TM according to the IE "RB information" in the IE "ESTABLISHED\_RABS" for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN; or
- 1> if there does not exist exactly one ciphering activation time in the IE "Radio bearer downlink ciphering activation time info" for each established signalling radio bearer included in the IE "Signalling radio bearer information" in the IE "ESTABLISHED\_RABS":
  - 2> ignore this attempt to change the ciphering configuration;
  - 2> set the variable INVALID\_CONFIGURATION to TRUE;
  - 2> perform the actions as specified in subclause 8.1.12.4c.
- 1> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to TRUE;
- 1> set the IE "Status" in the variable CIPHERING\_STATUS of the CN domains for which the IE "Status" of the variable SECURITY\_MODIFICATION is set to "Affected" to "Started";
- 1> apply the new ciphering configuration in the lower layers for all RBs that belong to a CN domain for which the IE "Status" of the variable SECURITY\_MODIFICATION is set to "Affected" and all signalling radio bearers:
  - 2> using the ciphering algorithm (UEA [40]) indicated by the IE "Ciphering algorithm" as part of the new ciphering configuration;
  - 2> for each radio bearer that belongs to a CN domain for which the IE "Status" of the variable SECURITY\_MODIFICATION is set to "Affected" and all signalling radio bearers:
    - 3> using the value of the IE "RB identity" in the variable ESTABLISHED\_RABS minus one as the value of BEARER [40] in the ciphering algorithm.
- 1> apply the new ciphering configuration as follows:
  - 2> consider an activation time in downlink to be pending:
    - 3> for UM-RLC until an UMD PDU with sequence number equal to or larger than activation time –1 has been received;
    - 3> for AM-RLC until all AMD PDUs with sequence numbers up to and including activation time –1 have been received;
    - 3> for TM-RLC until the CFN indicated in the activation time has been reached.
  - 2> if there are pending activation times in downlink set for ciphering by a previous procedure changing the ciphering configuration:
    - 3> apply the ciphering configuration included in the current message at this pending activation time;  
~~3> consider the ciphering keys that were to be applied following a previous procedure changing the ciphering configuration and which have not yet been applied due to the activation time not having elapsed for a given radio bearer, as part of the ciphering configuration received in the current message.~~
- 2> if the IE "Ciphering activation time for DPCH" is present in the IE "Ciphering mode info" and the UE was in CELL\_DCH state prior to this procedure:
  - 3> for radio bearers using RLC-TM:
    - 4> apply the old ciphering configuration for CFN less than the number indicated in the IE "Ciphering activation time for DPCH";
    - 4> apply the new ciphering configuration for CFN greater than or equal to the number indicated in IE "Ciphering activation time for DPCH".
- 2> if the UE was in CELL\_FACH state prior to this procedure and at completion of this procedure a transparent mode radio bearer exists and the IE "Ciphering activation time for DPCH" is not present in the IE "Ciphering mode info":

3> for radio bearers using RLC-TM:

- 4> apply the old ciphering configuration for CFN less than the number as indicated by the IE "COUNT-C activation time" in the transmitted uplink response message for the ciphering activation time for this radio bearer;
- 4> apply the new ciphering configuration for CFN greater than or equal to the number ~~as~~ indicated in the transmitted uplink response message for the ciphering activation time for this radio bearer.

~~NOTE:—This is indicated by the IE "COUNT-C activation time" in the transmitted uplink response message.~~

2> if the IE "Radio bearer downlink ciphering activation time info" is present:

3> apply the following procedure for each radio bearer and signalling radio bearers using RLC-AM or RLC-UM indicated by the IE "RB identity":

- 4> suspend uplink transmission on the radio bearer or the signalling radio bearer (except for the SRB where the response message is transmitted) according to the following:
  - 5> do not transmit RLC PDUs with sequence number greater than or equal to the uplink activation time, where the uplink activation time is selected according to the rules below.
- 4> select an "RLC send sequence number" at which (activation) time the new ciphering configuration shall be applied in uplink for that radio bearer according to the following:
  - 5> for each radio bearer and signalling radio bearer that has no pending ciphering activation time in uplink as set by a previous procedure changing the security configuration:
    - 6> set a suitable value that would ensure a minimised delay in the change to the latest security configuration.
  - 5> for each radio bearer and signalling radio bearer that has a pending ciphering activation time in uplink as set by a previous procedure changing the security configuration:
    - 6> set the same value as the pending ciphering activation time.
  - 5> consider this activation time in uplink to be elapsed when the selected activation time (as above) is equal to the "RLC send sequence number";
- 4> store the selected "RLC send sequence number" for that radio bearer in the entry for the radio bearer in the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
- 4> switch to the new ciphering configuration according to the following:
  - 5> use the old ciphering configuration for the transmitted and received RLC PDUs with RLC sequence numbers smaller than the corresponding RLC sequence numbers indicated in the IE "Radio bearer uplink ciphering activation time info" sent to UTRAN and in the received IE "Radio bearer downlink ciphering activation time info" received from UTRAN, respectively;
  - 5> use the new ciphering configuration for the transmitted and received RLC PDUs with RLC sequence numbers greater than or equal to the corresponding RLC sequence numbers indicated in the IE "Radio bearer uplink ciphering activation time info" sent to UTRAN and in the received IE "Radio bearer downlink ciphering activation time info" received from UTRAN, respectively;
  - 5> for a radio bearer using RLC-AM, when the RLC sequence number indicated in the IE "Radio bearer downlink ciphering activation time info" falls below the RLC receiving window and the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" falls below the RLC transmission window, the UE may release the old ciphering configuration for that radio bearer;
  - 5> if an RLC reset or re-establishment occurs before the activation time for the new ciphering configuration has been reached, ignore the activation time and apply the new ciphering configuration immediately after the RLC reset or RLC re-establishment.

If the IE "Ciphering mode info" is not present, the UE shall:

1> not change the ciphering configuration.

### 8.6.3.5 Integrity protection mode info

The IE "Integrity protection mode info" defines the new integrity protection configuration. At any given time, the UE needs to store at most three different integrity protection configurations (keysets) in total for all signalling radio bearers for all CN domains.

If the IE "Integrity protection mode info" is present and if the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE, the UE shall:

1> ignore this second attempt to change the integrity protection configuration; and

1> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to TRUE.

If the IE "Integrity protection mode info" is present and if the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to FALSE, the UE shall:

1> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to TRUE;

1> if IE "Integrity protection mode command" has the value "start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and this IE was included in the message SECURITY MODE COMMAND:

2> initialise the information for all signalling radio bearers in the variable INTEGRITY\_PROTECTION\_INFO according to the following:

3> set the IE "Uplink RRC Message sequence number" in the variable INTEGRITY\_PROTECTION\_INFO to zero;

3> do not set the IE "Downlink RRC Message sequence number" in the variable INTEGRITY\_PROTECTION\_INFO;

3> set the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO to zero for each signalling radio bearer in the IE "ESTABLISHED\_RABS".

2> set the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO to the value "Started";

2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:

3> using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";

3> using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].

2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer in the IE "ESTABLISHED\_RABS" except RB2 at the next received RRC message;

2> start applying the new integrity protection configuration in the downlink for signalling radio bearer RB2 from and including the received SECURITY MODE COMMAND message;

2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;

2> start applying the new integrity protection configuration in the uplink for signalling radio bearers other than RB2 at the uplink activation time included in the IE "Uplink integrity protection activation info".

1> if IE "Integrity protection mode command" has the value "start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and this IE was not included SECURITY MODE COMMAND:

NOTE: This case is used in SRNS relocation

- 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:
  - 3> using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";
  - 3> using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].
- 2> let RB<sub>m</sub> be the signalling radio bearer where the reconfiguration message was received and let RB<sub>n</sub> be the signalling radio bearer where the response message is transmitted;
- 2> prohibit transmission of RRC messages on all signalling radio bearers in the IE "ESTABLISHED\_RABS" except the radio bearer where the response message is transmitted;

2> consider the new integrity protection configuration to include any new keys that were activated through a security procedure received prior to the current message but not applied for the signalling radio bearer, due to the activation time for the corresponding signalling radio bearer not having elapsed;

- 2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer in the IE "ESTABLISHED\_RABS" except RB<sub>m</sub> at the next received RRC message disregarding any pending activation times for the corresponding signalling radio bearer;
- 2> start applying the new integrity protection configuration in the downlink for signalling radio bearer RB<sub>m</sub> from and including the received configuration message;
- 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB<sub>n</sub> from and including the transmitted response message;
- 2> start applying the new integrity protection configuration in the uplink for signalling radio bearers other than RB<sub>n</sub> from the first message onwards ~~at the uplink activation time included in the IE "Uplink integrity protection activation info".~~

NOTE : The UTRAN should ignore the information included in the IE "Uplink integrity protection info".

- 1> if IE "Integrity protection mode command" has the value "modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and this IE was included in SECURITY MODE COMMAND:
  - 2> store the (oldest currently used) integrity protection configuration until activation times have elapsed for the new integrity protection configuration to be applied on all signalling radio bearers;
  - 2> if there are pending activation times set for integrity protection by a previous procedure changing the integrity protection configuration:
    - 3> apply the integrity protection configuration at this pending activation time as indicated in this procedure.
  - 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each signalling radio bearer n, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info";
  - 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1;
    - 3> if present, use the algorithm indicated by the IE "Integrity protection algorithm" (UIA [40]);
  - 2> set the content of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO according to the following:
    - 3> for each established signalling radio bearer, stored in the variable ESTABLISHED\_RABS:
      - 4> select a value of the RRC sequence number at which (activation) time the new integrity protection configuration shall be applied in uplink for that signalling radio bearer according to the following:

- 5> for each signalling radio bearer that has no pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
  - 6> set a suitable value that would ensure a minimised delay in the change to the latest integrity protection configuration.
- 5> for signalling radio bearer that has a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
  - 6> set the same value as the pending activation time for integrity protection;
- 5> consider this (pending) activation time to be elapsed when the selected activation time (as above) is equal to the next RRC sequence number to be used, which means that the last RRC message using the old integrity protection configuration has been submitted to lower layers.
- 4> for signalling radio bearer RB0:
  - 5> set the value of the included RRC sequence number to greater than or equal to the current value of the RRC sequence number for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO, plus the value of the constant N302 plus one.
- 4> prohibit the transmission of RRC messages on all signalling radio bearers, except for RB2, with RRC SN greater than or equal to the value in the "RRC message sequence number list" for the signalling radio bearer in the IE "Uplink integrity protection activation info" of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 2> start applying the new integrity protection configuration in the uplink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Uplink integrity protection activation info", included in the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
- 2> start applying the new integrity protection configuration in the uplink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration;
- 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info";

NOTE: For signalling radio bearers that have a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration, UTRAN should set this value in IE "Downlink integrity protection activation info".

- 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration.

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and the IE "Integrity protection mode command info" was not included in the message SECURITY MODE COMMAND; or

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and the IE "Integrity protection mode info" was included in the message SECURITY MODE COMMAND, and the IE "Integrity protection algorithm" is not included; or

If the IE "Integrity protection mode command" has the value "Modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not Started"; or

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started", and the IE "Integrity protection mode command info" was included in the message SECURITY MODE COMMAND; or

If there does not exist exactly one integrity protection activation time in the IE "Downlink integrity protection activation info" for each established signalling radio bearer included in the IE "Signalling radio bearer information" in the IE "ESTABLISHED\_RABS"; or

If IE "Integrity protection mode command" has the value "Modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started", and the IE "Integrity protection mode info" was not included in the message SECURITY MODE COMMAND:

the UE shall:

- 1> ignore this attempt to change the integrity protection configuration; and
- 1> set the variable INVALID\_CONFIGURATION to TRUE.

If the IE "Integrity protection mode info" is not present, the UE shall:

- 1> not change the integrity protection configuration.

### 8.6.3.6 Void

### 8.6.4.8 RB mapping info

If the IE "RB mapping info" is included, the UE shall:

- 1> for each multiplexing option of the RB:
  - 2> if a transport channel that would not exist as a result of the message (i.e. removed in the same message in IE "Deleted DL TrCH information" and IE "Deleted UL TrCH information") is referred to:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if a multiplexing option that maps a logical channel corresponding to a TM-RLC entity onto RACH, CPCH, FACH or DSCH is included:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if the multiplexing option realises the radio bearer on the uplink (resp. on the downlink) using two logical channels with different values of the IE "Uplink transport channel type" (resp. of the IE "Downlink transport channel type"):
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if that RB is using TM and the IE "Segmentation indication" is set to TRUE and, based on the multiplexing configuration resulting from this message, the logical channel corresponding to it is mapped onto the same transport channel as another logical channel:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if the transport channel considered in that multiplexing option is different from RACH and if that RB is using AM and the set of RLC sizes applicable to the logical channel transferring data PDUs has more than one element:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if that RB is using UM or TM and the multiplexing option realises it using two logical channels:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> for each logical channel in that multiplexing option:
    - 3> if the value of the IE "RLC size list" is set to "Explicit list":
      - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is included in the same message, and the value (index) of any IE "RLC size index" in the IE "Explicit list" does not correspond to an "RLC size" in the IE transport format set of that transport channel given in the message; or

- 4> if the transport channel this logical channel is mapped on in this multiplexing option is different from RACH, and if a "Transport format set" for that transport channel is not included in the same message, and the value (index) of any IE "RLC size index" in the IE "Explicit list" does not correspond to an "RLC size" in the stored transport format set of that transport channel; or
- 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is included in the same message, and the value of any IE "Logical channel list" in the transport format set is not set to "Configured"; or
- 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is not included in the same message, and the value of any IE "Logical channel list" in the stored transport format set of that transport channel is not set to "Configured":
  - 5> set the variable INVALID\_CONFIGURATION to TRUE.
- 3> if the value of the IE "RLC size list" is set to "All":
  - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is included in the same message, and the value of any IE "Logical channel list" in the transport format set is not set to "Configured"; or
  - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is not included in the same message, and the value of any IE "Logical channel list" in the stored transport format set of that transport channel is not set to "Configured":
    - 5> set the variable INVALID\_CONFIGURATION to TRUE.
- 3> if the value of the IE "RLC size list" is set to "Configured":
  - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is included in the same message, and for none of the RLC sizes defined for that transport channel in the "Transport format set", the "Logical Channel List" is set to "All" or given as an "Explicit List" which contains this logical channel; or
  - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is not included in the same message, and for none of the RLC sizes defined in the transport format set stored for that transport channel, the "Logical Channel List" is set to "All" or given as an "Explicit List" which contains this logical channel:
    - 5> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if, as a result of the message this IE is included in, several radio bearers can be mapped onto the same transport channel, and the IE "Logical Channel Identity" was not included in the RB mapping info of any of those radio bearers for a multiplexing option on that transport channel or the same "Logical Channel Identity" was used more than once in the RB mapping info of those radio bearers for the multiplexing options on that transport channel:
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> delete all previously stored multiplexing options for that radio bearer;
- 1> store each new multiplexing option for that radio bearer;
- 1> select and configure the multiplexing options applicable for the transport channels to be used;
- 1> if the IE "Uplink transport channel type" is set to the value "RACH":
  - 2> in FDD:
    - 3> refer the IE "RLC size index" to the RACH Transport Format Set of the first PRACH received in the IE "PRACH system information list" received in SIB5 or SIB6.
  - 2> in TDD:
    - 3> use the first Transport Format of the PRACH of the IE "PRACH system information list" at the position equal to the value in the IE "RLC size index".



1> determine the sets of RLC sizes that apply to the logical channels used by that RB, based on the IEs "RLC size list" and/or the IEs "Logical Channel List" included in the applicable "Transport format set" (either the ones received in the same message or the ones stored if none were received); and

1> in case the selected multiplexing option is a multiplexing option on RACH:

2> ignore the RLC size indexes that do not correspond to any RLC size within the Transport Format Set stored for RACH.

1> if RACH is the transport channel to be used on the uplink, if that RB has a multiplexing option on RACH and if it is using AM:

2> apply the largest size amongst the ones derived according to the previous bullet for the RLC size (or RLC sizes in case the RB is realised using two logical channels) for the corresponding RLC entity.

Note: The IE "RB mapping info" is only included in IE "Predefined RB configurations" in system information when used for Inter-RAT handover to UTRAN and there is no AM RLC size change involved in this case.

1> if that RB is using AM and the RLC size applicable to the logical channel transporting data PDUs is different from the one derived from the previously stored configuration:

2> re-establish the corresponding RLC entity;

2> configure the corresponding RLC entity with the new RLC size;

2> for each AM RLC radio bearer in the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS whose RLC size is changed; and

2> for each AM RLC signalling radio bearer in the CN domain as indicated in the IE "CN domain identity" in the variable LATEST\_CONFIGURED\_CN\_DOMAIN whose RLC size is changed:

3> if the IE "Status" in the variable CIPHERING\_STATUS of this CN domain is set to "Started":

~~4> if this IE was included in system information:~~

~~5> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" for this CN domain that will be included in the CELL UPDATE message that will be sent before the next transmission.~~

4> if this IE was included in CELL UPDATE CONFIRM:

5> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" included in the latest transmitted CELL UPDATE message for this CN domain.

4> if this IE was included in a reconfiguration message:

5> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" that will be included in the reconfiguration complete message for this CN domain.

1> if that RB is using UM:

2> indicate the largest applicable RLC size to the corresponding RLC entity.

1> configure MAC multiplexing according to the selected multiplexing option (MAC multiplexing shall only be configured for a logical channel if the transport channel it is mapped on according to the selected multiplexing option is the same as the transport channel another logical channel is mapped on according to the multiplexing option selected for it);

1> configure the MAC with the logical channel priorities according to selected multiplexing option;

1> configure the MAC with the set of applicable RLC Sizes for each of the logical channels used for that RB;

1> if there is no multiplexing option applicable for the transport channels to be used:

2> set the variable INVALID\_CONFIGURATION to TRUE.

1> if there is more than one multiplexing option applicable for the transport channels to be used:

2> set the variable INVALID\_CONFIGURATION to TRUE.

In case IE "RLC info" includes IE "Downlink RLC mode" ("DL RLC logical channel info" is mandatory present) but IE "Number of downlink RLC logical channels" is absent in the corresponding IE "RB mapping info", the parameter values are exactly the same as for the corresponding UL logical channels. In case two multiplexing options are specified for the UL, the first options shall be used as default for the DL. As regards the IE "Channel type", the following rule should be applied to derive the DL channel type from the UL channel included in the IE:

Channel used in UL	DL channel type implied by "same as"
DCH	DCH
RACH	FACH
CPCH	FACH
USCH	DSCH

### 10.2.1 ACTIVE SET UPDATE

NOTE: Only for FDD.

This message is used by UTRAN to add, replace or delete radio links in the active set of the UE.

RLC-SAP: AM or UM

Logical channel: DCCH

Direction: UTRAN → UE

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message Type	MP		Message Type	
<b>UE information elements</b>				
RRC transaction identifier	MP		RRC transaction identifier 10.3.3.36	
Integrity check info	CH		Integrity check info 10.3.3.16	
<del>Integrity protection mode info</del>	<del>OP</del>		<del>Integrity protection mode info 10.3.3.19</del>	
<del>Ciphering mode info</del>	<del>OP</del>		<del>Ciphering mode info 10.3.3.5</del>	
Activation time	MD		Activation time 10.3.3.1	Default value is "now".
New U-RNTI	OP		U-RNTI 10.3.3.47	
<b>CN information elements</b>				
CN Information info	OP		CN Information info 10.3.1.3	
<b>RB information elements</b>				
<del>Downlink counter synchronisation info</del>	<del>OP</del>			
<del>&gt;RB with PDCP information list</del>	<del>OP</del>	1 to <maxRBall RABs>		<del>This IE is needed for each RB having PDCP in the case of lossless SRNS relocation</del>
<del>&gt;&gt;RB with PDCP information</del>	<del>MP</del>		<del>RB with PDCP information 10.3.4.22</del>	
<b>Phy CH information elements</b>				

Information Element/Group name	Need	Multi	Type and reference	Semantics description
<b>Uplink radio resources</b>				
Maximum allowed UL TX power	MD		Maximum allowed UL TX power 10.3.6.39	Default value is the existing "maximum UL TX power.
<b>Downlink radio resources</b>				
Radio link addition information	OP	1 to <maxRL-1>		Radio link addition information required for each RL to add
>Radio link addition information	MP		Radio link addition information 10.3.6.68	
Radio link removal information	OP	1 to <maxRL>		Radio link removal information required for each RL to remove
>Radio link removal information	MP		Radio link removal information 10.3.6.69	
TX Diversity Mode	MD		TX Diversity Mode 10.3.6.86	Default value is the existing TX diversity mode.
SSDT information	OP		SSDT information 10.3.6.77	

## 10.2.2 ACTIVE SET UPDATE COMPLETE

NOTE: For FDD only.

This message is sent by UE when active set update has been completed.

RLC-SAP: AM

Logical channel: DCCH

Direction: UE→UTRAN

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message Type	MP		Message Type	
<b>UE information elements</b>				
RRC transaction identifier	MP		RRC transaction identifier 10.3.3.36	
Integrity check info	CH		Integrity check info 10.3.3.16	
Uplink integrity protection activation info	OP		Integrity protection activation info 10.3.3.17	
<b>RB Information elements</b>				
Radio bearer uplink ciphering activation time info	OP		RB activation time info 10.3.4.13	
Uplink counter synchronisation info	OP			
>RB with PDCP information list	OP	1 to		This IE is needed for each RB

Information Element/Group name	Need	Multi	Type and reference	Semantics description
		<maxRBall RABs>		having PDCP in the case of lossless SRNS relocation
>>RB-with-PDCP-information	MP		RB-with PDCP information 10.3.4.22	
>START-list	MP	1 to <maxCNdomains>		START [40] values for all CN domains.
>>CN-domain-identity	MP		CN-domain identity 10.3.1.1	
>>START	MP		START 10.3.3.38	START value to be used in this CN domain.

### 10.2.3 ACTIVE SET UPDATE FAILURE

NOTE: Only for FDD.

This message is sent by UE if the update of the active set has failed, e.g. because the radio link is not a part of the active set.

RLC-SAP: AM

Logical channel: DCCH

Direction: UE→UTRAN

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message Type	MP		Message Type	
<b>UE information elements</b>				
RRC transaction identifier	MP		RRC transaction identifier 10.3.3.36	
Integrity check info	CH		Integrity check info 10.3.3.16	
Failure cause	MP		Failure cause and error information 10.3.3.14	

#### 10.3.3.4 Ciphering Algorithm

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Ciphering algorithm	MP		Enumerated (UEA0, UEA1)	

#### 10.3.3.5 Ciphering mode info

This information element contains the ciphering specific security mode control information.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Ciphering mode command	MP		Enumerated (start/restart, stop)	<del>The command "stop" is not used in this version of the protocol.</del>
Ciphering algorithm	<del>CV-</del> <del>notStop</del> MP		Ciphering algorithm 10.3.3.4	
Ciphering activation time for DPCH	OP		Activation time 10.3.3.1	Used for radio bearers mapped on RLC-TM. Only applicable if the UE is already in CELL_DCH state
Radio bearer downlink ciphering activation time info	OP		RB activation time info, 10.3.4.13	Used for radio bearers mapped on RLC-AM or RLC-UM

Condition	Explanation
<del>notStop</del>	<del>The IE is mandatory present if the IE "Ciphering mode command" has the value "start/restart", otherwise the IE is not needed in the message.</del>

### 10.3.3.6 CN domain specific DRX cycle length coefficient

A coefficient in the formula to count the paging occasions to be used by a specific UE (specified in [4]).

Information Element/Group name	Need	Multi	Type and reference	Semantics description
CN domain specific DRX cycle length coefficient	MP		Integer(6...9)	Refers to 'k' in the formula as specified in [4], Discontinuous reception

### 10.3.3.7 CPCH Parameters

NOTE: Only for FDD.

These parameters are used by any UE using any CPCH set allocated to the cell that is broadcasting this system information.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Initial Priority Delay	OP	1 to maxASC		Initial delays for ASC priority.
>NS_IP	MP		Integer (0...28)	Number of slots for initial fixed delay for each ASC priority level
Backoff control parameters	MP			
>N_ap_retrans_max	MP		Integer (1...64)	Max number of AP transmissions without AP-AICH response, a PHY parameter.
>N_access_fails	MP		Integer (1...64)	Max number of preamble ramping cycles when NAK response received, a MAC parameter.
>NF_bo_no aich	MP		Integer (0...31)	Number of frames for UE backoff after N <sub>ap_retrans_max</sub> unsuccessful AP access attempts, a MAC parameter.
>NS_bo_busy	MP		Integer (0...63)	Number of slots for UE fixed backoff after access attempt to busy CPCH, a MAC parameter.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
>NF_bo_all_busy	MP		Integer (0...31)	Max number of frames for UE backoff after access attempt to last busy CPCH, a MAC parameter. UE randomly selects backoff value from range (0..NF_bo_all_busy)
>NF_bo_mismatch	MP		Integer (0...127)	Max number of frames for the UE backoff after received mismatch on CD/CA-ICH, a MAC parameter. UE randomly selects backoff value from range (0..NF_bo_mismatch)
>T_CPCH	MP		Enumerated (0, 1)	CPCH channel timing used to determine Tau, a PHY parameter
Power Control Algorithm	MP		Enumerated (algorithm 1, algorithm 2)	Specifies algorithm to be used by UE to interpret TPC commands
TPC step size	CV- <i>algo</i>		Integer (1, 2)	In dB
DL DPCCH BER	MP		Integer (0..63)	The BER quality value shall be set in the range $0 \leq \text{DPCCH BER} \leq 1$ in the unit BER_dB where:  BER_dB_0: DPCCH BER = 0  BER_dB_1: $-\infty < \text{Log}_{10}(\text{DPCCH BER}) < -4.03$  BER_dB_2: $-4.03 \leq \text{Log}_{10}(\text{DPCCH BER}) < -3.965$  BER_dB_3: $-3.965 \leq \text{Log}_{10}(\text{DPCCH BER}) < -3.9$ ... BER_dB_61: $-0.195 \leq \text{Log}_{10}(\text{DPCCH BER}) < -0.13$  BER_dB_62: $-0.13 \leq \text{Log}_{10}(\text{DPCCH BER}) < -0.065$  BER_dB_63: $-0.065 \leq \text{Log}_{10}(\text{DPCCH BER}) \leq 0$

Condition	Explanation
<i>algo</i>	The IE is mandatory present if "Power Control Algorithm" is set to "algorithm 1", otherwise the IE is not needed

### 10.3.3.8 C-RNTI

The cell RNTI (C-RNTI) identifies an UE having a RRC connection within a cell.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
C-RNTI	MP		bit string(16)	

### 10.3.3.9 DRAC system information

Information element	Need	Multi	Type and reference	Semantics description
DRAC system information	MP	1 to <maxDRA Cclasses>		DRAC information is sent for each class of terminal
>Transmission probability	MP		Transmission probability 10.3.3.39	
>Maximum bit rate	MP		Maximum bit rate 10.3.3.20	

#### 10.3.3.9a DSCH-RNTI

In FDD, the DSCH-RNTI identifies an UE in CELL\_DCH using a DSCH within a cell. In TDD, the DSCH-RNTI identifies a UE in CELL\_DCH or CELL\_FACH using a DSCH or USCH within the cell.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
DSCH-RNTI	MP		bit string(16)	

#### ~~10.3.3.10 RRC State Indicator~~

~~Indicates to a UE the RRC state to be entered.~~

<del>Information Element/Group name</del>	<del>Need</del>	<del>Multi</del>	<del>Type and reference</del>	<del>Semantics description</del>
<del>RRC State indicator</del>	<del>MP</del>		<del>Enumerated(CELL_DCH, CELL_FACH, CELL_PCH, URA_PCH)</del>	

#### 10.3.3.35 RLC re-establish indicator

This IE is used to re-configure AM RLC on c-plane and u-plane.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
RLC re-establish indicator	MP		Boolean	TRUE means re-establish required FALSE means re-establish not required

#### 10.3.3.35a RRC State Indicator

Indicates to a UE the RRC state to be entered.

<u>Information Element/Group name</u>	<u>Need</u>	<u>Multi</u>	<u>Type and reference</u>	<u>Semantics description</u>
<u>RRC State indicator</u>	<u>MP</u>		<u>Enumerated(CELL_DCH, CELL_FACH, CELL_PCH, URA_PCH)</u>	

### 10.3.3.36 RRC transaction identifier

This IE contains an identification of the RRC procedure transaction local for the type of the message this IE was included within.

<b>Information Element/Group name</b>	<b>Need</b>	<b>Multi</b>	<b>Type and reference</b>	<b>Semantics description</b>
RRC transaction identifier	MP		Integer (0..3)	

### 10.3.3.37 Security capability

<b>Information Element/Group name</b>	<b>Need</b>	<b>Multi</b>	<b>Type and reference</b>	<b>Semantics description</b>
Ciphering algorithm capability	MP			
>UEA0	MP		Boolean	<del>The value TRUE means that an unciphered connection after the Security mode control procedure is accepted by the UE.</del>
>UEA1	MP		Boolean	<del>The value TRUE means that UEA1, Kasumi, is supported</del>
>Spare	MP	14	Boolean	Shall be set to FALSE by UEs complying with this version of the protocol.
Integrity protection algorithm capability	MP			
>UIA1	MP		Boolean	The value TRUE means that UIA1, Kasumi, is supported
>Spare	MP	15	Boolean	Shall be set to FALSE by UEs complying with this version of the protocol.

~~NOTE: The UE shall support at least one UEAx other than UEA0 and one UIAx.~~

### 10.3.3.38 START

There is a START value per CN domain. The START is used to initialise the 20 MSBs of all hyper frame numbers (MAC-d HFN, RLC UM HFN, RLC AM HFN, RRC HFN) for a CN domain.

<b>Information Element/Group name</b>	<b>Need</b>	<b>Multi</b>	<b>Type and Reference</b>	<b>Semantics description</b>
START	MP		Bit string (20)	The START [40] bits are numbered b0-b19, where b0 is the least significant bit.

```
-- *****
--
-- ACTIVE SET UPDATE (FDD only)
--
-- *****
```

```
ActiveSetUpdate ::= CHOICE {
```



```

r3
  activeSetUpdate-r3          SEQUENCE {
    v4xyNonCriticalExtensions SEQUENCE {
      activeSetUpdate-v4xyext ActiveSetUpdate-v4xyext-IEs,
      nonCriticalExtensions   SEQUENCE {} OPTIONAL
    } OPTIONAL
  },
  later-than-r3              SEQUENCE {
    rrc-TransactionIdentifier RRC-TransactionIdentifier,
    criticalExtensions        SEQUENCE {}
  }
}

ActiveSetUpdate-r3-IEs ::= SEQUENCE {
  -- User equipment IEs
  rrc-TransactionIdentifier RRC-TransactionIdentifier,
  -- dummy and dummy2 are not used in this version of the specification, they should
-- not be sent and if received they should be ignored.
  integrityProtectionModeInfodummy IntegrityProtectionModeInfo OPTIONAL,
  cipheringModeInfodummy2 CipheringModeInfo OPTIONAL,
  activationTime ActivationTime OPTIONAL,
  newU-RNTI U-RNTI OPTIONAL,
  -- Core network IEs
  cn-InformationInfo CN-InformationInfo OPTIONAL,
  -- Radio bearer IEs
  -- dummy3 is not used in this version of the specification, it should
-- not be sent and if received it should be ignored.
  dl-CounterSynchronisationInfodummy3 DL-CounterSynchronisationInfo OPTIONAL,
  -- Physical channel IEs
  maxAllowedUL-TX-Power MaxAllowedUL-TX-Power OPTIONAL,
  rl-AdditionInformationList RL-AdditionInformationList OPTIONAL,
  rl-RemovalInformationList RL-RemovalInformationList OPTIONAL,
  tx-DiversityMode TX-DiversityMode OPTIONAL,
  ssdt-Information SSDT-Information OPTIONAL
}

ActiveSetUpdate-v4xyext-IEs ::= SEQUENCE {
  -- Physical channel IEs
  -- ssdt-UL extends SSDT-Information. FDD only.
  ssdt-UL SSDT-UL-r4 OPTIONAL,
  -- The order of the RLs in IE cell-id-PerRL-List is the same as
  -- in IE RL-AdditionInformationList included in this message
  cell-id-PerRL-List CellIdentity-PerRL-List OPTIONAL
}

-- *****
--
-- ACTIVE SET UPDATE COMPLETE (FDD only)
--
-- *****

ActiveSetUpdateComplete ::= SEQUENCE {
  -- User equipment IEs
  rrc-TransactionIdentifier RRC-TransactionIdentifier,
  -- dummy is not used in this version of the specification, it should
-- not be sent and if received it should be ignored.
  ul-IntegProtActivationInfodummy IntegrityProtActivationInfo OPTIONAL,
  -- Radio bearer IEs
  -- dummy2 and dummy3 are not used in this version of the specification, they should
-- not be sent and if received they should be ignored.
  rb-UL-CiphActivationTimeInfodummy2 RB-ActivationTimeInfoList OPTIONAL,
  ul-CounterSynchronisationInfodummy3 UL-CounterSynchronisationInfo OPTIONAL,
  -- Extension mechanism for non- release99 information
  nonCriticalExtensions SEQUENCE {} OPTIONAL
}

-- *****
--
-- ACTIVE SET UPDATE FAILURE (FDD only)
--
-- *****

ActiveSetUpdateFailure ::= SEQUENCE {
  -- User equipment IEs
  rrc-TransactionIdentifier RRC-TransactionIdentifier,
  failureCause FailureCauseWithProtErr,
  -- Extension mechanism for non- release99 information

```

```

        nonCriticalExtensions          SEQUENCE {} OPTIONAL
    }
}
-----
ChipRateCapability ::=
    ENUMERATED {
        mcps3-84, mcps1-28 }

CipheringAlgorithm ::=
    ENUMERATED {
        uea0, uea1 }

CipheringModeCommand ::=
    CHOICE {
        startRestart
        stopCiphering dummy
        CipheringAlgorithm,
        NULL
    }

CipheringModeInfo ::=
    SEQUENCE {
        -- TABULAR: The ciphering algorithm is included in the CipheringModeCommand.
        cipheringModeCommand          CipheringModeCommand,
        activationTimeForDPCH          ActivationTime          OPTIONAL,
        rb-DL-CiphActivationTimeInfo    RB-ActivationTimeInfoList  OPTIONAL
    }

```

## 11.5 RRC information between network nodes

```
Internode-definitions DEFINITIONS AUTOMATIC TAGS ::=
```

```
BEGIN
```

```
IMPORTS
```

```

    HandoverToUTRANCommand,
    MeasurementReport,
    PhysicalChannelReconfiguration,
    RadioBearerReconfiguration,
    RadioBearerRelease,
    RadioBearerSetup,
    RRC-FailureInfo-r3-IEs,
    TransportChannelReconfiguration
FROM PDU-definitions

```

```

-- Core Network IEs :
    CN-DomainIdentity,
    CN-DomainInformationList,
    CN-DRX-CycleLengthCoefficient,
    NAS-SystemInformationGSM-MAP,
-- UTRAN Mobility IEs :
    CellIdentity,
    URA-Identity,
-- User Equipment IEs :
    C-RNTI,
    DL-PhysChCapabilityFDD-v380ext,
    FailureCauseWithProtErr,
    RRC-MessageSequenceNumber,
    STARTList,
    STARTSingle
    START-Value,
    U-RNTI,
    UE-RadioAccessCapability,
    UE-RadioAccessCapability-v370ext,
    UE-RadioAccessCapability-v380ext,
    UE-RadioAccessCapability-v3a0ext,
    UE-RadioAccessCapability-v4xyext,
-- Radio Bearer IEs :
    PredefinedConfigStatusList,
    PredefinedConfigValueTag,
    RAB-InformationSetupList,
    RAB-Identity,
    SRB-InformationSetupList,
-- Transport Channel IEs :
    CPCH-SetID,
    DL-CommonTransChInfo,
    DL-AddReconfTransChInfoList,
    DRAC-StaticInformationList,
    UL-CommonTransChInfo,
    UL-AddReconfTransChInfoList,
-- Measurement IEs :

```

```

MeasurementIdentity,
MeasurementReportingMode,
MeasurementType,
MeasurementType-r4,
AdditionalMeasurementID-List,
PositionEstimate,
UE-Positioning-IPDL-Parameters-TDD-r4-ext,
-- Other IEs :
InterRAT-UE-RadioAccessCapabilityList
FROM InformationElements

maxCNdomains,
maxNoOfMeas,

maxRB,
maxSRBsetup
FROM Constant-definitions
;

-- Part 1: Class definitions similar to what has been defined in 11.1 for RRC messages
-- Information that is tranferred in the same direction and across the same path is grouped
-- *****
--
-- RRC information, to target RNC
--
-- *****
-- RRC Information to target RNC sent either from source RNC or from another RAT

ToTargetRNC-Container ::= CHOICE {
    interRATHandoverInfo          InterRATHandoverInfoWithInterRATCapabilities-r3,
    srncRelocation                SRNC-RelocationInfo-r3,
    extension                      NULL
}

-- *****
--
-- RRC information, target RNC to source RNC
--
-- *****

Target-RNC-ToSourceRNC-Container ::= CHOICE {
    radioBearerSetup              RadioBearerSetup,
    radioBearerReconfiguration    RadioBearerReconfiguration,
    radioBearerRelease            RadioBearerRelease,
    transportChannelReconfiguration TransportChannelReconfiguration,
    physicalChannelReconfiguration PhysicalChannelReconfiguration,
    rrc-FailureInfo               RRC-FailureInfo-r3-IEs,
    extension                      NULL
}

-- Part 2: Container definitions, similar to the PDU definitions in 11.2 for RRC messages
-- In alphabetical order

-- *****
--
-- Handover to UTRAN information
--
-- *****

InterRATHandoverInfoWithInterRATCapabilities-r3 ::= CHOICE {
    r3                             SEQUENCE {
        -- IE InterRATHandoverInfoWithInterRATCapabilities-r3-IEs also
        -- includes non critical extensions
        interRATHandoverInfo-r3      InterRATHandoverInfoWithInterRATCapabilities-r3-IEs,
        v390NonCriticalExtensions    SEQUENCE {
            interRATHandoverInfoWithInterRATCapabilities-v390ext
        }
        InterRATHandoverInfoWithInterRATCapabilities-v390ext-IEs,
        -- Reserved for future non critical extension
        nonCriticalExtensions        SEQUENCE {} OPTIONAL
    } OPTIONAL
},
criticalExtensions                SEQUENCE {}
}

InterRATHandoverInfoWithInterRATCapabilities-r3-IEs ::= SEQUENCE {

```

```

-- The order of the IEs may not reflect the tabular format
-- but has been chosen to simplify the handling of the information in the BSC
-- Other IEs
ue-RATSpecificCapability      InterRAT-UE-RadioAccessCapabilityList  OPTIONAL,
-- interRATHandoverInfo, Octet string is used to obtain 8 bit length field prior to
-- actual information. This makes it possible for BSS to transparently handle information
-- received via GSM air interface even when it includes non critical extensions.
-- The octet string shall include the InterRATHandoverInfo information
-- The BSS can re-use the 04.18 length field received from the MS
interRATHandoverInfo          OCTET STRING (SIZE (0..255))
}

InterRATHandoverInfoWithInterRATCapabilities-v390ext-IEs ::= SEQUENCE {
  -- User equipment IEs
  failureCauseWithProtErr      FailureCauseWithProtErr          OPTIONAL
}

-- *****
--
-- SRNC Relocation information
--
-- *****

SRNC-RelocationInfo-r3 ::= CHOICE {
  r3                            SEQUENCE {
    sRNC-RelocationInfo-r3      SRNC-RelocationInfo-r3-IEs,
    v380NonCriticalExtensions    SEQUENCE {
      sRNC-RelocationInfo-v380ext SRNC-RelocationInfo-v380ext-IEs,
      -- Reserved for future non critical extension
      v390NonCriticalExtensions  SEQUENCE {
        sRNC-RelocationInfo-v390ext SRNC-RelocationInfo-v390ext-IEs,
        v3a0NonCriticalExtensions  SEQUENCE {
          sRNC-RelocationInfo-v3a0ext SRNC-RelocationInfo-v3a0ext-IEs,
          v4xyNonCriticalExtensions SEQUENCE {
            sRNC-RelocationInfo-v4xyext SRNC-RelocationInfo-v4xyext-IEs,
            v3b0NonCriticalExtensions SEQUENCE {
            SRNC-RelocationInfo-v3b0ext SRNC-RelocationInfo-v3b0ext-IEs,
            -- Reserved for future non critical extension
            nonCriticalExtensions SEQUENCE {} OPTIONAL
            -- Reserved for future non critical extension
            nonCriticalExtensions SEQUENCE {} OPTIONAL
          }
        } OPTIONAL
      } OPTIONAL
    } OPTIONAL
  },
  criticalExtensions            SEQUENCE {}
}

SRNC-RelocationInfo-r3-IEs ::= SEQUENCE {
  -- Non-RRC IEs
  stateOfRRC                    StateOfRRC,
  stateOfRRC-Procedure           StateOfRRC-Procedure,
  -- Ciphering related information IEs
  -- If the extension v380 is included use the extension for the ciphering status per CN domain
  cipheringStatus                CipheringStatus,
  calculationTimeForCiphering    CalculationTimeForCiphering      OPTIONAL,
  cipheringInfoPerRB-List        CipheringInfoPerRB-List          OPTIONAL,
  count-C-List                   COUNT-C-List                        OPTIONAL,
  integrityProtectionStatus       IntegrityProtectionStatus,
  srb-SpecificIntegrityProtInfo   SRB-SpecificIntegrityProtInfoList,
  implementationSpecificParams    ImplementationSpecificParams      OPTIONAL,
  -- User equipment IEs
  u-RNTI                          U-RNTI,
  c-RNTI                          C-RNTI                            OPTIONAL,
  ue-RadioAccessCapability        UE-RadioAccessCapability,
  ue-Positioning-LastKnownPos     UE-Positioning-LastKnownPos      OPTIONAL,
  -- Other IEs
  ue-RATSpecificCapability        InterRAT-UE-RadioAccessCapabilityList  OPTIONAL,
  -- UTRAN mobility IEs
  ura-Identity                    URA-Identity                            OPTIONAL,
  -- Core network IEs
  cn-CommonGSM-MAP-NAS-SysInfo    NAS-SystemInformationGSM-MAP,
  cn-DomainInformationList        CN-DomainInformationList          OPTIONAL,
  -- Measurement IEs
  ongoingMeasRepList              OngoingMeasRepList                OPTIONAL,
  -- Radio bearer IEs
  predefinedConfigStatusList      PredefinedConfigStatusList,

```

```

    srb-InformationList          SRB-InformationSetupList,
    rab-InformationList          RAB-InformationSetupList          OPTIONAL,
-- Transport channel IEs
    ul-CommonTransChInfo        UL-CommonTransChInfo            OPTIONAL,
    ul-TransChInfoList          UL-AddReconfTransChInfoList      OPTIONAL,
    modeSpecificInfo            CHOICE {
        fdd                     SEQUENCE {
            cpch-SetID          CPCH-SetID                    OPTIONAL,
            transChDRAC-Info    DRAC-StaticInformationList  OPTIONAL
        },
        tdd                     NULL
    },
    dl-CommonTransChInfo        DL-CommonTransChInfo            OPTIONAL,
    dl-TransChInfoList          DL-AddReconfTransChInfoList      OPTIONAL,
-- Measurement report
    measurementReport           MeasurementReport            OPTIONAL,
    nonCriticalExtensions        SEQUENCE {
        -- In case of TDD only up-Ipdl-Parameters-TDD is present, otherwise
        -- this IE is absent
        up-Ipdl-Parameters-TDD  UE-Positioning-IPDL-Parameters-TDD-r4-ext  OPTIONAL,
        -- Extension mechanism for non- release4 information
        nonCriticalExtensions    SEQUENCE {}
    }
}

SRNC-RelocationInfo-v380ext-IEs ::= SEQUENCE {
    -- Ciphering related information IEs
    cn-DomainIdentity           CN-DomainIdentity,
    cipheringStatusList         CipheringStatusList
}

SRNC-RelocationInfo-v390ext-IEs ::= SEQUENCE {
    cn-DomainInformationList-v390ext  CN-DomainInformationList-v390ext          OPTIONAL,
    ue-RadioAccessCapability-v370ext  UE-RadioAccessCapability-v370ext          OPTIONAL,
    ue-RadioAccessCapability-v380ext  UE-RadioAccessCapability-v380ext          OPTIONAL,
    dl-PhysChCapabilityFDD-v380ext    DL-PhysChCapabilityFDD-v380ext,
    failureCauseWithProtErr          FailureCauseWithProtErr                    OPTIONAL
}

SRNC-RelocationInfo-v3a0ext-IEs ::= SEQUENCE {
    -- cn-domain identity for IE startValueForCiphering-v3a0ext is specified
    -- in subsequent extension (SRNC-RelocationInfo-v3b0ext-IEs)
    startValueForCiphering-v3a0ext    START-Value,
    cipheringInfoForSRB1-v3a0ext      CipheringInfoForSRB1-v3a0ext,
    ue-RadioAccessCapability-v3a0ext  UE-RadioAccessCapability-v3a0ext          OPTIONAL
}

SRNC-RelocationInfo-v4xyext-IEs ::= SEQUENCE {
    ue-RadioAccessCapability-v4xyext  UE-RadioAccessCapability-v4xyext
}

SRNC-RelocationInfo-v3b0ext-IEs ::= SEQUENCE {
-- cn-domain identity for IE startValueForCiphering-v3a0ext included in previous extension
cn-DomainIdentity                 CN-DomainIdentity,
-- the remaining start values are contained in IE startValueForCiphering-v3b0ext
startValueForCiphering-v3b0ext    STARTList2
OPTIONAL
}

STARTList2 ::=
SEQUENCE (SIZE (2..maxCNdomains)) OF
STARTSingle

CipheringInfoForSRB1-v3a0ext ::= SEQUENCE {
    dl-UM-SN                       BIT STRING (SIZE (7))
}

CipheringStatusList ::=
    SEQUENCE (SIZE (1..maxCNdomains)) OF
    CipheringStatusCNdomain

CipheringStatusCNdomain ::=
    SEQUENCE {
        cn-DomainIdentity          CN-DomainIdentity,
        cipheringStatus            CipheringStatus
    }
}

SRNC-RelocationInfo-r4 ::=
    SEQUENCE {
        -- Non-RRC IEs
        stateOfRRC                 StateOfRRC,
        stateOfRRC-Procedure        StateOfRRC-Procedure,

```

```

    cipheringStatus          CipheringStatus,
    calculationTimeForCiphering  CalculationTimeForCiphering  OPTIONAL,
    cipheringInfoPerRB-List    CipheringInfoPerRB-List    OPTIONAL,
    integrityProtectionStatus  IntegrityProtectionStatus,
    srb-SpecificIntegrityProtInfoList SRB-SpecificIntegrityProtInfoList,
    implementationSpecificParams ImplementationSpecificParams  OPTIONAL,
-- User equipment IEs
    u-RNTI                    U-RNTI,
    c-RNTI                    C-RNTI                    OPTIONAL,
    ue-RadioAccessCapability  UE-RadioAccessCapability,
    ue-Positioning-LastKnownPos UE-Positioning-LastKnownPos  OPTIONAL,
-- Other IEs
    ue-RATSpecificCapability  InterRAT-UE-RadioAccessCapabilityList  OPTIONAL,
-- UTRAN mobility IEs
    ura-Identity              URA-Identity              OPTIONAL,
-- Core network IEs
    cn-CommonGSM-MAP-NAS-SysInfo NAS-SystemInformationGSM-MAP,
    cn-DomainInformationList  CN-DomainInformationList  OPTIONAL,
-- Measurement IEs
    ongoingMeasRepList        OngoingMeasRepList-r4    OPTIONAL,
-- Radio bearer IEs
    predefinedConfigStatusList PredefinedConfigStatusList,
    srb-InformationList       SRB-InformationSetupList,
    rab-InformationList       RAB-InformationSetupList  OPTIONAL,
-- Transport channel IEs
    ul-CommonTransChInfo     UL-CommonTransChInfo     OPTIONAL,
    ul-TransChInfoList       UL-AddReconfTransChInfoList  OPTIONAL,
    modeSpecificInfo         CHOICE {
        fdd                   SEQUENCE {
            cpch-SetID        CPCH-SetID        OPTIONAL,
            transChDRAC-Info  DRAC-StaticInformationList  OPTIONAL
        },
        tdd                   NULL
    },
    dl-CommonTransChInfo     DL-CommonTransChInfo     OPTIONAL,
    dl-TransChInfoList       DL-AddReconfTransChInfoList  OPTIONAL,
-- Measurement report
    measurementReport         MeasurementReport         OPTIONAL,
    nonCriticalExtensions     SEQUENCE {
        -- In case of TDD only up-Ipdl-Parameters-TDD is present, otherwise
        -- this IE is absent
        up-Ipdl-Parameters-TDD  UE-Positioning-IPDL-Parameters-TDD-r4-ext  OPTIONAL,
        -- Extension mechanism for non-release4 information
        nonCriticalExtensions  SEQUENCE {}
    }
}
-- IE definitions

```

---

## Annex A (informative): USIM parameters

### A.1 Introduction

This annex contains recommendations about the RRC parameters to be stored in the USIM.

