3GPP TSG-RAN2 Meeting #27
Orlando, USA, 18-22 of February

RP-020205

CR-Form-v5

CHANGE REQUEST

⌘ **25.331** **CR** **1282** ⌘ **rev** **5** ⌘ Current version: **3.9.0** ⌘

*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 **X** Radio Access Network **X** Core Network ☐

Title:	⌘	Security corrections
Source:	⌘	Alcatel, Ericsson, Nortel, Motorola
Work item code:	⌘	***Date:*** ⌘ 2002-02-22
Category:	⌘ **F**	***Release:*** ⌘ R99

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change: ⌘ The current specification is unclear on a number of points and require clarification.

Incorrect procedure for UE actions on receipt of HO TO UTRAN COMMAND.

Changes in this revision, r5, are highlighted in blue in subclause 8.3.6.3 - the only subclause affected in this revision.

Summary of change: ⌘

[A] 8.1.12.2.1 (and other)

It is clarified that "suspend" means that PDUs with SN>X shall not be transmitted.

8.1.12.2.1, 8.1.12.2.2, 8.1.12.5

OI 2.38 UTRAN procedures completed/corrected.

8.1.3.6 (and other)

[B] For integrity protection RRC messages with RRC SN >X are allowed to transmit when the integrity configuration has been changed. This is missing in some procedures, i.e. Cell update, at reception of security mode complete, transmission of response messages in normal case.

8.2.2.3

[C] / OI 2.41: The IE "Integrity protection mode info" with the IE "Integrity protection mode command" set to "modify" can only be received in SECURITY MODE COMMAND. This is removed from other reconfiguration messages.

8.5.8

[D] The first CFN of the TTI shall be used for ciphering in the whole TTI. This is clarified in 8.5.8. (See also CR to 25.321).

8.5.9

OI 2.25: It needs to be clarified that COUNT-C corresponding to non ciphered RB should NOT be included in the START value calculation.

8.6.3.4

[E] "Pending activation time" is clarified for downlink. This is needed as the UE in some cases shall apply a new configuration at a pending activation time.

8.6.3.5

OI 2.49: Added missing Integrity Protection invalid configuration check.

8.6.4.1

[F] The start of ciphering is missing when an SRB is setup (SRB4) and ciphering is already started for the CN domain (see similar text in RB setup, 8.6.4.3).

8.3.6.3 and 10.2.16.b

[G] UE shall, in case USIM is present, include in the HANDOVER TO UTRAN COMPLETE message the START values that were not transferred to the network via the other RAT. The specification is clarified, by referring to UE variable INTER_RAT_HANDOVER_INFO_TRANSFERRED.

8.6.4.1 (and others)

OI 2.37. The variable START_VALUE_TO_TRANSMIT needs to be set when SRB4 is setup in RB SETUP. It is also clarified that SRB4 and any RB needs to be from the same CN domain.

In revision2:

OI 21 (8.1.12.4.b and 8.2.2.12b)

Failure message when security procedure is interruped by cell update. UE shall not send failure message after having sent the SECURITY MODE COMPLETE message (see R2-020348)

Section 8.1.12.2.1 and 8.1.12.2.2: The restriction on the number of ciphering configurations and integrity protection algorithms that the UE needs to store is clarified.

8.5.9. The START value calculation is changed from MAX(HFN)+1 to MAX(HFN)+2 in order to avoid reuse in case of loss of data in UM before RB release.

8.1.8.2 The START value is included in the Initial Direct Transfer message. (Revision 5 changed this inclusion action as follows: the UE always includes the START value irrespective of whether it is different from the previously transferred value)

In revision 3:

- ASN.1 changes added

- STARTlist is added in the inter node containers

- SIM handling

- Timing initialised HHO

- HO from GSM

- ASN change for inter node containers

In revision 4:

- Activation time for TM RB corrected in 8.6.4.3
- OI 2.43: AM RLC PDU size change covered
- The actions of UE on receiving the Security Mode Command, sending the Security Mode Complete and upon receiving the acknowledgement to the complete depending on whether new keys have been received or not are clarified.
- It is clarified that if new keys are received the UE shall consider the latest transmitted START value to be zero for future procedures.