## A.2 Cipherring information

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Cipher key for each CN domain	MP	<1 to maxCNDo mains>		Cipher key is described in [40].
<del>&gt;Old-CK</del>	MP		Bit string (128)	
<del>&gt;New-CK</del>	MP		<del>Bit string (128)</del>	
Integrity key for each CN domain	MP	<1 to maxCNDo mains>		Integrity key is described in [40].
<del>&gt;Old-IK</del>	MP		Bit string (128)	
<del>&gt;New-IK</del>	MP		<del>Bit string (128)</del>	
THRESHOLD	MP		Bit string (20)	
START value for each CN domain	MP	<1 to maxCNDo mains>		START value is described in [40].
<del>&gt;Old-START</del>	MP		Bit string (20)	
<del>&gt;New-START</del>	MP		<del>Bit string (20)</del>	
KSI, Key set identifier for each CN domain	MP	<1 to maxCNDo mains>		Key set identifier is described in [40].
<del>&gt;Old-KSI</del>	MP		Bit string (3)	
<del>&gt;New-KSI</del>	MP		<del>Bit string (3)</del>	

## A.3 Frequency information

Neighbour cell list.

Information Element/Group name	Need	Multi	Type and reference	Semantics description	Version
FDD cell list	OP	<1 to maxFDDFr eqList>			
>UARFCN uplink (Nu)	OP		Integer(0..16383)	[21] If IE not present, default duplex distance of 190 MHz shall be used.	
>UARFCN downlink (Nd)	MP		Integer(0 .. 16383)	[21]	
>Primary scrambling code	OP	<1 to maxFDDFr eqCellList>	Primary CPICH info 10.3.6.60		
3.84 Mcps TDD cell list	OP	<1 to maxTDDFr eqList>			
>UARFCN (Nt)	MP		Integer(0 .. 16383)	[22]	
>Cell parameters ID	OP	<1 to maxTDDFr eqCellList>	Integer (0..127)	The Cell parameters ID is described in [32].	
1.28 Mcps TDD cell list	OP	<1 to maxTDDFr eqList>			REL-4
>UARFCN (Nt)	MP		Integer(0 ..	[22]	REL-4

Information Element/Group name	Need	Multi	Type and reference	Semantics description	Version
			16383)		
>Cell parameters ID	OP	<1 to maxTDDFr eqCellList>	Integer (0..127)	The Cell parameters ID is described in [32].	REL-4
GSM Neighbour cell list	OP				
>GSM neighbour cell info	MP	<1 to maxGSMCellList>			
>>BSIC	MP				
>>BCCH ARFCN	MP				



## CHANGE REQUEST

⌘ **25.331 CR 1492** ⌘ rev **-** ⌘ Current version: **5.0.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

**Title:** ⌘ Corrections to Security procedure on Missing integrity protection reset on relocation and counter check response actions for asymmetric bearer configurations

**Source:** ⌘ TSG-RAN WG2

**Work item code:** ⌘ TEI

**Date:** ⌘ May 13, 2002

**Category:** ⌘ **A**

**Release:** ⌘ REL-5

Use one of the following categories:

Use one of the following releases:

- F** (correction)
- A** (corresponds to a correction in an earlier release)
- B** (addition of feature),
- C** (functional modification of feature)
- D** (editorial modification)

- 2** (GSM Phase 2)
- R96** (Release 1996)
- R97** (Release 1997)
- R98** (Release 1998)
- R99** (Release 1999)

Detailed explanations of the above categories can be found in 3GPP [TR 21.900](#).

- REL-4** (Release 4)
- REL-5** (Release 5)

- Reason for change:** ⌘
1. It is not clear if SECURITY MODE COMMAND can change ciphering/integrity protection algorithms.
  2. It is not clear if SECURITY MODE COMMAND can be received with "modify" command for integrity protection for a CN domain for which integrity protection has been already configured, if new keys have not been received.
  3. In the COUNTER CHECK procedure it is not clear how the UE should set the COUNT-C values for a radio bearer which is configured only in one direction or is set to RLC-TM mode in one direction and UM in the other.
  4. ACTIVE SET UPDATE cannot be used to trigger actions at the UE for a SRNS Relocation.
  5. UE actions in case of pending activation times for integrity protection following SRNS Relocation are missing.
  6. UE actions in case of previously received new keys not having yet been activated due to activation times not elapsed at the time of SRNS Relocation are missing.
  7. Mis-alignment between Tabular and ASN.1. ASN.1 does not permit the transfer of START for every domain in the Relocation container between source and target as required..
  8. It is incorrectly stated that a R99 UE shall support any one of UIAx integrity protection algorithms when in fact UIA1 shall be supported.
  9. It is not clear in case of START calculation if "non-ciphered" radio bearers refers also to RBs with ciphering algorithm set to UEA0.
  10. It is incorrectly suggested in Annex a that the USIM stores both the new and old keys as well as the old and new START and KSI values. Only one value - the latest - is stored in the USIM.
  11. The ASN.1 still permits the ciphering mode command to be set to "stop".
  12. It is not stated that the UE shall check to see if a new FRESH value was received

before performing the integrity check on the message.

- 13. 10.3.3.10 is not correctly placed in the Tabular according to alphabetical order.
- 14. In 8.6.4.8 it is stated that if the IE "RB Mapping Info" is included in system information and there is a AM RLC size change the UE shall " *set the HFN values for the corresponding RLC entity equal to the value of the IE "START" for this CN domain that will be included in the CELL UPDATE message that will be sent before the next transmission.* " However since the CELL UPDATE will be sent only in the future it is not possible for the UE to set the START value in advance.

**Summary of change: ☞**

- 1. It is clarified that UTRAN should not change ciphering/integrity protection algorithm using the SECURITY MODE COMMAND procedure.
- 2. It is clarified that UTRAN should not transmit SECURITY MODE COMMAND with "modify" command for integrity protection for a CN domain for which integrity protection has been already configured, if new keys have not been received for that domain.
- 3. It is specified that UE shall set an unspecified value for the COUNT-C for the direction of the radio bearer that is either not configured or is set to RLC-TM.
- 4. All security related procedure text in the ACTIVE SET UPDATE procedure and procedure related to ACTIVE SET UPDATE and security in other procedures is deleted. The tabular and ASN.1 have been appropriately updated.
- 5. It is specified that the UE shall over-write any pending activation times for IP.
- 6. It is specified that UE shall use the pending new keys.
- 7. The ASN.1 is corrected to allow for START value for all domains to be transmitted.
- 8. The NOTE specifying UE support of UEAx and UIAx is deleted. A corresponding correction is made in 25.306.
- 9. It is clarified that "non ciphered" refers to ciphering status set to "not started" and RBs configured with ciphering algorithm UEA0 shall contribute to the START value calculation.
- 10. The suggestion that old values for START, Keys, etc. are stored in the USIM has been deleted.
- 11. The ASN.1 and tabular have been appropriately updated to state that stop is never to be used in any version of the protocol.
- 12. It is stated that if the IE "DL Counter Synchronisation Info" or "New URNTI" in case of RADIO BEARER RECONFIGURATION is present then the UE shall apply the FRESH value in the received message before performing the integrity check.
- 13. RRC State Indicator has been moved in the Tabular per the appropriate alphabetical order.
- 14. The requirement corresponding to the START value transmission in case of AM RLC size change due to system information IE "RB Mapping Info" is deleted since this occurs only in the case of Inter-RAT Handover to UTRAN and in this case there is no AM RLC size change.

**Consequences if not approved:**

- ☞ Incomplete specification related to security procedures causing uncertain UE behavior. Uncertain UE behavior in case of SRNS relocation.

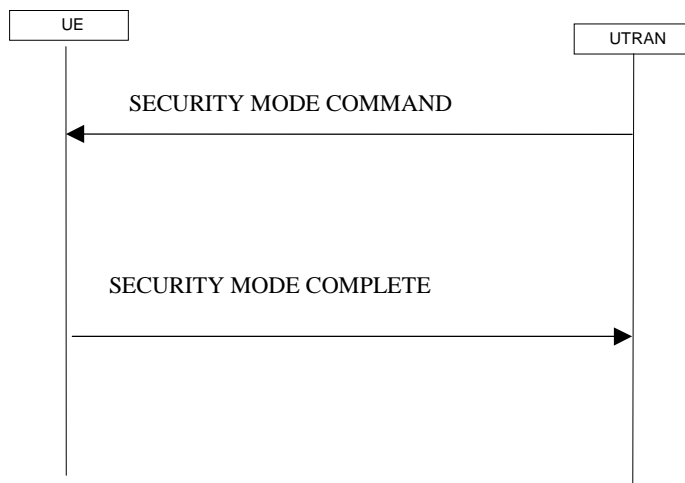
<b>Clauses affected:</b>	⌘	8.1.12.2.1, 8.1.12.2.2, 8.1.15.3, 8.3.4.3, 8.3.4.5a, 8.5.9, 8.5.10, 8.6.3.4, 8.6.3.5, 8.6.4.8, 10.2.1, 10.2.2, 10.3.3.5, 10.3.3.10, 10.3.3.35a (new), 10.3.3.37, 11, A.2	
<b>Other specs</b>	⌘	<input checked="" type="checkbox"/>	Other core specifications
<b>affected:</b>		<input type="checkbox"/>	Test specifications
		<input type="checkbox"/>	O&M Specifications
<b>Other comments:</b>	⌘		

**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.

## 8.1.12 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 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.

#### 8.1.12.2.2 Integrity protection configuration change

To start or modify integrity protection, UTRAN sends a SECURITY MODE COMMAND message on the downlink DCCH in AM RLC using the new integrity protection configuration. [UTRAN should not "modify" integrity protection for a CN domain to which a SECURITY MODE COMMAND configuring integrity protection has been previously sent for an ongoing signalling connection unless the application of new integrity keys needs to be signalled to the UE. UTRAN should not transmit a SECURITY MODE COMMAND to signal a change in integrity protection algorithm.](#)

When configuring Integrity protection, UTRAN should:

- 1> ensure that the UE needs to store at most three different Integrity protection configurations (keysets) at any given time. This includes the total number of Integrity protection configurations for all signalling radio bearers;
- 1> if Ciphering has already been started for the UE for the CN domain to be set in the IE "CN domain identity" in the SECURITY MODE COMMAND:
  - 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 "Ciphering mode info" in the SECURITY MODE COMMAND.
- 1> if Ciphering has already been configured for the UE for a CN domain different from the CN domain to be set in the IE "CN domain identity" in the SECURITY MODE COMMAND:
  - 2> include the IE "Ciphering mode info" in the SECURITY MODE COMMAND.

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> if this is the first SECURITY MODE COMMAND sent for this RRC connection:
  - 2> if new keys have been received:
    - 3> initialise the hyper frame numbers as follows:
      - 4> set all bits of the hyper frame numbers of the COUNT-I values for all signalling radio bearers to zero.

- 2> else (if new keys have not been received):
  - 3> use the value "START" in the most recently received IE "START list" or IE "START" that belongs to the CN domain indicated in the IE "CN domain identity" to initialise all hyper frame numbers of COUNT-I for all the signalling radio bearers by:
    - 4> setting the 20 most significant bits of the hyper frame numbers for all signalling radio bearers to the value "START" in the most recently received IE "START list" or IE "START" for that CN domain;
    - 4> setting the remaining bits of the hyper frame numbers equal to zero.
- 1> else (this is not the first SECURITY MODE COMMAND sent for this RRC connection):
  - 2> if new keys have been received:
    - 3> initialise the hyper frame number for COUNT-I for RB2 as follows:
      - 4> set all bits of the HFN of the COUNT-I value for RB2 to zero.
  - 2> if new keys have not been received:
    - 3> initialise the hyper frame number for COUNT-I for RB2 as follows:
      - 4> set the 20 most significant bits of the HFN of the downlink and uplink COUNT-I to the value of the most recently received IE "START" or IE "START LIST" for the CN domain to be set in the IE "CN Domain Identity";
      - 4> set the remaining bits of the HFN of the downlink and uplink COUNT-I to zero.
- 1> if the IE "Integrity protection mode command" has the value "Start":
  - 2> prohibit the transmission of signalling messages with any RRC SN on all signalling radio bearers, except RB2;
  - 2> set the FRESH value in the IE "Integrity protection initialisation number", included in the IE "Integrity protection mode info".
- 1> if the IE "Integrity protection mode command" has the value "Modify":
  - 2> for each signalling radio bearer RBn, except RB2:
    - 3> prohibit the transmission of signalling messages with RRC SN greater or equal to the RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info".
    - 2> set, for each signalling radio bearer RBn, that has no pending integrity protection activation time set by a previous security mode control procedure, an RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info", at which time the new integrity protection configuration shall be applied;
    - 2> set, for each signalling radio bearer RBn, that has a pending integrity protection activation time set by a previous security mode control procedure, the RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info", to the value used in the previous security mode control procedure, at which time the latest integrity protection configuration shall be applied.
- 1> transmit the SECURITY MODE COMMAND message on RB2 using the new integrity protection configuration.

### 8.1.12.3 Reception of SECURITY MODE COMMAND message by the UE

Upon reception of the SECURITY MODE COMMAND message, the UE shall:

- 1> if neither IE "Ciphering mode info" nor IE "Integrity protection mode info" is included in the SECURITY MODE COMMAND:

- 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the IE "Security capability" is the same as indicated by variable UE\_CAPABILITY\_TRANSFERRED, and the IE "GSM security capability" (if included in the SECURITY MODE COMMAND) is the same as indicated by the variable UE\_CAPABILITY\_TRANSFERRED:
  - 2> set the variable LATEST\_CONFIGURED\_CN\_DOMAIN equal to the IE "CN domain identity";
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for the CN domain indicated in the IE "CN domain identity" in the received SECURITY MODE COMMAND to the value "Affected";
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all CN domains other than the CN domain indicated in the IE "CN domain identity" to "Not affected";
  - 2> set the IE "RRC transaction identifier" in the SECURITY MODE COMPLETE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE COMMAND message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - 3> perform the actions as specified in subclause 8.6.3.4.
  - 2> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
    - 3> perform the actions as specified in subclause 8.6.3.5.
- 1> prior to sending the SECURITY MODE COMPLETE message:
  - 2> use the old ciphering configuration for this message;
  - 2> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - 3> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
    - 3> for each radio bearer and signalling radio bearer that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN:
      - 4> start or continue incrementing the COUNT-C values for all RLC-AM and RLC-UM signalling radio bearers at the ciphering activation time as specified in the procedure;
      - 4> continue incrementing the COUNT-C values for all RLC-AM and RLC-UM radio bearers.
    - 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN:
      - 4> for ciphering on signalling radio bearers using RLC-AM and RLC-UM in the downlink, at the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info" included in the SECURITY MODE COMMAND, for each signalling radio bearer:
        - 5> set the 20 most significant bits of the HFN component of the downlink COUNT-C to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
        - 5> set the remaining bits of the hyper frame numbers to zero.
    - 3> if new keys have been received:
      - 4> perform the actions in subclause 8.1.12.3.1.
  - 2> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
    - 3> include and set the IE "Uplink integrity protection activation info" to the value of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO for each signalling radio bearer;

- 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN, for RB2:
  - 4> in the downlink, for the received SECURITY MODE COMMAND message:
    - 5> set the 20 most significant bits of the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 5> set the remaining bits of the IE "Downlink RRC HFN" to zero.
  - 4> in the uplink, for the transmitted response message, SECURITY MODE COMPLETE:
    - 5> set the 20 most significant bits of the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 5> set the remaining bits of the IE "Uplink RRC HFN" to zero.
- 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN, for each signalling radio bearer other than RB2:
  - 4> if the IE "Integrity protection mode command" has the value "start":
    - 5> in the downlink, for this signalling radio bearer:
      - 6> set the 20 most significant bits of IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to the value START transmitted in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
      - 6> set the remaining bits of the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to zero;
    - 4> else:
      - 5> in the downlink, for the first message for which the RRC sequence number in a received RRC message for this signalling radio bearer is equal to or greater than the activation time as indicated in IE "Downlink integrity protection activation info" as included in the IE "Integrity protection mode info", for this signalling radio bearer:
        - 6> set the 20 most significant bits of the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
        - 6> set the remaining bits of the IE "Downlink RRC HFN" to zero.
  - 3> if new keys have been received:
    - 4> perform the actions in subclause 8.1.12.3.1.
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;
  - 2> transmit the SECURITY MODE COMPLETE message on the uplink DCCH in AM RLC;
  - 1> when the successful delivery of the SECURITY MODE COMPLETE message has been confirmed by RLC:
    - 2> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":



- 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN:
    - 4> for ciphering on signalling radio bearers using RLC-AM and RLC-UM in the uplink, at the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info" included in the SECURITY MODE COMPLETE, for each signalling radio bearer:
      - 5> set the HFN component of the uplink COUNT-C to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
      - 5> set the remaining bits of the hyper frame numbers to zero.
  - 3> if new keys have been received:
    - 4> perform the actions in subclause 8.1.12.3.1.
  - 3> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
  - 3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
  - 3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 2> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
- 3> if no new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN, for each signalling radio bearer other than RB2:
    - 4> if the IE "Integrity protection mode command" has the value "start":
      - 5> in the uplink, for this signalling radio bearer:
        - 6> set the 20 most significant bits of IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to the value START transmitted in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
        - 6> set the remaining bits of the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to zero.
    - 4> else:
      - 5> in the uplink, for the first transmitted RRC message for this signalling radio bearer with RRC sequence number equal to the activation time as indicated in IE "Uplink integrity protection activation info" included in the transmitted SECURITY MODE COMPLETE, for this signalling radio bearer:
        - 6> set the 20 most significant bits of the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to the value "START" in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
        - 6> set the remaining bits of the IE "Uplink RRC HFN" to zero.
  - 3> if new keys have been received:
    - 4> perform the actions in subclause 8.1.12.3.1.
  - 3> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
  - 3> set "Uplink RRC Message sequence number" for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO to a value such that next RRC message to be sent on uplink RB0 will use the new integrity protection configuration;
  - 3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and

- 3> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 2> clear the variable SECURITY\_MODIFICATION;
- 2> notify upper layers upon change of the security configuration;
- 2> and the procedure ends.
- 1> if the IE "Security capability" is not the same as indicated by the variable UE\_CAPABILITY\_TRANSFERRED, or the IE "GSM security capability" (if included in the SECURITY MODE COMMAND) is not the same as indicated by the variable UE\_CAPABILITY\_TRANSFERRED, or if the IE "GSM security capability" is not included in the SECURITY MODE COMMAND and is included in the variable UE\_CAPABILITY\_TRANSFERRED:
  - 2> release all its radio resources;
  - 2> indicate the release 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;
  - 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 2> clear the variable ESTABLISHED\_RABS;
  - 2> clear the variable SECURITY\_MODIFICATION;
  - 2> enter idle mode;
  - 2> perform actions when entering idle mode as specified in subclause 8.5.2;
  - 2> and the procedure ends.

#### 8.1.12.3.1 New ciphering and integrity protection keys

If a new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN, the UE shall:

- 1> set the START value for the CN domain indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN to zero;
- 1> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
  - 2> for integrity protection in the downlink on each signalling radio bearer except RB2:
    - 3> if IE "Integrity protection mode command" has the value "start":
      - 4> for the first received message on this signalling radio bearer:
        - 5> start using the new integrity key;
        - 5> for this signalling radio bearer:
          - 6> set the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to zero.
      - 3> else:
        - 4> for the first message for which the RRC sequence number in a received RRC message for this signalling radio bearer is equal to or greater than the activation time as indicated in IE "Downlink integrity protection activation info" as included in the IE "Integrity protection mode info":
          - 5> start using the new integrity key;
          - 5> for this signalling radio bearer:
            - 6> set the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to zero.

- 2> for integrity protection in the uplink on each signalling radio bearer except RB2:
  - 3> for the first message for which the RRC sequence number in a to be transmitted RRC message for this signalling radio bearer is equal to the activation time as indicated in IE "Uplink integrity protection activation info" included in the transmitted SECURITY MODE COMPLETE message:
    - 4> start using the new integrity key;
    - 4> for this signalling radio bearer:
      - 5> set the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to zero.
- 2> for integrity protection in the downlink on signalling radio bearer RB2:
  - 3> at the received SECURITY MODECOMMAND:
    - 4> start using the new integrity key;
    - 4> set the IE "Downlink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the downlink COUNT-I to zero.
- 2> for integrity protection in the uplink on signalling radio bearer RB2 :
  - 3> at the transmitted SECURITY MODE COMPLETE:
    - 4> start using the new integrity key;
    - 4> set the IE "Uplink RRC HFN" in the variable INTEGRITY\_PROTECTION\_INFO of the uplink COUNT-I to zero.
- 1> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
  - 2> for each signalling radio bearer and for each radio bearer for the CN domain indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN:
    - 3> if the IE "Status" in the variable CIPHERING\_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers using RLC-TM:
      - 4> at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info":
        - 5> start using the new key in uplink and downlink;
        - 5> set the HFN component of the COUNT-C to zero.
    - 3> if the IE "Status" in the variable CIPHERING\_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers and signalling radio bearers using RLC-AM and RLC-UM:
      - 4> in the downlink, at the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info":
        - 5> start using the new key;
        - 5> set the HFN component of the downlink COUNT-C to zero.
      - 4> in the uplink, at the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info":
        - 5> start using the new key;
        - 5> set the HFN component of the uplink COUNT-C to zero.
- 1> consider the value of the latest transmitted START value to be zero.

#### 8.1.12.4 Void

##### 8.1.12.4a Incompatible simultaneous security reconfiguration

If the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION becomes set to TRUE of the received SECURITY MODE COMMAND message, the UE shall:

- 1> transmit a SECURITY MODE FAILURE message on the uplink DCCH using AM RLC, using the ciphering and integrity protection configurations prior to the reception of this SECURITY MODE COMMAND;
- 1> set the IE "RRC transaction identifier" in the SECURITY MODE FAILURE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE COMMAND message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";
- 1> when the response message has been submitted to lower layers for transmission:
  - 2> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to FALSE;
  - 2> continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - 2> and the procedure ends.

##### 8.1.12.4b Cell update procedure during security reconfiguration

If:

- a cell update procedure according to subclause 8.3.1 is initiated; and
- the received SECURITY MODE COMMAND message causes either,
  - the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE; and/or
  - the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE;

the UE shall:

- 1> abort the ongoing integrity and/or ciphering reconfiguration;
- 1> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
- 1> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- 1> when the response message has been submitted to lower layers for transmission:
  - 2> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - 3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
    - 3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
    - 3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
    - 3> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
  - 2> continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received; and

- 2> clear the variable SECURITY\_MODIFICATION;
- 2> the procedure ends.

#### 8.1.12.4c Invalid configuration

If the variable INVALID\_CONFIGURATION is set to TRUE due to the received SECURITY MODE COMMAND message, the UE shall:

- 1> transmit a SECURITY MODE FAILURE message on the DCCH using AM RLC after setting the IEs as specified below:
  - 2> set the IE "RRC transaction identifier" in the SECURITY MODE FAILURE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE COMMAND message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
  - 2> set the IE "failure cause" to the cause value "invalid configuration".
- 1> when the response message has been submitted to lower layers for transmission:
  - 2> set the variable INVALID\_CONFIGURATION to FALSE;
  - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE;
  - 2> continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - 2> and the procedure ends.

#### 8.1.12.5 Reception of SECURITY MODE COMPLETE message by the UTRAN

UTRAN should apply integrity protection on the received SECURITY MODE COMPLETE message and all subsequent messages with the new integrity protection configuration, if changed. When UTRAN has received a SECURITY MODE COMPLETE message and the integrity protection has successfully been applied, UTRAN should:

- 1> if the IE "Ciphering mode info" was included in the SECURITY MODE COMMAND message:
  - 2> if new keys were received for the CN domain set in the IE "CN Domain Identity" in the SECURITY MODE COMMAND:
    - 3> set, at the downlink and uplink activation time, all the bits of the hyper frame numbers of the downlink and uplink COUNT-C values respectively for all radio bearers for this CN domain and all signalling radio bearers to zero.
  - 2> else (if new keys were not received):
    - 3> use, at the downlink and uplink activation time, the value "START" in the most recently received IE "START list" or IE "START" that belongs to the CN domain as indicated in the IE "CN domain identity" to initialise all hyper frame numbers of the downlink and uplink COUNT-C values respectively for all the signalling radio bearers as follows:
      - 4> set the 20 most significant bits of the hyper frame numbers of the COUNT-C for all signalling radio bearers to the value "START" in the most recently received IE "START list" or IE "START" for that CN domain;
      - 4> set the remaining bits of the hyper frame numbers equal to zero.
- 1> if the IE "Integrity protection mode info" was included in the SECURITY MODE COMMAND message:
  - 2> if this was not the first SECURITY MODE COMMAND message for this RRC connection:
    - 3> if new keys have been received for the CN domain set in the IE "CN Domain Identity" included in the transmitted SECURITY MODE COMMAND message:

- 4> initialise, at the downlink and uplink activation time, all hyper frame numbers of the downlink and uplink COUNT-I values respectively for all the signalling radio bearers other than RB2 as follows:
  - 5> set all bits of the hyper frame numbers of the uplink and downlink COUNT-I to zero.
- 3> if no new keys have been received for the CN domain set in the IE "CN Domain Identity" included in the transmitted SECURITY MODE COMMAND message:
  - 4> use, at the downlink and uplink activation time, the value "START" in the most recently received IE "START list" or IE "START" that belongs to the CN domain as indicated in the IE "CN domain identity" to initialise all hyper frame numbers of the downlink and uplink COUNT-I values respectively for all the signalling radio bearers other than RB2 as follows:
    - 5> set the 20 most significant bits of the hyper frame numbers of the downlink and uplink COUNT-I respectively for all signalling radio bearers to the value "START" in the most recently received IE "START list" or IE "START" for that CN domain;
    - 5> set the remaining bits of the hyper frame numbers equal to zero.
- 1> send an indication to upper layers that the new security configuration has been activated;
- 1> resume, in the downlink, all suspended radio bearers and all signalling radio bearers;
- 1> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- 1> if the IE "Integrity protection mode command" included in the SECURITY MODE COMMAND had the value "Start":
  - 2> start applying integrity protection in the downlink for all signalling radio bearers.
- 1> if the IE "Integrity protection mode command" included in the SECURITY MODE COMMAND had the value "Modify":
  - 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each signalling radio bearers RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info";
  - 2> continue applying the new integrity configuration for signalling radio bearer RB2;
  - 2> apply the new integrity protection configuration on the received signalling messages with RRC SN greater than or equal to the number associated with the signalling radio bearer in IE "Uplink integrity protection activation info".
- 1> apply the old ciphering configuration for the transmission of RLC PDUs with RLC sequence number less than the number indicated in the IE "Radio bearer downlink ciphering activation time info" included in the IE "Ciphering mode info";
- 1> apply the new ciphering configuration for the transmission of RLC PDUs with RLC sequence number greater than or equal to the number indicated in IE "Radio bearer downlink ciphering activation time info" included in the IE "Ciphering mode info";
- 1> apply the old integrity protection configuration on the received signalling messages with RRC SN smaller than the number associated with the signalling radio bearer in IE "Uplink integrity protection activation info";
- 1> for radio bearers using RLC-AM or RLC-UM:
  - 2> use the old ciphering configuration for received RLC PDUs with RLC sequence number less than the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" sent by the UE;
  - 2> use the new ciphering configuration for received RLC PDUs with RLC sequence number greater than or equal to the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" sent by the UE;
  - 2> if an RLC reset or re-establishment occurs after the SECURITY MODE COMPLETE message has been received by UTRAN before the activation time for the new ciphering configuration has been reached, ignore

the activation time and apply the new ciphering configuration immediately after the RLC reset or RLC re-establishment.

1> for radio bearers using RLC-TM:

2> use the old ciphering configuration for the received RLC PDUs before the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info" as included in the SECURITY MODE COMMAND;

2> use the new ciphering configuration for the received RLC PDUs at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info" as included in the SECURITY MODE COMMAND.

1> and the procedure ends.

### 8.1.12.6 Invalid SECURITY MODE COMMAND message

If the SECURITY MODE COMMAND message contains a protocol error causing the variable PROTOCOL\_ERROR\_REJECT to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows:

1> transmit a SECURITY MODE FAILURE message on the uplink DCCH using AM RLC;

1> set the IE "RRC transaction identifier" in the SECURITY MODE FAILURE message to the value of "RRC transaction identifier" in the entry for the SECURITY MODE COMMAND message in the table "Rejected transactions" in the variable TRANSACTIONS; and

1> clear that entry;

1> set the IE "failure cause" to the cause value "protocol error";

1> include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL\_ERROR\_INFORMATION;

1> when the response message has been submitted to lower layers for transmission:

2> continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;

2> and the procedure ends.

### 8.1.13 Signalling connection release procedure



Figure 8.1.13-1: Signalling connection release procedure, normal case

#### 8.1.13.1 General

The signalling connection release procedure is used to notify to the UE that one of its ongoing signalling connections has been released. The procedure does not initiate the release of the RRC connection.

### 8.1.13.2 Initiation of SIGNALLING CONNECTION RELEASE by the UTRAN

To initiate the procedure, the UTRAN transmits a SIGNALLING CONNECTION RELEASE message on DCCH using AM RLC.

### 8.1.13.3 Reception of SIGNALLING CONNECTION RELEASE by the UE

Upon reception of a SIGNALLING CONNECTION RELEASE message, the UE shall:

- 1> indicate the release of the signalling connection and pass the value of the IE "CN domain identity" to upper layers;
- 1> remove the signalling connection with the identity indicated by the IE "CN domain identity" from the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 1> clear the entry for the SIGNALLING CONNECTION RELEASE message in the table "Accepted transactions" in the variable TRANSACTIONS;
- 1> the procedure ends.

### 8.1.13.4 Invalid SIGNALLING CONNECTION RELEASE message

If the UE receives a SIGNALLING CONNECTION RELEASE message, which contains a protocol error causing the variable `PROTOCOL_ERROR_REJECT` to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows:

- 1> include the IE "Identification of received message"; and
  - 2> set the IE "Received message type" to SIGNALLING CONNECTION RELEASE;
  - 2> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the SIGNALLING CONNECTION RELEASE message in the table "Rejected transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry.
- 1> include the IE "Protocol error information" with contents set to the value of the variable `PROTOCOL_ERROR_INFORMATION`;
- 1> transmit an RRC STATUS message on the uplink DCCH using AM RLC
- 1> when the RRC STATUS message has been submitted to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the invalid SIGNALLING CONNECTION RELEASE message has not been received.

### 8.1.13.5 Invalid configuration

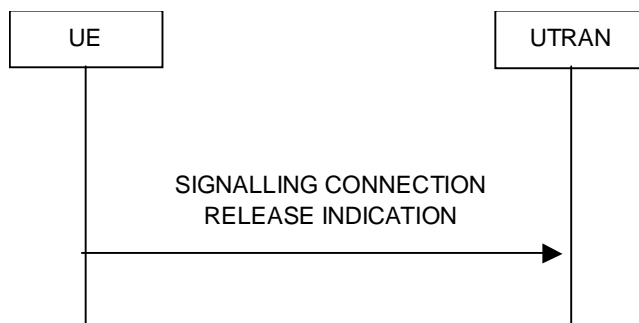
If radio access bearers for the CN domain indicated by the IE "CN domain identity" exist in the variable `ESTABLISHED_RABS`, the UE shall:

- 1> transmit an RRC STATUS message on the uplink DCCH using AM RLC;
- 1> include the IE "Identification of received message"; and
- 1> set the IE "Received message type" to SIGNALLING CONNECTION RELEASE; and
- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the SIGNALLING CONNECTION RELEASE message in the table "Accepted transactions" in the variable TRANSACTIONS and clear that entry;
- 1> include the IE "Protocol error information" with contents set to the value "Message not compatible with receiver state";
- 1> when the RRC STATUS message has been submitted to lower layers for transmission:



- 2> continue with any ongoing processes and procedures as if the invalid SIGNALLING CONNECTION RELEASE message has not been received.

### 8.1.14 Signalling connection release indication procedure



**Figure 8.1.14-1: Signalling connection release indication procedure, normal case**

#### 8.1.14.1 General

The signalling connection release indication procedure is used by the UE to indicate to the UTRAN that one of its signalling connections has been released. The procedure may in turn initiate the RRC connection release procedure.

#### 8.1.14.2 Initiation

The UE shall, on receiving a request to release (abort) the signalling connection from upper layers for a specific CN domain:

- 1> if a signalling connection in the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS for the specific CN domain identified with the IE "CN domain identity" exists:
  - 2> initiate the signalling connection release indication procedure.
- 1> otherwise:
  - 2> abort any ongoing establishment of signalling connection for that specific CN domain as specified in 8.1.3.5a.

Upon initiation of the signalling connection release indication procedure in CELL\_PCH or URA\_PCH state, the UE shall:

- 1> perform a cell update procedure, according to subclause 8.3.1, using the cause "uplink data transmission";
- 1> when the cell update procedure completed successfully:
  - 2> continue with the signalling connection release indication procedure as below.

The UE shall:

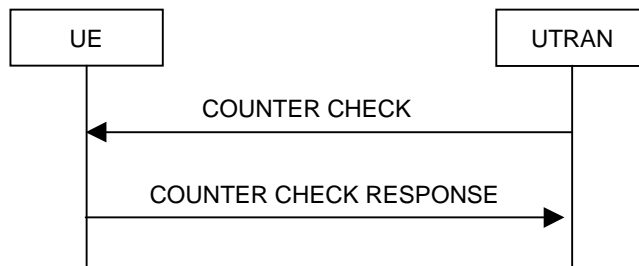
- 1> set the IE "CN Domain Identity" to the value indicated by the upper layers. The value of the IE indicates the CN domain whose associated signalling connection the upper layers are indicating to be released;
- 1> remove the signalling connection with the identity indicated by upper layers from the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 1> transmit a SIGNALLING CONNECTION RELEASE INDICATION message on DCCH using AM RLC.

When the SIGNALLING CONNECTION RELEASE INDICATION message has been submitted to lower layers for transmission the procedure ends.

### 8.1.14.3 Reception of SIGNALLING CONNECTION RELEASE INDICATION by the UTRAN

Upon reception of a SIGNALLING CONNECTION RELEASE INDICATION message, the UTRAN requests the release of the signalling connection from upper layers. Upper layers may then initiate the release of the signalling connection.

### 8.1.15 Counter check procedure



**Figure 8.1.15-1: Counter check procedure**

#### 8.1.15.1 General

The counter check procedure is used by the UTRAN to perform a local authentication. The purpose of the procedure is to check that the amount of data sent in both directions (uplink and downlink) over the duration of the RRC connection is identical at the UTRAN and at the UE (to detect a possible intruder – a 'man-in-the-middle' – from operating).

This procedure is only applicable to radio bearers, and only to radio bearers using RLC-AM or RLC-UM. It should be noted that this requires that the COUNT-C values for each UL and DL radio bearers using RLC-AM or RLC-UM continue to be incremented even if ciphering is not used. This procedure is not applicable to signalling radio bearers.

#### 8.1.15.2 Initiation

The UTRAN monitors the COUNT-C value associated with each radio bearer using UM or AM RLC. The procedure is triggered whenever any of these values reaches a critical checking value. The granularity of these checking values and the values themselves are defined to the UTRAN by the visited network. The UTRAN initiates the procedure by sending a COUNTER CHECK message on the downlink DCCH.

#### 8.1.15.3 Reception of a COUNTER CHECK message by the UE

When the UE receives a COUNTER CHECK message it shall compare the COUNT-C MSB values received in the IE "RB COUNT-C MSB information" in the COUNTER CHECK message to the COUNT-C MSB values of the corresponding radio bearers.

The UE shall:

- 1> set the IE "RRC transaction identifier" in the COUNTER CHECK RESPONSE message to the value of "RRC transaction identifier" in the entry for the COUNTER CHECK message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry.

If:

- there is one or more radio bearer(s) using UM or AM RLC mode stored in the variable ESTABLISHED\_RABS, which is (are) not included in the IE "RB COUNT-C MSB information"; or
- there is one or more radio bearer(s) included in the IE "RB COUNT-C MSB information", which is (are) not stored in the variable ESTABLISHED\_RABS; or

- for any radio bearer (excluding signalling radio bearers) using UM or AM RLC mode stored in the variable ESTABLISHED\_RABS and included in the IE "RB COUNT-C MSB information" with COUNT-C MSB values different from the MSB part of the COUNT-C values in the UE:

the UE shall:

- 1> include these radio bearers in the IE "RB COUNT-C information" in the COUNTER CHECK RESPONSE message. For any RB which is included in the IE "RB COUNT-C MSB information" in the COUNTER CHECK message but not stored in the variable ESTABLISHED\_RABS in the UE, the MSB part of COUNT-C values in the COUNTER CHECK RESPONSE message shall be set identical to COUNT-C-MSB values in the COUNTER CHECK message. The LSB part shall be filled with zeroes.

The UE shall:

- 1> if no COUNT-C exists for a radio bearer for a given direction (uplink or downlink) because:
  - 2> it is a uni-directional radio bearer configured only for the other direction (downlink or uplink respectively),  
or
  - 2> has been configured to RLC-TM mode in one direction (uplink or downlink) and RLC-UM in the other (downlink or uplink respectively),
  - 3> set the COUNT-C in the IE "RB COUNT-C information" in the COUNTER CHECK RESPONSE message, to any value;

- 1> submit a COUNTER CHECK RESPONSE message to lower layers for transmission on the uplink DCCH using AM RLC.

When the COUNTER CHECK RESPONSE message has been submitted to lower layers for transmission the procedure ends.

#### 8.1.15.4 Reception of the COUNTER CHECK RESPONSE message by UTRAN

If the UTRAN receives a COUNTER CHECK RESPONSE message that does not contain any COUNT-C values, the procedure ends.

If the UTRAN receives a COUNTER CHECK RESPONSE message that contains one or several COUNT-C values the UTRAN may release the RRC connection.

#### 8.1.15.5 Cell re-selection

If the UE performs cell re-selection anytime during this procedure it shall, without interrupting the procedure:

- 1> initiate the cell update procedure according to subclause 8.3.1.

#### 8.1.15.6 Invalid COUNTER CHECK message

If the UE receives a COUNTER CHECK message, which contains a protocol error causing the variable PROTOCOL\_ERROR\_REJECT to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows. The UE shall:

- 1> transmit an RRC STATUS message on the uplink DCCH using AM RLC;
- 1> include the IE "Identification of received message"; and
- 1> set the IE "Received message type" to COUNTER CHECK; and
- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the UE COUNTER CHECK message in the table "Rejected transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL\_ERROR\_INFORMATION;

- 1> when the RRC STATUS message has been submitted to lower layers for transmission:
- 2> continue with any ongoing processes and procedures as if the invalid COUNTER CHECK message has not been received.

-----

### 8.3.4 Active set update

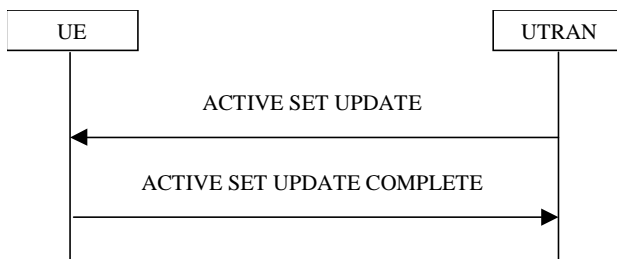


Figure 8.3.4-1: Active Set Update procedure, successful case

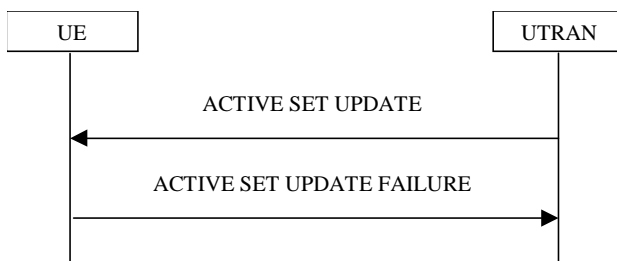


Figure 8.3.4-2: Active Set Update procedure, failure case

#### 8.3.4.1 General

The purpose of the active set update procedure is to update the active set of the connection between the UE and UTRAN. This procedure shall be used in CELL\_DCH state. The UE should keep on using the old RLs while configuring the new RLs. Also the UE should keep the transmitter turned on during the procedure. This procedure is only used in FDD mode.

#### 8.3.4.2 Initiation

The procedure is initiated when UTRAN orders a UE in CELL\_DCH state, to make the following modifications of the active set of the connection:

- a) Radio link addition;
- b) Radio link removal;
- c) Combined radio link addition and removal.

In case a) and c), UTRAN should:

- 1> prepare new additional radio link(s) in the UTRAN prior to the command to the UE.

In all cases, UTRAN should:

- 1> send an ACTIVE SET UPDATE message on downlink DCCH using AM or UM RLC.

UTRAN should include the following information:

- 1> IE "Radio Link Addition Information": Downlink DPCH information and other optional parameters relevant for the radio links to be added along with the IE "Primary CPICH info" used for the reference ID to indicate which radio link to add. This IE is needed in cases a) and c) listed above;

- 1> IE "Radio Link Removal Information": IE "Primary CPICH info" used for the reference ID to indicate which radio link to remove. This IE is needed in cases b) and c) listed above.

### 8.3.4.3 Reception of an ACTIVE SET UPDATE message by the UE

Upon reception of an ACTIVE SET UPDATE message the UE shall act upon all received information elements as specified in 8.6, unless specified otherwise in the following.

The UE may:

- 1> maintain a list of the set of cells to which the UE has Radio Links if the IE "Cell ID" is present.

The UE shall:

- 1> first add the RLs indicated in the IE "Radio Link Addition Information";
- 1> remove the RLs indicated in the IE "Radio Link Removal Information". If the UE active set is full or becomes full, an RL, which is included in the IE "Radio Link Removal Information" for removal, shall be removed before adding RL, which is included in the IE "Radio Link Addition Information" for addition;
- 1> perform the physical layer synchronisation procedure as specified in [29];

~~1> if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":~~

~~2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected".~~

~~1> if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":~~

~~2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.~~

~~1> if the variable PDCP\_SN\_INFO is non-empty:~~

~~2> include the IE "RB with PDCP information list" in the ACTIVE SET UPDATE COMPLETE message; and~~

~~2> set it to the value of the variable PDCP\_SN\_INFO.~~

1> if the IE "TFCI combining indicator" associated with a radio link to be added is set to TRUE:

2> if a DSCH transport channel is assigned and there is a 'hard' split in the TFCI field:

3> configure Layer 1 to soft-combine TFCI (field 2) of this new link with those links already in the TFCI (field 2) combining set.

~~1> if the received ACTIVE SET UPDATE message included the IE "Downlink counter synchronisation info":~~

~~2> calculate the START value according to subclause 8.5.9;~~

~~2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the ACTIVE SET UPDATE COMPLETE message.~~

1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE COMPLETE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and

1> clear that entry;

1> transmit an ACTIVE SET UPDATE COMPLETE message on the uplink DCCCH using AM RLC without waiting for the Physical Layer synchronization;

~~1> if the IE "Integrity protection mode info" was present in the ACTIVE SET UPDATE message:~~

~~2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted ACTIVE SET UPDATE COMPLETE message.~~

- ~~1> if the IE "Downlink counter synchronisation info" was included in the received ACTIVE SET UPDATE message:~~
    - ~~2> when RLC has confirmed the successful transmission of the response message:~~
      - ~~3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].~~
  - ~~1> if the variable PDCP\_SN\_INFO is empty:~~
    - ~~2> if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":~~
      - ~~3> when RLC has confirmed the successful transmission of the ACTIVE SET UPDATE COMPLETE message:~~
        - ~~4> perform the actions below.~~
    - ~~2> if the ACTIVE SET UPDATE message did not contain the IE "Ciphering mode info":~~
      - ~~3> when RLC has been requested to transmit the ACTIVE SET UPDATE COMPLETE message:~~
        - ~~4> perform the actions below.~~
  - ~~1> if the variable PDCP\_SN\_INFO is non-empty:~~
    - ~~2> when RLC has confirmed the successful transmission of the ACTIVE SET UPDATE COMPLETE message:~~
      - ~~3> for each radio bearer in the variable PDCP\_SN\_INFO:~~
        - ~~4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":~~
          - ~~5> configure the RLC entity for that radio bearer to "continue".~~
      - ~~3> clear the variable PDCP\_SN\_INFO.~~
  - ~~1> if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":~~
    - ~~2> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;~~
    - ~~2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and~~
    - ~~2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.~~
  - ~~1> if the ACTIVE SET UPDATE message contained the IE "Integrity protection mode info":~~
    - ~~2> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;~~
    - ~~2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and~~
    - ~~2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.~~
  - ~~1> clear the variable SECURITY\_MODIFICATION;~~
- 1> the procedure ends on the UE side.

#### 8.3.4.4 Unsupported configuration in the UE

If UTRAN instructs the UE to use a configuration that it does not support, the UE shall:

- 1> keep the active set as it was before the ACTIVE SET UPDATE message was received;
- 1> transmit an ACTIVE SET UPDATE FAILURE message on the DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and

- 1> clear that entry;
- 1> set the IE "failure cause" to "configuration unsupported";
- 1> when the ACTIVE SET UPDATE FAILURE message has been submitted to lower layers for transmission:
  - 2> the procedure ends on the UE side.

### 8.3.4.5 Invalid configuration

If any of the following conditions are valid:

- a radio link indicated by the IE "Downlink DPCH info for each RL" in the IE "Radio link addition information" has a different spreading factor than the spreading factor for the radio links in the active set that will be established at the time indicated by the IE "Activation time"; and/or
- a radio link in the IE "Radio link addition information" is also present in the IE "Radio Link Removal Information"; and/or
- the IE "Radio Link Removal Information" contains all the radio links which are part of or will be part of the active set at the time indicated by the IE "Activation time"; and/or
- the IE "TX Diversity Mode" is not set to "none" and it indicates a diversity mode that is different from the one currently used in all or part of the active set; and/or
- a radio link indicated by the IE "Radio Link Removal Information" does not exist in the active set; and/or
- after the removal of all radio links indicated by the IE "Radio Link Removal Information" and the addition of all radio links indicated by the IE "Radio Link Addition Information" the active set would contain more than the maximum allowed number of radio links; and/or
- the variable INVALID\_CONFIGURATION is set to TRUE:

the UE shall:

- 1> keep the active set as it was before the ACTIVE SET UPDATE message was received;
- 1> transmit an ACTIVE SET UPDATE FAILURE message on the DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to "Invalid configuration";
- 1> When the ACTIVE SET UPDATE FAILURE message has been submitted to lower layers for transmission:
  - 2> the procedure ends on the UE side.

#### 8.3.4.5a ~~Incompatible simultaneous reconfiguration~~ Void

~~If the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION becomes set to TRUE due to the received ACTIVE SET UPDATE message, the UE shall:~~

- ~~1> transmit a ACTIVE SET UPDATE FAILURE message on the uplink DCCH using AM RLC;~~
- ~~1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and~~
- ~~1> clear that entry;~~
- ~~1> set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";~~

- ~~1> when the ACTIVE SET UPDATE FAILURE message has been delivered to lower layers for transmission:~~
- ~~2> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to FALSE;~~
- ~~2> continue with any ongoing processes and procedures as if the ACTIVE SET UPDATE message has not been received;~~
- ~~2> and the procedure ends.~~

~~If the variable ORDERED\_RECONFIGURATION is set to TRUE; and~~

- ~~1> if the activation time for the procedure that has set variable ORDERED\_RECONFIGURATION and the activation time for the Active Set Update procedure are within a time window of 5 frames, the UE may:~~
- ~~2> transmit a ACTIVE SET UPDATE FAILURE message on the uplink DCCH using AM RLC;~~
- ~~2> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and~~
- ~~2> clear that entry;~~
- ~~2> set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";~~
- ~~2> when the ACTIVE SET UPDATE FAILURE message has been delivered to lower layers for transmission:~~
  - ~~3> continue with any ongoing processes and procedures as if the ACTIVE SET UPDATE message has not been received;~~
  - ~~3> and the procedure ends.~~

#### 8.3.4.6 Reception of the ACTIVE SET UPDATE COMPLETE message by the UTRAN

When the UTRAN has received the ACTIVE SET UPDATE COMPLETE message,

- 1> the UTRAN may remove radio link(s) that are indicated to remove to the UE in case b) and c); and
- 1> the procedure ends on the UTRAN side.

#### 8.3.4.7 Reception of the ACTIVE SET UPDATE FAILURE message by the UTRAN

When the UTRAN has received the ACTIVE SET UPDATE FAILURE message, the UTRAN may delete radio links that were included in the IE "Radio Link Addition Information" for addition. The procedure ends on the UTRAN side.

#### 8.3.4.8 Invalid ACTIVE SET UPDATE message

If the ACTIVE SET UPDATE message contains a protocol error causing the variable PROTOCOL\_ERROR\_REJECT to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows. The UE shall:

- 1> transmit a ACTIVE SET UPDATE FAILURE message on the uplink DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Rejected transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to the cause value "protocol error";
- 1> include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL\_ERROR\_INFORMATION;
- 1> when the ACTIVE SET UPDATE FAILURE message has been delivered to lower layers for transmission:



- 2> continue with any ongoing processes and procedures as if the invalid ACTIVE SET UPDATE message has not been received;
- 2> and the procedure ends.

#### 8.3.4.9 Reception of an ACTIVE SET UPDATE message in wrong state

If the UE is in another state than CELL\_DCH state upon reception of the ACTIVE SET UPDATE message, the UE shall perform procedure specific error handling as follows. The UE shall:

- 1> transmit a ACTIVE SET UPDATE FAILURE message on the uplink DCCH using AM RLC;
- 1> set the IE "RRC transaction identifier" in the ACTIVE SET UPDATE FAILURE message to the value of "RRC transaction identifier" in the entry for the ACTIVE SET UPDATE message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> set the IE "failure cause" to the cause value "protocol error";
- 1> include the IE "Protocol error information" with the IE "Protocol error cause" set to "Message not compatible with receiver state";
- 1> when the ACTIVE SET UPDATE FAILURE message has been delivered to lower layers for transmission:
  - 2> continue with any ongoing processes and procedures as if the ACTIVE SET UPDATE message has not been received;
  - 2> and the procedure ends.

#### 8.5.9 START value calculation

In connected mode, the START value for CN domain 'X' is calculated as

Let  $START_X$  = the START value for CN domain 'X' prior to the calculation below:

$START_X' = MSB_{20} ( MAX \{ COUNT-C, COUNT-I \mid \text{radio bearers and signalling radio bearers using the most recently configured } CK_X \text{ and } IK_X \}) + 2.$

- if  $START_X' =$  the maximum value = 1048575 then  $START_X = START_X'$ ;
- if the current  $START_X < START_X'$  then  $START_X = START_X'$ , otherwise  $START_X$  is unchanged.

NOTE: Here, "most recently configured" means that if there is more than one key in use for a CN domain, due to non-expiry of the ciphering and/or integrity protection activation time for any signalling radio bearers and/or radio bearers, do not include the COUNT-I/COUNT-C for these signalling radio bearers and/or radio bearers in the calculation of the  $START_X'$ .

COUNT-C corresponding to non-ciphered radio bearers ([i.e. RBs with ciphering status set to "not started"](#)) shall not be included in the calculation of the  $START_X'$ . If a radio bearer is released and the radio bearer was ciphered, the values of the COUNT-C at the time the radio bearer is released shall be taken into account in the calculation of the  $START_X'$ .

#### 8.5.10 Integrity protection

If the "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" then the UE shall:

- 1> perform integrity protection (and integrity checking) on all RRC messages, with the following exceptions:
  - HANDOVER TO UTRAN COMPLETE
  - PAGING TYPE 1
  - PUSCH CAPACITY REQUEST

PHYSICAL SHARED CHANNEL ALLOCATION  
RRC CONNECTION REQUEST  
RRC CONNECTION SETUP  
RRC CONNECTION SETUP COMPLETE  
RRC CONNECTION REJECT  
RRC CONNECTION RELEASE (CCCH only)  
SYSTEM INFORMATION  
SYSTEM INFORMATION CHANGE INDICATION  
TRANSPORT FORMAT COMBINATION CONTROL (TM DCCH only)

If the "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started" then integrity protection (and integrity checking) shall not be performed on any RRC message.

For each signalling radio bearer, the UE shall use two RRC hyper frame numbers:

- "Uplink RRC HFN";
- "Downlink RRC HFN".

and two message sequence numbers:

- "Uplink RRC Message sequence number";
- "Downlink RRC Message sequence number".

The above information is stored in the variable INTEGRITY\_PROTECTION\_INFO per signalling radio bearer (RB0-RB4).

Upon the first activation of integrity protection for an RRC connection, UE and UTRAN initialise the "Uplink RRC Message sequence number" and "Downlink RRC Message sequence number" for all signalling radio bearers as specified in subclauses 8.6.3.5 and 8.5.10.1.

The RRC message sequence number (RRC SN) is incremented for every integrity protected RRC message.

If the IE "Integrity Protection Mode Info" is present in a received message, the UE shall:

1> perform the actions in subclause 8.6.3.5 before proceeding with the integrity check of the received message.

### 8.5.10.1 Integrity protection in downlink

If the UE receives an RRC message on signalling radio bearer with RB identity n, the "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and the IE 'Integrity check info' is present the UE shall:

- 1> check the value of the IE "RRC message sequence number" included in the IE "Integrity check info";
- 2> if the "Downlink RRC Message sequence number" is not present in the variable INTEGRITY\_PROTECTION\_INFO:
  - 3> initialise the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO with the value of the IE "RRC message sequence number" included in the IE "Integrity check info" of the received message.
- 2> if the "Downlink RRC Message sequence number" is present in the variable INTEGRITY\_PROTECTION\_INFO:
  - 3> if the RRC message sequence number is lower than the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO:

- 4> increment "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO with one.
- 3> if the RRC message sequence number is equal to the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO:
  - 4> discard the message.
- 1> calculate an expected message authentication code in accordance with subclause 8.5.10.3;
- 1> compare the expected message authentication code with the value of the received IE "message authentication code" contained in the IE "Integrity check info";
  - 2> if the expected message authentication code and the received message authentication code are the same, the integrity check is successful:
    - 3> update the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO with the value of the IE "RRC message sequence number" included in the IE "Integrity check info" of the received RRC message.
  - 2> if the calculated expected message authentication code and the received message authentication code differ:
    - 3> if the IE "RRC message sequence number" included in the IE "Integrity check info" is lower than the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO (in this case the "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO was incremented by one, as stated above):
      - 4> decrement "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY\_PROTECTION\_INFO by one.
    - 3> discard the message.

If the UE receives an RRC message on signalling radio bearer with identity n, the "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and the IE 'Integrity check info' is not present the UE shall:

- 1> discard the message.
- 

### 8.6.3.3 Generic state transition rules depending on received information elements

The IE "RRC State Indicator" indicates the state the UE shall enter. The UE shall enter the state indicated by the IE "RRC State Indicator" even if the received message includes other IEs relevant only for states other than indicated by the IE "RRC State Indicator". E.g. if the RRC state indicator is set to CELL\_FACH while other IEs provide information about a configuration including dedicated channels, the UE shall enter CELL\_FACH state. If however the UE has no information about the configuration corresponding to the state indicated by the IE "RRC State Indicator", it shall consider the requested configuration as invalid.

The UE shall, if the IE "RRC State Indicator" in the received message has the value:

- 1> "CELL\_FACH":
  - 2> enter CELL\_FACH state as dictated by the procedure governing the message received.
- 1> "CELL\_DCH":
  - 2> if neither DPCH is assigned in the message nor is the UE in CELL\_DCH:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> else:
    - 3> enter CELL\_DCH state as dictated by the procedure governing the message received.
- 1> "CELL\_PCH":

- 2> if the received message is RRC CONNECTION SETUP and IE "RRC State Indicator" is set to CELL\_PCH:
  - 3> set the variable INVALID\_CONFIGURATION to TRUE.
- 2> else:
  - 3> enter CELL\_PCH state as dictated by the procedure governing the message received.

1> "URA\_PCH":

- 2> if the received message is RRC CONNECTION SETUP and IE "RRC State Indicator" is set to URA\_PCH:
  - 3> set the variable INVALID\_CONFIGURATION to TRUE.
- 2> else:
  - 3> enter URA\_PCH state as dictated by the procedure governing the message received.

#### 8.6.3.4 Cipherring mode info

The IE "Cipherring mode info" defines the new cipherring configuration. At any given time, the UE needs to store at most two different cipherring configurations (keyset and algorithm) per CN domain at any given time in total for all radio bearers and three configurations in total for all signalling radio bearers.

If the IE "Cipherring mode info" is present and if the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE, the UE shall:

- 1> ignore this second attempt to change the cipherring configuration; and
- 1> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to TRUE.

If the IE "Cipherring mode info" is present and if the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to FALSE, the UE shall:

- 1> if the IE "Status" in the variable CIPHERING STATUS has the value "Not started", and this IE was included in a message that is not the message SECURITY MODE COMMAND; or
- 1> if there does not exist exactly one cipherring activation time in the IE "Radio bearer downlink cipherring activation time info" for each established RLC-AM and RLC-UM radio bearers included in the IE "RB information" in the IE "ESTABLISHED\_RABS" for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN; or
- 1> if the IE "Cipherring activation time for DPCH" is not included in message ACTIVE SET UPDATE or SECURITY MODE COMMAND, and there exist radio bearers using RLC-TM according to the IE "RB information" in the IE "ESTABLISHED\_RABS" for the CN domain as indicated in the variable LATEST\_CONFIGURED\_CN\_DOMAIN; or
- 1> if there does not exist exactly one cipherring activation time in the IE "Radio bearer downlink cipherring activation time info" for each established signalling radio bearer included in the IE "Signalling radio bearer information" in the IE "ESTABLISHED\_RABS":
  - 2> ignore this attempt to change the cipherring configuration;
  - 2> set the variable INVALID\_CONFIGURATION to TRUE;
  - 2> perform the actions as specified in subclause 8.1.12.4c.
- 1> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to TRUE;
- 1> set the IE "Status" in the variable CIPHERING\_STATUS of the CN domains for which the IE "Status" of the variable SECURITY\_MODIFICATION is set to "Affected" to "Started";
- 1> apply the new cipherring configuration in the lower layers for all RBs that belong to a CN domain for which the IE "Status" of the variable SECURITY\_MODIFICATION is set to "Affected" and all signalling radio bearers:

- 2> using the ciphering algorithm (UEA [40]) indicated by the IE "Ciphering algorithm" as part of the new ciphering configuration;
  - 2> for each radio bearer that belongs to a CN domain for which the IE "Status" of the variable SECURITY\_MODIFICATION is set to "Affected" and all signalling radio bearers:
    - 3> using the value of the IE "RB identity" in the variable ESTABLISHED\_RABS minus one as the value of BEARER [40] in the ciphering algorithm.
  - 1> apply the new ciphering configuration as follows:
    - 2> consider an activation time in downlink to be pending:
      - 3> for UM-RLC until an UMD PDU with sequence number equal to or larger than activation time –1 has been received;
      - 3> for AM-RLC until all AMD PDUs with sequence numbers up to and including activation time –1 have been received;
      - 3> for TM-RLC until the CFN indicated in the activation time has been reached.
    - 2> if there are pending activation times in downlink set for ciphering by a previous procedure changing the ciphering configuration:
      - 3> apply the ciphering configuration included in the current message at this pending activation time;
        - 3> consider the ciphering keys that were to be applied following a previous procedure changing the ciphering configuration and which have not yet been applied due to the activation time not having elapsed for a given radio bearer, as part of the ciphering configuration received in the current message.
    - 2> if the IE "Ciphering activation time for DPCH" is present in the IE "Ciphering mode info" and the UE was in CELL\_DCH state prior to this procedure:
      - 3> for radio bearers using RLC-TM:
        - 4> apply the old ciphering configuration for CFN less than the number indicated in the IE "Ciphering activation time for DPCH";
        - 4> apply the new ciphering configuration for CFN greater than or equal to the number indicated in IE "Ciphering activation time for DPCH".
    - 2> if the UE was in CELL\_FACH state prior to this procedure and at completion of this procedure a transparent mode radio bearer exists and the IE "Ciphering activation time for DPCH" is not present in the IE "Ciphering mode info":
      - 3> for radio bearers using RLC-TM:
        - 4> apply the old ciphering configuration for CFN less than the number as indicated by the IE "COUNT-C activation time" in the transmitted uplink response message for the ciphering activation time for this radio bearer;
        - 4> apply the new ciphering configuration for CFN greater than or equal to the number ~~as~~ indicated in the transmitted uplink response message for the ciphering activation time for this radio bearer.
- ~~NOTE: This is indicated by the IE "COUNT-C activation time" in the transmitted uplink response message.~~
- 2> if the IE "Radio bearer downlink ciphering activation time info" is present:
    - 3> apply the following procedure for each radio bearer and signalling radio bearers using RLC-AM or RLC-UM indicated by the IE "RB identity":
      - 4> suspend uplink transmission on the radio bearer or the signalling radio bearer (except for the SRB where the response message is transmitted) according to the following:
        - 5> do not transmit RLC PDUs with sequence number greater than or equal to the uplink activation time, where the uplink activation time is selected according to the rules below.

- 4> select an "RLC send sequence number" at which (activation) time the new ciphering configuration shall be applied in uplink for that radio bearer according to the following:
  - 5> for each radio bearer and signalling radio bearer that has no pending ciphering activation time in uplink as set by a previous procedure changing the security configuration:
    - 6> set a suitable value that would ensure a minimised delay in the change to the latest security configuration.
  - 5> for each radio bearer and signalling radio bearer that has a pending ciphering activation time in uplink as set by a previous procedure changing the security configuration:
    - 6> set the same value as the pending ciphering activation time.
- 5> consider this activation time in uplink to be elapsed when the selected activation time (as above) is equal to the "RLC send sequence number";
- 4> store the selected "RLC send sequence number" for that radio bearer in the entry for the radio bearer in the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
- 4> switch to the new ciphering configuration according to the following:
  - 5> use the old ciphering configuration for the transmitted and received RLC PDUs with RLC sequence numbers smaller than the corresponding RLC sequence numbers indicated in the IE "Radio bearer uplink ciphering activation time info" sent to UTRAN and in the received IE "Radio bearer downlink ciphering activation time info" received from UTRAN, respectively;
  - 5> use the new ciphering configuration for the transmitted and received RLC PDUs with RLC sequence numbers greater than or equal to the corresponding RLC sequence numbers indicated in the IE "Radio bearer uplink ciphering activation time info" sent to UTRAN and in the received IE "Radio bearer downlink ciphering activation time info" received from UTRAN, respectively;
  - 5> for a radio bearer using RLC-AM, when the RLC sequence number indicated in the IE "Radio bearer downlink ciphering activation time info" falls below the RLC receiving window and the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" falls below the RLC transmission window, the UE may release the old ciphering configuration for that radio bearer;
  - 5> if an RLC reset or re-establishment occurs before the activation time for the new ciphering configuration has been reached, ignore the activation time and apply the new ciphering configuration immediately after the RLC reset or RLC re-establishment.

If the IE "Ciphering mode info" is not present, the UE shall:

- 1> not change the ciphering configuration.

### 8.6.3.5 Integrity protection mode info

The IE "Integrity protection mode info" defines the new integrity protection configuration. At any given time, the UE needs to store at most three different integrity protection configurations (keysets) in total for all signalling radio bearers for all CN domains.

If the IE "Integrity protection mode info" is present and if the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE, the UE shall:

- 1> ignore this second attempt to change the integrity protection configuration; and
- 1> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to TRUE.

If the IE "Integrity protection mode info" is present and if the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to FALSE, the UE shall:

- 1> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to TRUE;

- 1> if IE "Integrity protection mode command" has the value "start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and this IE was included in the message SECURITY MODE COMMAND:
  - 2> initialise the information for all signalling radio bearers in the variable INTEGRITY\_PROTECTION\_INFO according to the following:
    - 3> set the IE "Uplink RRC Message sequence number" in the variable INTEGRITY\_PROTECTION\_INFO to zero;
    - 3> do not set the IE "Downlink RRC Message sequence number" in the variable INTEGRITY\_PROTECTION\_INFO;
    - 3> set the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO to zero for each signalling radio bearer in the IE "ESTABLISHED\_RABS".
  - 2> set the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO to the value "Started";
  - 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:
    - 3> using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";
    - 3> using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].
  - 2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer in the IE "ESTABLISHED\_RABS" except RB2 at the next received RRC message;
  - 2> start applying the new integrity protection configuration in the downlink for signalling radio bearer RB2 from and including the received SECURITY MODE COMMAND message;
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearers other than RB2 at the uplink activation time included in the IE "Uplink integrity protection activation info".
- 1> if IE "Integrity protection mode command" has the value "start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and this IE was not included SECURITY MODE COMMAND:

NOTE: This case is used in SRNS relocation

- 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:
  - 3> using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";
  - 3> using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].
- 2> let RB<sub>m</sub> be the signalling radio bearer where the reconfiguration message was received and let RB<sub>n</sub> be the signalling radio bearer where the response message is transmitted;
- 2> prohibit transmission of RRC messages on all signalling radio bearers in the IE "ESTABLISHED\_RABS" except the radio bearer where the response message is transmitted;
- 2> [consider the new integrity protection configuration to include any new keys that were activated through a security procedure received prior to the current message but not applied for the signalling radio bearer, due to the activation time for the corresponding signalling radio bearer not having elapsed;](#)

- 2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer in the IE "ESTABLISHED\_RABS" except RBm at the next received RRC message disregarding any pending activation times for the corresponding signalling radio bearer;
- 2> start applying the new integrity protection configuration in the downlink for signalling radio bearer RBm from and including the received configuration message;
- 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RBn from and including the transmitted response message;
- 2> start applying the new integrity protection configuration in the uplink for signalling radio bearers other than RBn from the first message onwards at the uplink activation time included in the IE "Uplink integrity protection activation info".

NOTE : The UTRAN should ignore the information included in the IE "Uplink integrity protection info".

- 1> if IE "Integrity protection mode command" has the value "modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and this IE was included in SECURITY MODE COMMAND:
  - 2> store the (oldest currently used) integrity protection configuration until activation times have elapsed for the new integrity protection configuration to be applied on all signalling radio bearers;
  - 2> if there are pending activation times set for integrity protection by a previous procedure changing the integrity protection configuration:
    - 3> apply the integrity protection configuration at this pending activation time as indicated in this procedure.
  - 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each signalling radio bearer n, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info";
  - 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1;
    - 3> if present, use the algorithm indicated by the IE "Integrity protection algorithm" (UIA [40]);
  - 2> set the content of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO according to the following:
    - 3> for each established signalling radio bearer, stored in the variable ESTABLISHED\_RABS:
      - 4> select a value of the RRC sequence number at which (activation) time the new integrity protection configuration shall be applied in uplink for that signalling radio bearer according to the following:
        - 5> for each signalling radio bearer that has no pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
          - 6> set a suitable value that would ensure a minimised delay in the change to the latest integrity protection configuration.
        - 5> for signalling radio bearer that has a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
          - 6> set the same value as the pending activation time for integrity protection;
        - 5> consider this (pending) activation time to be elapsed when the selected activation time (as above) is equal to the next RRC sequence number to be used, which means that the last RRC message using the old integrity protection configuration has been submitted to lower layers.
      - 4> for signalling radio bearer RB0:
        - 5> set the value of the included RRC sequence number to greater than or equal to the current value of the RRC sequence number for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO, plus the value of the constant N302 plus one.



4> prohibit the transmission of RRC messages on all signalling radio bearers, except for RB2, with RRC SN greater than or equal to the value in the "RRC message sequence number list" for the signalling radio bearer in the IE "Uplink integrity protection activation info" of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.

2> start applying the new integrity protection configuration in the uplink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Uplink integrity protection activation info", included in the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;

2> start applying the new integrity protection configuration in the uplink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration;

2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info";

NOTE: For signalling radio bearers that have a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration, UTRAN should set this value in IE "Downlink integrity protection activation info".

2> start applying the new integrity protection configuration in the downlink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration.

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and the IE "Integrity protection mode command info" was not included in the message SECURITY MODE COMMAND; or

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and the IE "Integrity protection mode info" was included in the message SECURITY MODE COMMAND, and the IE "Integrity protection algorithm" is not included; or

If the IE "Integrity protection mode command" has the value "Modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not Started"; or

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started", and the IE "Integrity protection mode command info" was included in the message SECURITY MODE COMMAND; or

If there does not exist exactly one integrity protection activation time in the IE "Downlink integrity protection activation info" for each established signalling radio bearer included in the IE "Signalling radio bearer information" in the IE "ESTABLISHED\_RABS"; or

If IE "Integrity protection mode command" has the value "Modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started", and the IE "Integrity protection mode info" was not included in the message SECURITY MODE COMMAND:

the UE shall:

1> ignore this attempt to change the integrity protection configuration; and

1> set the variable INVALID\_CONFIGURATION to TRUE.

If the IE "Integrity protection mode info" is not present, the UE shall:

1> not change the integrity protection configuration.

### 8.6.3.6 Void

### 8.6.4.8 RB mapping info

If the IE "RB mapping info" is included, the UE shall:

- 1> for each multiplexing option of the RB:
  - 2> if a transport channel that would not exist as a result of the message (i.e. removed in the same message in IE "Deleted DL TrCH information" and IE "Deleted UL TrCH information") is referred to:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if a multiplexing option that maps a logical channel corresponding to a TM-RLC entity onto RACH, CPCH, FACH or DSCH or HS-DSCH is included:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if the multiplexing option realises the radio bearer on the uplink (resp. on the downlink) using two logical channels with different values of the IE "Uplink transport channel type" (resp. of the IE "Downlink transport channel type"):
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if that RB is using TM and the IE "Segmentation indication" is set to TRUE and, based on the multiplexing configuration resulting from this message, the logical channel corresponding to it is mapped onto the same transport channel as another logical channel:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if the transport channel considered in that multiplexing option is different from RACH and if that RB is using AM and the set of RLC sizes applicable to the logical channel transferring data PDUs has more than one element:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
  - 2> if that RB is using UM or TM and the multiplexing option realises it using two logical channels:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
- 2> for each logical channel in that multiplexing option:
  - 3> if the value of the IE "RLC size list" is set to "Explicit list":
    - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is included in the same message, and the value (index) of any IE "RLC size index" in the IE "Explicit list" does not correspond to an "RLC size" in the IE transport format set of that transport channel given in the message; or
    - 4> if the transport channel this logical channel is mapped on in this multiplexing option is different from RACH, and if a "Transport format set" for that transport channel is not included in the same message, and the value (index) of any IE "RLC size index" in the IE "Explicit list" does not correspond to an "RLC size" in the stored transport format set of that transport channel; or
    - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is included in the same message, and the value of any IE "Logical channel list" in the transport format set is not set to "Configured"; or
    - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is not included in the same message, and the value of any IE "Logical channel list" in the stored transport format set of that transport channel is not set to "Configured":
      - 5> set the variable INVALID\_CONFIGURATION to TRUE.
  - 3> if the value of the IE "RLC size list" is set to "All":

- 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is included in the same message, and the value of any IE "Logical channel list" in the transport format set is not set to "Configured"; or
- 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is not included in the same message, and the value of any IE "Logical channel list" in the stored transport format set of that transport channel is not set to "Configured":
  - 5> set the variable INVALID\_CONFIGURATION to TRUE.
- 3> if the value of the IE "RLC size list" is set to "Configured":
  - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is included in the same message, and for none of the RLC sizes defined for that transport channel in the "Transport format set", the "Logical Channel List" is set to "All" or given as an "Explicit List" which contains this logical channel; or
  - 4> if a "Transport format set" for the transport channel this logical channel is mapped on in this multiplexing option is not included in the same message, and for none of the RLC sizes defined in the transport format set stored for that transport channel, the "Logical Channel List" is set to "All" or given as an "Explicit List" which contains this logical channel:
    - 5> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if, as a result of the message this IE is included in, several radio bearers can be mapped onto the same transport channel, and the IE "Logical Channel Identity" was not included in the RB mapping info of any of those radio bearers for a multiplexing option on that transport channel or the same "Logical Channel Identity" was used more than once in the RB mapping info of those radio bearers for the multiplexing options on that transport channel:
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> delete all previously stored multiplexing options for that radio bearer;
- 1> store each new multiplexing option for that radio bearer;
- 1> select and configure the multiplexing options applicable for the transport channels to be used;
- 1> if the IE "Uplink transport channel type" is set to the value "RACH":
  - 2> in FDD:
    - 3> refer the IE "RLC size index" to the RACH Transport Format Set of the first PRACH received in the IE "PRACH system information list" received in SIB5 or SIB6.
  - 2> in TDD:
    - 3> use the first Transport Format of the PRACH of the IE "PRACH system information list" at the position equal to the value in the IE "RLC size index".
- 1> determine the sets of RLC sizes that apply to the logical channels used by that RB, based on the IEs "RLC size list" and/or the IEs "Logical Channel List" included in the applicable "Transport format set" (either the ones received in the same message or the ones stored if none were received); and
- 1> in case the selected multiplexing option is a multiplexing option on RACH:
  - 2> ignore the RLC size indexes that do not correspond to any RLC size within the Transport Format Set stored for RACH.
- 1> if RACH is the transport channel to be used on the uplink, if that RB has a multiplexing option on RACH and if it is using AM:
  - 2> apply the largest size amongst the ones derived according to the previous bullet for the RLC size (or RLC sizes in case the RB is realised using two logical channels) for the corresponding RLC entity.

Note: The IE "RB mapping info" is only included in IE "Predefined RB configurations" in system information when used for Inter-RAT handover to UTRAN and there is no AM RLC size change involved in this case.

- 1> if that RB is using AM and the RLC size applicable to the logical channel transporting data PDUs is different from the one derived from the previously stored configuration:
  - 2> re-establish the corresponding RLC entity;
  - 2> configure the corresponding RLC entity with the new RLC size;
  - 2> for each AM RLC radio bearer in the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS whose RLC size is changed; and
  - 2> for each AM RLC signalling radio bearer in the CN domain as indicated in the IE "CN domain identity" in the variable LATEST\_CONFIGURED\_CN\_DOMAIN whose RLC size is changed:
  - 3> if the IE "Status" in the variable CIPHERING\_STATUS of this CN domain is set to "Started":

~~4> if this IE was included in system information:~~

~~5> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" for this CN domain that will be included in the CELL UPDATE message that will be sent before the next transmission.~~

4> if this IE was included in CELL UPDATE CONFIRM:

5> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" included in the latest transmitted CELL UPDATE message for this CN domain.

4> if this IE was included in a reconfiguration message:

5> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" that will be included in the reconfiguration complete message for this CN domain.

1> if that RB is using UM:

2> indicate the largest applicable RLC size to the corresponding RLC entity.

1> configure MAC multiplexing according to the selected multiplexing option (MAC multiplexing shall only be configured for a logical channel if the transport channel it is mapped on according to the selected multiplexing option is the same as the transport channel another logical channel is mapped on according to the multiplexing option selected for it);

1> configure the MAC with the logical channel priorities according to selected multiplexing option;

1> configure the MAC with the set of applicable RLC Sizes for each of the logical channels used for that RB;

1> if there is no multiplexing option applicable for the transport channels to be used:

2> set the variable INVALID\_CONFIGURATION to TRUE.

1> if there is more than one multiplexing option applicable for the transport channels to be used:

2> set the variable INVALID\_CONFIGURATION to TRUE.

In case IE "RLC info" includes IE "Downlink RLC mode" ("DL RLC logical channel info" is mandatory present) but IE "Number of downlink RLC logical channels" is absent in the corresponding IE "RB mapping info", the parameter values are exactly the same as for the corresponding UL logical channels. In case two multiplexing options are specified for the UL, the first options shall be used as default for the DL. As regards the IE "Channel type", the following rule should be applied to derive the DL channel type from the UL channel included in the IE:

Channel used in UL	DL channel type implied by "same as"
DCH	DCH
RACH	FACH
CPCH	FACH
USCH	DSCH

#### 8.6.4.9 RLC Info

If the IE "RLC Info" is included, the UE shall:

- 1> configure the transmitting and receiving RLC entities in the UE for that radio bearer accordingly;
- 1> if IE "Polling Info" is absent:
  - 2> remove any previously stored configuration for the IE "Polling Info".

If the IE "Transmission RLC discard" is not included for UM RLC or TM RLC, RLC discard procedure shall not be used for that radio bearer.

#### 8.6.4.10 PDCP Info

For RFC 3095:

- 1> the chosen MAX\_CID shall not be greater than the value "Maximum number of ROHC context sessions" as indicated in the IE "PDCP Capability";
- 1> the configuration for the PACKET\_SIZES\_ALLOWED is FFS.

If IE "PDCP info" is included, the UE shall:

- 1> if the radio bearer is connected to a CS domain radio access bearer:
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the IE "PDCP PDU header" is set to the value "absent":
  - 2> if the IE "Support for lossless SRNS relocation" is true:
    - 3> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the IE "PDCP PDU header" is set to the value "present":
  - 2> if the IE "Support for lossless SRNS relocation" is false:
    - 3> if the IE "Header compression information" is absent:
      - 4> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the IE "Header compression information" is absent:
  - 2> not use Header compression after the successful completion of this procedure;
  - 2> remove any stored configuration for the IE "Header compression information".
- 1> configure the PDCP entity for that radio bearer accordingly;
- 1> configure the RLC entity for that radio bearer according to the value of the IE "Support for lossless SRNS relocation".

#### 8.6.4.11 PDCP SN Info

If the IE "PDCP SN Info" is included, the UE shall:

- 1> transfer the sequence number to the PDCP entity for the radio bearer;

1> configure the RLC entity for the radio bearer to stop;

1> include the current PDCP receive sequence number and the radio bearer identity for the radio bearer in the variable PDCP\_SN\_INFO.

#### 8.6.4.12 NAS Synchronisation Indicator

If the IE "NAS Synchronisation Indicator" is present in a message, the UE shall:

1> forward the content to upper layers along with the IE "CN domain identity" of the associated RAB stored in the variable ESTABLISHED\_RABS at the CFN indicated in the IE "Activation time" in order to synchronise actions in NAS and AS.

### 8.6.5 Transport channel information elements

#### 8.6.5.1 Transport Format Set

If the IE "Transport format set" is included, the UE shall:

1> if the transport format set is a RACH TFS received in System Information Block type 5 or 6, and CHOICE "Logical Channel List" has the value "Explicit List":

2> ignore that System Information Block.

1> if the transport format set for a downlink transport channel is received in a System Information Block, and CHOICE "Logical Channel List" has a value different from 'ALL':

2> ignore that System Information Block.

1> if the transport format set for a downlink transport channel is received in a message on a DCCH, and CHOICE "Logical Channel List" has a value different from 'ALL':

2> keep the transport format set if this exists for that transport channel;

2> set the variable INVALID\_CONFIGURATION to TRUE.