In revision 5:

The procedure text for HO TO UTRAN COMMAND has been modified to clarify the actions by the UE. It is clarified that the UE shall send the START values in the USIM in the response message. It is clarified that the UE shall use the START value sent to the other-RAT prior to handover for initialising the HFN for TM bearers until the activation time sent in the HO TO UTRAN COMPLETE. The HFN for TM bearers shall not be incremented every CFN cycle until the activation time. For signalling bearers the HFN shall be initialised with the same START value; however, in this case the HFN shall be incremented. For UM and AM bearers set up through the HO to UTRAN command the HFN shall be initialised with the START value sent in the response message.

Impact analysis:

Impacted functionality: Ciphering and integrity protection

Correction: Clarifications of the security finctionality

Correction to a function where the specification was unclear. Would not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.

If the UE does not implement the change, but the UTRAN does OR if If the UTRAN does not implement the change, but the UE does:

- The HFN value may get out of sync when SRB4 is setup in RB SETUP, leading to ciphering failure

- UE and UTRAN may have different interpreation on if unciphered RBs shall be included in the START calculation, which would lead to ciphering failure.

- Unclear specifiation may lead to interoperability problems.
- Unclear specification as to the HFN values used for the signalling bearers after receiving the HO to UTRAN command and ciphering procedure for TM bearers.

Consequences if not approved:	⌘	Missing actions for UE in various scenarios leading to non-functioning security feature. Potential misinterpretation of security functionality. Unclear behavior. Risk for ciphering failure in case of RB setup of SRB4 and other scenarios.

Clauses affected:	⌘	8.1.3.6, 8.1.8.2, 8.1.8.3, 8.1.12.2, 8.1.12.2.1, 8.1.12.2.2, 8.1.12.3, 8.1.12.3.1, 8.1.12.4, 8.1.12.4a, 8.1.12.4b, 8.1.12.5, 8.2.2.2, 8.2.2.3, 8.2.2.4, 8.2.2.12b, 8.3.1.5, 8.3.1.6, 8.3.3.3, 8.3.4.3, 8.3.6.3, 8.6.7.4, 8.5.2, 8.5.8, 8.5.9, 8.5.10.3, 8.6.3.4, 8.6.3.5, 8.6.4.1, 8.6.4.3, 8.6.4.8, 8.6.6.28, 10.2.16b, 10.2.16c, 10.3.3.5, 10.3.3.16, 11.2, 11.5, 13.4.x (new section), 13.4.11b (new section), 14.12.4.2
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	This CR is an update of the CR1282 submitted to RAN for approval. It corrects the functionality related to the HO to UTRAN command relatd to the aspects of ciphering.

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. 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.

8.1.3.6 Reception of an RRC CONNECTION SETUP message by the UE

The UE shall compare the value of the IE "Initial UE identity" in the received RRC CONNECTION SETUP message with the value of the variable INITIAL_UE_IDENTITY.

If the values are different, the UE shall:

- ignore the rest of the message.

If the values are identical, the UE shall:

- stop timer T300, and act upon all received information elements as specified in subclause 8.6, unless specified otherwise in the following:
  - if the UE will be in the CELL_FACH state at the conclusion of this procedure:
    - if the IE "Frequency info" is included:
      - select a suitable UTRA cell according to [4] on that frequency;
    - select PRACH according to subclause 8.5.17;
    - select Secondary CCPCH according to subclause 8.5.19;
    - ignore the IE "UTRAN DRX cycle length coefficient" and stop using DRX.
- perform the physical layer synchronization procedure as specified in [29];
- enter a state according to subclause 8.6.3.3;
- submit an RRC CONNECTION SETUP COMPLETE message to the lower layers on the uplink DCCH after successful state transition per subclause 8.6.3.3, with the contents set as specified below:
  - set the IE "RRC transaction identifier" to:
    - the value of "RRC transaction identifier" in the entry for the RRC CONNECTION SETUP message in the table "Accepted transactions" in the variable TRANSACTIONS; and
    - clear that entry.
  - if the USIM or SIM is present:
    - set the "START" for each CN domain in the IE "START list" in the RRC CONNECTION SETUP COMPLETE message with the corresponding START value that is stored in the USIM [50], if present, or as stored in the UE if the USIM is not present; and then
    - set the START value stored in the USIM [50], if present, and for the SIMas stored in the UE if the USIM is not present, for any CN domain to the value "THRESHOLD" of the variable START_THRESHOLD.
  - if neitherthe the USIM ornor SIM is not present:
    - set the "START" for each CN domain in the IE "START list" in the RRC CONNECTION SETUP COMPLETE message to zero;
    - set the value of "THRESHOLD" in the variable "START_THRESHOLD" to the default value [40].
  - retrieve its UTRA UE radio access capability information elements from variable UE_CAPABILITY_REQUESTED; and then
  - include this in IE "UE radio access capability" and IE "UE radio access capability extension", provided this IE is included in variable UE_CAPABILITY_REQUESTED;
  - retrieve its inter-RAT-specific UE radio access capability information elements from variable UE_CAPABILITY_REQUESTED; and then
  - include this in IE "UE system specific capability".

When the RRC CONNECTION SETUP COMPLETE message has been submitted to lower layers for transmission the UE shall:

- if the UE has entered CELL_FACH state:
  - start timer T305 using its initial value 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.
- store the contents of the variable UE_CAPABILITY_REQUESTED in the variable UE_CAPABILITY_TRANSFERRED;
- initialise variables upon entering UTRA RRC connected mode as specified in subclause 13.4;
- consider the procedure to be successful;

And the procedure ends.

8.1.8.2 Initiation of Initial direct transfer procedure in the UE

In the UE, the initial direct transfer procedure shall be initiated, when the upper layers request establishment of a signalling connection. This request also includes a request for the transfer of a NAS message.

Upon initiation of the initial direct transfer procedure when the UE is in idle mode, the UE shall:

- set the variable ESTABLISHMENT_CAUSE to the cause for establishment indicated by upper layers;
- perform an RRC connection establishment procedure, according to subclause 8.1.3;
- if the RRC connection establishment procedure was not successful:
  - indicate failure to establish the signalling connection to upper layers and end the procedure.
- when the RRC connection establishment procedure is completed successfully:
  - continue with the initial direct transfer procedure as below.

Upon initiation of the initial direct transfer procedure when the UE is in CELL_PCH or URA_PCH state, the UE shall:

- perform a cell update procedure, according to subclause 8.3.1, using the cause "uplink data transmission";
- when the cell update procedure completed successfully:
  - continue with the initial direct transfer procedure as below.

The UE shall, in the INITIAL DIRECT TRANSFER message:

- set the IE "NAS message" as received from upper layers; and
- set the IE "CN domain identity" as indicated by the upper layers; and
- set the IE "Intra Domain NAS Node Selector" as follows:
  - derive the IE "Intra Domain NAS Node Selector" from TMSI/PMTSI, IMSI, or IMEI; and
  - provide the coding of the IE "Intra Domain NAS Node Selector" according to the following priorities:
    1. derive the routing parameter for IDNNS from TMSI (CS domain) or PTMSI (PS domain) whenever a valid TMSI/PTMSI is available;
    2. base the routing parameter for IDNNS on IMSI when no valid TMSI/PTMSI is available;
    3. base the routing parameter for IDNNS on IMEI only if no (U)SIM is inserted in the UE.
- calculate the START according to subclause 8.5.9 for the CN domain as ~~indicated by upper layers~~set in the IE "CN Domain Identity"; and

- ~~if the calculated START value for the CN domain as indicated by upper layers is different from what has been transmitted to the UTRAN in a former message:~~

  - include the calculated START value for that CN domain in the IE "START";

In CELL_FACH state, the UE shall:

- include a 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);
- include in the IE "Measured results on RACH" all requested reporting quantities for cells for which measurements are reported.