1> if the value of any IE "RB identity" (and "Logical Channel" for RBs using two UL logical channels) in the IE "Logical channel list" does not correspond to a logical channel indicated to be mapped onto this transport channel in any RB multiplexing option (either included in the same message or previously stored and not changed by this message); or

1> if the "Logical Channel List" for any of the RLC sizes defined for that transport channel is set to "Configured" while it is set to "All" or given as an "Explicit List" for any other RLC size; or

1> if the "Logical Channel List" for any of the RLC sizes defined for that transport channel is set to "All" and for any logical channel mapped to this transport channel, the value of the "RLC size list" (either provided in the IE "RB mapping info" if included in the same message, or stored) is not set to "Configured"; or

1> if the "Logical Channel List" for any of the RLC sizes defined for that transport channel is given as an "Explicit List" that contains a logical channel for which the value of the "RLC size list" (either provided in the IE "RB mapping info" if included in the same message, or stored) is not set to "Configured"; or

1> if the "Logical Channel List" for all the RLC sizes defined for that transport channel are given as "Explicit List" and if one of the logical channels mapped onto this transport channel is not included in any of those lists; or

1> if the "Logical Channel List" for the RLC sizes defined for that transport channel is set to "Configured" and for any logical channel mapped onto that transport channel, the value of the "RLC size list" (either provided in the IE "RB mapping info" if included in the same message, or stored) is also set to "Configured"; or

1> if the IE "Transport Format Set" was not received within the IE "PRACH system information list" and if the "Logical Channel List" for the RLC sizes defined for that transport channel is set to "Configured" and for any logical channel mapped onto that transport channel, the "RLC size list" (either provided in the IE "RB mapping info" if included in the same message, or stored) is given as an "Explicit List" that includes an "RLC size index" that does not correspond to any RLC size in this "Transport Format Set":

- 2> keep the transport format set if this exists for that transport channel;
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the total number of configured transport formats for the transport channel exceeds maxTF:
- 2> keep the transport format set if this exists for that transport channel;
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the IE "Transport format set" is considered as valid according to the rules above:
- 2> remove a previously stored transport format set if this exists for that transport channel;
  - 2> store the transport format set for that transport channel;
  - 2> consider the first instance of the parameter *Number of TBs and TTI List* within the *Dynamic transport format information* to correspond to transport format 0 for this transport channel, the second to transport format 1 and so on;
  - 2> if the IE "Transport format Set" has the choice "Transport channel type" set to "Dedicated transport channel":
    - 3> calculate the transport block size for all transport formats in the TFS using the following
 
$$\text{TB size} = \text{RLC size} + \text{MAC header size},$$
 where:
      - MAC header size is calculated according to [15] if MAC multiplexing is used. Otherwise it is 0 bits;
      - 'RLC size' reflects the RLC PDU size.
  - 2> if the IE "Transport format Set" has the choice "Transport channel type" set to "Common transport channel":
    - 3> calculate the transport block size for all transport formats in the TFS using the following:
 
$$\text{TB size} = \text{RLC size}.$$
  - 2> if the IE "Number of Transport blocks"  $\neq 0$  and IE "RLC size" = 0, no RLC PDU data exists but only parity bits exist for that transport format;
  - 2> if the IE "Number of Transport blocks" = 0, neither RLC PDU neither data nor parity bits exist for that transport format;
  - 2> configure the MAC with the new transport format set (with computed transport block sizes) for that transport channel;
  - 2> if the RB multiplexing option for a RB mapped onto that transport channel (based on the stored RB multiplexing option) is not modified by this message:
    - 3> determine the sets of RLC sizes that apply to the logical channels used by that RB, based on the IE "Logical Channel List" and/or the IE "RLC Size List" from the previously stored RB multiplexing option.
  - 3> if the IE "Transport Format Set" was received within the IE "PRACH system information list":
    - 4> ignore the RLC size indexes in the stored RB multiplexing option that do not correspond to any RLC size in the received Transport Format Set.
  - 3> if the IE "Transport Format Set" was received within the IE "PRACH system information list", if that RB is using AM and if RACH is the transport channel to be used on the uplink:
    - 4> apply the largest size amongst the ones derived according to the previous bullet for the RLC size (or RLC sizes in case the RB is realised using two logical channels) for the corresponding RLC entity.
  - 3> if the IE "Transport Format Set" was not received within the IE "PRACH system information list", and if that RB is using AM and the set of RLC sizes applicable to the logical channel transferring data PDUs has more than one element:

- 4> set the variable INVALID\_CONFIGURATION to true.
- 3> if that RB is using AM and the RLC size applicable to the logical channel transporting data PDUs is different from the one derived from the previously stored configuration:
  - 4> re-establish the corresponding RLC entity;
  - 4> configure the corresponding RLC entity with the new RLC size;
  - 4> for each AM RLC radio bearer in the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS whose RLC size is changed; and
  - 4> for each AM RLC signalling radio bearer in the CN domain as indicated in the IE "CN domain identity" in the variable LATEST\_CONFIGURED\_CN\_DOMAIN whose RLC size is changed:
    - 5> if this IE was included in system information and if the IE "Status" in variable CIPHERING\_STATUS of this CN domain is set to "Started":
      - 6> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" for this CN domain that will be included in the CELL UPDATE message that will be sent before the next transmission.
    - 5> if this IE was included in CELL UPDATE CONFIRM and if the IE "Status" in the variable CIPHERING\_STATUS of this CN domain is set to "Started":
      - 6> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" included in the latest transmitted CELL UPDATE message for this CN domain.
    - 5> if this IE was included in a reconfiguration message and if the IE "Status" in the variable CIPHERING\_STATUS of this CN domain is set to "Started":
      - 6> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" that will be included in the reconfiguration complete message for this CN domain.
    - 5> if this IE was included in ACTIVE SET UPDATE and if the IE "Status" in the variable CIPHERING\_STATUS of this CN domain is set to "Started":
      - 6> set the HFN values for the corresponding RLC entity equal to the value of the IE "START" that will be included in the ACTIVE SET UPDATE COMPLETE message for this CN domain.
- 3> if that RB is using UM:
  - 4> indicate the largest applicable RLC size to the corresponding RLC entity.
- 3> configure MAC with the set of applicable RLC Sizes for each of the logical channels used for that RB.

For configuration restrictions on Blind Transport Format Detection, see [27].

## 10.2 Radio Resource Control messages

### 10.2.1 ACTIVE SET UPDATE

NOTE: Only for FDD.

This message is used by UTRAN to add, replace or delete radio links in the active set of the UE.

RLC-SAP: AM or UM

Logical channel: DCCH

Direction: UTRAN → UE



Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message Type	MP		Message Type	
<b>UE information elements</b>				
RRC transaction identifier	MP		RRC transaction identifier 10.3.3.36	
Integrity check info	CH		Integrity check info 10.3.3.16	
<del>Integrity protection mode info</del>	<del>OP</del>		<del>Integrity protection mode info 10.3.3.19</del>	
<del>Ciphering mode info</del>	<del>OP</del>		<del>Ciphering mode info 10.3.3.5</del>	
Activation time	MD		Activation time 10.3.3.1	Default value is "now".
New U-RNTI	OP		U-RNTI 10.3.3.47	
<b>CN information elements</b>				
CN Information info	OP		CN Information info 10.3.1.3	
<b>RB information elements</b>				
<del>Downlink counter synchronisation info</del>	<del>OP</del>			
<del>&gt;RB with PDCP information list</del>	<del>OP</del>	1 to <maxRBall RABs>		<del>This IE is needed for each RB having PDCP in the case of lossless SRNS relocation</del>
<del>&gt;&gt;RB with PDCP information</del>	<del>MP</del>		<del>RB with PDCP information 10.3.4.22</del>	
<b>Phy CH information elements</b>				
<b>Uplink radio resources</b>				
Maximum allowed UL TX power	MD		Maximum allowed UL TX power 10.3.6.39	Default value is the existing "maximum UL TX power."
<b>Downlink radio resources</b>				
Radio link addition information	OP	1 to <maxRL-1>		Radio link addition information required for each RL to add
>Radio link addition information	MP		Radio link addition information 10.3.6.68	
Radio link removal information	OP	1 to <maxRL>		Radio link removal information required for each RL to remove
>Radio link removal information	MP		Radio link removal information 10.3.6.69	
TX Diversity Mode	MD		TX Diversity Mode 10.3.6.86	Default value is the existing TX diversity mode.
SSDT information	OP		SSDT information 10.3.6.77	

## 10.2.2 ACTIVE SET UPDATE COMPLETE

NOTE: For FDD only.

This message is sent by UE when active set update has been completed.

RLC-SAP: AM

Logical channel: DCCH

Direction: UE→UTRAN

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message Type	MP		Message Type	
<b>UE information elements</b>				
RRC transaction identifier	MP		RRC transaction identifier 10.3.3.36	
Integrity check info	CH		Integrity check info 10.3.3.16	
<del>Uplink integrity protection activation info</del>	<del>OP</del>		<del>Integrity protection activation info 10.3.3.17</del>	
<b>RB Information elements</b>				
<del>Radio bearer uplink ciphering activation time info</del>	<del>OP</del>		<del>RB activation time info 10.3.4.13</del>	
<del>Uplink counter synchronisation info</del>	<del>OP</del>			
<del>&gt;RB with PDCP information list</del>	<del>OP</del>	<del>1 to &lt;maxRBall RABs&gt;</del>		<del>This IE is needed for each RB having PDCP in the case of lossless SRNS relocation</del>
<del>&gt;&gt;RB with PDCP information</del>	<del>MP</del>		<del>RB with PDCP information 10.3.4.22</del>	
<del>&gt;START list</del>	<del>MP</del>	<del>1 to &lt;maxCNdomains&gt;</del>		<del>START [40] values for all CN domains.</del>
<del>&gt;&gt;CN domain identity</del>	<del>MP</del>		<del>CN domain identity 10.3.1.1</del>	
<del>&gt;&gt;START</del>	<del>MP</del>		<del>START 10.3.3.38</del>	<del>START value to be used in this CN domain.</del>

## 10.2.3 ACTIVE SET UPDATE FAILURE

NOTE: Only for FDD.

This message is sent by UE if the update of the active set has failed, e.g. because the radio link is not a part of the active set.

RLC-SAP: AM

Logical channel: DCCH

Direction: UE→UTRAN

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message Type	MP		Message Type	
<b>UE information elements</b>				
RRC transaction identifier	MP		RRC transaction identifier 10.3.3.36	
Integrity check info	CH		Integrity check info 10.3.3.16	
Failure cause	MP		Failure cause and error information 10.3.3.14	

### 10.2.4 ASSISTANCE DATA DELIVERY

This message is sent by UTRAN to convey UE positioning assistance data to the UE.

RLC-SAP: AM

Logical channel: DCCH

Direction: UTRAN→UE

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message Type	MP		Message Type	
<b>UE information elements</b>				
RRC transaction identifier	MP		RRC transaction identifier 10.3.3.36	
Integrity check info	CH		Integrity check info 10.3.3.16	
<b>Measurement Information elements</b>				
UE positioning OTDOA assistance data for UE-based	OP		UE positioning OTDOA assistance data for UE-based 10.3.7.103a	
UE positioning GPS assistance data	OP		UE positioning GPS assistance data 10.3.7.90	

-----

#### 10.3.3.5 Cipherring mode info

This information element contains the cipherring specific security mode control information.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Ciphering mode command	MP		Enumerated (start/restart, stop)	<del>The command "stop" is not used in this version of the protocol.</del>
Ciphering algorithm	<del>MPCV-</del> <del>notStop</del>		Ciphering algorithm 10.3.3.4	
Ciphering activation time for DPCH	OP		Activation time 10.3.3.1	Used for radio bearers mapped on RLC-TM. Only applicable if the UE is already in CELL_DCH state
Radio bearer downlink ciphering activation time info	OP		RB activation time info, 10.3.4.13	Used for radio bearers mapped on RLC-AM or RLC-UM

Condition	Explanation
<del>notStop</del>	<del>The IE is mandatory present if the IE "Ciphering mode command" has the value "start/restart", otherwise the IE is not needed in the message.</del>

~~10.3.3.10 RRC State Indicator~~

~~Indicates to a UE the RRC state to be entered.~~

Information Element/Group name	Need	Multi	Type and reference	Semantics description
<del>RRC State indicator</del>	<del>MP</del>		<del>Enumerated( CELL_DCH, CELL_FACH, CELL_PCH, URA_PCH)</del>	

10.3.3.35 RLC re-establish indicator

This IE is used to re-configure AM RLC on c-plane and u-plane.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
RLC re-establish indicator	MP		Boolean	TRUE means re-establish required FALSE means re-establish not required

10.3.3.35a RRC State Indicator

Indicates to a UE the RRC state to be entered.

<u>Information Element/Group name</u>	<u>Need</u>	<u>Multi</u>	<u>Type and reference</u>	<u>Semantics description</u>
<u>RRC State indicator</u>	<u>MP</u>		<u>Enumerated(CELL_DCH, CELL_FACH, CELL_PCH, URA_PCH)</u>	

### 10.3.3.36 RRC transaction identifier

This IE contains an identification of the RRC procedure transaction local for the type of the message this IE was included within.

<b>Information Element/Group name</b>	<b>Need</b>	<b>Multi</b>	<b>Type and reference</b>	<b>Semantics description</b>
RRC transaction identifier	MP		Integer (0..3)	

### 10.3.3.37 Security capability

<b>Information Element/Group name</b>	<b>Need</b>	<b>Multi</b>	<b>Type and reference</b>	<b>Semantics description</b>
Ciphering algorithm capability	MP			
>UEA0	MP		Boolean	<del>The value TRUE means that an unciphered connection after the Security mode control procedure is accepted by the UE.</del>
>UEA1	MP		Boolean	<del>The value TRUE means that UEA1, Kasumi, is supported</del>
>Spare	MP	14	Boolean	Shall be set to FALSE by UEs complying with this version of the protocol.
Integrity protection algorithm capability	MP			
>UIA1	MP		Boolean	The value TRUE means that UIA1, Kasumi, is supported
>Spare	MP	15	Boolean	Shall be set to FALSE by UEs complying with this version of the protocol.

~~NOTE: The UE shall support at least one UEAx other than UEA0 and one UIAx.~~

### 10.3.3.38 START

There is a START value per CN domain. The START is used to initialise the 20 MSBs of all hyper frame numbers (MAC-d HFN, RLC UM HFN, RLC AM HFN, RRC HFN) for a CN domain.

<b>Information Element/Group name</b>	<b>Need</b>	<b>Multi</b>	<b>Type and Reference</b>	<b>Semantics description</b>
START	MP		Bit string (20)	The START [40] bits are numbered b0-b19, where b0 is the least significant bit.

## 11.2 PDU definitions

-----  
 --  
 -- TABULAR: The message type and integrity check info are not

```

-- visible in this module as they are defined in the class module.
-- Also, all FDD/TDD specific choices have the FDD option first
-- and TDD second, just for consistency.
--
--*****
PDU-definitions DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

--*****
--
-- IE parameter types from other modules
--
--*****

IMPORTS

-- Core Network IEs :
  CN-DomainIdentity,
  CN-InformationInfo,
  CN-InformationInfoFull,
  NAS-Message,
  PagingRecordTypeID,
-- UTRAN Mobility IEs :
  CellIdentity,
  CellIdentity-PerRL-List,
  URA-Identity,
-- User Equipment IEs :
  ActivationTime,
  C-RNTI,
  CapabilityUpdateRequirement,
  CapabilityUpdateRequirement-r4,
  CapabilityUpdateRequirement-r4-ext,
  CellUpdateCause,
  CipheringAlgorithm,
  CipheringModeInfo,
  DSCH-RNTI,
  EstablishmentCause,
  FailureCauseWithProtErr,
  FailureCauseWithProtErrTrId,
  H-RNTI,
  InitialUE-Identity,
  IntegrityProtActivationInfo,
  IntegrityProtectionModeInfo,
  N-308,
  PagingCause,
  PagingRecordList,
  ProtocolErrorIndicator,
  ProtocolErrorIndicatorWithMoreInfo,
  Rb-timer-indicator,
  RedirectionInfo,
  RejectionCause,
  ReleaseCause,
  RRC-StateIndicator,
  RRC-TransactionIdentifier,
  SecurityCapability,
  START-Value,
  STARTList,
  U-RNTI,
  U-RNTI-Short,
  UE-RadioAccessCapability,
  UE-RadioAccessCapability-r4-ext,
  UE-RadioAccessCapability-r5-ext,
  UE-RadioAccessCapability-v370ext,
  UE-RadioAccessCapability-v380ext,
  UE-RadioAccessCapability-v3a0ext,
  UE-RadioAccessCapability-v4xyext,
  DL-PhysChCapabilityFDD-v380ext,
  UE-ConnTimersAndConstants,
  UE-ConnTimersAndConstants-v3a0ext,
  UE-SecurityInformation,
  URA-UpdateCause,
  UTRAN-DRX-CycleLengthCoefficient,
  WaitTime,
-- Radio Bearer IEs :
  DefaultConfigIdentity,
  DefaultConfigMode,

```

```

DL-CounterSynchronisationInfo,
PredefinedConfigIdentity,
PredefinedConfigStatusList,
RAB-Info,
RAB-Info-Post,
RAB-InformationList,
RAB-InformationReconfigList,
RAB-InformationSetupList,
RAB-InformationSetupList-r4,
RB-ActivationTimeInfoList,
RB-COUNT-C-InformationList,
RB-COUNT-C-MSB-InformationList,
RB-IdentityList,
RB-InformationAffectedList,
RB-InformationAffectedList-r5,
RB-InformationReconfigList,
RB-InformationReconfigList-r4,
RB-InformationReconfigList-r5,
RB-InformationReleaseList,
RB-WithPDCP-InfoList, SRB-InformationSetupList,
SRB-InformationSetupList2,
UL-CounterSynchronisationInfo,
-- Transport Channel IEs:
CPCH-SetID,
DL-AddReconfTransChInfo2List,
DL-AddReconfTransChInfoList,
DL-AddReconfTransChInfoList-r4,
DL-AddReconfTransChInfoList-r5,
DL-CommonTransChInfo,
DL-CommonTransChInfo-r4,
DL-DeletedTransChInfoList,
DL-DeletedTransChInfoList-r5,
DRAC-StaticInformationList,
TFC-Subset,
TFCS-Identity,
UL-AddReconfTransChInfoList,
UL-CommonTransChInfo,
UL-CommonTransChInfo-r4,
UL-DeletedTransChInfoList,
-- Physical Channel IEs :
Alpha,
CCTrCH-PowerControlInfo,
CCTrCH-PowerControlInfo-r4,
ConstantValue,
ConstantValueTdd,
CPCH-SetInfo,
DL-CommonInformation,
DL-CommonInformation-r4,
DL-CommonInformationPost,
DL-HSPDSCH-Information,
DL-InformationPerRL,
DL-InformationPerRL-List,
DL-InformationPerRL-List-r4,
DL-InformationPerRL-List-r5,
DL-InformationPerRL-ListPostFDD,
DL-InformationPerRL-PostTDD,
DL-InformationPerRL-PostTDD-LCR-r4,
DL-PDSCH-Information,
DPCH-CompressedModeStatusInfo,
FrequencyInfo,
FrequencyInfoFDD,
FrequencyInfoTDD,
MaxAllowedUL-TX-Power,
OpenLoopPowerControl-IPDL-TDD-r4,
PDSCH-CapacityAllocationInfo,
PDSCH-CapacityAllocationInfo-r4,
PDSCH-Identity,
PrimaryCCPCH-TX-Power,
PUSCH-CapacityAllocationInfo,
PUSCH-CapacityAllocationInfo-r4,
PUSCH-Identity,
RL-AdditionInformationList,
RL-RemovalInformationList,
SpecialBurstScheduling,
SSDT-Information,
TFC-ControlDuration,
SSDT-UL-r4,
TimeslotList,

```

```

TimeslotList-r4,
TX-DiversityMode,
UL-ChannelRequirement,
UL-ChannelRequirement-r4,
UL-ChannelRequirement-r5,
UL-ChannelRequirementWithCPCH-SetID,
UL-ChannelRequirementWithCPCH-SetID-r4,
UL-ChannelRequirementWithCPCH-SetID-r5,
UL-DPCH-Info,
UL-DPCH-Info-r4,
UL-DPCH-InfoPostFDD,
UL-DPCH-InfoPostTDD,
UL-DPCH-InfoPostTDD-LCR-r4,
UL-SynchronisationParameters-r4,
UL-TimingAdvance,
UL-TimingAdvanceControl,
UL-TimingAdvanceControl-r4,
-- Measurement IEs :
AdditionalMeasurementID-List,
Frequency-Band,
EventResults,
InterFreqEventResults-LCR-r4-ext,
InterRAT-TargetCellDescription,
MeasuredResults,
MeasuredResults-v390ext,
MeasuredResultsList,
MeasuredResultsList-LCR-r4-ext,
MeasuredResultsOnRACH,
MeasurementCommand,
MeasurementCommand-r4,
MeasurementIdentity,
MeasurementReportingMode,
PrimaryCCPCH-RSCP,
SFN-Offset-Validity,
TimeslotListWithISCP,
TrafficVolumeMeasuredResultsList,
UE-Positioning-GPS-AssistanceData,
UE-Positioning-Measurement-v390ext,
UE-Positioning-OTDOA-AssistanceData,
UE-Positioning-OTDOA-AssistanceData-r4ext,
UE-Positioning-OTDOA-AssistanceData-UEB,
UE-Positioning-IPDL-Parameters-TDD-r4-ext,
-- Other IEs :
BCCH-ModificationInfo,
CDMA2000-MessageList,
GSM-MessageList,
InterRAT-ChangeFailureCause,
InterRAT-HO-FailureCause,
InterRAT-UE-RadioAccessCapabilityList,
InterRAT-UE-SecurityCapList,
IntraDomainNasNodeSelector,
ProtocolErrorMoreInformation,
Rplmn-Information,
Rplmn-Information-r4,
SegCount,
SegmentIndex,
SFN-Prime,
SIB-Data-fixed,
SIB-Data-variable,
SIB-Type
FROM InformationElements

maxSIBperMsg
FROM Constant-definitions;

-- *****
--
-- ACTIVE SET UPDATE (FDD only)
--
-- *****

ActiveSetUpdate ::= CHOICE {
    r3
        activeSetUpdate-r3
        v4xyNonCriticalExtensions
        activeSetUpdate-v4xyext
        nonCriticalExtensions
    } OPTIONAL
    SEQUENCE {
        ActiveSetUpdate-r3-IEs,
        SEQUENCE {
            ActiveSetUpdate-v4xyext-IEs,
            SEQUENCE {} OPTIONAL
        } OPTIONAL
    }
},

```



```

later-than-r3
  rrc-TransactionIdentifier      RRC-TransactionIdentifier,
  criticalExtensions             SEQUENCE {}
}

ActiveSetUpdate-r3-IEs ::= SEQUENCE {
  -- User equipment IEs
  rrc-TransactionIdentifier      RRC-TransactionIdentifier,
  -- dummy and dummy2 are not used in this version of the specification, they should
  -- not be sent and if received they should be ignored.
  dummyintegrityProtectionModeInfo IntegrityProtectionModeInfo      OPTIONAL,
  dummy2cipheringModeInfo          CipheringModeInfo                OPTIONAL,
  activationTime                 ActivationTime                    OPTIONAL,
  newU-RNTI                      U-RNTI                          OPTIONAL,
  -- Core network IEs
  cn-InformationInfo             CN-InformationInfo              OPTIONAL,
  -- Radio bearer IEs
  -- dummy3 is not used in this version of the specification, it should
  -- not be sent and if received it should be ignored.
  dl-CounterSynchronisationInfodummy3 DL-CounterSynchronisationInfo      OPTIONAL,
  -- Physical channel IEs
  maxAllowedUL-TX-Power          MaxAllowedUL-TX-Power          OPTIONAL,
  rl-AdditionInformationList      RL-AdditionInformationList      OPTIONAL,
  rl-RemovalInformationList       RL-RemovalInformationList       OPTIONAL,
  tx-DiversityMode               TX-DiversityMode                OPTIONAL,
  ssdt-Information               SSDT-Information                OPTIONAL
}

ActiveSetUpdate-v4xyext-IEs ::= SEQUENCE {
  -- Physical channel IEs
  -- ssdt-UL extends SSdT-Information. FDD only.
  ssdt-UL                        SSdT-UL-r4                        OPTIONAL,
  -- The order of the RLs in IE cell-id-PerRL-List is the same as
  -- in IE RL-AdditionInformationList included in this message
  cell-id-PerRL-List             CellIdentity-PerRL-List       OPTIONAL
}

-- *****
--
-- ACTIVE SET UPDATE COMPLETE (FDD only)
--
-- *****

ActiveSetUpdateComplete ::= SEQUENCE {
  -- User equipment IEs
  rrc-TransactionIdentifier      RRC-TransactionIdentifier,
  -- dummy is not used in this version of the specification, it should
  -- not be sent and if received it should be ignored.
  ul-IntegProtActivationInfodummy IntegrityProtActivationInfo      OPTIONAL,
  -- Radio bearer IEs
  -- dummy2 and dummy3 are not used in this version of the specification, they should
  -- not be sent and if received they should be ignored.
  rb-UL-CiphActivationTimeInfodummy2 RB-ActivationTimeInfoList      OPTIONAL,
  ul-CounterSynchronisationInfodummy3 UL-CounterSynchronisationInfo      OPTIONAL,
  -- Extension mechanism for non- release99 information
  nonCriticalExtensions          SEQUENCE {} OPTIONAL
}

-- *****
--
-- ACTIVE SET UPDATE FAILURE (FDD only)
--
-- *****

ActiveSetUpdateFailure ::= SEQUENCE {
  -- User equipment IEs
  rrc-TransactionIdentifier      RRC-TransactionIdentifier,
  failureCause                   FailureCauseWithProtErr,
  -- Extension mechanism for non- release99 information
  nonCriticalExtensions          SEQUENCE {} OPTIONAL
}

-- *****
--
-- Assistance Data Delivery
--

```

```

-- *****
AssistanceDataDelivery ::= CHOICE {
  r3                               SEQUENCE {
    assistanceDataDelivery-r3      AssistanceDataDelivery-r3-IEs,
    v3aoNonCriticalExetensions     SEQUENCE {
      assistanceDataDelivery-v3a0ext AssistanceDataDelivery-v3a0ext,
      v4xyNonCriticalExtensions    SEQUENCE {
        assistanceDataDelivery-v4xyext
          nonCriticalExtensions    AssistanceDataDelivery-v4xyext-IEs,
          SEQUENCE {}              OPTIONAL
        } OPTIONAL
      } OPTIONAL
    },
    later-than-r3                  SEQUENCE {
      rrc-TransactionIdentifier    RRC-TransactionIdentifier,
      criticalExtensions           SEQUENCE {}
    }
  }

AssistanceDataDelivery-r3-IEs ::= SEQUENCE {
  -- User equipment IEs
  rrc-TransactionIdentifier      RRC-TransactionIdentifier,
  -- Measurement Information Elements
  ue-positioning-GPS-AssistanceData UE-Positioning-GPS-AssistanceData
  OPTIONAL,
  ue-positioning-OTDOA-AssistanceData-UEB UE-Positioning-OTDOA-AssistanceData-UEB
  OPTIONAL
}

AssistanceDataDelivery-v3a0ext ::= SEQUENCE {
  sfn-Offset-Validity            SFN-Offset-Validity    OPTIONAL
}

AssistanceDataDelivery-v4xyext-IEs ::= SEQUENCE {
  ue-Positioning-OTDOA-AssistanceData-r4ext UE-Positioning-OTDOA-AssistanceData-r4ext  OPTIONAL
}

-- *****
--
-- CELL CHANGE ORDER FROM UTRAN
--
-- *****

CellChangeOrderFromUTRAN ::= CHOICE {
  r3                               SEQUENCE {
    cellChangeOrderFromUTRAN-IEs    CellChangeOrderFromUTRAN-r3-IEs,
    nonCriticalExtensions            SEQUENCE {} OPTIONAL
  },
  later-than-r3                    SEQUENCE {
    rrc-TransactionIdentifier        RRC-TransactionIdentifier,
    criticalExtensions               SEQUENCE {}
  }
}

CellChangeOrderFromUTRAN-r3-IEs ::= SEQUENCE {
  -- User equipment IEs
  rrc-TransactionIdentifier          RRC-TransactionIdentifier,
  -- dummy is not used in this version of the specification, it should
  -- not be sent and if received it should be ignored.
  dummy                             IntegrityProtectionModeInfo    OPTIONAL,
  activationTime                     ActivationTime                  OPTIONAL,
  rab-InformationList                 RAB-InformationList            OPTIONAL,
  interRAT-TargetCellDescription     InterRAT-TargetCellDescription
}

```

## 11.3 Information element definitions

```
InformationElements DEFINITIONS AUTOMATIC TAGS ::=
```

```

-- *****
--
-- CORE NETWORK INFORMATION ELEMENTS (10.3.1)
--
-- *****

```

BEGIN

IMPORTS

```
hiPDSCHidentities,  
hiPUSCHidentities,  
hiRM,  
maxAC,  
maxAdditionalMeas,  
maxASC,  
maxASCmap,  
maxASCPersist,  
maxCCTrCH,  
maxCellMeas,  
maxCellMeas-1,  
maxCNdomains,  
maxCPCHsets,  
maxDPCH-DLchan,  
maxDPDCH-UL,  
maxDRACclasses,  
maxFACHPCH,  
maxFreq,  
maxFreqBandsFDD,  
maxFreqBandsTDD,  
maxFreqBandsGSM,  
maxHProcesses,  
maxHSDSCHTBIndex,  
maxHSDSCHTBIndex-tdd384,  
maxHSSCHs,  
maxInterSysMessages,  
maxLoCHperRLC,  
maxMAC-d-PDUsizes,  
maxMeasEvent,  
maxMeasIntervals,  
maxMeasParEvent,  
maxNumCDMA2000Freqs,  
maxNumFDDFreqs,  
maxNumGSMFreqRanges,  
maxNumTDDFreqs,  
maxOtherRAT,  
maxOtherRAT-16,  
maxPage1,  
maxPCPCH-Apsig,  
maxPCPCH-ApsubCh,  
maxPCPCH-Cdsig,  
maxPCPCH-CDsubCh,  
maxPCPCH-SF,  
maxPCPCHs,  
maxPDCPAlgoType,  
maxPDSCH,  
maxPDSCH-TFCIgroups,  
maxPRACH,  
maxPRACH-FPACH,  
maxPredefConfig,  
maxPUSCH,  
maxQueueIDs,  
maxRABsetup,  
maxRAT,  
maxRB,  
maxRBallRABs,  
maxRBMuxOptions,  
maxRBperRAB,  
maxReportedGSMCells,  
maxSRBsetup,  
maxRL,  
maxRL-1,  
maxROHC-PacketSizes-r4,  
maxROHC-Profile-r4,  
maxSCCPCH,  
maxSat,  
maxSIB,  
maxSIB-FACH,  
maxSystemCapability,  
maxTF,  
maxTF-CPCH,  
maxTFC,  
maxTFCsub,  
maxTFCI-2-Combs,
```

```

maxTGPS,
maxTrCH,
maxTrCHpreconf,
maxTS,
maxTS-1,
maxTS-LCR,
maxTS-LCR-1,
maxURA
FROM Constant-definitions;

Ansi-41-IDNNS ::=                               BIT STRING (SIZE (14))

CN-DomainIdentity ::=                           ENUMERATED {
                                                cs-domain,
                                                ps-domain }

CN-DomainInformation ::=                       SEQUENCE {
  cn-DomainIdentity                             CN-DomainIdentity,
  cn-DomainSpecificNAS-Info                     NAS-SystemInformationGSM-MAP
}

CN-DomainInformationFull ::=                   SEQUENCE {
  cn-DomainIdentity                             CN-DomainIdentity,
  cn-DomainSpecificNAS-Info                     NAS-SystemInformationGSM-MAP,
  cn-DRX-CycleLengthCoeff                      CN-DRX-CycleLengthCoefficient
}

CN-DomainInformationList ::=                   SEQUENCE (SIZE (1..maxCNdomains)) OF
  CN-DomainInformation

CN-DomainInformationListFull ::=               SEQUENCE (SIZE (1..maxCNdomains)) OF
  CN-DomainInformationFull

CN-DomainSysInfo ::=                           SEQUENCE {
  cn-DomainIdentity                             CN-DomainIdentity,
  cn-Type                                         CHOICE {
    gsm-MAP                                       NAS-SystemInformationGSM-MAP,
    ansi-41                                       NAS-SystemInformationANSI-41
  },
  cn-DRX-CycleLengthCoeff                      CN-DRX-CycleLengthCoefficient
}

CN-DomainSysInfoList ::=                       SEQUENCE (SIZE (1..maxCNdomains)) OF
  CN-DomainSysInfo

CN-InformationInfo ::=                         SEQUENCE {
  plmn-Identity                                 PLMN-Identity                               OPTIONAL,
  cn-CommonGSM-MAP-NAS-SysInfo                 NAS-SystemInformationGSM-MAP                 OPTIONAL,
  cn-DomainInformationList                     CN-DomainInformationList                     OPTIONAL
}

CN-InformationInfoFull ::=                     SEQUENCE {
  plmn-Identity                                 PLMN-Identity                               OPTIONAL,
  cn-CommonGSM-MAP-NAS-SysInfo                 NAS-SystemInformationGSM-MAP                 OPTIONAL,
  cn-DomainInformationListFull                 CN-DomainInformationListFull                 OPTIONAL
}

Digit ::=                                     INTEGER (0..9)

Gsm-map-IDNNS ::=                               SEQUENCE {
  routingbasis                                  CHOICE {
    localPTMSI                                   SEQUENCE {
      routingparameter                           RoutingParameter
    },
    tMSIofsamePLMN                               SEQUENCE {
      routingparameter                           RoutingParameter
    },
    tMSIofdifferentPLMN                         SEQUENCE {
      routingparameter                           RoutingParameter
    },
    iMSIresponsetopaging                        SEQUENCE {
      routingparameter                           RoutingParameter
    },
    iMSIUEinitiatedEvent                        SEQUENCE {
      routingparameter                           RoutingParameter
    },
    iMEI                                          SEQUENCE {
      routingparameter                           RoutingParameter
    }
  }
}

```

```

    },
    spare1
        routingparameter
    },
    spare2
        routingparameter
    }
},
enteredparameter
}

IMEI ::=
    SEQUENCE (SIZE (15)) OF
        IMEI-Digit

IMEI-Digit ::=
    INTEGER (0..15)

IMSI-GSM-MAP ::=
    SEQUENCE (SIZE (6..15)) OF
        Digit

IntraDomainNasNodeSelector ::=
    SEQUENCE {
        version
            CHOICE {
                release99
                    SEQUENCE {
                        cn-Type
                            CHOICE {
                                gsm-Map-IDNNS
                                ansi-41-IDNNS
                            }
                        },
                later
                    SEQUENCE {
                        futurecoding
                            BIT STRING (SIZE (15))
                    }
            }
    }

LAI ::=
    SEQUENCE {
        plmn-Identity
        lac
        BIT STRING (SIZE (16))
    }

MCC ::=
    SEQUENCE (SIZE (3)) OF
        Digit

MNC ::=
    SEQUENCE (SIZE (2..3)) OF
        Digit

NAS-Message ::=
    OCTET STRING (SIZE (1..4095))

NAS-Synchronisation-Indicator ::=
    BIT STRING(SIZE(4))

NAS-SystemInformationGSM-MAP ::=
    OCTET STRING (SIZE (1..8))

P-TMSI-GSM-MAP ::=
    BIT STRING (SIZE (32))

PagingRecordTypeID ::=
    ENUMERATED {
        imsi-GSM-MAP,
        tmsi-GSM-MAP-P-TMSI,
        imsi-DS-41,
        tmsi-DS-41 }

PLMN-Identity ::=
    SEQUENCE {
        mcc
        mnc
        MCC,
        MNC
    }

PLMN-Type ::=
    CHOICE {
        gsm-MAP
            SEQUENCE {
                plmn-Identity
            },
        ansi-41
            SEQUENCE {
                p-REV
                min-P-REV
                sid
                nid
            },
        gsm-MAP-and-ANSI-41
            SEQUENCE {
                plmn-Identity
                p-REV
                min-P-REV
                sid
            }
    }

```

```

        nid                                NID
    },
    spare                                NULL
}

RAB-Identity ::=
    gsm-MAP-RAB-Identity                 CHOICE {
    ansi-4l-RAB-Identity                 BIT STRING (SIZE (8)),
                                        BIT STRING (SIZE (8))
}

RAI ::=
    lai                                  SEQUENCE {
    rac                                  LAI,
                                        RoutingAreaCode
}

RoutingAreaCode ::=
    BIT STRING (SIZE (8))

RoutingParameter ::=
    BIT STRING (SIZE (10))

TMSI-GSM-MAP ::=
    BIT STRING (SIZE (32))

-- *****
--
--     UTRAN MOBILITY INFORMATION ELEMENTS (10.3.2)
--
-- *****

AccessClassBarred ::=
    ENUMERATED {
        barred, notBarred }

AccessClassBarredList ::=
    SEQUENCE (SIZE (maxAC)) OF
        AccessClassBarred

AllowedIndicator ::=
    ENUMERATED {
        allowed, notAllowed }

CellAccessRestriction ::=
    cellBarred                           SEQUENCE {
    cellReservedForOperatorUse           CellBarred,
    cellReservationExtension             ReservedIndicator,
    accessClassBarredList               AccessClassBarredList           OPTIONAL
}

CellBarred ::=
    barred                                CHOICE {
        intraFreqCellReselectionInd     SEQUENCE {
        t-Barred                          AllowedIndicator,
                                        T-Barred
    },
    notBarred                            NULL
}

CellIdentity ::=
    BIT STRING (SIZE (28))

CellIdentity-PerRL-List ::=
    SEQUENCE (SIZE (1..maxRL)) OF CellIdentity

CellSelectReselectInfoSIB-3-4 ::=
    mappingInfo                           MappingInfo           OPTIONAL,
    cellSelectQualityMeasure              CHOICE {
        cpich-Ec-N0                       SEQUENCE {
            -- Default value for q-HYST-2-S is q-HYST-1-S
            q-HYST-2-S                       Q-Hyst-S           OPTIONAL
            -- Default value for q-HYST-2-S is q-HYST-1-S
        },
        cpich-RSCP                          NULL
    },
    modeSpecificInfo                      CHOICE {
        fdd                                  SEQUENCE {
            s-Intrasearch                    S-SearchQual       OPTIONAL,
            s-Intersearch                    S-SearchQual       OPTIONAL,
            s-SearchHCS                      S-SearchRXLEV      OPTIONAL,
            rat-List                          RAT-FDD-InfoList   OPTIONAL,
            q-QualMin                         Q-QualMin,
            q-RxlevMin                       Q-RxlevMin
        },
        tdd                                  SEQUENCE {
            s-Intrasearch                    S-SearchRXLEV      OPTIONAL,
            s-Intersearch                    S-SearchRXLEV      OPTIONAL,
            s-SearchHCS                      S-SearchRXLEV      OPTIONAL,

```

```

        rat-List
        q-RxlevMin
    },
    q-Hyst-1-S
    t-Reselection-S
    hcs-ServingCellInformation
    maxAllowedUL-TX-Power
}

MapParameter ::=
    INTEGER (0..99)

Mapping ::=
    SEQUENCE {
        rat
        mappingFunctionParameterList
    }

Mapping-LCR-r4 ::=
    SEQUENCE {
        mappingFunctionParameterList
    }

MappingFunctionParameter ::=
    SEQUENCE {
        functionType
        mapParameter1
        mapParameter2
        -- The presence of upperLimit is conditional on the number of repetition
        upperLimit
    }

MappingFunctionParameterList ::=
    SEQUENCE (SIZE (1..maxMeasIntervals)) OF
        MappingFunctionParameter

MappingFunctionType ::=
    ENUMERATED {
        linear,
        functionType2,
        functionType3,
        functionType4 }

-- In MappingInfo list, mapping for FDD and 3.84Mcps TDD is defined.
-- For 1.28Mcps TDD, Mapping-LCR-r4 is used instead.
MappingInfo ::=
    SEQUENCE (SIZE (1..maxRAT)) OF
        Mapping

-- Actual value Q-Hyst-S = IE value * 2
Q-Hyst-S ::=
    INTEGER (0..20)

RAT ::=
    ENUMERATED {
        ultra-FDD,
        ultra-TDD,
        gsm,
        cdma2000 }

RAT-FDD-Info ::=
    SEQUENCE {
        rat-Identififer
        s-SearchRAT
        s-HCS-RAT
        s-Limit-SearchRAT
    }

RAT-FDD-InfoList ::=
    SEQUENCE (SIZE (1..maxOtherRAT)) OF
        RAT-FDD-Info

RAT-Identififer ::=
    ENUMERATED {
        gsm, cdma2000 }

RAT-TDD-Info ::=
    SEQUENCE {
        rat-Identififer
        s-SearchRAT
        s-HCS-RAT
        s-Limit-SearchRAT
    }

RAT-TDD-InfoList ::=
    SEQUENCE (SIZE (1..maxOtherRAT)) OF
        RAT-TDD-Info

ReservedIndicator ::=
    ENUMERATED {
        reserved,
        notReserved }

```

```

-- Actual value S-SearchedQual = IE value * 2
S-SearchQual ::=                INTEGER (-16..10)

-- Actual value S-SearchRXLEV = (IE value * 2) + 1
S-SearchRXLEV ::=                INTEGER (-53..45)

T-Barred ::=                      ENUMERATED {
                                s10, s20, s40, s80,
                                s160, s320, s640, s1280 }

T-Reselection-S ::=              INTEGER (0..31)

-- For UpperLimit, the used range depends on the RAT used.
UpperLimit ::=                   INTEGER (1..91)

URA-Identity ::=                 BIT STRING (SIZE (16))

URA-IdentityList ::=             SEQUENCE (SIZE (1..maxURA)) OF
                                URA-Identity

-- *****
--
--     USER EQUIPMENT INFORMATION ELEMENTS (10.3.3)
--
-- *****

AccessStratumReleaseIndicator ::= ENUMERATED {
                                rel-4, spare15, spare14, spare13,
                                spare12, spare11, spare10, spare9, spare8,
                                spare7, spare6, spare5, spare4, spare3,
                                spare2, spare1 }

-- TABULAR : for ActivationTime, value 'now' always appear as default, and is encoded
-- by absence of the field
ActivationTime ::=                INTEGER (0..255)

BackoffControlParams ::=          SEQUENCE {
    n-AP-RetransMax                N-AP-RetransMax,
    n-AccessFails                  N-AccessFails,
    nf-BO-NoAICH                   NF-BO-NoAICH,
    ns-BO-Busy                      NS-BO-Busy,
    nf-BO-AllBusy                  NF-BO-AllBusy,
    nf-BO-Mismatch                 NF-BO-Mismatch,
    t-CPCH                         T-CPCH
}

C-RNTI ::=                        BIT STRING (SIZE (16))

CapabilityUpdateRequirement ::=   SEQUENCE {
    ue-RadioCapabilityFDDUpdateRequirement-FDD  BOOLEAN,
    -- ue-RadioCapabilityTDDUpdateRequirement-TDD is for 3.84Mcps TDD update requirement
    ue-RadioCapabilityTDDUpdateRequirement-TDD  BOOLEAN,
    systemSpecificCapUpdateReqList              SystemSpecificCapUpdateReqList    OPTIONAL
}

CapabilityUpdateRequirement-r4-ext ::= SEQUENCE {
    ue-RadioCapabilityUpdateRequirement-TDD128  BOOLEAN
}

CapabilityUpdateRequirement-r4 ::= SEQUENCE {
    ue-RadioCapabilityFDDUpdateRequirement-FDD  BOOLEAN,
    ue-RadioCapabilityTDDUpdateRequirement-TDD384  BOOLEAN,
    ue-RadioCapabilityTDDUpdateRequirement-TDD128  BOOLEAN,
    systemSpecificCapUpdateReqList              SystemSpecificCapUpdateReqList    OPTIONAL
}

CellUpdateCause ::=              ENUMERATED {
                                cellReselection,
                                periodicalCellUpdate,
                                uplinkDataTransmission,
                                utran-pagingResponse,
                                re-enteredServiceArea,
                                radiolinkFailure,
                                rlc-unrecoverableError,
                                spare1 }

ChipRateCapability ::=            ENUMERATED {

```



```

        mcps3-84, mcps1-28 }

CipheringAlgorithm ::=
    ENUMERATED {
        uea0, uea1 }

CipheringModeCommand ::=
    CHOICE {
        startRestart
        stopCipheringdummy
    }

CipheringModeInfo ::=
    SEQUENCE {
        -- TABULAR: The ciphering algorithm is included in the CipheringModeCommand.
        cipheringModeCommand          CipheringModeCommand,
        activationTimeForDPCH          ActivationTime          OPTIONAL,
        rb-DL-CiphActivationTimeInfo  RB-ActivationTimeInfoList OPTIONAL
    }

CN-DRX-CycleLengthCoefficient ::= INTEGER (6..9)

```

## 11.5 RRC information between network nodes

```
Internode-definitions DEFINITIONS AUTOMATIC TAGS ::=
```

```
BEGIN
```

```
IMPORTS
```

```

    HandoverToUTRANCommand,
    MeasurementReport,
    PhysicalChannelReconfiguration,
    RadioBearerReconfiguration,
    RadioBearerRelease,
    RadioBearerSetup,
    RRC-FailureInfo-r3-IEs,
    TransportChannelReconfiguration
FROM PDU-definitions

```

```

-- Core Network IEs :
    CN-DomainIdentity,
    CN-DomainInformationList,
    CN-DRX-CycleLengthCoefficient,
    NAS-SystemInformationGSM-MAP,
-- UTRAN Mobility IEs :
    CellIdentity,
    URA-Identity,
-- User Equipment IEs :
    C-RNTI,
    DL-PhysChCapabilityFDD-v380ext,
    FailureCauseWithProtErr,
    RRC-MessageSequenceNumber,
    STARTList,
    STARTSingle,
    START-Value,
    U-RNTI,
    UE-RadioAccessCapability,
    UE-RadioAccessCapability-v370ext,
    UE-RadioAccessCapability-v380ext,
    UE-RadioAccessCapability-v3a0ext,
    UE-RadioAccessCapability-v4xyext,
-- Radio Bearer IEs :
    PredefinedConfigStatusList,
    PredefinedConfigValueTag,
    RAB-InformationSetupList,
    RAB-Identity,
    SRB-InformationSetupList,
-- Transport Channel IEs :
    CPCH-SetID,
    DL-CommonTransChInfo,
    DL-AddReconfTransChInfoList,
    DRAC-StaticInformationList,
    UL-CommonTransChInfo,
    UL-AddReconfTransChInfoList,
-- Measurement IEs :
    MeasurementIdentity,
    MeasurementReportingMode,

```

```

    MeasurementType,
    MeasurementType-r4,
    AdditionalMeasurementID-List,
    PositionEstimate,
    UE-Positioning-IPDL-Parameters-TDD-r4-ext,
-- Other IEs :
InterRAT-UE-RadioAccessCapabilityList
FROM InformationElements

    maxCNdomains,
    maxNoOfMeas,

    maxRB,
    maxSRBsetup
FROM Constant-definitions
;

-- Part 1: Class definitions similar to what has been defined in 11.1 for RRC messages
-- Information that is transferred in the same direction and across the same path is grouped

-- *****
--
-- RRC information, to target RNC
--
-- *****
-- RRC Information to target RNC sent either from source RNC or from another RAT

ToTargetRNC-Container ::= CHOICE {
    interRATHandoverInfo          InterRATHandoverInfoWithInterRATCapabilities-r3,
    srncRelocation                SRNC-RelocationInfo-r3,
    extension                     NULL
}

-- *****
--
-- RRC information, target RNC to source RNC
--
-- *****

Target-RNC-ToSourceRNC-Container ::= CHOICE {
    radioBearerSetup              RadioBearerSetup,
    radioBearerReconfiguration    RadioBearerReconfiguration,
    radioBearerRelease            RadioBearerRelease,
    transportChannelReconfiguration TransportChannelReconfiguration,
    physicalChannelReconfiguration PhysicalChannelReconfiguration,
    rrc-FailureInfo               RRC-FailureInfo-r3-IEs,
    extension                     NULL
}

-- Part 2: Container definitions, similar to the PDU definitions in 11.2 for RRC messages
-- In alphabetical order

-- *****
--
-- Handover to UTRAN information
--
-- *****

InterRATHandoverInfoWithInterRATCapabilities-r3 ::= CHOICE {
    r3                             SEQUENCE {
        -- IE InterRATHandoverInfoWithInterRATCapabilities-r3-IEs also
        -- includes non critical extensions
        interRATHandoverInfo-r3    InterRATHandoverInfoWithInterRATCapabilities-r3-IEs,
        v390NonCriticalExtensions  SEQUENCE {
            interRATHandoverInfoWithInterRATCapabilities-v390ext
            InterRATHandoverInfoWithInterRATCapabilities-v390ext-IEs,
            -- Reserved for future non critical extension
            nonCriticalExtensions  SEQUENCE {} OPTIONAL
        }
    },
    criticalExtensions             SEQUENCE {}
}

InterRATHandoverInfoWithInterRATCapabilities-r3-IEs ::= SEQUENCE {
    -- The order of the IEs may not reflect the tabular format
    -- but has been chosen to simplify the handling of the information in the BSC

```

```

-- Other IEs
ue-RATSpecificCapability      InterRAT-UE-RadioAccessCapabilityList  OPTIONAL,
-- interRATHandoverInfo, Octet string is used to obtain 8 bit length field prior to
-- actual information. This makes it possible for BSS to transparently handle information
-- received via GSM air interface even when it includes non critical extensions.
-- The octet string shall include the InterRATHandoverInfo information
-- The BSS can re-use the 04.18 length field received from the MS
interRATHandoverInfo         OCTET STRING (SIZE (0..255))
}

InterRATHandoverInfoWithInterRATCapabilities-v390ext-IEs ::= SEQUENCE {
  -- User equipment IEs
  failureCauseWithProtErr      FailureCauseWithProtErr              OPTIONAL
}

-- *****
--
-- SRNC Relocation information
--
-- *****

SRNC-RelocationInfo-r3 ::= CHOICE {
  r3
    SRNC-RelocationInfo-r3      SEQUENCE {
      SRNC-RelocationInfo-r3-IEs,
      v380NonCriticalExtensions SEQUENCE {
        SRNC-RelocationInfo-v380ext SRNC-RelocationInfo-v380ext-IEs,
        -- Reserved for future non critical extension
        v390NonCriticalExtensions SEQUENCE {
          SRNC-RelocationInfo-v390ext SRNC-RelocationInfo-v390ext-IEs,
          v3a0NonCriticalExtensions SEQUENCE {
            SRNC-RelocationInfo-v3a0ext SRNC-RelocationInfo-v3a0ext-IEs,
            v4xyNonCriticalExtensions SEQUENCE {
              SRNC-RelocationInfo-v4xyext SRNC-RelocationInfo-v4xyext-IEs,
              v3b0NonCriticalExtensions SEQUENCE {
                SRNC-RelocationInfo-v3b0ext SRNC-RelocationInfo-v3b0ext-IEs,
                -- Reserved for future non critical extension
                nonCriticalExtensions SEQUENCE {} OPTIONAL
                nonCriticalExtensions SEQUENCE {} OPTIONAL
              }
            }
          }
        }
      }
    }
  },
  criticalExtensions SEQUENCE {}
}

SRNC-RelocationInfo-r3-IEs ::= SEQUENCE {
  -- Non-RRC IEs
  stateOfRRC          StateOfRRC,
  stateOfRRC-Procedure StateOfRRC-Procedure,
  -- Ciphering related information IEs
  -- If the extension v380 is included use the extension for the ciphering status per CN domain
  cipheringStatus      CipheringStatus,
  calculationTimeForCiphering CalculationTimeForCiphering  OPTIONAL,
  cipheringInfoPerRB-List CipheringInfoPerRB-List      OPTIONAL,
  count-C-List         COUNT-C-List          OPTIONAL,
  integrityProtectionStatus IntegrityProtectionStatus,
  srb-SpecificIntegrityProtInfo SRB-SpecificIntegrityProtInfoList,
  implementationSpecificParams ImplementationSpecificParams  OPTIONAL,
  -- User equipment IEs
  u-RNTI              U-RNTI,
  c-RNTI              C-RNTI              OPTIONAL,
  ue-RadioAccessCapability UE-RadioAccessCapability,
  ue-Positioning-LastKnownPos UE-Positioning-LastKnownPos  OPTIONAL,
  -- Other IEs
  ue-RATSpecificCapability InterRAT-UE-RadioAccessCapabilityList  OPTIONAL,
  -- UTRAN mobility IEs
  ura-Identity        URA-Identity          OPTIONAL,
  -- Core network IEs
  cn-CommonGSM-MAP-NAS-SysInfo NAS-SystemInformationGSM-MAP,
  cn-DomainInformationList CN-DomainInformationList  OPTIONAL,
  -- Measurement IEs
  ongoingMeasRepList  OngoingMeasRepList          OPTIONAL,
  -- Radio bearer IEs
  predefinedConfigStatusList PredefinedConfigStatusList,
  srb-InformationList  SRB-InformationSetupList,
  rab-InformationList  RAB-InformationSetupList  OPTIONAL,

```

```

-- Transport channel IEs
  ul-CommonTransChInfo      UL-CommonTransChInfo      OPTIONAL,
  ul-TransChInfoList        UL-AddReconfTransChInfoList  OPTIONAL,
  modeSpecificInfo          CHOICE {
    fdd                      SEQUENCE {
      cpch-SetID             CPCH-SetID             OPTIONAL,
      transChDRAC-Info      DRAC-StaticInformationList  OPTIONAL
    },
    tdd                      NULL
  },
  dl-CommonTransChInfo      DL-CommonTransChInfo      OPTIONAL,
  dl-TransChInfoList        DL-AddReconfTransChInfoList  OPTIONAL,
-- Measurement report
  measurementReport         MeasurementReport         OPTIONAL,
  nonCriticalExtensions      SEQUENCE {
    -- In case of TDD only up-Ipdl-Parameters-TDD is present, otherwise
    -- this IE is absent
    up-Ipdl-Parameters-TDD  UE-Positioning-IPDL-Parameters-TDD-r4-ext  OPTIONAL,
    -- Extension mechanism for non- release4 information
    nonCriticalExtensions   SEQUENCE {}
  }
}

SRNC-RelocationInfo-v380ext-IEs ::= SEQUENCE {
  -- Ciphering related information IEs
  cn-DomainIdentity         CN-DomainIdentity,
  cipheringStatusList       CipheringStatusList
}

SRNC-RelocationInfo-v390ext-IEs ::= SEQUENCE {
  cn-DomainInformationList-v390ext  CN-DomainInformationList-v390ext  OPTIONAL,
  ue-RadioAccessCapability-v370ext  UE-RadioAccessCapability-v370ext  OPTIONAL,
  ue-RadioAccessCapability-v380ext  UE-RadioAccessCapability-v380ext  OPTIONAL,
  dl-PhysChCapabilityFDD-v380ext    DL-PhysChCapabilityFDD-v380ext,
  failureCauseWithProtErr          FailureCauseWithProtErr          OPTIONAL
}

SRNC-RelocationInfo-v3a0ext-IEs ::= SEQUENCE {
  -- cn-domain identity for IE startValueForCiphering-v3a0ext is specified
  -- in subsequent extension \(SRNC-RelocationInfo-v3b0ext-IEs\)
  startValueForCipheringstartValueForCiphering-v3a0ext  START-Value,
  cipheringInfoForSRB1-v3a0ext      CipheringInfoForSRB1-v3a0ext,
  ue-RadioAccessCapability-v3a0ext  UE-RadioAccessCapability-v3a0ext  OPTIONAL
}

SRNC-RelocationInfo-v4xyext-IEs ::= SEQUENCE {
  ue-RadioAccessCapability-v4xyext  UE-RadioAccessCapability-v4xyext
}

SRNC-RelocationInfo-v3b0ext-IEs ::= SEQUENCE {
  -- cn-domain identity for IE startValueForCiphering-v3a0ext included in previous extension
  cn-DomainIdentity CN-DomainIdentity,
  -- the remaining start values are contained in IE startValueForCiphering-v3b0ext
  startValueForCiphering-v3b0ext STARTList2  OPTIONAL
}

STARTList2 ::= SEQUENCE \(SIZE \(2..maxCNdomains\)\) OF
STARTSingle

CipheringInfoForSRB1-v3a0ext ::= SEQUENCE {
  dl-UM-SN  BIT STRING (SIZE (7))
}

CipheringStatusList ::= SEQUENCE (SIZE (1..maxCNdomains)) OF
  CipheringStatusCNdomain

CipheringStatusCNdomain ::= SEQUENCE {
  cn-DomainIdentity  CN-DomainIdentity,
  cipheringStatus    CipheringStatus
}

SRNC-RelocationInfo-r4 ::= SEQUENCE {
  -- Non-RRC IEs
  stateOfRRC          StateOfRRC,
  stateOfRRC-Procedure  StateOfRRC-Procedure,
  cipheringStatus      CipheringStatus,
  calculationTimeForCiphering  CalculationTimeForCiphering  OPTIONAL,
  cipheringInfoPerRB-List  CipheringInfoPerRB-List  OPTIONAL,

```

```

    integrityProtectionStatus      IntegrityProtectionStatus,
    srb-SpecificIntegrityProtInfo  SRB-SpecificIntegrityProtInfoList,
    implementationSpecificParams  ImplementationSpecificParams      OPTIONAL,
-- User equipment IEs
    u-RNTI                          U-RNTI,
    c-RNTI                          C-RNTI                                OPTIONAL,
    ue-RadioAccessCapability        UE-RadioAccessCapability,
    ue-Positioning-LastKnownPos    UE-Positioning-LastKnownPos        OPTIONAL,
-- Other IEs
    ue-RATSpecificCapability        InterRAT-UE-RadioAccessCapabilityList  OPTIONAL,
-- UTRAN mobility IEs
    ura-Identity                    URA-Identity                        OPTIONAL,
-- Core network IEs
    cn-CommonGSM-MAP-NAS-SysInfo    NAS-SystemInformationGSM-MAP,
    cn-DomainInformationList        CN-DomainInformationList            OPTIONAL,
-- Measurement IEs
    ongoingMeasRepList              OngoingMeasRepList-r4              OPTIONAL,
-- Radio bearer IEs
    predefinedConfigStatusList      PredefinedConfigStatusList,
    srb-InformationList             SRB-InformationSetupList,
    rab-InformationList             RAB-InformationSetupList            OPTIONAL,
-- Transport channel IEs
    ul-CommonTransChInfo            UL-CommonTransChInfo                OPTIONAL,
    ul-TransChInfoList              UL-AddReconfTransChInfoList        OPTIONAL,
    modeSpecificInfo                CHOICE {
        fdd                          SEQUENCE {
            cpch-SetID                CPCH-SetID                          OPTIONAL,
            transChDRAC-Info          DRAC-StaticInformationList          OPTIONAL
        },
        tdd                          NULL
    },
    dl-CommonTransChInfo            DL-CommonTransChInfo                OPTIONAL,
    dl-TransChInfoList              DL-AddReconfTransChInfoList        OPTIONAL,
-- Measurement report
    measurementReport               MeasurementReport                    OPTIONAL,
    nonCriticalExtensions            SEQUENCE {
        -- In case of TDD only up-Ipdl-Parameters-TDD is present, otherwise
        -- this IE is absent
        up-Ipdl-Parameters-TDD       UE-Positioning-IPDL-Parameters-TDD-r4-ext  OPTIONAL,
        -- Extension mechanism for non- release4 information
        nonCriticalExtensions         SEQUENCE {}
    }
}
}
}

-- IE definitions

CalculationTimeForCipherng ::= SEQUENCE {
    cell-Id      CellIdentity,
    sfn          INTEGER (0..4095)
}

CipherngInfoPerRB ::= SEQUENCE {
    dl-HFN      BIT STRING (SIZE (20..25)),
    ul-HFN      BIT STRING (SIZE (20..25))
}

-- TABULAR: CipherngInfoPerRB-List, multiplicity value numberOfRadioBearers
-- has been replaced with maxRB.
CipherngInfoPerRB-List ::= SEQUENCE (SIZE (1..maxRB)) OF
    CipherngInfoPerRB

CipherngStatus ::= ENUMERATED {
    started, notStarted }

CN-DomainInformation-v390ext ::= SEQUENCE {
    cn-DRX-CycleLengthCoeff  CN-DRX-CycleLengthCoefficient
}

CN-DomainInformationList-v390ext ::= SEQUENCE (SIZE (1..maxCNdomains)) OF
    CN-DomainInformation-v390ext

COUNT-C-List ::= SEQUENCE (SIZE (1..maxCNdomains)) OF
    COUNT-CSingle

COUNT-CSingle ::= SEQUENCE {
    cn-DomainIdentity  CN-DomainIdentity,
    count-C            BIT STRING (SIZE (32))
}

```

Error! No text of specified style in document.

Error! No text of specified style in document.

## Annex A (informative): USIM parameters

### A.1 Introduction

This annex contains recommendations about the RRC parameters to be stored in the USIM.

### A.2 Cipherring information

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Cipher key for each CN domain	MP	<1 to maxCNDomain>		Cipher key is described in [40].
<del>&gt;Old-CK</del>	MP		Bit string (128)	
<del>&gt;New-CK</del>	MP		<del>Bit string (128)</del>	
Integrity key for each CN domain	MP	<1 to maxCNDomain>		Integrity key is described in [40].
<del>&gt;Old-IK</del>	MP		Bit string (128)	
<del>&gt;New-IK</del>	MP		<del>Bit string (128)</del>	
THRESHOLD	MP		Bit string (20)	
START value for each CN domain	MP	<1 to maxCNDomain>		START value is described in [40].
<del>&gt;Old-START</del>	MP		Bit string (20)	
<del>&gt;New-START</del>	MP		<del>Bit string (20)</del>	
KSI, Key set identifier for each CN domain	MP	<1 to maxCNDomain>		Key set identifier is described in [40].
<del>&gt;Old-KSI</del>	MP		Bit string (3)	
<del>&gt;New-KSI</del>	MP		<del>Bit string (3)</del>	

### A.3 Frequency information

Neighbour cell list.

Information Element/Group name	Need	Multi	Type and reference	Semantics description	Version
FDD cell list	OP	<1 to maxFDDFrequencyList>			
>UARFCN uplink (Nu)	OP		Integer(0..16383)	[21] If IE not present, default duplex distance of 190 MHz shall be used.	
>UARFCN downlink (Nd)	MP		Integer(0 .. 16383)	[21]	
>Primary scrambling code	OP	<1 to maxFDDFrequencyCellList>	Primary CPICH info 10.3.6.60		

Information Element/Group name	Need	Multi	Type and reference	Semantics description	Version
3.84 Mcps TDD cell list	OP	<1 to maxTDDFr eqList>			
>UARFCN (Nt)	MP		Integer(0 .. 16383)	[22]	
>Cell parameters ID	OP	<1 to maxTDDFr eqCellList>	Integer (0..127)	The Cell parameters ID is described in [32].	
1.28 Mcps TDD cell list	OP	<1 to maxTDDFr eqList>			REL-4
>UARFCN (Nt)	MP		Integer(0 .. 16383)	[22]	REL-4
>Cell parameters ID	OP	<1 to maxTDDFr eqCellList>	Integer (0..127)	The Cell parameters ID is described in [32].	REL-4
GSM Neighbour cell list	OP				
>GSM neighbour cell info	MP	<1 to maxGSMCellList>			
>>BSIC	MP				
>>BCCH ARFCN	MP				



# CHANGE REQUEST

⌘ **25.331 CR 1493** ⌘ rev **-** ⌘ Current version: **3.10.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Corrections to cell update interactions with security and SRNS Relocation		
<b>Source:</b>	⌘ TSG-RAN WG2		
<b>Work item code:</b>	⌘ TEI	<b>Date:</b>	⌘ May 13, 2002
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ R99
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> 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)

<b>Reason for change:</b> ⌘	<ol style="list-style-type: none"> <li>1. The actions for the UE in case of CELL UPDATE and UTRAN MOBILITY INFORMATION when performing a security reconfiguration during a CELL UPDATE CONFIRM procedure causing security reconfiguration are missing.</li> <li>2. It is stated that in case of a CELL UPDATE being triggered during security reconfiguration, the UE shall abort and revert back to its previous configuration. This would however require the UE to abandon the re-establishment of RB2 and revert back to the previous RB2 configuration - this is however not possible.</li> <li>3. It is incorrectly stated that in case of SRNS relocation the HFN components have to be modified following the re-establishment of the associated RB, when in fact only the HFN components of the COUNT-C values for that RB needs to be modified.</li> <li>4. Transmission on RB0 is prohibited - this would prevent a CELL UPDATE being sent during security reconfiguration.</li> </ol>
<b>1. Summary of change:</b> ⌘	<ol style="list-style-type: none"> <li>1. It is stated that the UE shall not abort the security reconfiguration if a CELL UPDATE occurs during a CELL UPDATE CONFIRM triggering a SRNS Relocation. UE actions in case of UTRAN MOBILITY INFORMATION procedure are stated - UE shall start a cell update procedure and continue with the UTRAN MOBILITY INFORMATION.</li> <li>2. It is stated that the UE shall release its radio resources if a cell reselection is triggered during a RB Reconfiguration procedure triggering SRNS Relocation. A note is added that the UTRAN should use RB Control messages for triggering SRNS Relocation only in case of CELL_DCH to CELL_DCH transitions. UE behavior in other cases is unspecified.</li> <li>3. It is now stated that only the HFN components of the COUNT-C values need to be modified or set following RB re-establishment during the SRNS relocation.</li> <li>4. Transmission on RB0 is now allowed during security reconfiguration.</li> </ol>

<b>Consequences if not approved:</b>	⌘ 1. UE actions on cell update in case of UTRAN MOBILITY INFORMATION causing security reconfiguration on SRNS relocation will be unspecified leading to unknown UE behavior. UE actions in case of cell update during an ongoing CELL UPDATE CONFIRM causing security reconfiguration will be difficult to implement causing unknown UE behavior. 2. UE implementation will not be possible leading to unknown UE behavior. 3. HFN components of COUNT-I may also be incorrectly modified causing loss of connection due to security failure. 4. CELL UPDATE will not be sent causing loss of connection.  <b>Isolated Impact Analysis:</b>  Corrected Feature: Security Reconfiguration during SRNS relocation  Both the UE and UTRAN need to implement the changes in this CR for the security feature to function correctly when SRNS relocation is triggered, else the two entities will not be synchronised causing loss of connection.  <b>Impact on T1 test specifications:</b> Security is in general not well covered in T1 at present and this CR is not foreseen to affect current T1 tests but the corrected functionality will affect future test cases produced by T1 related to security.

<b>Clauses affected:</b>	⌘ 8.2.2.3, 8.2.2.4, 8.2.2.12b, 8.3.1.6, 8.3.1.7, 8.3.1.12, 8.3.3.3, 8.3.3.5, 8.6.3.5			
<b>Other specs affected:</b>	⌘ <table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td style="width: 20px; height: 15px;"></td></tr> <tr><td style="width: 20px; height: 15px;"></td></tr> <tr><td style="width: 20px; height: 15px;"></td></tr> </table> Other core specifications      ⌘ 25.331 v4.4.0, CR 1494 25.331 v5.0.0, CR 1495 Test specifications O&M Specifications			
<b>Other comments:</b>	⌘			

**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.

### 8.2.2.3 Reception of RADIO BEARER SETUP or RADIO BEARER RECONFIGURATION or RADIO BEARER RELEASE or TRANSPORT CHANNEL RECONFIGURATION or PHYSICAL CHANNEL RECONFIGURATION message by the UE

The UE shall be able to receive any of the following messages:

- RADIO BEARER SETUP message; or
- RADIO BEARER RECONFIGURATION message; or
- RADIO BEARER RELEASE message; or
- TRANSPORT CHANNEL RECONFIGURATION message; or
- PHYSICAL CHANNEL RECONFIGURATION message;

and perform a hard handover, even if no prior UE measurements have been performed on the target cell and/or frequency.

If the UE receives:

- a RADIO BEARER SETUP message; or
- a RADIO BEARER RECONFIGURATION message; or
- a RADIO BEARER RELEASE message; or
- a TRANSPORT CHANNEL RECONFIGURATION message; or
- a PHYSICAL CHANNEL RECONFIGURATION message;

it shall:

- 1> set the variable ORDERED\_RECONFIGURATION to TRUE;
- 1> perform the physical layer synchronisation procedure as specified in [29];
- 1> act upon all received information elements as specified in subclause 8.6, unless specified in the following and perform the actions below.

The UE may first release the physical channel configuration used at reception of the reconfiguration message. The UE shall then:

- 1> in FDD, if the IE "PDSCH code mapping" is included but the IE "PDSCH with SHO DCH Info" is not included and if the DCH has only one link in its active set:
  - 2> act upon the IE "PDSCH code mapping" as specified in subclause 8.6; and
  - 2> infer that the PDSCH will be transmitted from the cell from which the downlink DPCH is transmitted.
- 1> enter a state according to subclause 8.6.3.3.

In case the UE receives a RADIO BEARER RECONFIGURATION message including the IE "RB information to reconfigure" that only includes the IE "RB identity", the UE shall:

- 1> handle the message as if IE "RB information to reconfigure" was absent.

NOTE: The RADIO BEARER RECONFIGURATION message always includes the IE "RB information to reconfigure". UTRAN has to include it even if it does not require the reconfiguration of any RB.

If after state transition the UE enters CELL\_DCH state, the UE shall, after the state transition:

- 1> remove any C-RNTI from MAC;
- 1> clear the variable C\_RNTI.

In FDD, if after state transition the UE leaves CELL\_DCH state, the UE shall, after the state transition:

- 1> remove any DSCH-RNTI from MAC;
- 1> clear the variable DSCH\_RNTI.

If the UE was in CELL\_DCH state upon reception of the reconfiguration message and remains in CELL\_DCH state, the UE shall:

- 1> if the IE "Uplink DPCH Info" is absent, not change its current UL Physical channel configuration;
- 1> if the IE "Downlink information for each radio link" is absent, not change its current DL Physical channel configuration.

If after state transition the UE enters CELL\_FACH state, the UE shall, after the state transition:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4] on that frequency.
- 1> if the IE "Frequency info" is not included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4].
- 1> if the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selects another cell than indicated by this IE or the received reconfiguration message did not include the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD):
  - 2> initiate a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";
  - 2> when the cell update procedure completed successfully:
    - 3> if the UE is in CELL\_PCH or URA\_PCH state:
      - 4> initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
      - 4> proceed as below.
- 1> start timer T305 using its initial value if timer T305 is not running and if periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" in system information block type 1;
- 1> select PRACH according to subclause 8.5.17;
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> use the transport format set given in system information;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 2> ignore that IE and stop using DRX.
- 1> if the contents of the variable C\_RNTI is empty:
  - 2> perform a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";
  - 2> when the cell update procedure completed successfully:
    - 3> if the UE is in CELL\_PCH or URA\_PCH state:
      - 4> initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
      - 4> proceed as below.

If the UE was in CELL\_FACH state upon reception of the reconfiguration message and remains in CELL\_FACH state, the UE shall:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4] on that frequency;
  - 2> if the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE or the received reconfiguration message did not include the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD):
    - 3> initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
    - 3> when the cell update procedure completed successfully:
      - 4> proceed as below.

The UE shall transmit a response message as specified in subclause 8.2.2.4, setting the information elements as specified below. The UE shall:

- 1> if the received reconfiguration message included the IE "Downlink counter synchronisation info"; or
- 1> if the received reconfiguration message is a RADIO BEARER RECONFIGURATION and the IE "New U-RNTI" is included:
  - 2> re-establish RB2;
  - 2> set the new uplink and downlink HFN **component of COUNT-C** of RB2 to MAX(uplink HFN **component of COUNT-C** of RB2, downlink HFN **component of COUNT-C** of RB2);
  - 2> increment by one the downlink and uplink **values of the** HFN **component of COUNT-C values** for RB2;
  - 2> calculate the START value according to subclause 8.5.9;
  - 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message did not include the IE "Downlink counter synchronisation info":
  - 2> if the variable START\_VALUE\_TO\_TRANSMIT is set:
    - 3> include and set the IE "START" to the value of that variable.
  - 2> if the variable START\_VALUE\_TO\_TRANSMIT is not set and the IE "New U-RNTI" is included:
    - 3> calculate the START value according to subclause 8.5.9;
    - 3> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
  - 2> if the received reconfiguration message caused a change in the RLC size for any RB using RLC-AM:
    - 3> calculate the START value according to subclause 8.5.9;
    - 3> include the calculated START values for the CN domain associated with the corresponding RB identity in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info":
  - 2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the received reconfiguration message did not contain the IE "Ciphering activation time for DPCH" in IE "Ciphering mode info":

- 2> if prior to this procedure there exist no transparent mode RLC radio bearers:
  - 3> if, at the conclusion of this procedure, the UE will be in CELL\_DCH state; and
  - 3> if, at the conclusion of this procedure, at least one transparent mode RLC radio bearer exists:
    - 4> include the IE "COUNT-C activation time" and specify a CFN value for this IE.
- 2> if prior to this procedure there exists at least one transparent mode RLC radio bearer:
  - 3> if, at the conclusion of this procedure, no transparent mode RLC radio bearers exist:
    - 4> include the IE "COUNT-C activation time" and specify a CFN value for this IE.
- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the received message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> if the variable PDCP\_SN\_INFO is not empty:
  - 2> include the IE "RB with PDCP information list" and set it to the value of the variable PDCP\_SN\_INFO.
- 1> in TDD, if the procedure is used to perform a handover to a cell where timing advance is enabled, and the UE can calculate the timing advance value in the new cell (i.e. in a synchronous TDD network):
  - 2> set the IE "Uplink Timing Advance" according to subclause 8.6.6.26.
- 1> if the IE "Integrity protection mode info" was present in the received reconfiguration message:
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.

If after state transition the UE enters CELL\_PCH or URA\_PCH state, the UE shall, after the state transition and transmission of the response message:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4] on that frequency.
- 1> if the IE "Frequency info" is not included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4].
- 1> prohibit periodical status transmission in RLC;
- 1> remove any C-RNTI from MAC;
- 1> clear the variable C\_RNTI;
- 1> start timer T305 using its initial value if timer T305 is not running and if periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" in system information block type 1;
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 2> use the value in the IE "UTRAN DRX Cycle length coefficient" for calculating Paging occasion and PICH Monitoring Occasion as specified in subclause 8.6.3.2.
- 1> if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the UE enters CELL\_PCH state from CELL\_DCH state, and the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell

than indicated by this IE or the received reconfiguration message did not include the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD):

2> initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";

2> when the cell update procedure completed successfully:

3> the procedure ends.

1> if the UE enters CELL\_PCH state from CELL\_FACH state, and the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE:

2> initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";

2> when the cell update procedure is successfully completed:

3> the procedure ends.

1> if the UE enters URA\_PCH state, and after cell selection the criteria for URA update caused by "URA reselection" according to subclause 8.3.1 is fulfilled:

2> initiate a URA update procedure according to subclause 8.3.1 using the cause "URA reselection";

2> when the URA update procedure is successfully completed:

3> the procedure ends.

#### 8.2.2.4 Transmission of a response message by the UE, normal case

In case the procedure was triggered by reception of a RADIO BEARER SETUP message, the UE shall:

1> transmit a RADIO BEARER SETUP COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a RADIO BEARER RECONFIGURATION message, the UE shall:

1> transmit a RADIO BEARER RECONFIGURATION COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a RADIO BEARER RELEASE message, the UE shall:

1> transmit a RADIO BEARER RELEASE COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a TRANSPORT CHANNEL RECONFIGURATION message, the UE shall:

1> transmit a TRANSPORT CHANNEL RECONFIGURATION COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a PHYSICAL CHANNEL RECONFIGURATION message, the UE shall:

1> transmit a PHYSICAL CHANNEL RECONFIGURATION COMPLETE as response message on the uplink DCCH using AM RLC.

If the new state is CELL\_DCH or CELL\_FACH, the response message shall be transmitted using the new configuration after the state transition, and the UE shall:

1> if the IE "Downlink counter synchronisation info" was included in the reconfiguration message; or

1> if the received reconfiguration message is a RADIO BEARER RECONFIGURATION and the IE "New U-RNTI" is included:

2> when RLC has confirmed the successful transmission of the response message:

- 3> re-establish all AM and UM RLC entities with RB identities larger than 4 and set the first 20 bits of all the HFN component of the respective COUNT-C values to the START value included in the response message for the corresponding CN domain;
  - 3> re-establish the RLC entities with RB identities 1, 3 and 4 and set the first 20 bits of all the HFN component of the respective COUNT-C values to the START value included in the response message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
  - 3> set the remaining bits of the HFN component of the COUNT-C values of all UM RLC entities to zero;
  - 3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].
- 1> if the variable PDCP\_SN\_INFO is empty:
    - 2> if the received reconfiguration message contained the IE "Ciphering mode info":
      - 3> when RLC has confirmed the successful transmission of the response message:
        - 4> notify upper layers upon change of the security configuration;
        - 4> perform the actions below.
      - 2> if the received reconfiguration message did not contain the IE "Ciphering mode info":
        - 3> when RLC has been requested to transmit the response message:
          - 4> perform the actions below.
    - 1> if the variable PDCP\_SN\_INFO is non-empty:
      - 2> when RLC has confirmed the successful transmission of the response message:
        - 3> for each radio bearer in the variable PDCP\_SN\_INFO:
          - 4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
            - 5> configure the RLC entity for that radio bearer to "continue".
          - 3> perform the actions below.

If the new state is CELL\_PCH or URA\_PCH, the response message shall be transmitted using the old configuration before the state transition, but the new C-RNTI shall be used if the IE "New C-RNTI" was included in the received reconfiguration message, and the UE shall:

- 1> when RLC has confirmed the successful transmission of the response message:
  - 2> for each radio bearer in the variable PDCP\_SN\_INFO:
    - 3> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
      - 4> configure the RLC entity for that radio bearer to "continue".
    - 2> enter the new state (CELL\_PCH or URA\_PCH, respectively);
    - 2> perform the actions below.

The UE shall:

- 1> set the variable ORDERED\_RECONFIGURATION to FALSE;
- 1> if the received reconfiguration message contained the IE "Ciphering mode info":
  - 2> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
  - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and



- 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the received reconfiguration message contained the IE "Integrity protection mode info":
  - 2> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
  - 2> set "Uplink RRC Message sequence number" for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO to a value such that next RRC message to be sent on uplink RB0 will use the new integrity protection configuration;
  - 2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 1> clear the variable PDCP\_SN\_INFO;
- 1> clear the variable START\_VALUE\_TO\_TRANSMIT;
- 1> clear the variable SECURITY\_MODIFICATION.

### 8.2.2.12b Cell update procedure during security reconfiguration

If:

- a cell update procedure according to subclause 8.3.1 is initiated; and
- the received reconfiguration message causes either:
  - the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE; and/or
  - the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE;

the UE shall:

- 1> release all radio resources;
- 1> indicate the release 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; and
- 1> clear any entry for the RRC CONNECTION RELEASE message in the tables "Accepted transactions" and "Rejected transactions" in the variable TRANSACTIONS;
- 1> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 1> clear the variable ESTABLISHED\_RABS;
- 1> if the received reconfiguration message contained the IE "Ciphering mode info":
  - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> clear the variable SECURITY\_MODIFICATION;
- 1> if the received reconfiguration message contained the IE "Integrity protection mode info":
  - 2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
- 1> enter idle mode;
- 1> perform the actions specified in subclause 8.5.2 when entering idle mode.
- 1> and the procedure ends.

NOTE: UTRAN should use RB Control messages to perform a SRNS relocation only in case of state transitions from Cell-DCH to Cell-DCH.

- ~~1> abort the ongoing integrity and/or ciphering reconfiguration;~~
- ~~1> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;~~
- ~~1> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;~~
- ~~1> if the received reconfiguration message contained the IE "Ciphering mode info":~~
  - ~~2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and~~
  - ~~2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;~~
- ~~1> if the received reconfiguration message contained the IE "Integrity protection mode info":~~
  - ~~2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and~~
  - ~~2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.~~
- ~~1> continue with any ongoing processes and procedures as if the reconfiguration message was not received.~~

~~The procedure ends.~~

### 8.2.2.13 Invalid received message

If the received reconfiguration message contains a protocol error causing the variable `PROTOCOL_ERROR_REJECT` to be set to TRUE according to clause 9, the UE shall perform procedure specific error handling as follows. The UE shall:

- 1> transmit a failure response message as specified in subclause 8.2.2.9, setting the information elements as specified below:
  - 2> include the IE "RRC transaction identifier"; and
  - 2> set it to the value of "RRC transaction identifier" in the entry for the received message in the table "Rejected transactions" in the variable `TRANSACTIONS`; and
  - 2> clear that entry;
  - 2> set the IE "failure cause" to the cause value "protocol error";
  - 2> include the IE "Protocol error information" with contents set to the value of the variable `PROTOCOL_ERROR_INFORMATION`.

The procedure ends.

## 8.2.3 Radio bearer release

See subclause 8.2.2 (Reconfiguration procedures).

### 8.3.1.6 Reception of the CELL UPDATE CONFIRM/URA UPDATE CONFIRM message by the UE

When the UE receives a CELL UPDATE CONFIRM/URA UPDATE CONFIRM message; and

- if the message is received on the CCCH, and IE "U-RNTI" is present and has the same value as the variable `U_RNTI`; or
- if the message is received on DCCH:

the UE shall:

- 1> stop timer T302;
- 1> in case of a cell update procedure and the CELL UPDATE CONFIRM message:
  - 2> includes "RB information elements"; and/or
  - 2> includes "Transport channel information elements"; and/or
  - 2> includes "Physical channel information elements"; and
  - 2> if the variable ORDERED\_RECONFIGURATION is set to FALSE:
    - 3> set the variable ORDERED\_RECONFIGURATION to TRUE.
- 1> act upon all received information elements as specified in subclause 8.6, unless specified otherwise in the following:
  - 2> if the IE "Frequency info" is included in the message:
    - 3> if the IE "RRC State Indicator" is set to the value "CELL\_FACH" or "CELL\_PCH" or "URA\_PCH":
      - 4> select a suitable UTRA cell according to [4] on that frequency;
      - 4> act as specified in subclause 8.3.1.12.
    - 3> if the IE "RRC State Indicator" is set to the value "CELL\_DCH":
      - 4> act on the IE "Frequency info" as specified in subclause 8.6.6.1.
  - 2> use the transport channel(s) applicable for the physical channel types that is used; and
  - 2> if the IE "TFS" is neither included nor previously stored in the UE for that transport channel(s):
    - 3> use the TFS given in system information.
  - 2> if none of the TFS stored is compatible with the physical channel:
    - 3> delete the stored TFS;
    - 3> use the TFS given in system information.
  - 2> perform the physical layer synchronisation procedure as specified in [29];
  - 2> if the CELL UPDATE CONFIRM message includes the IE "RLC re-establish indicator (RB2, RB3 and RB4)":
    - 3> re-establish the RLC entities for signalling radio bearer RB2, signalling radio bearer RB3 and signalling radio bearer RB4 (if established);
    - 3> if the value of the IE "Status" in the variable CIPHERING\_STATUS of the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN is set to "Started":
      - 4> set the HFN **component of the respective COUNT-C** values for AM RLC entities with RB identity 2, RB identity 3 and RB identity 4 (if established) equal to the START value included in the latest transmitted CELL UPDATE message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN.
  - 2> if the CELL UPDATE CONFIRM message includes the IE "RLC re-establish indicator (RB5 and upwards)":
    - 3> for radio bearers with RB identity 5 and upwards:
      - 4> re-establish the AM RLC entities;
      - 4> if the value of the IE "Status" in the variable CIPHERING\_STATUS of the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS is set to "Started":

5> set the HFN **component of the respective COUNT-C** values for AM RLC entities equal to the START value included in this CELL UPDATE message for the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS.

1> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":

2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected".

1> enter a state according to subclause 8.6.3.3 applied on the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message.

If the UE after state transition enters CELL\_DCH state, it shall:

1> not prohibit periodical status transmission in RLC;

1> for each CN domain for which a transparent mode radio bearer exists and for which the IE "Status" in the variable CIPHERING\_STATUS is set to "Started" for that CN domain:

2> choose an activation time for the ciphering on transparent mode radio bearers and include it in the response message in the IE "COUNT-C activation time";

2> set the 20 MSB of the MAC-d HFN with the corresponding START value in the most recently sent IE "START list";

2> set the remaining LSB of the MAC-d HFN to zero;

2> apply ciphering on the transparent mode radio bearers;

2> start incrementing the COUNT-C value from the CFN that has been included in the IE "COUNT-C activation time".

If the UE after state transition remains in CELL\_FACH state, it shall

1> start the timer T305 using its initial value if timer T305 is not running and periodical cell update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity";

1> select PRACH according to subclause 8.5.17;

1> select Secondary CCPCH according to subclause 8.5.19;

1> not prohibit periodical status transmission in RLC;

1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:

2> ignore that IE and stop using DRX.

If the UE after state transition enters URA\_PCH or CELL\_PCH state, it shall:

1> prohibit periodical status transmission in RLC;

1> clear the variable C\_RNTI;

1> stop using that C\_RNTI just cleared from the variable C\_RNTI in MAC;

1> start the timer T305 using its initial value if timer T305 is not running 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";

1> select Secondary CCPCH according to subclause 8.5.19;

1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:

2> use the value in the IE "UTRAN DRX Cycle length coefficient" for calculating Paging Occasion and PICH Monitoring Occasion as specified in subclause 8.6.3.2 in CELL\_PCH state.

1> if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:

2> set the variable INVALID\_CONFIGURATION to TRUE.

If the UE after the state transition remains in CELL\_FACH state; and

1> the contents of the variable C\_RNTI are empty:

it shall check the value of V302; and:

1> if V302 is equal to or smaller than N302:

2> if, caused by the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:

3> the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE; and/or

3> the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE:

4> abort the ongoing integrity and/or ciphering reconfiguration;

4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":

5> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and

5> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.

4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":

5> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and

5> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.

2> in case of a URA update procedure:

3> stop the URA update procedure; and

3> continue with a cell update procedure.

2> set the contents of the CELL UPDATE message according to subclause 8.3.1.3, except for the IE "Cell update cause" which shall be set to "cell reselection";

2> submit the CELL UPDATE message for transmission on the uplink CCCH;

2> increment counter V302;

2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.

1> if V302 is greater than N302:

2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;

2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;

2> in case of a cell update procedure:

3> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.

2> in case of a URA update procedure:

3> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.

2> release all its radio resources;

2> 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;

- 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 2> clear the variable ESTABLISHED\_RABS;
- 2> enter idle mode;
- 2> other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
- 2> and the procedure ends.