The UE shall:

- transmit the INITIAL DIRECT TRANSFER message on the uplink DCCH using AM RLC on signalling radio bearer RB3;
- when the INITIAL DIRECT TRANSFER message has been submitted to lower layers for transmission:
  - confirm the establishment of a signalling connection to upper layers; and
  - add the signalling connection with the identity indicated by the IE "CN domain identity" in the variable ESTABLISHED_SIGNALLING_CONNECTIONS; and
  - the procedure ends.

When not stated otherwise elsewhere, the UE may also initiate the initial direct transfer procedure when another procedure is ongoing, and in that case the state of the latter procedure shall not be affected.

A new signalling connection request may be received from upper layers during transition to idle mode. In those cases, from the time of the indication of release to upper layers until the UE has entered idle mode, any such upper layer request to establish a new signalling connection shall be queued. This request shall be processed after the UE has entered idle mode.

8.1.8.3 Reception of INITIAL DIRECT TRANSFER message by the UTRAN

On reception of the INITIAL DIRECT TRANSFER message the NAS message should be routed using the IE "CN Domain Identity". UTRAN may also use the IE "Intra Domain NAS Node Selector" for routing among the CN nodes for the addressed CN domain.

If no signalling connection exists towards the chosen node, then a signalling connection is established.

If the IE "Measured results on RACH" is present in the message, the UTRAN should extract the contents to be used for radio resource control.

When the UTRAN receives an INITIAL DIRECT TRANSFER message, it shall not affect the state of any other ongoing RRC procedures, when not stated otherwise elsewhere.

~~UTRAN should:~~

~~- If the IE "START" is included in the INITIAL DIRECT TRANSFER message~~The UTRAN should:

- set the START value for the CN domain indicated in the IE "CN domain identity" to the value of the IE "START";

8.1.12.2 Initiation

8.1.12.2.1 Ciphering configuration change

To ~~stop or~~ 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.

[OI 2.35] When configuring ciphering, UTRAN should assensure 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. This includes the total number of ciphering configurations for all signalling radio bearers and radio bearers. 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:

- if this is the first SECURITY MODE COMMAND sent for this RRC connection:
  - use 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 for all the signalling radio bearers; while:
    - setting the 20 most significant bits of the hyper frame numbers for all signalling radio bearers to the value "START" for that CN domain;
    - setting the remaining bits of the hyper frame numbers equal to zero.
- (indentation change) suspend all radio bearers using RLC-AM or RLC-UM and suspend 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:;
  - suspend 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;
  - (indentation change) do 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; /* Indentation changed to B32*/
- 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";
- 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";
- 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;
- if a transparent mode radio bearer for this CN domain exists:
  - include the IE "Ciphering activation time for DPCH" in IE "Ciphering mode info", at which time the new ciphering configuration shall be applied;
- 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;
- 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;
- if Integrity protection has already been started for the UE; and
  - 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:
    - include the IE “Integrity protection mode info” in the SECURITY MODE COMMAND

- if Integrity protection has already been started for the UE; and

  - 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:

    - include the IE “Integrity protection mode info” in the SECURITY MODE COMMAND

- transmit the SECURITY MODE COMMAND message on ~~the downlink DCCH in AM RLC~~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.

~~[OI 2.35]~~ When configuring Integrity protection, UTRAN should: ~~as~~

- 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.

- 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; and

  - 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:

    - include the IE “Ciphering mode info” in the SECURITY MODE COMMAND;

- 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;

  - 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:

- if this is the first SECURITY MODE COMMAND sent for this RRC connection:

  - if new keys have been received:

    - initialise the hyper frame numbers as follows:

      - set all bits of the hyper frame numbers of the COUNT-I values for all signalling radio bearers to zero;

  - else (if new keys have not been received):

    - use 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 COUNT-I for all the signalling radio bearers; ~~while~~by:

      - 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;

      - setting the remaining bits of the hyper frame numbers equal to zero;

- else (this is not the first SECURITY MODE COMMAND sent for this RRC connection):

  - if new keys have been received;