If the UE after the state transition remains in CELL\_FACH state; and

- a C-RNTI is stored in the variable C\_RNTI;

or

- the UE after the state transition moves to another state than the CELL\_FACH state:

the UE shall:

- 1> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
  - 2> include and set the IE "Radio bearer uplink ciphering activation time info" in any response message transmitted below to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> in case of a cell update procedure:
  - 2> set the IE "RRC transaction identifier" in any response message transmitted below to the value of "RRC transaction identifier" in the entry for the CELL UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry.
- 1> in case of a URA update procedure:
  - 2> set the IE "RRC transaction identifier" in any response message transmitted below to the value of "RRC transaction identifier" in the entry for the URA UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
- 1> if the variable PDCP\_SN\_INFO is non-empty:
  - 2> include the IE "RB with PDCP information list" in any response message transmitted below and set it to the value of the variable PDCP\_SN\_INFO.
- 1> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message included the IE "Downlink counter synchronisation info":
  - 2> re-establish RB2;
  - 2> set the new uplink and downlink HFN component of the COUNT-C of RB2 to MAX(uplink HFN component of the COUNT-C of RB2, downlink HFN component of the COUNT-C of RB2);
  - 2> increment by one the downlink and uplink values of the HFN component of the COUNT-C values for RB2;
  - 2> calculate the START value according to subclause 8.5.9;
  - 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in any response message transmitted below.
- 1> transmit a response message as specified in subclause 8.3.1.7;
- 1> if the IE "Integrity protection mode info" was present in the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:

- 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.
- 1> if the variable ORDERED\_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:
  - 2> set the variable ORDERED\_RECONFIGURATION to FALSE.
- 1> clear the variable PDCP\_SN\_INFO;
- 1> when the response message transmitted per subclause 8.3.1.7 to the UTRAN has been confirmed by RLC:
  - 2> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
    - 3> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
    - 3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
    - 3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
  - 2> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
    - 3> set "Uplink RRC Message sequence number" for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO to a value such that next RRC message to be sent on uplink RB0 will use the new integrity protection configuration;
    - 3> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
    - 3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE.
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 1> in case of a cell update procedure:
  - 2> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- 1> in case of a URA update procedure:
  - 2> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- 1> set the variable CELL\_UPDATE\_STARTED to FALSE;
- 1> clear the variable SECURITY\_MODIFICATION.

The procedure ends.

### 8.3.1.7 Transmission of a response message to UTRAN

If the CELL UPDATE CONFIRM message:

- includes the IE "RB information to release list";

the UE shall:

- 1> transmit a RADIO BEARER RELEASE COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include the IE "RB information to release list"; and
- includes the IE "RB information to reconfigure list"; or

- includes the IE "RB information to be affected list":

the UE shall:

- 1> transmit a RADIO BEARER RECONFIGURATION COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- includes "Transport channel information elements":

the UE shall:

- 1> transmit a TRANSPORT CHANNEL RECONFIGURATION COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- does not include "Transport channel information elements"; and
- includes "Physical channel information elements":

the UE shall:

- 1> transmit a PHYSICAL CHANNEL RECONFIGURATION COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- does not include "Transport channel information elements"; and
- does not include "Physical channel information elements"; and
- includes "CN information elements"; or
- includes the IE "Ciphering mode info"; or
- includes the IE "Integrity protection mode info"; or
- includes the IE "New C-RNTI"; or
- includes the IE "New U-RNTI":

the UE shall:

- 1> transmit a UTRAN MOBILITY INFORMATION CONFIRM as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- does not include "Transport channel information elements"; and
- does not include "Physical channel information elements"; and
- does not include "CN information elements"; and
- does not include the IE "Ciphering mode info"; and
- does not include the IE "Integrity protection mode info"; and
- does not include the IE "New C-RNTI"; and
- does not include the IE "New U-RNTI":



the UE shall:

- 1> transmit no response message.

If the URA UPDATE CONFIRM message:

- includes "CN information elements"; or
- includes the IE "Ciphering mode info"; or
- includes the IE "Integrity protection mode info"; or
- includes any one or both of the IEs "New C-RNTI" and "New U-RNTI":

the UE shall:

- 1> transmit a UTRAN MOBILITY INFORMATION CONFIRM as response message using AM RLC.

If the URA UPDATE CONFIRM message:

- does not include "CN information elements"; and
- does not include the IE "Ciphering mode info"; and
- does not include the IE "Integrity protection mode info"; and
- does not include the IE "New U-RNTI"; and
- does not include the IE "New C-RNTI":

the UE shall:

- 1> transmit no response message.

If the new state is CELL\_DCH or CELL\_FACH, the response message shall be transmitted using the new configuration after the state transition., and the UE shall:

- 1> if the IE "Downlink counter synchronisation info" was included in the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:
  - 2> when RLC has confirmed the successful transmission of the response message:
    - 3> re-establish all AM and UM RLC entities with RB identities larger than 4 and set the first 20 bits of all the HFN component of the respective COUNT-C values to the START value included in the response message for the corresponding CN domain;
    - 3> re-establish the RLC entities with RB identities 1, 3 and 4 and set the first 20 bits of all the HFN component of the respective COUNT-C values to the START value included in the response message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 3> set the remaining bits of the HFN component of the COUNT-C values of all UM RLC entities to zero;
    - 3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].
- 1> if the variable PDCP\_SN\_INFO is empty:
  - 2> if the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
    - 3> when RLC has confirmed the successful transmission of the response message:
      - 4> continue with the remainder of the procedure.
  - 2> if the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message did not contain the IE "Ciphering mode info":
    - 3> when RLC has been requested to transmit the response message,

4> continue with the remainder of the procedure.

1> if the variable PDCP\_SN\_INFO non-empty:

2> when RLC has confirmed the successful transmission of the response message:

3> for each radio bearer in the variable PDCP\_SN\_INFO:

4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":

5> configure the RLC entity for that radio bearer to "continue".

3> continue with the remainder of the procedure.

If the new state is CELL\_PCH or URA\_PCH, the response message shall be transmitted in CELL\_FACH state, and the UE shall:

1> when RLC has confirmed the successful transmission of the response message:

2> for each radio bearer in the variable PDCP\_SN\_INFO:

3> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":

4> configure the RLC entity for that radio bearer to "continue".

2> enter the new state (CELL\_PCH or URA\_PCH, respectively).

1> continue with the remainder of the procedure.

---

### 8.3.1.12 T302 expiry or cell reselection

If any or several of the following conditions are true:

- expiry of timer T302;
- reselection to another UTRA cell (including the previously serving cell) before completion of the cell update or URA update procedure;

the UE shall:

1> stop T302 if it is running;

1> if the UE was in CELL\_DCH state prior to the initiation of the procedure; and

2> if timers T314 and T315 have elapsed while T302 was running:

3> enter idle mode.

3> 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. Other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2.

3> and the procedure ends.

2> if timer T314 has elapsed while T302 was running and,

3> if "T314 expired" in the variable RB\_TIMER\_INDICATOR is set to FALSE and

3> if T315 is still running:

4> release locally all radio bearers which are associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT314";

4> indicate release of those radio access bearers to upper layers;

- 4> delete all information about those radio access bearers from the variable ESTABLISHED\_RABS;
- 4> set "T314 expired" in the variable RB\_TIMER\_INDICATOR to TRUE.
- 2> if timer T315 has elapsed while T302 was running and,
  - 3> if "T315 expired" in the variable RB\_TIMER\_INDICATOR is set to FALSE and,
    - 3> if T314 is still running:
      - 4> release locally all radio bearers which are associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT315";
      - 4> indicate release of those radio access bearers to upper layers;
      - 4> delete all information about those radio access bearers from the variable ESTABLISHED\_RABS;
      - 4> set "T315 expired" in the variable RB\_TIMER\_INDICATOR to TRUE.
- 1> check whether it is still in "in service area" (see subclause 8.5.5.2);

~~1> if, caused by the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE;~~

~~2> abort the ongoing integrity and/or ciphering reconfiguration;~~

~~2> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":~~

~~3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and~~

~~3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.~~

~~2> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":~~

~~3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and~~

~~3> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.~~

1> if the variable ORDERED\_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:

2> set the variable ORDERED\_RECONFIGURATION to FALSE.

1> in case of a cell update procedure:

2> clear any entry for the CELL UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS.

1> in case of a URA update procedure:

2> clear any entry for the URA UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS.

If the UE detects "in service area" if it has not entered idle mode, and:

1> if V302 is equal to or smaller than N302, the UE shall:

2> if the UE performed cell re-selection:

3> delete its C-RNTI;

2> in case of a cell update procedure:

3> set the contents of the CELL UPDATE message according to subclause 8.3.1.3;

- 3> if a CELL\_UPDATE\_CONFIRM message was received and caused the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE, and
- 3> if the IE "Downlink counter synchronisation info" was included in the received CELL\_UPDATE\_CONFIRM message:
  - 4> apply the new security (integrity protection) configuration received in the CELL\_UPDATE\_CONFIRM on the CELL\_UPDATE message;
- 3> submit the CELL\_UPDATE message for transmission on the uplink CCCH.
- 2> in case of a URA update procedure:
  - 3> set the contents of the URA\_UPDATE message according to subclause 8.3.1.3;
  - 3> if a URA\_UPDATE\_CONFIRM message was received and caused the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE, and
  - 3> if the IE "Downlink counter synchronisation info" was included in the received URA\_UPDATE\_CONFIRM message:
    - 4> apply the new security (integrity protection) configuration received in the URA\_UPDATE\_CONFIRM on the URA\_UPDATE message;
  - 3> submit the URA\_UPDATE message for transmission on the uplink CCCH.
- 2> increment counter V302;
- 2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.
- 1> if V302 is greater than N302, the UE shall:
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
  - 2> clear the variable PDCP\_SN\_INFO;
  - 2> in case of a cell update procedure:
    - 3> clear the entry for the CELL\_UPDATE\_CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 2> in case of a URA update procedure:
    - 3> clear the entry for the URA\_UPDATE\_CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 2> release all its radio resources;
  - 2> 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;
  - 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 2> clear the variable ESTABLISHED\_RABS;
  - 2> set the variable CELL\_UPDATE\_STARTED to FALSE;
  - 2> enter idle mode;
  - 2> other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
  - 2> and the procedure ends.

If the UE does not detect "in service area", it shall:

- 1> continue searching for "in service area".

### 8.3.3.3 Reception of UTRAN MOBILITY INFORMATION message by the UE

When the UE receives a UTRAN MOBILITY INFORMATION message, it shall:

- 1> act on received information elements as specified in subclause 8.6;
- 1> if the IE "UE Timers and constants in connected mode" is present:
  - 2> store the values of the IE "UE Timers and constants in connected mode" in the variable TIMERS\_AND\_CONSTANTS, replacing any previously stored value for each timer and constant; and
  - 2> for each updated timer value:
    - 3> start using the new value next time the timer is started;
  - 2> for each updated constant value:
    - 3> start using the new value directly;
- 1> if the IE "CN domain specific DRX cycle length coefficient" is present:
  - 2> store the value of the IE "CN domain specific DRX cycle length coefficient" for that CN domain, replacing any previously stored value; and
  - 2> use the value to determine the connected mode paging occasions according to [4].
- 1> set the IE "RRC transaction identifier" in the UTRAN MOBILITY INFORMATION CONFIRM message to the value of "RRC transaction identifier" in the entry for the UTRAN MOBILITY INFORMATION message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected";
- 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
  - 2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the variable PDCP\_SN\_INFO is non-empty:
  - 2> include the IE "RB with PDCP information list" in the UTRAN MOBILITY INFORMATION CONFIRM message and set it to the value of the variable PDCP\_SN\_INFO.
- 1> if the received UTRAN MOBILITY INFORMATION message included the IE "Downlink counter synchronisation info":
  - 2> re-establish RB2;
  - 2> set the new uplink and downlink HFN component of COUNT-C of RB2 to MAX(uplink HFN component of COUNT-C of RB2, downlink HFN component of COUNT-C of RB2);
  - 2> increment by one the downlink and uplink values of the HFN component of COUNT-C values for RB2;
  - 2> calculate the START value according to subclause 8.5.9;

- 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the UTRAN MOBILITY INFORMATION CONFIRM message.
- 1> transmit a UTRAN MOBILITY INFORMATION CONFIRM message on the uplink DCCH using AM RLC;
- 1> if the IE "Integrity protection mode info" was present in the UTRAN MOBILITY INFORMATION message:
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted UTRAN MOBILITY INFORMATION CONFIRM message.
- 1> if the IE "Downlink counter synchronisation info" was included in the received UTRAN MOBILITY INFORMATION message:
  - 2> when RLC has confirmed the successful transmission of the response message:
    - 3> re-establish all AM and UM RLC entities with RB identities larger than 4 and set the first 20 bits of all ~~their~~ the HFN ~~component of the respective COUNT-C~~ values to the START value included in the response message for the corresponding CN domain;
    - 3> re-establish the RLC entities with RB identities 1, 3 and 4 and set the first 20 bits of all ~~the~~ HFN ~~component of the respective COUNT-C~~ values to the START value included in the response message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 3> set the remaining bits of the HFN ~~component of the COUNT-C values~~ of all UM RLC entities to zero;
    - 3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].
  - 1> if the variable PDCP\_SN\_INFO is empty; and
    - 2> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
      - 3> when RLC has confirmed the successful transmission of the UTRAN MOBILITY INFORMATION CONFIRM message, perform the actions below.
    - 2> if the UTRAN MOBILITY INFORMATION message did not contain the IE "Ciphering mode info":
      - 3> when RLC has been requested to transmit the UTRAN MOBILITY INFORMATION CONFIRM message, perform the actions below.
  - 1> if the variable PDCP\_SN\_INFO is non-empty:
    - 2> when RLC has confirmed the successful transmission of the UTRAN MOBILITY INFORMATION CONFIRM message:
      - 3> for each radio bearer in the variable PDCP\_SN\_INFO:
        - 4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
          - 5> configure the RLC entity for that radio bearer to "continue".
      - 3> clear the variable PDCP\_SN\_INFO.
  - 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
    - 2> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
    - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
    - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
  - 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Integrity protection mode info":
    - 2> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
    - 2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and

2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.

1> clear the variable SECURITY\_MODIFICATION.

The procedure ends.

### 8.3.3.5 Cell re-selection

If the UE performs cell re-selection, the UE shall:

1> initiate a cell update procedure according to subclause 8.3.1;

1> if the UTRAN MOBILITY INFORMATION message contains the IE "New C-RNTI"; and

1> if the UE has not yet submitted the UTRAN MOBILITY INFORMATION CONFIRM message to lower layers for transmission **and**

**1> if the IE "Downlink counter synchronisation info" was not included in the received UTRAN MOBILITY INFORMATION message;**

2> transmit a UTRAN MOBILITY INFORMATION FAILURE message on the uplink DCCH using AM RLC;

2> set the IE "RRC transaction identifier" in the UTRAN MOBILITY INFORMATION FAILURE message to the value of "RRC transaction identifier" in the entry for the UTRAN MOBILITY INFORMATION message in the table "Accepted transactions" in the variable TRANSACTIONS; and

2> clear that entry.

2> set the IE "failure cause" to the cause value "cell update occurred";

2> when the UTRAN MOBILITY INFORMATION FAILURE message has been submitted to lower layers for transmission:

3> continue with any ongoing processes and procedures as if the invalid UTRAN MOBILITY INFORMATION message has not been received and the procedure ends.

1> otherwise:

2> **if a UTRAN MOBILITY INFORMATION message was received and caused the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE, and**

**2> if the IE "Downlink counter synchronisation info" was included in the received UTRAN MOBILITY INFORMATION message:**

**3> apply the new security (integrity protection) configuration received in the UTRAN MOBILITY INFORMATION message on the CELL UPDATE message to be transmitted;**

**2> continue the procedure normally;**

#### 8.3.3.5a Incompatible simultaneous security reconfiguration

If the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION becomes set to TRUE of the received UTRAN MOBILITY INFORMATION message, the UE shall:

1> transmit a UTRAN MOBILITY INFORMATION FAILURE message on the uplink DCCH using AM RLC;

1> set the IE "RRC transaction identifier" in the UTRAN MOBILITY INFORMATION FAILURE message to the value of "RRC transaction identifier" in the entry for the UTRAN MOBILITY INFORMATION message in the table "Accepted transactions" in the variable TRANSACTIONS; and

1> clear that entry;

- 1> set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";
- 1> when the UTRAN MOBILITY INFORMATION FAILURE message has been delivered to lower layers for transmission:
  - 2> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to FALSE;
  - 2> continue with any ongoing processes and procedures as if the UTRAN MOBILITY INFORMATION message has not been received;
  - 2> and the procedure ends.

### 8.6.3.5 Integrity protection mode info

The IE "Integrity protection mode info" defines the new integrity protection configuration. At any given time, the UE needs to store at most three different integrity protection configurations (keysets) in total for all signalling radio bearers for all CN domains.

If the IE "Integrity protection mode info" is present and if the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE, the UE shall:

- 1> ignore this second attempt to change the integrity protection configuration; and
- 1> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to TRUE.

If the IE "Integrity protection mode info" is present and if the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to FALSE, the UE shall:

- 1> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to TRUE;
- 1> if IE "Integrity protection mode command" has the value "start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and this IE was included in the message SECURITY MODE COMMAND:
  - 2> initialise the information for all signalling radio bearers in the variable INTEGRITY\_PROTECTION\_INFO according to the following:
    - 3> set the IE "Uplink RRC Message sequence number" in the variable INTEGRITY\_PROTECTION\_INFO to zero;
    - 3> do not set the IE "Downlink RRC Message sequence number" in the variable INTEGRITY\_PROTECTION\_INFO;
    - 3> set the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO to zero for each signalling radio bearer in the IE "ESTABLISHED\_RABS".
  - 2> set the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO to the value "Started";
  - 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:
    - 3> using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";
    - 3> using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].
  - 2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer in the IE "ESTABLISHED\_RABS" except RB2 at the next received RRC message;
  - 2> start applying the new integrity protection configuration in the downlink for signalling radio bearer RB2 from and including the received SECURITY MODE COMMAND message;



- 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearers other than RB2 at the uplink activation time included in the IE "Uplink integrity protection activation info".
- 1> if IE "Integrity protection mode command" has the value "start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and this IE was not included SECURITY MODE COMMAND:

NOTE: This case is used in SRNS relocation

- 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:
    - 3> using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";
    - 3> using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].
  - 2> let RB<sub>m</sub> be the signalling radio bearer where the reconfiguration message was received and let RB<sub>n</sub> be the signalling radio bearer where the response message is transmitted;
  - 2> prohibit transmission of RRC messages on all signalling radio bearers in the IE "ESTABLISHED\_RABS" except on RB<sub>0</sub> and the radio bearer where the response message is transmitted;
  - 2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer in the IE "ESTABLISHED\_RABS" except RB<sub>m</sub> at the next received RRC message;
  - 2> start applying the new integrity protection configuration in the downlink for signalling radio bearer RB<sub>m</sub> from and including the received configuration message;
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB<sub>n</sub> from and including the transmitted response message;
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearers other than RB<sub>n</sub> at the uplink activation time included in the IE "Uplink integrity protection activation info".
- 1> if IE "Integrity protection mode command" has the value "modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and this IE was included in SECURITY MODE COMMAND:
- 2> store the (oldest currently used) integrity protection configuration until activation times have elapsed for the new integrity protection configuration to be applied on all signalling radio bearers;
  - 2> if there are pending activation times set for integrity protection by a previous procedure changing the integrity protection configuration:
    - 3> apply the integrity protection configuration at this pending activation time as indicated in this procedure.
  - 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each signalling radio bearer n, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info";
  - 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1;
    - 3> if present, use the algorithm indicated by the IE "Integrity protection algorithm" (UIA [40]);
  - 2> set the content of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO according to the following:
    - 3> for each established signalling radio bearer, stored in the variable ESTABLISHED\_RABS:

- 4> select a value of the RRC sequence number at which (activation) time the new integrity protection configuration shall be applied in uplink for that signalling radio bearer according to the following:
  - 5> for each signalling radio bearer that has no pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
    - 6> set a suitable value that would ensure a minimised delay in the change to the latest integrity protection configuration.
  - 5> for signalling radio bearer that has a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
    - 6> set the same value as the pending activation time for integrity protection;
  - 5> consider this (pending) activation time to be elapsed when the selected activation time (as above) is equal to the next RRC sequence number to be used, which means that the last RRC message using the old integrity protection configuration has been submitted to lower layers.
- 4> for signalling radio bearer RB0:
  - 5> set the value of the included RRC sequence number to greater than or equal to the current value of the RRC sequence number for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO, plus the value of the constant N302 plus one.
- 4> prohibit the transmission of RRC messages on all signalling radio bearers, except for RB2, with RRC SN greater than or equal to the value in the "RRC message sequence number list" for the signalling radio bearer in the IE "Uplink integrity protection activation info" of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 2> start applying the new integrity protection configuration in the uplink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Uplink integrity protection activation info", included in the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
- 2> start applying the new integrity protection configuration in the uplink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration;
- 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info";

NOTE: For signalling radio bearers that have a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration, UTRAN should set this value in IE "Downlink integrity protection activation info".

- 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration.

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and the IE "Integrity protection mode command info" was not included in the message SECURITY MODE COMMAND; or

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and the IE "Integrity protection mode info" was included in the message SECURITY MODE COMMAND, and the IE "Integrity protection algorithm" is not included; or

If the IE "Integrity protection mode command" has the value "Modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not Started"; or

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started", and the IE "Integrity protection mode command info" was included in the message SECURITY MODE COMMAND; or

If there does not exist exactly one integrity protection activation time in the IE "Downlink integrity protection activation info" for each established signalling radio bearer included in the IE "Signalling radio bearer information" in the IE "ESTABLISHED\_RABS"; or

If IE "Integrity protection mode command" has the value "Modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started", and the IE "Integrity protection mode info" was not included in the message SECURITY MODE COMMAND:

the UE shall:

- 1> ignore this attempt to change the integrity protection configuration; and
- 1> set the variable INVALID\_CONFIGURATION to TRUE.

If the IE "Integrity protection mode info" is not present, the UE shall:

- 1> not change the integrity protection configuration.

# CHANGE REQUEST

⌘ **25.331 CR 1494** ⌘ rev **-** ⌘ Current version: **4.4.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Corrections to cell update interactions with security and SRNS Relocation		
<b>Source:</b>	⌘ TSG-RAN WG2		
<b>Work item code:</b>	⌘ TEI	<b>Date:</b>	⌘ May 13, 2002
<b>Category:</b>	⌘ <b>A</b>	<b>Release:</b>	⌘ REL-4
	<i>Use <u>one</u> of the following categories:</i> <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<i>Use <u>one</u> of the following releases:</i> <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>REL-4</b> (Release 4) <b>REL-5</b> (Release 5)

<b>Reason for change:</b> ⌘	<ol style="list-style-type: none"> <li>1. The actions for the UE in case of CELL UPDATE and UTRAN MOBILITY INFORMATION when performing a security reconfiguration during a CELL UPDATE CONFIRM procedure causing security reconfiguration are missing.</li> <li>2. It is stated that in case of a CELL UPDATE being triggered during security reconfiguration, the UE shall abort and revert back to its previous configuration. This would however require the UE to abandon the re-establishment of RB2 and revert back to the previous RB2 configuration - this is however not possible.</li> <li>3. It is incorrectly stated that in case of SRNS relocation the HFN components have to be modified following the re-establishment of the associated RB, when in fact only the HFN components of the COUNT-C values for that RB needs to be modified.</li> <li>4. Transmission on RB0 is prohibited - this would prevent a CELL UPDATE being sent during security reconfiguration.</li> </ol>
<b>1. Summary of change:</b> ⌘	<ol style="list-style-type: none"> <li>1. It is stated that the UE shall not abort the security reconfiguration if a CELL UPDATE occurs during a CELL UPDATE CONFIRM triggering a SRNS Relocation. UE actions in case of UTRAN MOBILITY INFORMATION procedure are stated - UE shall start a cell update procedure and continue with the UTRAN MOBILITY INFORMATION.</li> <li>2. It is stated that the UE shall release its radio resources if a cell reselection is triggered during a RB Reconfiguration procedure triggering SRNS Relocation. A note is added that the UTRAN should use RB Control messages for triggering SRNS Relocation only in case of CELL_DCH to CELL_DCH transitions. UE behavior in other cases is unspecified.</li> <li>3. It is now stated that only the HFN components of the COUNT-C values need to be modified or set following RB re-establishment during the SRNS relocation.</li> <li>4. Transmission on RB0 is now allowed during security reconfiguration.</li> </ol>

<b>Consequences if not approved:</b>	⌘	<ol style="list-style-type: none"> <li>1. UE actions on cell update in case of UTRAN MOBILITY INFORMATION causing security reconfiguration on SRNS relocation will be unspecified leading to unknown UE behavior. UE actions in case of cell update during an ongoing CELL UPDATE CONFIRM causing security reconfiguration will be difficult to implement causing unknown UE behavior.</li> <li>2. UE implementation will not be possible leading to unknown UE behavior.</li> <li>3. HFN components of COUNT-I may also be incorrectly modified causing loss of connection due to security failure.</li> <li>4. CELL UPDATE will not be sent causing loss of connection.</li> </ol>
--------------------------------------	---	--

<b>Clauses affected:</b>	⌘	8.2.2.3; 8.2.2.4; 8.2.2.12b; 8.3.1.6; 8.3.1.7; 8.3.1.12; 8.3.3.3; 8.3.3.5; 8.6.3.5										
<b>Other specs affected:</b>	⌘	<table border="1"> <tr> <td>Other core specifications</td> <td>⌘</td> <td>25.331 v3.10.0, CR 1493</td> </tr> <tr> <td>Test specifications</td> <td></td> <td>25.331 v5.0.0, CR 1495</td> </tr> <tr> <td>O&amp;M Specifications</td> <td></td> <td></td> </tr> </table>	Other core specifications	⌘	25.331 v3.10.0, CR 1493	Test specifications		25.331 v5.0.0, CR 1495	O&M Specifications			
Other core specifications	⌘	25.331 v3.10.0, CR 1493										
Test specifications		25.331 v5.0.0, CR 1495										
O&M Specifications												
<b>Other comments:</b>	⌘											

**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.

### 8.2.2.3 Reception of RADIO BEARER SETUP or RADIO BEARER RECONFIGURATION or RADIO BEARER RELEASE or TRANSPORT CHANNEL RECONFIGURATION or PHYSICAL CHANNEL RECONFIGURATION message by the UE

The UE shall be able to receive any of the following messages:

- RADIO BEARER SETUP message; or
- RADIO BEARER RECONFIGURATION message; or
- RADIO BEARER RELEASE message; or
- TRANSPORT CHANNEL RECONFIGURATION message; or
- PHYSICAL CHANNEL RECONFIGURATION message;

and perform a hard handover, even if no prior UE measurements have been performed on the target cell and/or frequency.

If the UE receives:

- a RADIO BEARER SETUP message; or
- a RADIO BEARER RECONFIGURATION message; or
- a RADIO BEARER RELEASE message; or
- a TRANSPORT CHANNEL RECONFIGURATION message; or
- a PHYSICAL CHANNEL RECONFIGURATION message;

it shall:

- 1> set the variable ORDERED\_RECONFIGURATION to TRUE;
- 1> perform the physical layer synchronisation procedure as specified in [29];
- 1> act upon all received information elements as specified in subclause 8.6, unless specified in the following and perform the actions below.

The UE may:

- 1> maintain a list of the set of cells to which the UE has Radio Links if the IE "Cell ID" is present.

The UE may first release the physical channel configuration used at reception of the reconfiguration message. The UE shall then:

- 1> in FDD, if the IE "PDSCH code mapping" is included but the IE "PDSCH with SHO DCH Info" is not included and if the DCH has only one link in its active set:
  - 2> act upon the IE "PDSCH code mapping" as specified in subclause 8.6; and
  - 2> infer that the PDSCH will be transmitted from the cell from which the downlink DPCH is transmitted.
- 1> enter a state according to subclause 8.6.3.3.

In case the UE receives a RADIO BEARER RECONFIGURATION message including the IE "RB information to reconfigure" that only includes the IE "RB identity", the UE shall:

- 1> handle the message as if IE "RB information to reconfigure" was absent.

**NOTE:** The RADIO BEARER RECONFIGURATION message always includes the IE "RB information to reconfigure". UTRAN has to include it even if it does not require the reconfiguration of any RB.

If after state transition the UE enters CELL\_DCH state, the UE shall, after the state transition:

- 1> remove any C-RNTI from MAC;
- 1> clear the variable C\_RNTI.

In FDD, if after state transition the UE leaves CELL\_DCH state, the UE shall, after the state transition:

- 1> remove any DSCH-RNTI from MAC;
- 1> clear the variable DSCH\_RNTI.

If the UE was in CELL\_DCH state upon reception of the reconfiguration message and remains in CELL\_DCH state, the UE shall:

- 1> if the IE "Uplink DPCH Info" is absent, not change its current UL Physical channel configuration;
- 1> if the IE "Downlink information for each radio link" is absent, not change its current DL Physical channel configuration.

If after state transition the UE enters CELL\_FACH state, the UE shall, after the state transition:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4] on that frequency.
- 1> if the IE "Frequency info" is not included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4].
- 1> if the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selects another cell than indicated by this IE or the received reconfiguration message did not include the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD):
  - 2> initiate a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";
  - 2> when the cell update procedure completed successfully:
    - 3> if the UE is in CELL\_PCH or URA\_PCH state:
      - 4> initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
      - 4> proceed as below.
- 1> start timer T305 using its initial value if timer T305 is not running and if periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" in system information block type 1;

1> select PRACH according to subclause 8.5.17;

1> select Secondary CCPCH according to subclause 8.5.19;

1> use the transport format set given in system information;

1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:

- 2> ignore that IE and stop using DRX.

1> if the contents of the variable C\_RNTI is empty:

- 2> perform a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";
- 2> when the cell update procedure completed successfully:
  - 3> if the UE is in CELL\_PCH or URA\_PCH state:

- 4> initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
- 4> proceed as below.

If the UE was in CELL\_FACH state upon reception of the reconfiguration message and remains in CELL\_FACH state, the UE shall:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4] on that frequency;
- 2> if the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE or the received reconfiguration message did not include the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD):
  - 3> initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
  - 3> when the cell update procedure completed successfully:
    - 4> proceed as below.

The UE shall transmit a response message as specified in subclause 8.2.2.4, setting the information elements as specified below. The UE shall:

- 1> if the received reconfiguration message included the IE "Downlink counter synchronisation info"; or
- 1> if the received reconfiguration message is a RADIO BEARER RECONFIGURATION and the IE "New U-RNTI" is included:
  - 2> re-establish RB2;
  - 2> set the new uplink and downlink HFN **component of COUNT-C** of RB2 to MAX(uplink HFN **component of COUNT-C** of RB2, downlink HFN **component of COUNT-C** of RB2);
  - 2> increment by one the downlink and uplink **values of the HFN component of COUNT-C values** for RB2;
  - 2> calculate the START value according to subclause 8.5.9;
  - 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message did not include the IE "Downlink counter synchronisation info":
  - 2> if the variable START\_VALUE\_TO\_TRANSMIT is set:
    - 3> include and set the IE "START" to the value of that variable.
  - 2> if the variable START\_VALUE\_TO\_TRANSMIT is not set and the IE "New U-RNTI" is included:
    - 3> calculate the START value according to subclause 8.5.9;
    - 3> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
  - 2> if the received reconfiguration message caused a change in the RLC size for any RB using RLC-AM:
    - 3> calculate the START value according to subclause 8.5.9;
    - 3> include the calculated START values for the CN domain associated with the corresponding RB identity in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected".



- 1> if the received reconfiguration message contained the IE "Ciphering mode info":
  - 2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the received reconfiguration message did not contain the IE "Ciphering activation time for DPCH" in IE "Ciphering mode info":
  - 2> if prior to this procedure there exist no transparent mode RLC radio bearers:
    - 3> if, at the conclusion of this procedure, the UE will be in CELL\_DCH state; and
    - 3> if, at the conclusion of this procedure, at least one transparent mode RLC radio bearer exists:
      - 4> include the IE "COUNT-C activation time" and specify a CFN value for this IE.
  - 2> if prior to this procedure there exists at least one transparent mode RLC radio bearer:
    - 3> if, at the conclusion of this procedure, no transparent mode RLC radio bearers exist:
      - 4> include the IE "COUNT-C activation time" and specify a CFN value for this IE.
- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the received message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> if the variable PDCP\_SN\_INFO is not empty:
  - 2> include the IE "RB with PDCP information list" and set it to the value of the variable PDCP\_SN\_INFO.
- 1> in TDD, if the procedure is used to perform a handover to a cell where timing advance is enabled, and the UE can calculate the timing advance value in the new cell (i.e. in a synchronous TDD network):
  - 2> set the IE "Uplink Timing Advance" according to subclause 8.6.6.26.
- 1> if the IE "Integrity protection mode info" was present in the received reconfiguration message:
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.

If after state transition the UE enters CELL\_PCH or URA\_PCH state, the UE shall, after the state transition and transmission of the response message:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4] on that frequency.
- 1> if the IE "Frequency info" is not included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4].
- 1> prohibit periodical status transmission in RLC;
- 1> remove any C-RNTI from MAC;
- 1> clear the variable C\_RNTI;
- 1> start timer T305 using its initial value if timer T305 is not running and if periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" in system information block type 1;
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 2> use the value in the IE "UTRAN DRX Cycle length coefficient" for calculating Paging occasion and PICH Monitoring Occasion as specified in subclause 8.6.3.2.

- 1> if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the UE enters CELL\_PCH state from CELL\_DCH state, and the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE or the received reconfiguration message did not include the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD):
  - 2> initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
  - 2> when the cell update procedure completed successfully:
    - 3> the procedure ends.
- 1> if the UE enters CELL\_PCH state from CELL\_FACH state, and the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE:
  - 2> initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
  - 2> when the cell update procedure is successfully completed:
    - 3> the procedure ends.
- 1> if the UE enters URA\_PCH state, and after cell selection the criteria for URA update caused by "URA reselection" according to subclause 8.3.1 is fulfilled:
  - 2> initiate a URA update procedure according to subclause 8.3.1 using the cause "URA reselection";
  - 2> when the URA update procedure is successfully completed:
    - 3> the procedure ends.

#### 8.2.2.4 Transmission of a response message by the UE, normal case

In case the procedure was triggered by reception of a RADIO BEARER SETUP message, the UE shall:

- 1> transmit a RADIO BEARER SETUP COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a RADIO BEARER RECONFIGURATION message, the UE shall:

- 1> transmit a RADIO BEARER RECONFIGURATION COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a RADIO BEARER RELEASE message, the UE shall:

- 1> transmit a RADIO BEARER RELEASE COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a TRANSPORT CHANNEL RECONFIGURATION message, the UE shall:

- 1> transmit a TRANSPORT CHANNEL RECONFIGURATION COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a PHYSICAL CHANNEL RECONFIGURATION message, the UE shall:

- 1> transmit a PHYSICAL CHANNEL RECONFIGURATION COMPLETE as response message on the uplink DCCH using AM RLC.

If the new state is CELL\_DCH or CELL\_FACH, the response message shall be transmitted using the new configuration after the state transition, and the UE shall:

- 1> if the IE "Downlink counter synchronisation info" was included in the reconfiguration message; or

- 1> if the received reconfiguration message is a RADIO BEARER RECONFIGURATION and the IE "New U-RNTI" is included:
  - 2> when RLC has confirmed the successful transmission of the response message:
    - 3> re-establish all AM and UM RLC entities with RB identities larger than 4 and set the first 20 bits of all the HFN component of the respective COUNT-C values to the START value included in the response message for the corresponding CN domain;
    - 3> re-establish the RLC entities with RB identities 1, 3 and 4 and set the first 20 bits of all the HFN component of the respective COUNT-C values to the START value included in the response message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 3> set the remaining bits of the HFN component of the COUNT-C values of all UM RLC entities to zero;
    - 3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].
  - 1> if the variable PDCP\_SN\_INFO is empty:
    - 2> if the received reconfiguration message contained the IE "Ciphering mode info":
      - 3> when RLC has confirmed the successful transmission of the response message:
        - 4> notify upper layers upon change of the security configuration;
        - 4> perform the actions below.
      - 2> if the received reconfiguration message did not contain the IE "Ciphering mode info":
        - 3> when RLC has been requested to transmit the response message:
          - 4> perform the actions below.
    - 1> if the variable PDCP\_SN\_INFO is non-empty:
      - 2> when RLC has confirmed the successful transmission of the response message:
        - 3> for each radio bearer in the variable PDCP\_SN\_INFO:
          - 4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
            - 5> configure the RLC entity for that radio bearer to "continue".
          - 3> perform the actions below.

If the new state is CELL\_PCH or URA\_PCH, the response message shall be transmitted using the old configuration before the state transition, but the new C-RNTI shall be used if the IE "New C-RNTI" was included in the received reconfiguration message, and the UE shall:

- 1> when RLC has confirmed the successful transmission of the response message:
  - 2> for each radio bearer in the variable PDCP\_SN\_INFO:
    - 3> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
      - 4> configure the RLC entity for that radio bearer to "continue".
    - 2> enter the new state (CELL\_PCH or URA\_PCH, respectively);
    - 2> perform the actions below.

The UE shall:

- 1> set the variable ORDERED\_RECONFIGURATION to FALSE;
- 1> if the received reconfiguration message contained the IE "Ciphering mode info":

- 2> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
- 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
- 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the received reconfiguration message contained the IE "Integrity protection mode info":
  - 2> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
  - 2> set "Uplink RRC Message sequence number" for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO to a value such that next RRC message to be sent on uplink RB0 will use the new integrity protection configuration;
  - 2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 1> clear the variable PDCP\_SN\_INFO;
- 1> clear the variable START\_VALUE\_TO\_TRANSMIT;
- 1> clear the variable SECURITY\_MODIFICATION.

### 8.2.2.12b Cell update procedure during security reconfiguration

If:

- a cell update procedure according to subclause 8.3.1 is initiated; and
- the received reconfiguration message causes either:
  - the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE; and/or
  - the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE:

the UE shall:

- 1> release all radio resources:
  - 1> indicate the release 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; and
  - 1> clear any entry for the RRC CONNECTION RELEASE message in the tables "Accepted transactions" and "Rejected transactions" in the variable TRANSACTIONS;
  - 1> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 1> clear the variable ESTABLISHED\_RABS;
  - 1> if the received reconfiguration message contained the IE "Ciphering mode info":
    - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
    - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
    - 2> clear the variable SECURITY\_MODIFICATION;
  - 1> if the received reconfiguration message contained the IE "Integrity protection mode info":
    - 2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
    - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
- 1> enter idle mode;

~~1> perform the actions specified in subclause 8.5.2 when entering idle mode.~~

~~1> and the procedure ends.~~

NOTE: UTRAN should use RB Control messages to perform a SRNS relocation only in case of state transitions from Cell-DCH to Cell-DCH.

- ~~1> abort the ongoing integrity and/or ciphering reconfiguration;~~
- ~~1> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC AM or RLC UM;~~
- ~~1> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;~~
- ~~1> if the received reconfiguration message contained the IE "Ciphering mode info":~~
  - ~~2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and~~
  - ~~2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;~~
- ~~1> if the received reconfiguration message contained the IE "Integrity protection mode info":~~
  - ~~2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and~~
  - ~~2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.~~
- ~~1> continue with any ongoing processes and procedures as if the reconfiguration message was not received.~~

~~The procedure ends.~~

### 8.3.1.6 Reception of the CELL UPDATE CONFIRM/URA UPDATE CONFIRM message by the UE

When the UE receives a CELL UPDATE CONFIRM/URA UPDATE CONFIRM message; and

- if the message is received on the CCCH, and IE "U-RNTI" is present and has the same value as the variable U\_RNTI; or
- if the message is received on DCCH:

the UE may:

- 1> maintain a list of the set of cells to which the UE has Radio Links if the IE "Cell ID" is present.

the UE shall:

- 1> stop timer T302;
- 1> in case of a cell update procedure and the CELL UPDATE CONFIRM message:
  - 2> includes "RB information elements"; and/or
  - 2> includes "Transport channel information elements"; and/or
  - 2> includes "Physical channel information elements"; and
  - 2> if the variable ORDERED\_RECONFIGURATION is set to FALSE:
    - 3> set the variable ORDERED\_RECONFIGURATION to TRUE.
- 1> act upon all received information elements as specified in subclause 8.6, unless specified otherwise in the following:
  - 2> if the IE "Frequency info" is included in the message:
    - 3> if the IE "RRC State Indicator" is set to the value "CELL\_FACH" or "CELL\_PCH" or "URA\_PCH":

- 4> select a suitable UTRA cell according to [4] on that frequency;
- 4> act as specified in subclause 8.3.1.12.
- 3> if the IE "RRC State Indicator" is set to the value "CELL\_DCH":
  - 4> act on the IE "Frequency info" as specified in subclause 8.6.6.1.
- 2> use the transport channel(s) applicable for the physical channel types that is used; and
- 2> if the IE "TFS" is neither included nor previously stored in the UE for that transport channel(s):
  - 3> use the TFS given in system information.
- 2> if none of the TFS stored is compatible with the physical channel:
  - 3> delete the stored TFS;
  - 3> use the TFS given in system information.
- 2> perform the physical layer synchronisation procedure as specified in [29];
- 2> if the CELL UPDATE CONFIRM message includes the IE "RLC re-establish indicator (RB2, RB3 and RB4)":
  - 3> re-establish the RLC entities for signalling radio bearer RB2, signalling radio bearer RB3 and signalling radio bearer RB4 (if established);
  - 3> if the value of the IE "Status" in the variable CIPHERING\_STATUS of the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN is set to "Started":
    - 4> set the HFN **component of the respective COUNT-C** values for AM RLC entities with RB identity 2, RB identity 3 and RB identity 4 (if established) equal to the START value included in the latest transmitted CELL UPDATE message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN.
- 2> if the CELL UPDATE CONFIRM message includes the IE "RLC re-establish indicator (RB5 and upwards)":
  - 3> for radio bearers with RB identity 5 and upwards:
    - 4> re-establish the AM RLC entities;
    - 4> if the value of the IE "Status" in the variable CIPHERING\_STATUS of the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS is set to "Started":
      - 5> set the HFN **component of the respective COUNT-C** values for AM RLC entities equal to the START value included in this CELL UPDATE message for the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS.
- 1> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected".
- 1> enter a state according to subclause 8.6.3.3 applied on the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message.

If the UE after state transition enters CELL\_DCH state, it shall:

- 1> not prohibit periodical status transmission in RLC;
- 1> for each CN domain for which a transparent mode radio bearer exists and for which the IE "Status" in the variable CIPHERING\_STATUS is set to "Started" for that CN domain:

- 2> choose an activation time for the ciphering on transparent mode radio bearers and include it in the response message in the IE "COUNT-C activation time";
- 2> set the 20 MSB of the MAC-d HFN with the corresponding START value in the most recently sent IE "START list";
- 2> set the remaining LSB of the MAC-d HFN to zero;
- 2> apply ciphering on the transparent mode radio bearers;
- 2> start incrementing the COUNT-C value from the CFN that has been included in the IE "COUNT-C activation time".

If the UE after state transition remains in CELL\_FACH state, it shall

- 1> start the timer T305 using its initial value if timer T305 is not running and periodical cell update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity";
- 1> select PRACH according to subclause 8.5.17;
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> not prohibit periodical status transmission in RLC;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 2> ignore that IE and stop using DRX.

If the UE after state transition enters URA\_PCH or CELL\_PCH state, it shall:

- 1> prohibit periodical status transmission in RLC;
- 1> clear the variable C\_RNTI;
- 1> stop using that C\_RNTI just cleared from the variable C\_RNTI in MAC;
- 1> start the timer T305 using its initial value if timer T305 is not running 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";
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 2> use the value in the IE "UTRAN DRX Cycle length coefficient" for calculating Paging Occasion and PICH Monitoring Occasion as specified in subclause 8.6.3.2 in CELL\_PCH state.
- 1> if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.

If the UE after the state transition remains in CELL\_FACH state; and

- 1> the contents of the variable C\_RNTI are empty:

it shall check the value of V302; and:

- 1> if V302 is equal to or smaller than N302:
  - 2> if, caused by the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:
    - 3> the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE; and/or
    - 3> the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE;
    - 4> abort the ongoing integrity and/or ciphering reconfiguration;

- 4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
  - 5> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
  - 5> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
  - 5> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
  - 5> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 2> in case of a URA update procedure:
  - 3> stop the URA update procedure; and
  - 3> continue with a cell update procedure.
- 2> set the contents of the CELL UPDATE message according to subclause 8.3.1.3, except for the IE "Cell update cause" which shall be set to "cell reselection";
- 2> submit the CELL UPDATE message for transmission on the uplink CCCH;
- 2> increment counter V302;
- 2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.
- 1> if V302 is greater than N302:
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
  - 2> in case of a cell update procedure:
    - 3> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 2> in case of a URA update procedure:
    - 3> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 2> release all its radio resources;
  - 2> 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;
  - 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 2> clear the variable ESTABLISHED\_RABS;
  - 2> enter idle mode;
  - 2> other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
  - 2> and the procedure ends.

If the UE after the state transition remains in CELL\_FACH state; and

- a C-RNTI is stored in the variable C\_RNTI;

or



- the UE after the state transition moves to another state than the CELL\_FACH state:

the UE shall:

- 1> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
  - 2> include and set the IE "Radio bearer uplink ciphering activation time info" in any response message transmitted below to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> in case of a cell update procedure:
  - 2> set the IE "RRC transaction identifier" in any response message transmitted below to the value of "RRC transaction identifier" in the entry for the CELL UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry.
- 1> in case of a URA update procedure:
  - 2> set the IE "RRC transaction identifier" in any response message transmitted below to the value of "RRC transaction identifier" in the entry for the URA UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
- 1> if the variable PDCP\_SN\_INFO is non-empty:
  - 2> include the IE "RB with PDCP information list" in any response message transmitted below and set it to the value of the variable PDCP\_SN\_INFO.
- 1> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message included the IE "Downlink counter synchronisation info":
  - 2> re-establish RB2;
  - 2> set the new uplink and downlink HFN component of the COUNT-C of RB2 to MAX(uplink HFN component of the COUNT-C of RB2, downlink HFN component of the COUNT-C of RB2);
  - 2> increment by one the downlink and uplink values of the HFN component of the COUNT-C values for RB2;
  - 2> calculate the START value according to subclause 8.5.9;
  - 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in any response message transmitted below.
- 1> transmit a response message as specified in subclause 8.3.1.7;
- 1> if the IE "Integrity protection mode info" was present in the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.
- 1> if the variable ORDERED\_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:
  - 2> set the variable ORDERED\_RECONFIGURATION to FALSE.
- 1> clear the variable PDCP\_SN\_INFO;
- 1> when the response message transmitted per subclause 8.3.1.7 to the UTRAN has been confirmed by RLC:
  - 2> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info":

- 3> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
- 3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
- 3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 2> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
  - 3> set "Uplink RRC Message sequence number" for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO to a value such that next RRC message to be sent on uplink RB0 will use the new integrity protection configuration;
  - 3> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
  - 3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE.
- 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 1> in case of a cell update procedure:
  - 2> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- 1> in case of a URA update procedure:
  - 2> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- 1> set the variable CELL\_UPDATE\_STARTED to FALSE;
- 1> clear the variable SECURITY\_MODIFICATION.

The procedure ends.

### 8.3.1.7 Transmission of a response message to UTRAN

If the CELL UPDATE CONFIRM message:

- includes the IE "RB information to release list":

the UE shall:

- 1> transmit a RADIO BEARER RELEASE COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include the IE "RB information to release list"; and
- includes the IE "RB information to reconfigure list"; or
- includes the IE "RB information to be affected list":

the UE shall:

- 1> transmit a RADIO BEARER RECONFIGURATION COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- includes "Transport channel information elements":

the UE shall:

- 1> transmit a TRANSPORT CHANNEL RECONFIGURATION COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- does not include "Transport channel information elements"; and
- includes "Physical channel information elements":

the UE shall:

- 1> transmit a PHYSICAL CHANNEL RECONFIGURATION COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- does not include "Transport channel information elements"; and
- does not include "Physical channel information elements"; and
- includes "CN information elements"; or
- includes the IE "Ciphering mode info"; or
- includes the IE "Integrity protection mode info"; or
- includes the IE "New C-RNTI"; or
- includes the IE "New U-RNTI":

the UE shall:

- 1> transmit a UTRAN MOBILITY INFORMATION CONFIRM as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- does not include "Transport channel information elements"; and
- does not include "Physical channel information elements"; and
- does not include "CN information elements"; and
- does not include the IE "Ciphering mode info"; and
- does not include the IE "Integrity protection mode info"; and
- does not include the IE "New C-RNTI"; and
- does not include the IE "New U-RNTI":

the UE shall:

- 1> transmit no response message.

If the URA UPDATE CONFIRM message:

- includes "CN information elements"; or
- includes the IE "Ciphering mode info"; or
- includes the IE "Integrity protection mode info"; or
- includes any one or both of the IEs "New C-RNTI" and "New U-RNTI":

the UE shall:

- 1> transmit a UTRAN MOBILITY INFORMATION CONFIRM as response message using AM RLC.

If the URA UPDATE CONFIRM message:

- does not include "CN information elements"; and
- does not include the IE "Ciphering mode info"; and
- does not include the IE "Integrity protection mode info"; and
- does not include the IE "New U-RNTI"; and
- does not include the IE "New C-RNTI":

the UE shall:

- 1> transmit no response message.

If the new state is CELL\_DCH or CELL\_FACH, the response message shall be transmitted using the new configuration after the state transition., and the UE shall:

- 1> if the IE "Downlink counter synchronisation info" was included in the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:
  - 2> when RLC has confirmed the successful transmission of the response message:
    - 3> re-establish all AM and UM RLC entities with RB identities larger than 4 and set the first 20 bits of all the HFN component of the COUNT-C values to the START value included in the response message for the corresponding CN domain;
    - 3> re-establish the RLC entities with RB identities 1, 3 and 4 and set the first 20 bits of all the HFN component of the COUNT-C values to the START value included in the response message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 3> set the remaining bits of the HFN component of the COUNT-C values of all UM RLC entities to zero;
    - 3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].
  - 1> if the variable PDCP\_SN\_INFO is empty:
    - 2> if the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
      - 3> when RLC has confirmed the successful transmission of the response message:
        - 4> continue with the remainder of the procedure.
      - 2> if the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message did not contain the IE "Ciphering mode info":
        - 3> when RLC has been requested to transmit the response message,
          - 4> continue with the remainder of the procedure.
    - 1> if the variable PDCP\_SN\_INFO non-empty:
      - 2> when RLC has confirmed the successful transmission of the response message:
        - 3> for each radio bearer in the variable PDCP\_SN\_INFO:
          - 4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
            - 5> configure the RLC entity for that radio bearer to "continue".
        - 3> continue with the remainder of the procedure.

If the new state is CELL\_PCH or URA\_PCH, the response message shall be transmitted in CELL\_FACH state, and the UE shall:

- 1> when RLC has confirmed the successful transmission of the response message:
  - 2> for each radio bearer in the variable PDCP\_SN\_INFO:
    - 3> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
      - 4> configure the RLC entity for that radio bearer to "continue".
  - 2> enter the new state (CELL\_PCH or URA\_PCH, respectively).
- 1> continue with the remainder of the procedure.

### 8.3.1.12 T302 expiry or cell reselection

If any or several of the following conditions are true:

- expiry of timer T302;
- reselection to another UTRA cell (including the previously serving cell) before completion of the cell update or URA update procedure;

the UE shall:

- 1> stop T302 if it is running;
- 1> if the UE was in CELL\_DCH state prior to the initiation of the procedure; and
  - 2> if timers T314 and T315 have elapsed while T302 was running:
    - 3> enter idle mode.
    - 3> 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. Other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2.
    - 3> and the procedure ends.
  - 2> if timer T314 has elapsed while T302 was running and,
    - 3> if "T314 expired" in the variable RB\_TIMER\_INDICATOR is set to FALSE and
    - 3> if T315 is still running:
      - 4> release locally all radio bearers which are associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT314";
      - 4> indicate release of those radio access bearers to upper layers;
      - 4> delete all information about those radio access bearers from the variable ESTABLISHED\_RABS;
      - 4> set "T314 expired" in the variable RB\_TIMER\_INDICATOR to TRUE.
  - 2> if timer T315 has elapsed while T302 was running and,
    - 3> if "T315 expired" in the variable RB\_TIMER\_INDICATOR is set to FALSE and,
    - 3> if T314 is still running:
      - 4> release locally all radio bearers which are associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT315";
      - 4> indicate release of those radio access bearers to upper layers;

- 4> delete all information about those radio access bearers from the variable ESTABLISHED\_RABS;
- 4> set "T315 expired" in the variable RB\_TIMER\_INDICATOR to TRUE.

1> check whether it is still in "in service area" (see subclause 8.5.5.2);

- ~~1> if, caused by the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE:~~
  - ~~2> abort the ongoing integrity and/or ciphering reconfiguration;~~
  - ~~2> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":~~
    - ~~3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and~~
    - ~~3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.~~
  - ~~2> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":~~
    - ~~3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and~~
    - ~~3> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.~~

1> if the variable ORDERED\_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:

- 2> set the variable ORDERED\_RECONFIGURATION to FALSE.

1> in case of a cell update procedure:

- 2> clear any entry for the CELL UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS.

1> in case of a URA update procedure:

- 2> clear any entry for the URA UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS.

If the UE detects "in service area" if it has not entered idle mode, and:

1> if V302 is equal to or smaller than N302, the UE shall:

- 2> if the UE performed cell re-selection:

- 3> delete its C-RNTI.

2> in case of a cell update procedure:

- 3> set the contents of the CELL UPDATE message according to subclause 8.3.1.3;

- 3> if, a CELL UPDATE CONFIRM message was received and caused the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE, and

- 3> if the IE "Downlink counter synchronisation info" was included in the received CELL UPDATE CONFIRM message;

- 4> apply the new security (integrity protection) configuration received in the CELL UPDATE CONFIRM on the CELL UPDATE message;

- 3> submit the CELL UPDATE message for transmission on the uplink CCCH.

2> in case of a URA update procedure:

- 3> set the contents of the URA UPDATE message according to subclause 8.3.1.3;

3> if a URA UPDATE CONFIRM message was received and caused the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE, and

3> if the IE "Downlink counter synchronisation info" was included in the received URA UPDATE CONFIRM message:

4> apply the new security (integrity protection) configuration received in the URA UPDATE CONFIRM on the URA UPDATE message:

3> submit the URA UPDATE message for transmission on the uplink CCCH.

2> increment counter V302;

2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.

1> if V302 is greater than N302, the UE shall:

2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;

2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;

2> clear the variable PDCP\_SN\_INFO;

2> in case of a cell update procedure:

3> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.

2> in case of a URA update procedure:

3> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.

2> release all its radio resources;

2> 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;

2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;

2> clear the variable ESTABLISHED\_RABS;

2> set the variable CELL\_UPDATE\_STARTED to FALSE;

2> enter idle mode;

2> other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;

2> and the procedure ends.

If the UE does not detect "in service area", it shall:

1> continue searching for "in service area".

### 8.3.3.3 Reception of UTRAN MOBILITY INFORMATION message by the UE

When the UE receives a UTRAN MOBILITY INFORMATION message, it shall:

1> act on received information elements as specified in subclause 8.6;

1> if the IE "UE Timers and constants in connected mode" is present:

- 2> store the values of the IE "UE Timers and constants in connected mode" in the variable TIMERS\_AND\_CONSTANTS, replacing any previously stored value for each timer and constant; and
- 2> for each updated timer value:
  - 3> start using the new value next time the timer is started;
- 2> for each updated constant value:
  - 3> start using the new value directly;
- 1> if the IE "CN domain specific DRX cycle length coefficient" is present:
  - 2> store the value of the IE "CN domain specific DRX cycle length coefficient" for that CN domain, replacing any previously stored value; and
  - 2> use the value to determine the connected mode paging occasions according to [4].
- 1> set the IE "RRC transaction identifier" in the UTRAN MOBILITY INFORMATION CONFIRM message to the value of "RRC transaction identifier" in the entry for the UTRAN MOBILITY INFORMATION message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected";
- 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
  - 2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the variable PDCP\_SN\_INFO is non-empty:
  - 2> include the IE "RB with PDCP information list" in the UTRAN MOBILITY INFORMATION CONFIRM message and set it to the value of the variable PDCP\_SN\_INFO.
- 1> if the received UTRAN MOBILITY INFORMATION message included the IE "Downlink counter synchronisation info":
  - 2> re-establish RB2;
  - 2> set the new uplink and downlink HFN **component of COUNT-C** of RB2 to MAX(uplink HFN **component of COUNT-C** of RB2, downlink HFN **component of COUNT-C** of RB2);
  - 2> increment by one the downlink and uplink **values of the HFN component of COUNT-C values** for RB2;
  - 2> calculate the START value according to subclause 8.5.9;
  - 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the UTRAN MOBILITY INFORMATION CONFIRM message.
- 1> transmit a UTRAN MOBILITY INFORMATION CONFIRM message on the uplink DCCH using AM RLC;
- 1> if the IE "Integrity protection mode info" was present in the UTRAN MOBILITY INFORMATION message:
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted UTRAN MOBILITY INFORMATION CONFIRM message.
- 1> if the IE "Downlink counter synchronisation info" was included in the received UTRAN MOBILITY INFORMATION message:
  - 2> when RLC has confirmed the successful transmission of the response message:



- 3> re-establish all AM and UM RLC entities with RB identities larger than 4 and set the first 20 bits of all the HFN **component of COUNT-C** values to the START value included in the response message for the corresponding CN domain;
  - 3> re-establish the RLC entities with RB identities 1, 3 and 4 and set the first 20 bits of all the HFN **component of COUNT-C** values to the START value included in the response message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
  - 3> set the remaining bits of the HFN **component of COUNT-C** values of all UM RLC entities to zero;
  - 3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].
- 1> if the variable PDCP\_SN\_INFO is empty; and
    - 2> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
      - 3> when RLC has confirmed the successful transmission of the UTRAN MOBILITY INFORMATION CONFIRM message, perform the actions below.
    - 2> if the UTRAN MOBILITY INFORMATION message did not contain the IE "Ciphering mode info":
      - 3> when RLC has been requested to transmit the UTRAN MOBILITY INFORMATION CONFIRM message, perform the actions below.
  - 1> if the variable PDCP\_SN\_INFO is non-empty:
    - 2> when RLC has confirmed the successful transmission of the UTRAN MOBILITY INFORMATION CONFIRM message:
      - 3> for each radio bearer in the variable PDCP\_SN\_INFO:
        - 4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
          - 5> configure the RLC entity for that radio bearer to "continue".
      - 3> clear the variable PDCP\_SN\_INFO.
  - 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
    - 2> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
    - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
    - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
  - 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Integrity protection mode info":
    - 2> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
    - 2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
    - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
  - 1> clear the variable SECURITY\_MODIFICATION.

The procedure ends.

#### 8.3.3.4 Reception of an UTRAN MOBILITY INFORMATION CONFIRM message by the UTRAN

When the network receives UTRAN MOBILITY INFORMATION CONFIRM message, UTRAN may delete any old U-RNTI. The procedure ends.

### 8.3.3.5 Cell re-selection

If the UE performs cell re-selection, the UE shall:

- 1> initiate a cell update procedure according to subclause 8.3.1;
- 1> if the UTRAN MOBILITY INFORMATION message contains the IE "New C-RNTI"; and
- 1> if the UE has not yet submitted the UTRAN MOBILITY INFORMATION CONFIRM message to lower layers for transmission; **and**
- 1> if the IE "Downlink counter synchronisation info" was not included in the received UTRAN MOBILITY INFORMATION message;**
  - 2> transmit a UTRAN MOBILITY INFORMATION FAILURE message on the uplink DCCH using AM RLC;
  - 2> set the IE "RRC transaction identifier" in the UTRAN MOBILITY INFORMATION FAILURE message to the value of "RRC transaction identifier" in the entry for the UTRAN MOBILITY INFORMATION message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry.
  - 2> set the IE "failure cause" to the cause value "cell update occurred";
  - 2> when the UTRAN MOBILITY INFORMATION FAILURE message has been submitted to lower layers for transmission:
    - 3> continue with any ongoing processes and procedures as if the invalid UTRAN MOBILITY INFORMATION message has not been received and the procedure ends.
- 1> otherwise:
  - 2> if a UTRAN MOBILITY INFORMATION message was received and caused the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE, and**
  - 2> if the IE "Downlink counter synchronisation info" was included in the received UTRAN MOBILITY INFORMATION message:**
    - 3> apply the new security (integrity protection) configuration received in the UTRAN MOBILITY INFORMATION message on the CELL UPDATE message to be transmitted;**
  - 2> continue the procedure normally.

### 8.6.3.5 Integrity protection mode info

The IE "Integrity protection mode info" defines the new integrity protection configuration. At any given time, the UE needs to store at most three different integrity protection configurations (keysets) in total for all signalling radio bearers for all CN domains.

If the IE "Integrity protection mode info" is present and if the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE, the UE shall:

- 1> ignore this second attempt to change the integrity protection configuration; and
- 1> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to TRUE.

If the IE "Integrity protection mode info" is present and if the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to FALSE, the UE shall:

- 1> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to TRUE;
- 1> if IE "Integrity protection mode command" has the value "start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and this IE was included in the message SECURITY MODE COMMAND:

- 2> initialise the information for all signalling radio bearers in the variable INTEGRITY\_PROTECTION\_INFO according to the following:
    - 3> set the IE "Uplink RRC Message sequence number" in the variable INTEGRITY\_PROTECTION\_INFO to zero;
    - 3> do not set the IE "Downlink RRC Message sequence number" in the variable INTEGRITY\_PROTECTION\_INFO;
    - 3> set the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO to zero for each signalling radio bearer in the IE "ESTABLISHED\_RABS".
  - 2> set the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO to the value "Started";
  - 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:
    - 3> using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";
    - 3> using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].
  - 2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer in the IE "ESTABLISHED\_RABS" except RB2 at the next received RRC message;
  - 2> start applying the new integrity protection configuration in the downlink for signalling radio bearer RB2 from and including the received SECURITY MODE COMMAND message;
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearers other than RB2 at the uplink activation time included in the IE "Uplink integrity protection activation info".
- 1> if IE "Integrity protection mode command" has the value "start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and this IE was not included SECURITY MODE COMMAND:

NOTE: This case is used in SRNS relocation

- 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:
  - 3> using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";
  - 3> using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].
- 2> let RB<sub>m</sub> be the signalling radio bearer where the reconfiguration message was received and let RB<sub>n</sub> be the signalling radio bearer where the response message is transmitted;
- 2> prohibit transmission of RRC messages on all signalling radio bearers in the IE "ESTABLISHED\_RABS" except on RB<sub>0</sub> and the radio bearer where the response message is transmitted;
- 2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer in the IE "ESTABLISHED\_RABS" except RB<sub>m</sub> at the next received RRC message;
- 2> start applying the new integrity protection configuration in the downlink for signalling radio bearer RB<sub>m</sub> from and including the received configuration message;
- 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB<sub>n</sub> from and including the transmitted response message;

- 2> start applying the new integrity protection configuration in the uplink for signalling radio bearers other than RBn at the uplink activation time included in the IE "Uplink integrity protection activation info".
- 1> if IE "Integrity protection mode command" has the value "modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and this IE was included in SECURITY MODE COMMAND:
    - 2> store the (oldest currently used) integrity protection configuration until activation times have elapsed for the new integrity protection configuration to be applied on all signalling radio bearers;
    - 2> if there are pending activation times set for integrity protection by a previous procedure changing the integrity protection configuration:
      - 3> apply the integrity protection configuration at this pending activation time as indicated in this procedure.
    - 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each signalling radio bearer n, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info";
    - 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1;
      - 3> if present, use the algorithm indicated by the IE "Integrity protection algorithm" (UIA [40]);
    - 2> set the content of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO according to the following:
      - 3> for each established signalling radio bearer, stored in the variable ESTABLISHED\_RABS:
        - 4> select a value of the RRC sequence number at which (activation) time the new integrity protection configuration shall be applied in uplink for that signalling radio bearer according to the following:
          - 5> for each signalling radio bearer that has no pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
            - 6> set a suitable value that would ensure a minimised delay in the change to the latest integrity protection configuration.
          - 5> for signalling radio bearer that has a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
            - 6> set the same value as the pending activation time for integrity protection;
          - 5> consider this (pending) activation time to be elapsed when the selected activation time (as above) is equal to the next RRC sequence number to be used, which means that the last RRC message using the old integrity protection configuration has been submitted to lower layers.
        - 4> for signalling radio bearer RB0:
          - 5> set the value of the included RRC sequence number to greater than or equal to the current value of the RRC sequence number for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO, plus the value of the constant N302 plus one.
        - 4> prohibit the transmission of RRC messages on all signalling radio bearers, except for RB2, with RRC SN greater than or equal to the value in the "RRC message sequence number list" for the signalling radio bearer in the IE "Uplink integrity protection activation info" of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
      - 2> start applying the new integrity protection configuration in the uplink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Uplink integrity protection activation info", included in the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
      - 2> start applying the new integrity protection configuration in the uplink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration;

- 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info";

NOTE: For signalling radio bearers that have a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration, UTRAN should set this value in IE "Downlink integrity protection activation info".

- 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration.

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and the IE "Integrity protection mode command info" was not included in the message SECURITY MODE COMMAND; or

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and the IE "Integrity protection mode info" was included in the message SECURITY MODE COMMAND, and the IE "Integrity protection algorithm" is not included; or

If the IE "Integrity protection mode command" has the value "Modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not Started"; or

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started", and the IE "Integrity protection mode command info" was included in the message SECURITY MODE COMMAND; or

If there does not exist exactly one integrity protection activation time in the IE "Downlink integrity protection activation info" for each established signalling radio bearer included in the IE "Signalling radio bearer information" in the IE "ESTABLISHED\_RABS"; or

If IE "Integrity protection mode command" has the value "Modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started", and the IE "Integrity protection mode info" was not included in the message SECURITY MODE COMMAND:

the UE shall:

- 1> ignore this attempt to change the integrity protection configuration; and
- 1> set the variable INVALID\_CONFIGURATION to TRUE.

If the IE "Integrity protection mode info" is not present, the UE shall:

- 1> not change the integrity protection configuration.

### 8.6.3.6 Void

# CHANGE REQUEST

⌘ **25.331 CR 1495** ⌘ rev **-** ⌘ Current version: **5.0.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Corrections to cell update interactions with security and SRNS Relocation		
<b>Source:</b>	⌘ TSG-RAN WG2		
<b>Work item code:</b>	⌘ TEI	<b>Date:</b>	⌘ May 13, 2002
<b>Category:</b>	⌘ <b>A</b>	<b>Release:</b>	⌘ REL-5
	<i>Use <u>one</u> of the following categories:</i> <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<i>Use <u>one</u> of the following releases:</i> <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>REL-4</b> (Release 4) <b>REL-5</b> (Release 5)

<b>Reason for change:</b> ⌘	<ol style="list-style-type: none"> <li>1. The actions for the UE in case of CELL UPDATE and UTRAN MOBILITY INFORMATION when performing a security reconfiguration during a CELL UPDATE CONFIRM procedure causing security reconfiguration are missing.</li> <li>2. It is stated that in case of a CELL UPDATE being triggered during security reconfiguration, the UE shall abort and revert back to its previous configuration. This would however require the UE to abandon the re-establishment of RB2 and revert back to the previous RB2 configuration - this is however not possible.</li> <li>3. It is incorrectly stated that in case of SRNS relocation the HFN components have to be modified following the re-establishment of the associated RB, when in fact only the HFN components of the COUNT-C values for that RB needs to be modified.</li> <li>4. Transmission on RB0 is prohibited - this would prevent a CELL UPDATE being sent during security reconfiguration.</li> </ol>
<b>1. Summary of change:</b> ⌘	<ol style="list-style-type: none"> <li>1. It is stated that the UE shall not abort the security reconfiguration if a CELL UPDATE occurs during a CELL UPDATE CONFIRM triggering a SRNS Relocation. UE actions in case of UTRAN MOBILITY INFORMATION procedure are stated - UE shall start a cell update procedure and continue with the UTRAN MOBILITY INFORMATION.</li> <li>2. It is stated that the UE shall release its radio resources if a cell reselection is triggered during a RB Reconfiguration procedure triggering SRNS Relocation. A note is added that the UTRAN should use RB Control messages for triggering SRNS Relocation only in case of CELL_DCH to CELL_DCH transitions. UE behavior in other cases is unspecified.</li> <li>3. It is now stated that only the HFN components of the COUNT-C values need to be modified or set following RB re-establishment during the SRNS relocation.</li> <li>4. Transmission on RB0 is now allowed during security reconfiguration.</li> </ol>

<b>Consequences if not approved:</b>	⌘	<ol style="list-style-type: none"> <li>1. UE actions on cell update in case of UTRAN MOBILITY INFORMATION causing security reconfiguration on SRNS relocation will be unspecified leading to unknown UE behavior. UE actions in case of cell update during an ongoing CELL UPDATE CONFIRM causing security reconfiguration will be difficult to implement causing unknown UE behavior.</li> <li>2. UE implementation will not be possible leading to unknown UE behavior.</li> <li>3. HFN components of COUNT-I may also be incorrectly modified causing loss of connection due to security failure.</li> <li>4. CELL UPDATE will not be sent causing loss of connection.</li> </ol>
--------------------------------------	---	--

<b>Clauses affected:</b>	⌘	8.2.2.3; 8.2.2.4; 8.2.2.12b; 8.3.1.6; 8.3.1.7; 8.3.1.12; 8.3.3.3; 8.3.3.5; 8.6.3.5										
<b>Other specs affected:</b>	⌘	<table border="1"> <tr> <td>Other core specifications</td> <td>⌘</td> <td>25.331 v3.10.0, CR 1493</td> </tr> <tr> <td>Test specifications</td> <td></td> <td>25.331 v4.4.0, CR 1494</td> </tr> <tr> <td>O&amp;M Specifications</td> <td></td> <td></td> </tr> </table>	Other core specifications	⌘	25.331 v3.10.0, CR 1493	Test specifications		25.331 v4.4.0, CR 1494	O&M Specifications			
Other core specifications	⌘	25.331 v3.10.0, CR 1493										
Test specifications		25.331 v4.4.0, CR 1494										
O&M Specifications												
<b>Other comments:</b>	⌘											

**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.

### 8.2.2.3 Reception of RADIO BEARER SETUP or RADIO BEARER RECONFIGURATION or RADIO BEARER RELEASE or TRANSPORT CHANNEL RECONFIGURATION or PHYSICAL CHANNEL RECONFIGURATION message by the UE

The UE shall be able to receive any of the following messages:

- RADIO BEARER SETUP message; or
- RADIO BEARER RECONFIGURATION message; or
- RADIO BEARER RELEASE message; or
- TRANSPORT CHANNEL RECONFIGURATION message; or
- PHYSICAL CHANNEL RECONFIGURATION message;

and perform a hard handover, even if no prior UE measurements have been performed on the target cell and/or frequency.

If the UE receives:

- a RADIO BEARER SETUP message; or
- a RADIO BEARER RECONFIGURATION message; or
- a RADIO BEARER RELEASE message; or
- a TRANSPORT CHANNEL RECONFIGURATION message; or
- a PHYSICAL CHANNEL RECONFIGURATION message;

it shall:

- 1> set the variable ORDERED\_RECONFIGURATION to TRUE;
- 1> perform the physical layer synchronisation procedure as specified in [29];
- 1> act upon all received information elements as specified in subclause 8.6, unless specified in the following and perform the actions below.

The UE may:

- 1> maintain a list of the set of cells to which the UE has Radio Links if the IE "Cell ID" is present.

The UE may first release the physical channel configuration used at reception of the reconfiguration message. The UE shall then:

- 1> in FDD, if the IE "PDSCH code mapping" is included but the IE "PDSCH with SHO DCH Info" is not included and if the DCH has only one link in its active set:
  - 2> act upon the IE "PDSCH code mapping" as specified in subclause 8.6; and
  - 2> infer that the PDSCH will be transmitted from the cell from which the downlink DPCH is transmitted.
- 1> enter a state according to subclause 8.6.3.3.

In case the UE receives a RADIO BEARER RECONFIGURATION message including the IE "RB information to reconfigure" that only includes the IE "RB identity", the UE shall:

- 1> handle the message as if IE "RB information to reconfigure" was absent.



NOTE: The RADIO BEARER RECONFIGURATION message always includes the IE "RB information to reconfigure". UTRAN has to include it even if it does not require the reconfiguration of any RB.

If after state transition the UE enters CELL\_DCH state, the UE shall, after the state transition:

- 1> remove any C-RNTI from MAC;
- 1> clear the variable C\_RNTI.

In FDD, if after state transition the UE leaves CELL\_DCH state, the UE shall, after the state transition:

- 1> remove any DSCH-RNTI from MAC;
- 1> clear the variable DSCH\_RNTI.

If the UE was in CELL\_DCH state upon reception of the reconfiguration message and remains in CELL\_DCH state, the UE shall:

- 1> if the IE "Uplink DPCH Info" is absent, not change its current UL Physical channel configuration;
- 1> if the IE "Downlink information for each radio link" is absent, not change its current DL Physical channel configuration;
- 1> if "DPCH frame offset" is included for one or more RLS in the active set:
  - 2> use its value to determine the beginning of the DPCH frame in accordance with the following:
    - 3> if the received IE "DPCH frame offset" is across the value range border compared to the DPCH frame offset currently used by the UE:
      - 4> consider it to be a request to adjust the timing with 256 chips across the frame border (e.g. if the UE receives value 0 while the value currently used is 38144 consider this as a request to adjust the timing with +256 chips).
    - 3> if after taking into account value range borders, the received IE "DPCH frame offset" corresponds to a request to adjust the timing with a step exceeding 256 chips:
      - 4> set the variable INVALID\_CONFIGURATION to FALSE.
  - 3> and the procedure ends.
- 2> adjust the radio link timing accordingly.

If after state transition the UE enters CELL\_FACH state, the UE shall, after the state transition:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4] on that frequency.
- 1> if the IE "Frequency info" is not included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4].
- 1> if the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selects another cell than indicated by this IE or the received reconfiguration message did not include the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD):
  - 2> initiate a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";
  - 2> when the cell update procedure completed successfully:
    - 3> if the UE is in CELL\_PCH or URA\_PCH state:
      - 4> initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
      - 4> proceed as below.

- 1> start timer T305 using its initial value if timer T305 is not running and if periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" in system information block type 1;
- 1> select PRACH according to subclause 8.5.17;
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> use the transport format set given in system information;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 2> ignore that IE and stop using DRX.
- 1> remove any H-RNTI stored;
- 1> clear the variable H\_RNTI;
- 1> if the contents of the variable C\_RNTI is empty:
  - 2> perform a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";
  - 2> when the cell update procedure completed successfully:
    - 3> if the UE is in CELL\_PCH or URA\_PCH state:
      - 4> initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
      - 4> proceed as below.

If the UE was in CELL\_FACH state upon reception of the reconfiguration message and remains in CELL\_FACH state, the UE shall:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4] on that frequency;
  - 2> if the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE or the received reconfiguration message did not include the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD):
    - 3> initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
    - 3> when the cell update procedure completed successfully:
      - 4> proceed as below.

The UE shall transmit a response message as specified in subclause 8.2.2.4, setting the information elements as specified below. The UE shall:

- 1> if the received reconfiguration message included the IE "Downlink counter synchronisation info"; or
- 1> if the received reconfiguration message is a RADIO BEARER RECONFIGURATION and the IE "New U-RNTI" is included:
  - 2> re-establish RB2;
  - 2> set the new uplink and downlink HFN **component of COUNT-C** of RB2 to MAX(uplink HFN **component of COUNT-C** of RB2, downlink HFN **component of COUNT-C** of RB2);
  - 2> increment by one the downlink and uplink values of the HFN **component of COUNT-C** ~~values~~ for RB2;
  - 2> calculate the START value according to subclause 8.5.9;
  - 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".

- 1> if the received reconfiguration message did not include the IE "Downlink counter synchronisation info":
  - 2> if the variable START\_VALUE\_TO\_TRANSMIT is set:
    - 3> include and set the IE "START" to the value of that variable.
  - 2> if the variable START\_VALUE\_TO\_TRANSMIT is not set and the IE "New U-RNTI" is included:
    - 3> calculate the START value according to subclause 8.5.9;
    - 3> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
  - 2> if the received reconfiguration message caused a change in the RLC size for any RB using RLC-AM:
    - 3> calculate the START value according to subclause 8.5.9;
    - 3> include the calculated START values for the CN domain associated with the corresponding RB identity in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info":
  - 2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the received reconfiguration message did not contain the IE "Ciphering activation time for DPCH" in IE "Ciphering mode info":
  - 2> if prior to this procedure there exist no transparent mode RLC radio bearers:
    - 3> if, at the conclusion of this procedure, the UE will be in CELL\_DCH state; and
    - 3> if, at the conclusion of this procedure, at least one transparent mode RLC radio bearer exists:
      - 4> include the IE "COUNT-C activation time" and specify a CFN value for this IE.
  - 2> if prior to this procedure there exists at least one transparent mode RLC radio bearer:
    - 3> if, at the conclusion of this procedure, no transparent mode RLC radio bearers exist:
      - 4> include the IE "COUNT-C activation time" and specify a CFN value for this IE.
- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the received message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> if the variable PDCP\_SN\_INFO is not empty:
  - 2> include the IE "RB with PDCP information list" and set it to the value of the variable PDCP\_SN\_INFO.
- 1> in TDD, if the procedure is used to perform a handover to a cell where timing advance is enabled, and the UE can calculate the timing advance value in the new cell (i.e. in a synchronous TDD network):
  - 2> set the IE "Uplink Timing Advance" according to subclause 8.6.6.26.
- 1> if the IE "Integrity protection mode info" was present in the received reconfiguration message:
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.

If after state transition the UE enters CELL\_PCH or URA\_PCH state, the UE shall, after the state transition and transmission of the response message:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4] on that frequency.
- 1> if the IE "Frequency info" is not included in the received reconfiguration message:
  - 2> select a suitable UTRA cell according to [4].
- 1> prohibit periodical status transmission in RLC;
- 1> remove any C-RNTI from MAC;
- 1> clear the variable C\_RNTI;
- 1> remove any H-RNTI stored;
- 1> clear the variable H\_RNTI;
- 1> start timer T305 using its initial value if timer T305 is not running and if periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" in system information block type 1;
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 2> use the value in the IE "UTRAN DRX Cycle length coefficient" for calculating Paging occasion and PICH Monitoring Occasion as specified in subclause 8.6.3.2.
- 1> if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:
  - 2> set the variable INVALID\_CONFIGURATION to TRUE.
- 1> if the UE enters CELL\_PCH state from CELL\_DCH state, and the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE or the received reconfiguration message did not include the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD):
  - 2> initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
  - 2> when the cell update procedure completed successfully:
    - 3> the procedure ends.
- 1> if the UE enters CELL\_PCH state from CELL\_FACH state, and the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE:
  - 2> initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
  - 2> when the cell update procedure is successfully completed:
    - 3> the procedure ends.
- 1> if the UE enters URA\_PCH state, and after cell selection the criteria for URA update caused by "URA reselection" according to subclause 8.3.1 is fulfilled:
  - 2> initiate a URA update procedure according to subclause 8.3.1 using the cause "URA reselection";
  - 2> when the URA update procedure is successfully completed:
    - 3> the procedure ends.

#### 8.2.2.4 Transmission of a response message by the UE, normal case

In case the procedure was triggered by reception of a RADIO BEARER SETUP message, the UE shall:

- 1> transmit a RADIO BEARER SETUP COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a RADIO BEARER RECONFIGURATION message, the UE shall:

- 1> transmit a RADIO BEARER RECONFIGURATION COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a RADIO BEARER RELEASE message, the UE shall:

- 1> transmit a RADIO BEARER RELEASE COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a TRANSPORT CHANNEL RECONFIGURATION message, the UE shall:

- 1> transmit a TRANSPORT CHANNEL RECONFIGURATION COMPLETE as response message on the uplink DCCH using AM RLC.

In case the procedure was triggered by reception of a PHYSICAL CHANNEL RECONFIGURATION message, the UE shall:

- 1> transmit a PHYSICAL CHANNEL RECONFIGURATION COMPLETE as response message on the uplink DCCH using AM RLC.

If the new state is CELL\_DCH or CELL\_FACH, the response message shall be transmitted using the new configuration after the state transition, and the UE shall:

- 1> if the IE "Downlink counter synchronisation info" was included in the reconfiguration message; or
- 1> if the received reconfiguration message is a RADIO BEARER RECONFIGURATION and the IE "New U-RNTI" is included:
  - 2> when RLC has confirmed the successful transmission of the response message:
    - 3> re-establish all AM and UM RLC entities with RB identities larger than 4 and set the first 20 bits of all the ~~HFN~~ **component of COUNT-C** values to the START value included in the response message for the corresponding CN domain;
    - 3> re-establish the RLC entities with RB identities 1, 3 and 4 and set the first 20 bits of all the ~~HFN~~ **component of COUNT-C** values to the START value included in the response message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 3> set the remaining bits of the HFN **component of COUNT-C** values of all UM RLC entities to zero;
    - 3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].

1> if the variable PDCP\_SN\_INFO is empty:

- 2> if the received reconfiguration message contained the IE "Ciphering mode info":
  - 3> when RLC has confirmed the successful transmission of the response message:
    - 4> notify upper layers upon change of the security configuration;
    - 4> perform the actions below.
- 2> if the received reconfiguration message did not contain the IE "Ciphering mode info":
  - 3> when RLC has been requested to transmit the response message:
    - 4> perform the actions below.

- 1> if the variable PDCP\_SN\_INFO is non-empty:
  - 2> when RLC has confirmed the successful transmission of the response message:
    - 3> for each radio bearer in the variable PDCP\_SN\_INFO:
      - 4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
        - 5> configure the RLC entity for that radio bearer to "continue".
    - 3> perform the actions below.

If the new state is CELL\_PCH or URA\_PCH, the response message shall be transmitted using the old configuration before the state transition, but the new C-RNTI shall be used if the IE "New C-RNTI" was included in the received reconfiguration message, and the UE shall:

- 1> when RLC has confirmed the successful transmission of the response message:
  - 2> for each radio bearer in the variable PDCP\_SN\_INFO:
    - 3> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
      - 4> configure the RLC entity for that radio bearer to "continue".
    - 2> enter the new state (CELL\_PCH or URA\_PCH, respectively);
    - 2> perform the actions below.

The UE shall:

- 1> set the variable ORDERED\_RECONFIGURATION to FALSE;
- 1> if the received reconfiguration message contained the IE "Ciphering mode info":
  - 2> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
  - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the received reconfiguration message contained the IE "Integrity protection mode info":
  - 2> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
  - 2> set "Uplink RRC Message sequence number" for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO to a value such that next RRC message to be sent on uplink RB0 will use the new integrity protection configuration;
  - 2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 1> clear the variable PDCP\_SN\_INFO;
- 1> clear the variable START\_VALUE\_TO\_TRANSMIT;
- 1> clear the variable SECURITY\_MODIFICATION.

#### 8.2.2.12b Cell update procedure during security reconfiguration

If:

- a cell update procedure according to subclause 8.3.1 is initiated; and
- the received reconfiguration message causes either:
  - the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE; and/or

- the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE:

the UE shall:

1> release all radio resources;

1> indicate the release 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; and

1> clear any entry for the RRC CONNECTION RELEASE message in the tables "Accepted transactions" and "Rejected transactions" in the variable TRANSACTIONS;

1> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;

1> clear the variable ESTABLISHED\_RABS;

1> if the received reconfiguration message contained the IE "Ciphering mode info":

2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and

2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;

2> clear the variable SECURITY\_MODIFICATION;

1> if the received reconfiguration message contained the IE "Integrity protection mode info":

2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and

2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;

1> enter idle mode;

1> perform the actions specified in subclause 8.5.2 when entering idle mode.

1> and the procedure ends.

NOTE: UTRAN should use RB Control messages to perform a SRNS relocation only in case of state transitions from Cell-DCH to Cell-DCH.

~~1> abort the ongoing integrity and/or ciphering reconfiguration;~~

~~1> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;~~

~~1> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;~~

~~1> if the received reconfiguration message contained the IE "Ciphering mode info":~~

~~2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and~~

~~2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;~~

~~1> if the received reconfiguration message contained the IE "Integrity protection mode info":~~

~~2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and~~

~~2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.~~

~~1> continue with any ongoing processes and procedures as if the reconfiguration message was not received.~~

~~The procedure ends.~~

### 8.3.1.6 Reception of the CELL UPDATE CONFIRM/URA UPDATE CONFIRM message by the UE

When the UE receives a CELL UPDATE CONFIRM/URA UPDATE CONFIRM message; and

- if the message is received on the CCCH, and IE "U-RNTI" is present and has the same value as the variable U\_RNTI; or
- if the message is received on DCCH:

the UE may:

- 1> maintain a list of the set of cells to which the UE has Radio Links if the IE "Cell ID" is present.

the UE shall:

- 1> stop timer T302;

- 1> in case of a cell update procedure and the CELL UPDATE CONFIRM message:

- 2> includes "RB information elements"; and/or

- 2> includes "Transport channel information elements"; and/or

- 2> includes "Physical channel information elements"; and

- 2> if the variable ORDERED\_RECONFIGURATION is set to FALSE:

- 3> set the variable ORDERED\_RECONFIGURATION to TRUE.

- 1> act upon all received information elements as specified in subclause 8.6, unless specified otherwise in the following:

- 2> if the IE "Frequency info" is included in the message:

- 3> if the IE "RRC State Indicator" is set to the value "CELL\_FACH" or "CELL\_PCH" or "URA\_PCH":

- 4> select a suitable UTRA cell according to [4] on that frequency;

- 4> act as specified in subclause 8.3.1.12.

- 3> if the IE "RRC State Indicator" is set to the value "CELL\_DCH":

- 4> act on the IE "Frequency info" as specified in subclause 8.6.6.1.

- 2> use the transport channel(s) applicable for the physical channel types that is used; and

- 2> if the IE "TFS" is neither included nor previously stored in the UE for that transport channel(s):

- 3> use the TFS given in system information.

- 2> if none of the TFS stored is compatible with the physical channel:

- 3> delete the stored TFS;

- 3> use the TFS given in system information.

- 2> perform the physical layer synchronisation procedure as specified in [29];

- 2> if the CELL UPDATE CONFIRM message includes the IE "RLC re-establish indicator (RB2, RB3 and RB4)":

- 3> re-establish the RLC entities for signalling radio bearer RB2, signalling radio bearer RB3 and signalling radio bearer RB4 (if established);

- 3> if the value of the IE "Status" in the variable CIPHERING\_STATUS of the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN is set to "Started":

- 4> set the HFN **components of the respective COUNT-C** values for AM RLC entities with RB identity 2, RB identity 3 and RB identity 4 (if established) equal to the START value included in the latest transmitted CELL UPDATE message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN.



- 2> if the CELL UPDATE CONFIRM message includes the IE "RLC re-establish indicator (RB5 and upwards)":
  - 3> for radio bearers with RB identity 5 and upwards:
    - 4> re-establish the AM RLC entities;
    - 4> if the value of the IE "Status" in the variable CIPHERING\_STATUS of the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS is set to "Started":
      - 5> set the HFN **components of the respective COUNT-C** values for AM RLC entities equal to the START value included in this CELL UPDATE message for the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED\_RABS.

1> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":

- 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected".

1> enter a state according to subclause 8.6.3.3 applied on the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message.

If the UE after state transition enters CELL\_DCH state, it shall:

- 1> not prohibit periodical status transmission in RLC;
- 1> for each CN domain for which a transparent mode radio bearer exists and for which the IE "Status" in the variable CIPHERING\_STATUS is set to "Started" for that CN domain:
  - 2> choose an activation time for the ciphering on transparent mode radio bearers and include it in the response message in the IE "COUNT-C activation time";
  - 2> set the 20 MSB of the MAC-d HFN with the corresponding START value in the most recently sent IE "START list";
  - 2> set the remaining LSB of the MAC-d HFN to zero;
  - 2> apply ciphering on the transparent mode radio bearers;
  - 2> start incrementing the COUNT-C value from the CFN that has been included in the IE "COUNT-C activation time".

If the UE after state transition remains in CELL\_FACH state, it shall

- 1> start the timer T305 using its initial value if timer T305 is not running and periodical cell update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity";
- 1> select PRACH according to subclause 8.5.17;
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> not prohibit periodical status transmission in RLC;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 2> ignore that IE and stop using DRX.

If the UE after state transition enters URA\_PCH or CELL\_PCH state, it shall:

- 1> prohibit periodical status transmission in RLC;
- 1> clear the variable C\_RNTI;
- 1> stop using that C\_RNTI just cleared from the variable C\_RNTI in MAC;

1> start the timer T305 using its initial value if timer T305 is not running 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";

1> select Secondary CCPCH according to subclause 8.5.19;

1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:

2> use the value in the IE "UTRAN DRX Cycle length coefficient" for calculating Paging Occasion and PICH Monitoring Occasion as specified in subclause 8.6.3.2 in CELL\_PCH state.

1> if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:

2> set the variable INVALID\_CONFIGURATION to TRUE.

If the UE after the state transition remains in CELL\_FACH state; and

1> the contents of the variable C\_RNTI are empty:

it shall check the value of V302; and:

1> if V302 is equal to or smaller than N302:

2> if, caused by the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:

3> the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE; and/or

3> the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE:

4> abort the ongoing integrity and/or ciphering reconfiguration;

4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":

5> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and

5> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.

4> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":

5> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and

5> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.

2> in case of a URA update procedure:

3> stop the URA update procedure; and

3> continue with a cell update procedure.

2> set the contents of the CELL UPDATE message according to subclause 8.3.1.3, except for the IE "Cell update cause" which shall be set to "cell reselection";

2> submit the CELL UPDATE message for transmission on the uplink CCCH;

2> increment counter V302;

2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.

1> if V302 is greater than N302:

2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;

2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;

2> in case of a cell update procedure:

- 3> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- 2> in case of a URA update procedure:
  - 3> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 2> release all its radio resources;
  - 2> 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;
  - 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
  - 2> clear the variable ESTABLISHED\_RABS;
  - 2> enter idle mode;
  - 2> other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
  - 2> and the procedure ends.

If the UE after the state transition remains in CELL\_FACH state; and

- a C-RNTI is stored in the variable C\_RNTI;

or

- the UE after the state transition moves to another state than the CELL\_FACH state:

the UE shall:

- 1> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
  - 2> include and set the IE "Radio bearer uplink ciphering activation time info" in any response message transmitted below to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> in case of a cell update procedure:
  - 2> set the IE "RRC transaction identifier" in any response message transmitted below to the value of "RRC transaction identifier" in the entry for the CELL UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry.
- 1> in case of a URA update procedure:
  - 2> set the IE "RRC transaction identifier" in any response message transmitted below to the value of "RRC transaction identifier" in the entry for the URA UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS; and
  - 2> clear that entry;
- 1> if the variable PDCP\_SN\_INFO is non-empty:
  - 2> include the IE "RB with PDCP information list" in any response message transmitted below and set it to the value of the variable PDCP\_SN\_INFO.
- 1> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message included the IE "Downlink counter synchronisation info":
  - 2> re-establish RB2;

- 2> set the new uplink and downlink HFN component of the COUNT-C of RB2 to MAX(uplink HFN component of the COUNT-C of RB2, downlink HFN component of the COUNT-C of RB2);
  - 2> increment by one the downlink and uplink values of the HFN component of the COUNT-C values for RB2;
  - 2> calculate the START value according to subclause 8.5.9;
  - 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in any response message transmitted below.
- 1> transmit a response message as specified in subclause 8.3.1.7;
- 1> if the IE "Integrity protection mode info" was present in the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:
    - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.
  - 1> if the variable ORDERED\_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:
    - 2> set the variable ORDERED\_RECONFIGURATION to FALSE.
  - 1> clear the variable PDCP\_SN\_INFO;
  - 1> when the response message transmitted per subclause 8.3.1.7 to the UTRAN has been confirmed by RLC:
    - 2> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
      - 3> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
      - 3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
      - 3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
    - 2> if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
      - 3> set "Uplink RRC Message sequence number" for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO to a value such that next RRC message to be sent on uplink RB0 will use the new integrity protection configuration;
      - 3> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
      - 3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE.
    - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
  - 1> in case of a cell update procedure:
    - 2> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 1> in case of a URA update procedure:
    - 2> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - 1> set the variable CELL\_UPDATE\_STARTED to FALSE;
  - 1> clear the variable SECURITY\_MODIFICATION.

The procedure ends.

### 8.3.1.7 Transmission of a response message to UTRAN

If the CELL UPDATE CONFIRM message:

- includes the IE "RB information to release list":

the UE shall:

- 1> transmit a RADIO BEARER RELEASE COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include the IE "RB information to release list"; and
- includes the IE "RB information to reconfigure list"; or
- includes the IE "RB information to be affected list":

the UE shall:

- 1> transmit a RADIO BEARER RECONFIGURATION COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- includes "Transport channel information elements":

the UE shall:

- 1> transmit a TRANSPORT CHANNEL RECONFIGURATION COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- does not include "Transport channel information elements"; and
- includes "Physical channel information elements":

the UE shall:

- 1> transmit a PHYSICAL CHANNEL RECONFIGURATION COMPLETE as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- does not include "Transport channel information elements"; and
- does not include "Physical channel information elements"; and
- includes "CN information elements"; or
- includes the IE "Ciphering mode info"; or
- includes the IE "Integrity protection mode info"; or
- includes the IE "New C-RNTI"; or
- includes the IE "New U-RNTI":

the UE shall:

- 1> transmit a UTRAN MOBILITY INFORMATION CONFIRM as response message using AM RLC.

If the CELL UPDATE CONFIRM message:

- does not include "RB information elements"; and
- does not include "Transport channel information elements"; and
- does not include "Physical channel information elements"; and
- does not include "CN information elements"; and
- does not include the IE "Ciphering mode info"; and
- does not include the IE "Integrity protection mode info"; and
- does not include the IE "New C-RNTI"; and
- does not include the IE "New U-RNTI";

the UE shall:

- 1> transmit no response message.

If the URA UPDATE CONFIRM message:

- includes "CN information elements"; or
- includes the IE "Ciphering mode info"; or
- includes the IE "Integrity protection mode info"; or
- includes any one or both of the IEs "New C-RNTI" and "New U-RNTI";

the UE shall:

- 1> transmit a UTRAN MOBILITY INFORMATION CONFIRM as response message using AM RLC.

If the URA UPDATE CONFIRM message:

- does not include "CN information elements"; and
- does not include the IE "Ciphering mode info"; and
- does not include the IE "Integrity protection mode info"; and
- does not include the IE "New U-RNTI"; and
- does not include the IE "New C-RNTI";

the UE shall:

- 1> transmit no response message.

If the new state is CELL\_DCH or CELL\_FACH, the response message shall be transmitted using the new configuration after the state transition., and the UE shall:

- 1> if the IE "Downlink counter synchronisation info" was included in the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:
  - 2> when RLC has confirmed the successful transmission of the response message:
    - 3> re-establish all AM and UM RLC entities with RB identities larger than 4 and set the first 20 bits of all the HFN **component of the respective COUNT-C** values to the START value included in the response message for the corresponding CN domain;
    - 3> re-establish the RLC entities with RB identities 1, 3 and 4 and set the first 20 bits of all the HFN **component of the respective COUNT-C** values to the START value included in the response message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 3> set the remaining bits of the HFN **component of the COUNT-C** values of all UM RLC entities to zero;

3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].

1> if the variable PDCP\_SN\_INFO is empty:

2> if the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":

3> when RLC has confirmed the successful transmission of the response message:

4> continue with the remainder of the procedure.

2> if the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message did not contain the IE "Ciphering mode info":

3> when RLC has been requested to transmit the response message,

4> continue with the remainder of the procedure.

1> if the variable PDCP\_SN\_INFO non-empty:

2> when RLC has confirmed the successful transmission of the response message:

3> for each radio bearer in the variable PDCP\_SN\_INFO:

4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":

5> configure the RLC entity for that radio bearer to "continue".

3> continue with the remainder of the procedure.

If the new state is CELL\_PCH or URA\_PCH, the response message shall be transmitted in CELL\_FACH state, and the UE shall:

1> when RLC has confirmed the successful transmission of the response message:

2> for each radio bearer in the variable PDCP\_SN\_INFO:

3> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":

4> configure the RLC entity for that radio bearer to "continue".

2> enter the new state (CELL\_PCH or URA\_PCH, respectively).

1> continue with the remainder of the procedure.

### 8.3.1.12 T302 expiry or cell reselection

If any or several of the following conditions are true:

- expiry of timer T302;
- reselection to another UTRA cell (including the previously serving cell) before completion of the cell update or URA update procedure;

the UE shall:

1> stop T302 if it is running;

1> if the UE was in CELL\_DCH state prior to the initiation of the procedure; and

2> if timers T314 and T315 have elapsed while T302 was running:

3> enter idle mode.

3> 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. Other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2.

- 3> and the procedure ends.
- 2> if timer T314 has elapsed while T302 was running and,
  - 3> if "T314 expired" in the variable RB\_TIMER\_INDICATOR is set to FALSE and
  - 3> if T315 is still running:
    - 4> release locally all radio bearers which are associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT314";
    - 4> indicate release of those radio access bearers to upper layers;
    - 4> delete all information about those radio access bearers from the variable ESTABLISHED\_RABS;
    - 4> set "T314 expired" in the variable RB\_TIMER\_INDICATOR to TRUE.
- 2> if timer T315 has elapsed while T302 was running and,
  - 3> if "T315 expired" in the variable RB\_TIMER\_INDICATOR is set to FALSE and,
  - 3> if T314 is still running:
    - 4> release locally all radio bearers which are associated with any radio access bearers for which in the variable ESTABLISHED\_RABS the value of the IE "Re-establishment timer" is set to "useT315";
    - 4> indicate release of those radio access bearers to upper layers;
    - 4> delete all information about those radio access bearers from the variable ESTABLISHED\_RABS;
    - 4> set "T315 expired" in the variable RB\_TIMER\_INDICATOR to TRUE.
- 1> check whether it is still in "in service area" (see subclause 8.5.5.2);
- ~~1> if, caused by the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message the IE "Reconfiguration" in the variable CIPHERING\_STATUS is set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE:~~
- ~~2> abort the ongoing integrity and/or ciphering reconfiguration;~~
- ~~2> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":~~
  - ~~3> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and~~
  - ~~3> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.~~
- ~~2> if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":~~
  - ~~3> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and~~
  - ~~3> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.~~
- 1> if the variable ORDERED\_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:
  - 2> set the variable ORDERED\_RECONFIGURATION to FALSE.
- 1> in case of a cell update procedure:
  - 2> clear any entry for the CELL UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS.
- 1> in case of a URA update procedure:



- 2> clear any entry for the URA UPDATE CONFIRM message in the table "Accepted transactions" in the variable TRANSACTIONS.

If the UE detects "in service area" if it has not entered idle mode, and:

- 1> if V302 is equal to or smaller than N302, the UE shall:

- 2> if the UE performed cell re-selection:

- 3> delete its C-RNTI.

- 2> in case of a cell update procedure:

- 3> set the contents of the CELL UPDATE message according to subclause 8.3.1.3;

- 3> if a CELL UPDATE CONFIRM message was received and caused the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE, and

- 3> if the IE "Downlink counter synchronisation info" was included in the received CELL UPDATE CONFIRM message;

- 4> apply the new security (integrity protection) configuration received in the CELL UPDATE CONFIRM on the CELL UPDATE message;

- 3> submit the CELL UPDATE message for transmission on the uplink CCCH.

- 2> in case of a URA update procedure:

- 3> set the contents of the URA UPDATE message according to subclause 8.3.1.3;

- 3> if a URA UPDATE CONFIRM message was received and caused the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE, and

- 3> if the IE "Downlink counter synchronisation info" was included in the received URA UPDATE CONFIRM message;

- 4> apply the new security (integrity protection) configuration received in the URA UPDATE CONFIRM on the URA UPDATE message;

- 3> submit the URA UPDATE message for transmission on the uplink CCCH.

- 2> increment counter V302;

- 2> restart timer T302 when the MAC layer indicates success or failure to transmit the message.

- 1> if V302 is greater than N302, the UE shall:

- 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO;

- 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;

- 2> clear the variable PDCP\_SN\_INFO;

- 2> in case of a cell update procedure:

- 3> clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.

- 2> in case of a URA update procedure:

- 3> clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.

- 2> release all its radio resources;

- 2> 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;
- 2> clear the variable ESTABLISHED\_SIGNALLING\_CONNECTIONS;
- 2> clear the variable ESTABLISHED\_RABS;
- 2> set the variable CELL\_UPDATE\_STARTED to FALSE;
- 2> enter idle mode;
- 2> other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
- 2> and the procedure ends.

If the UE does not detect "in service area", it shall:

- 1> continue searching for "in service area".

### 8.3.3.3 Reception of UTRAN MOBILITY INFORMATION message by the UE

When the UE receives a UTRAN MOBILITY INFORMATION message, it shall:

- 1> act on received information elements as specified in subclause 8.6;
- 1> if the IE "UE Timers and constants in connected mode" is present:
  - 2> store the values of the IE "UE Timers and constants in connected mode" in the variable TIMERS\_AND\_CONSTANTS, replacing any previously stored value for each timer and constant; and
  - 2> for each updated timer value:
    - 3> start using the new value next time the timer is started;
  - 2> for each updated constant value:
    - 3> start using the new value directly;
- 1> if the IE "CN domain specific DRX cycle length coefficient" is present:
  - 2> store the value of the IE "CN domain specific DRX cycle length coefficient" for that CN domain, replacing any previously stored value; and
  - 2> use the value to determine the connected mode paging occasions according to [4].
- 1> set the IE "RRC transaction identifier" in the UTRAN MOBILITY INFORMATION CONFIRM message to the value of "RRC transaction identifier" in the entry for the UTRAN MOBILITY INFORMATION message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - 2> set the IE "Status" in the variable SECURITY\_MODIFICATION for all the CN domains in the variable SECURITY\_MODIFICATION to "Affected";
- 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
  - 2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the variable PDCP\_SN\_INFO is non-empty:

- 2> include the IE "RB with PDCP information list" in the UTRAN MOBILITY INFORMATION CONFIRM message and set it to the value of the variable PDCP\_SN\_INFO.
- 1> if the received UTRAN MOBILITY INFORMATION message included the IE "Downlink counter synchronisation info":
- 2> re-establish RB2;
  - 2> set the new uplink and downlink HFN component of COUNT-C of RB2 to MAX(uplink HFN component of COUNT-C of RB2, downlink HFN component of COUNT-C of RB2);
  - 2> increment by one the downlink and uplink values of the HFN component of COUNT-C values for RB2;
  - 2> calculate the START value according to subclause 8.5.9;
  - 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the UTRAN MOBILITY INFORMATION CONFIRM message.
- 1> transmit a UTRAN MOBILITY INFORMATION CONFIRM message on the uplink DCCH using AM RLC;
- 1> if the IE "Integrity protection mode info" was present in the UTRAN MOBILITY INFORMATION message:
- 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted UTRAN MOBILITY INFORMATION CONFIRM message.
- 1> if the IE "Downlink counter synchronisation info" was included in the received UTRAN MOBILITY INFORMATION message:
- 2> when RLC has confirmed the successful transmission of the response message:
    - 3> re-establish all AM and UM RLC entities with RB identities larger than 4 and set the first 20 bits of all the HFN component of the respective COUNT-C values to the START value included in the response message for the corresponding CN domain;
    - 3> re-establish the RLC entities with RB identities 1, 3 and 4 and set the first 20 bits of all the HFN component of the respective COUNT-C values to the START value included in the response message for the CN domain stored in the variable LATEST\_CONFIGURED\_CN\_DOMAIN;
    - 3> set the remaining bits of the HFN component of the COUNT-C values of all UM RLC entities to zero;
    - 3> re-initialise the PDCP header compression entities of each radio bearer in the variable ESTABLISHED\_RABS as specified in [36].
- 1> if the variable PDCP\_SN\_INFO is empty; and
- 2> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
    - 3> when RLC has confirmed the successful transmission of the UTRAN MOBILITY INFORMATION CONFIRM message, perform the actions below.
  - 2> if the UTRAN MOBILITY INFORMATION message did not contain the IE "Ciphering mode info":
    - 3> when RLC has been requested to transmit the UTRAN MOBILITY INFORMATION CONFIRM message, perform the actions below.
- 1> if the variable PDCP\_SN\_INFO is non-empty:
- 2> when RLC has confirmed the successful transmission of the UTRAN MOBILITY INFORMATION CONFIRM message:
    - 3> for each radio bearer in the variable PDCP\_SN\_INFO:
      - 4> if the IE "RB started" in the variable ESTABLISHED\_RABS is set to "started":
        - 5> configure the RLC entity for that radio bearer to "continue".
    - 3> clear the variable PDCP\_SN\_INFO.

- 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
  - 2> resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
  - 2> set the IE "Reconfiguration" in the variable CIPHERING\_STATUS to FALSE; and
  - 2> clear the variable RB\_UPLINK\_CIPHERING\_ACTIVATION\_TIME\_INFO.
- 1> if the UTRAN MOBILITY INFORMATION message contained the IE "Integrity protection mode info":
  - 2> allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
  - 2> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to FALSE; and
  - 2> clear the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
- 1> clear the variable SECURITY\_MODIFICATION.

The procedure ends.

#### 8.3.3.4 Reception of an UTRAN MOBILITY INFORMATION CONFIRM message by the UTRAN

When the network receives UTRAN MOBILITY INFORMATION CONFIRM message, UTRAN may delete any old U-RNTI. The procedure ends.

#### 8.3.3.5 Cell re-selection

If the UE performs cell re-selection, the UE shall:

- 1> initiate a cell update procedure according to subclause 8.3.1;
- 1> if the UTRAN MOBILITY INFORMATION message contains the IE "New C-RNTI"; and
- 1> if the UE has not yet submitted the UTRAN MOBILITY INFORMATION CONFIRM message to lower layers for transmission and
  - 1> if the IE "Downlink counter synchronisation info" was not included in the received UTRAN MOBILITY INFORMATION message;
    - 2> transmit a UTRAN MOBILITY INFORMATION FAILURE message on the uplink DCCH using AM RLC;
    - 2> set the IE "RRC transaction identifier" in the UTRAN MOBILITY INFORMATION FAILURE message to the value of "RRC transaction identifier" in the entry for the UTRAN MOBILITY INFORMATION message in the table "Accepted transactions" in the variable TRANSACTIONS; and
    - 2> clear that entry.
    - 2> set the IE "failure cause" to the cause value "cell update occurred";
    - 2> when the UTRAN MOBILITY INFORMATION FAILURE message has been submitted to lower layers for transmission:
      - 3> continue with any ongoing processes and procedures as if the invalid UTRAN MOBILITY INFORMATION message has not been received and the procedure ends.
- 1> otherwise:
  - 2> if a UTRAN MOBILITY INFORMATION message was received and caused the IE "Reconfiguration" in the variable CIPHERING\_STATUS to be set to TRUE and/or the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to be set to TRUE, and
  - 2> if the IE "Downlink counter synchronisation info" was included in the received UTRAN MOBILITY INFORMATION message;

3> apply the new security (integrity protection) configuration received in the UTRAN MOBILITY INFORMATION message on the CELL UPDATE message to be transmitted;

2> continue the procedure normally.

### 8.6.3.5 Integrity protection mode info

The IE "Integrity protection mode info" defines the new integrity protection configuration. At any given time, the UE needs to store at most three different integrity protection configurations (keysets) in total for all signalling radio bearers for all CN domains.

If the IE "Integrity protection mode info" is present and if the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to TRUE, the UE shall:

- 1> ignore this second attempt to change the integrity protection configuration; and
- 1> set the variable INCOMPATIBLE\_SECURITY\_RECONFIGURATION to TRUE.

If the IE "Integrity protection mode info" is present and if the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO is set to FALSE, the UE shall:

- 1> set the IE "Reconfiguration" in the variable INTEGRITY\_PROTECTION\_INFO to TRUE;
- 1> if IE "Integrity protection mode command" has the value "start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and this IE was included in the message SECURITY MODE COMMAND:
  - 2> initialise the information for all signalling radio bearers in the variable INTEGRITY\_PROTECTION\_INFO according to the following:
    - 3> set the IE "Uplink RRC Message sequence number" in the variable INTEGRITY\_PROTECTION\_INFO to zero;
    - 3> do not set the IE "Downlink RRC Message sequence number" in the variable INTEGRITY\_PROTECTION\_INFO;
    - 3> set the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO to zero for each signalling radio bearer in the IE "ESTABLISHED\_RABS".
  - 2> set the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO to the value "Started";
  - 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:
    - 3> using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";
    - 3> using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].
  - 2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer in the IE "ESTABLISHED\_RABS" except RB2 at the next received RRC message;
  - 2> start applying the new integrity protection configuration in the downlink for signalling radio bearer RB2 from and including the received SECURITY MODE COMMAND message;
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearers other than RB2 at the uplink activation time included in the IE "Uplink integrity protection activation info".
- 1> if IE "Integrity protection mode command" has the value "start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and this IE was not included SECURITY MODE COMMAND:

NOTE: This case is used in SRNS relocation

- 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:
    - 3> using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";
    - 3> using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].
  - 2> let RB<sub>m</sub> be the signalling radio bearer where the reconfiguration message was received and let RB<sub>n</sub> be the signalling radio bearer where the response message is transmitted;
  - 2> prohibit transmission of RRC messages on all signalling radio bearers in the IE "ESTABLISHED\_RABS" except on RB<sub>0</sub> and the radio bearer where the response message is transmitted;
  - 2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer in the IE "ESTABLISHED\_RABS" except RB<sub>m</sub> at the next received RRC message;
  - 2> start applying the new integrity protection configuration in the downlink for signalling radio bearer RB<sub>m</sub> from and including the received configuration message;
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB<sub>n</sub> from and including the transmitted response message;
  - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearers other than RB<sub>n</sub> at the uplink activation time included in the IE "Uplink integrity protection activation info".
- 1> if IE "Integrity protection mode command" has the value "modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started" and this IE was included in SECURITY MODE COMMAND:
- 2> store the (oldest currently used) integrity protection configuration until activation times have elapsed for the new integrity protection configuration to be applied on all signalling radio bearers;
  - 2> if there are pending activation times set for integrity protection by a previous procedure changing the integrity protection configuration:
    - 3> apply the integrity protection configuration at this pending activation time as indicated in this procedure.
  - 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each signalling radio bearer n, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info";
  - 2> perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1;
    - 3> if present, use the algorithm indicated by the IE "Integrity protection algorithm" (UIA [40]);
  - 2> set the content of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO according to the following:
    - 3> for each established signalling radio bearer, stored in the variable ESTABLISHED\_RABS:
      - 4> select a value of the RRC sequence number at which (activation) time the new integrity protection configuration shall be applied in uplink for that signalling radio bearer according to the following:
        - 5> for each signalling radio bearer that has no pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
          - 6> set a suitable value that would ensure a minimised delay in the change to the latest integrity protection configuration.

- 5> for signalling radio bearer that has a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
    - 6> set the same value as the pending activation time for integrity protection;
  - 5> consider this (pending) activation time to be elapsed when the selected activation time (as above) is equal to the next RRC sequence number to be used, which means that the last RRC message using the old integrity protection configuration has been submitted to lower layers.
  - 4> for signalling radio bearer RB0:
    - 5> set the value of the included RRC sequence number to greater than or equal to the current value of the RRC sequence number for signalling radio bearer RB0 in the variable INTEGRITY\_PROTECTION\_INFO, plus the value of the constant N302 plus one.
  - 4> prohibit the transmission of RRC messages on all signalling radio bearers, except for RB2, with RRC SN greater than or equal to the value in the "RRC message sequence number list" for the signalling radio bearer in the IE "Uplink integrity protection activation info" of the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO.
  - 2> start applying the new integrity protection configuration in the uplink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Uplink integrity protection activation info", included in the variable INTEGRITY\_PROTECTION\_ACTIVATION\_INFO;
  - 2> start applying the new integrity protection configuration in the uplink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration;
  - 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info";
- NOTE: For signalling radio bearers that have a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration, UTRAN should set this value in IE "Downlink integrity protection activation info".
- 2> start applying the new integrity protection configuration in the downlink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration.

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and the IE "Integrity protection mode command info" was not included in the message SECURITY MODE COMMAND; or

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not started", and the IE "Integrity protection mode info" was included in the message SECURITY MODE COMMAND, and the IE "Integrity protection algorithm" is not included; or

If the IE "Integrity protection mode command" has the value "Modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Not Started"; or

If IE "Integrity protection mode command" has the value "Start" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started", and the IE "Integrity protection mode command info" was included in the message SECURITY MODE COMMAND; or

If there does not exist exactly one integrity protection activation time in the IE "Downlink integrity protection activation info" for each established signalling radio bearer included in the IE "Signalling radio bearer information" in the IE "ESTABLISHED\_RABS"; or

If IE "Integrity protection mode command" has the value "Modify" and the IE "Status" in the variable INTEGRITY\_PROTECTION\_INFO has the value "Started", and the IE "Integrity protection mode info" was not included in the message SECURITY MODE COMMAND:

the UE shall:

- 1> ignore this attempt to change the integrity protection configuration; and

Error! No text of specified style in document.

**27**

Error! No text of specified style in document.

1> set the variable INVALID\_CONFIGURATION to TRUE.

If the IE "Integrity protection mode info" is not present, the UE shall:

1> not change the integrity protection configuration.

### 8.6.3.6 Void



## CHANGE REQUEST

⌘ **25.331 CR 1496** ⌘ rev **-** ⌘ Current version: **3.10.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ "Out of service" area definition		
<b>Source:</b>	⌘ TSG-RAN WG2		
<b>Work item code:</b>	⌘ TEI	<b>Date:</b>	⌘ 2002-05-02
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ R99
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> 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)

<b>Reason for change:</b>	⌘ Criteria for UE detection of 'out of service area' are not properly specified.
<b>Summary of change:</b>	⌘ A reference is included to the appropriate RAN4 specification.
	<p><b>Impact analysis:</b></p> <p><u>Impacted functionality:</u> UE timer handling</p> <p><u>Correction:</u> Correction to a function where the specification was missing rules. Would not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.</p> <p><u>Interoperability:</u></p> <p>Isolated impact: the impact is isolated; only the corrected functionality is affected</p>
<b>Consequences if not approved:</b>	⌘ Definition of 'out of service area' will be missing, leading to ambiguity of when to start timers T316 and T317.

<b>Clauses affected:</b>	⌘ 7.2.2.1, 7.2.2.2, 8.5.5.1		
<b>Other specs affected:</b>	<input checked="" type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘	25.133 25.331 v4.4.0, CR 1497 25.331 v5.0.0, CR 1498
<b>Other comments:</b>	⌘		

### How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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.

## 7.2 Processes in UE modes/states

NOTE: This subclause specifies what processes shall be active in the UE in the different RRC modes/states. The related procedures and the conditions on which they are triggered are specified either in clause 8 or elsewhere in the relevant process definition.

### 7.2.1 UE Idle mode

UE processes that are active in UE Idle mode are specified in [4].

The UE shall perform a periodic search for higher priority PLMNs as specified in [25].

### 7.2.2 UTRA RRC Connected mode

In this specification unless otherwise mentioned "connected mode" shall refer to "UTRA RRC connected mode".

#### 7.2.2.1 URA\_PCH or CELL\_PCH state

In the URA\_PCH or CELL\_PCH state the UE shall perform the following actions:

NOTE: Neither DCCH nor DTCH are available in these states.

1> if the UE is "in service area":

- 2> maintain up-to-date system information as broadcast by the serving cell as specified in the subclause 8.1.1;
- 2> perform cell reselection process as specified in [4];
- 2> perform a periodic search for higher priority PLMNs as specified in [25];

NOTE: If the DRX cycle length is 80ms, then a search for higher priority PLMNs may not identify all the available PLMNs due to the paging occasion on the current serving cell coinciding with the MIB of the cell of interest.

- 2> monitor the paging occasions and PICH monitoring occasions determined according to subclauses 8.6.3.1a and 8.6.3.2 and receive paging information on the PCH mapped on the S-CCPCH selected by the UE according to the procedure in subclause 8.5.19;
- 2> act on RRC messages received on PCCH and BCCH;
- 2> perform measurements process according to measurement control information as specified in subclause 8.4 and in subclause 14.4;
- 2> maintain up-to-date BMC data if it supports Cell Broadcast Service (CBS) as specified in [37];
- 2> run timer T305 for periodical URA update if the UE is in URA\_PCH or for periodical cell update if the UE is in CELL\_PCH.

1> if the UE is "out of service area":

- 2> perform cell reselection process as specified in [4];
- 2> run timer T316;
- 2> run timer T305.

#### 7.2.2.2 CELL\_FACH state

In the CELL\_FACH state the UE shall perform the following actions:

NOTE: DCCH and, if configured, DTCH are available in this state.

1> if the UE is "in service area":

- 2> maintain up-to-date system information as broadcast by the serving cell as specified in subclause 8.1.1;
  - 2> perform cell reselection process as specified in [4];
  - 2> perform measurements process according to measurement control information as specified in subclause 8.4 and in subclause 14.4;
  - 2> run timer T305 (periodical cell update);
  - 2> listen to all FACH transport channels mapped on the S-CCPCH selected by the UE according to the procedure in subclause 8.5.19;
  - 2> act on RRC messages received on BCCH, CCCH and DCCH;
  - 2> act on RRC messages received on, if available, SHCCH (TDD only).
- 1> if the UE is "out of service area":
- 2> perform cell reselection process as specified in [4];
  - 2> run timers T305 (periodical cell update), and T317 (cell update when re-entering "in service") or T307 (transition to Idle mode).

### 7.2.2.3 CELL\_DCH state

In the CELL\_DCH state the UE shall perform the following actions:

NOTE: DCCH and, if configured, DTCH are available in this state.

- 1> read system information broadcast on FACH as specified in subclause 8.1.1.3 (applicable only to UEs with certain capabilities and in FDD mode);
- 1> read the system information as specified in subclause 8.1.1 (for UEs in TDD mode);
- 1> perform measurements process according to measurement control information as specified in subclause 8.4 and in clause 14;
- 1> act on RRC messages received on DCCH;
- 1> act on RRC messages received on BCCH (applicable only to UEs with certain capabilities and in FDD mode);
- 1> act on RRC messages received on BCCH (TDD only) and, if available, SHCCH (TDD only).

## 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

~~When a suitable cell is not found based on the description in [4], the UE considers it as having detected "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> 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> 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> 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 REQUEST

⌘ **25.331 CR 1497** ⌘ rev **-** ⌘ Current version: **4.4.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ "Out of service" area definition		
<b>Source:</b>	⌘ TSG-RAN WG2		
<b>Work item code:</b>	⌘ TEI	<b>Date:</b>	⌘ 2002-05-02
<b>Category:</b>	⌘ <b>A</b>	<b>Release:</b>	⌘ REL-4
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> 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)

<b>Reason for change:</b>	⌘ Criteria for UE detection of 'out of service area' are not properly specified.
<b>Summary of change:</b>	⌘ A reference is included to the appropriate RAN4 specification.
	<p><b>Impact analysis:</b></p> <p><u>Impacted functionality:</u> UE timer handling</p> <p><u>Correction:</u> Correction to a function where the specification was missing rules. Would not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.</p> <p><u>Interoperability:</u></p> <p>Isolated impact: the impact is isolated; only the corrected functionality is affected</p>
<b>Consequences if not approved:</b>	⌘ Definition of 'out of service area' will be missing, leading to ambiguity of when to start timers T316 and T317.

<b>Clauses affected:</b>	⌘ 7.2.2.1, 7.2.2.2, 8.5.5.1		
<b>Other specs affected:</b>	<input checked="" type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘	25.133 25.331 v3.10.0, CR 1496 25.331 v5.0.0, CR 1498
<b>Other comments:</b>	⌘		

### **How to create CRs using this form:**

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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.



## 7.2 Processes in UE modes/states

NOTE: This subclause specifies what processes shall be active in the UE in the different RRC modes/states. The related procedures and the conditions on which they are triggered are specified either in clause 8 or elsewhere in the relevant process definition.

### 7.2.1 UE Idle mode

UE processes that are active in UE Idle mode are specified in [4].

The UE shall perform a periodic search for higher priority PLMNs as specified in [25].

### 7.2.2 UTRA RRC Connected mode

In this specification unless otherwise mentioned "connected mode" shall refer to "UTRA RRC connected mode".

#### 7.2.2.1 URA\_PCH or CELL\_PCH state

In the URA\_PCH or CELL\_PCH state the UE shall perform the following actions:

NOTE: Neither DCCH nor DTCH are available in these states.

1> if the UE is "in service area":

- 2> maintain up-to-date system information as broadcast by the serving cell as specified in the subclause 8.1.1;
- 2> perform cell reselection process as specified in [4];
- 2> perform a periodic search for higher priority PLMNs as specified in [25];

NOTE: If the DRX cycle length is 80ms, then a search for higher priority PLMNs may not identify all the available PLMNs due to the paging occasion on the current serving cell coinciding with the MIB of the cell of interest.

- 2> monitor the paging occasions and PICH monitoring occasions determined according to subclauses 8.6.3.1a and 8.6.3.2 and receive paging information on the PCH mapped on the S-CCPCH selected by the UE according to the procedure in subclause 8.5.19;
- 2> act on RRC messages received on PCCH and BCCH;
- 2> perform measurements process according to measurement control information as specified in subclause 8.4 and in subclause 14.4;
- 2> maintain up-to-date BMC data if it supports Cell Broadcast Service (CBS) as specified in [37];
- 2> run timer T305 for periodical URA update if the UE is in URA\_PCH or for periodical cell update if the UE is in CELL\_PCH.

1> if the UE is "out of service area":

- 2> perform cell reselection process as specified in [4];
- 2> run timer T316;
- 2> run timer T305.

#### 7.2.2.2 CELL\_FACH state

In the CELL\_FACH state the UE shall perform the following actions:

NOTE: DCCH and, if configured, DTCH are available in this state.

1> if the UE is "in service area":

- 2> maintain up-to-date system information as broadcast by the serving cell as specified in subclause 8.1.1;
  - 2> perform cell reselection process as specified in [4];
  - 2> perform measurements process according to measurement control information as specified in subclause 8.4 and in subclause 14.4;
  - 2> run timer T305 (periodical cell update);
  - 2> listen to all FACH transport channels mapped on the S-CCPCH selected by the UE according to the procedure in subclause 8.5.19;
  - 2> act on RRC messages received on BCCH, CCCH and DCCH;
  - 2> act on RRC messages received on, if available, SHCCH (TDD only).
- 1> if the UE is "out of service area":
- 2> perform cell reselection process as specified in [4];
  - 2> run timers T305 (periodical cell update), and T317 (cell update when re-entering "in service") or T307 (transition to Idle mode).

### 7.2.2.3 CELL\_DCH state

In the CELL\_DCH state the UE shall perform the following actions:

NOTE: DCCH and, if configured, DTCH are available in this state.

- 1> read system information broadcast on FACH as specified in subclause 8.1.1.3 (applicable only to UEs with certain capabilities and in FDD mode);
- 1> read the system information as specified in subclause 8.1.1 (for UEs in TDD mode);
- 1> perform measurements process according to measurement control information as specified in subclause 8.4 and in clause 14;
- 1> act on RRC messages received on DCCH;
- 1> act on RRC messages received on BCCH (applicable only to UEs with certain capabilities and in FDD mode);
- 1> act on RRC messages received on BCCH (TDD only) and, if available, SHCCH (TDD only).

## 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

~~When a suitable cell is not found based on the description in [4], the UE considers it as having detected "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> 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> 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> 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 REQUEST

⌘ **25.331 CR 1498** ⌘ rev **-** ⌘ Current version: **5.0.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ "Out of service" area definition		
<b>Source:</b>	⌘ TSG-RAN WG2		
<b>Work item code:</b>	⌘ TEI	<b>Date:</b>	⌘ 2002-05-02
<b>Category:</b>	⌘ <b>A</b>	<b>Release:</b>	⌘ REL-5
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> 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)

<b>Reason for change:</b>	⌘ Criteria for UE detection of 'out of service area' are not properly specified.		
<b>Summary of change:</b>	⌘ A reference is included to the appropriate RAN4 specification.		
	<p><b>Impact analysis:</b></p> <p><u>Impacted functionality:</u> UE timer handling</p> <p><u>Correction:</u> Correction to a function where the specification was missing rules. Would not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.</p> <p><u>Interoperability:</u></p> <p>Isolated impact: the impact is isolated; only the corrected functionality is affected</p>		
<b>Consequences if not approved:</b>	⌘ Definition of 'out of service area' will be missing, leading to ambiguity of when to start timers T316 and T317.		

<b>Clauses affected:</b>	⌘ 7.2.2.1, 7.2.2.2, 8.5.5.1		
<b>Other specs affected:</b>	<input checked="" type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘	25.133 25.331 v3.10.0, CR 1496 25.331 v4.4.0, CR 1497
<b>Other comments:</b>	⌘		

### **How to create CRs using this form:**

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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.

## 7.2 Processes in UE modes/states

NOTE: This subclause specifies what processes shall be active in the UE in the different RRC modes/states. The related procedures and the conditions on which they are triggered are specified either in clause 8 or elsewhere in the relevant process definition.

### 7.2.1 UE Idle mode

UE processes that are active in UE Idle mode are specified in [4].

The UE shall perform a periodic search for higher priority PLMNs as specified in [25].

### 7.2.2 UTRA RRC Connected mode

In this specification unless otherwise mentioned "connected mode" shall refer to "UTRA RRC connected mode".

#### 7.2.2.1 URA\_PCH or CELL\_PCH state

In the URA\_PCH or CELL\_PCH state the UE shall perform the following actions:

NOTE: Neither DCCH nor DTCH are available in these states.

1> if the UE is "in service area":

- 2> maintain up-to-date system information as broadcast by the serving cell as specified in the subclause 8.1.1;
- 2> perform cell reselection process as specified in [4];
- 2> perform a periodic search for higher priority PLMNs as specified in [25];

NOTE: If the DRX cycle length is 80ms, then a search for higher priority PLMNs may not identify all the available PLMNs due to the paging occasion on the current serving cell coinciding with the MIB of the cell of interest.

- 2> monitor the paging occasions and PICH monitoring occasions determined according to subclauses 8.6.3.1a and 8.6.3.2 and receive paging information on the PCH mapped on the S-CCPCH selected by the UE according to the procedure in subclause 8.5.19;
- 2> act on RRC messages received on PCCH and BCCH;
- 2> perform measurements process according to measurement control information as specified in subclause 8.4 and in subclause 14.4;
- 2> maintain up-to-date BMC data if it supports Cell Broadcast Service (CBS) as specified in [37];
- 2> run timer T305 for periodical URA update if the UE is in URA\_PCH or for periodical cell update if the UE is in CELL\_PCH.

1> if the UE is "out of service area":

- 2> perform cell reselection process as specified in [4];
- 2> run timer T316;
- 2> run timer T305.

#### 7.2.2.2 CELL\_FACH state

In the CELL\_FACH state the UE shall perform the following actions:

NOTE: DCCH and, if configured, DTCH are available in this state.

1> if the UE is "in service area":

- 2> maintain up-to-date system information as broadcast by the serving cell as specified in subclause 8.1.1;
  - 2> perform cell reselection process as specified in [4];
  - 2> perform measurements process according to measurement control information as specified in subclause 8.4 and in subclause 14.4;
  - 2> run timer T305 (periodical cell update);
  - 2> listen to all FACH transport channels mapped on the S-CCPCH selected by the UE according to the procedure in subclause 8.5.19;
  - 2> act on RRC messages received on BCCH, CCCH and DCCH;
  - 2> act on RRC messages received on, if available, SHCCH (TDD only).
- 1> if the UE is "out of service area":
- 2> perform cell reselection process as specified in [4];
  - 2> run timers T305 (periodical cell update), and T317 (cell update when re-entering "in service") or T307 (transition to Idle mode).

### 7.2.2.3 CELL\_DCH state

In the CELL\_DCH state the UE shall perform the following actions:

NOTE: DCCH and, if configured, DTCH are available in this state.

- 1> read system information broadcast on FACH as specified in subclause 8.1.1.3 (applicable only to UEs with certain capabilities and in FDD mode);
- 1> read the system information as specified in subclause 8.1.1 (for UEs in TDD mode);
- 1> perform measurements process according to measurement control information as specified in subclause 8.4 and in clause 14;
- 1> act on RRC messages received on DCCH;
- 1> act on RRC messages received on BCCH (applicable only to UEs with certain capabilities and in FDD mode);
- 1> act on RRC messages received on BCCH (TDD only) and, if available, SHCCH (TDD only).



## 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

~~When a suitable cell is not found based on the description in [4], the UE considers it as having detected "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> 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> 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> 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.