    - initialise the hyper frame number for COUNT-I for RB2 as follows:

      - set all bits of the HFN of the COUNT-I value for RB2 to zero;

  - if new keys have not been received;

    - initialize the hyper frame number for COUNT-I for RB2 as follows:

- 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 the IE "CN Domain Identity";

- set the remaining bits of the HFN of the downlink and uplink COUNT-I to zero;

- if the IE "Integrity protection mode command" has the value "Start":

  - prohibit the transmission of signalling messages with any RRC SN on all signalling radio bearers, except RB2;

  - set the FRESH value in the IE "Integrity protection initialisation number", included in the IE "Integrity protection mode info";

- if the IE "Integrity protection mode command" has the value "Modify":

  - for each signalling radio bearer RBn, except RB2:

    - 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";

  - 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;

  - 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;

- 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:

- if ~~the not at least one of the~~ neither IE~~s~~ "Ciphering mode info" nor ~~and the~~ IE "Integrity protection mode info"~~"~~ ~~are both not~~ is included in the SECURITY MODE COMMAND:

  - set the variable INVALID_CONFIGURATION to TRUE.

- 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:

  - set the variable LATEST_CONFIGURED_CN_DOMAIN equal to the IE "CN domain identity";

  - set the IE “Status” in the variable SECURITY_MODIFICATION for the CN domain ~~as~~ indicated in the IE "CN domain identity" in the received SECURITY MODE COMMAND to the value “Affected”;

  - set the IE “Status” in the variable SECURITY_MODIFICATION for ~~in~~ all ~~other~~ CN domains other than the CN domain ~~as~~ indicated in the IE "CN domain identity" to “Not affected”

  - ~~if the value of the IE "Status" in the variable "INTEGRITY_PROTECTION_INFO" is "Not started":~~

    - ~~use the value "START" in the most recently sent 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 for all the signalling radio bearers; while~~by

- ~~initialisingsetting the 20 MSBmost significant bits of the hyper frame numbers component of COUNT-C and COUNT-I for all signalling radio bearers withto the START value for that CN domain;~~

- ~~setting the remaining bits of the hyper frame numbers components of COUNT-C and COUNT-I equal to zero.~~

- 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
- clear that entry;
- if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
  - perform the actions as specified in subclause 8.6.3.4.
- if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
  - perform the actions as specified in subclause 8.6.3.5.

- prior to sending the SECURITY MODE COMPLETE message:
  - use the old ciphering configuration for this message;
  - if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable~~.~~ RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO
    - for each radio bearer and signalling radio bearer that belongs to the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN:
      - 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;
      - ~~-~~continue incrementing the COUNT-C values for all RLC-AM and RLC-UM radio bearers ~~at the ciphering activation time as specified in the procedure~~;

    - ~~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, the UE shall:~~
      - ~~for ciphering on radio bearers using RLC-TM at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info":~~
        - ~~set the HFN component of the 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.~~
      - ~~for ciphering on radio bearers and 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:~~
        - ~~set 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.~~
      - ~~for ciphering on radio bearers and 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:~~
        - ~~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.~~

- 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 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:

    - 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;

    - set the remaining bits of the hyper frame numbers to zero;

- if new keys have been received perform the actions in subclause 8.1.12.3.1.

- if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":

  - 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.;

  - 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, ~~the UE shall for each signalling radio bearer~~for RB2:

    ~~- if the IE "Integrity protection mode command" has the value "start":~~

      ~~- in the downlink, for this signalling radio bearer, set the 20 most significant bits of IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zeroto the value START included in the most recently transmitted IE "START list" or IE "START" that belongs to the CN domain indicated in the variable LATEST_CONFIGURED_CN_DOMAIN;~~

      ~~- set the remaining bits of the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO to zero;~~

    ~~- else:~~

    - in the downlink, for the received SECURITY MODE COMMAND message ~~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":~~:

      - 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.;

      - set the remaining bits of the IE "Downlink RRC HFN" to zero;

    - in the uplink, for the ~~first~~ transmitted ~~RRC~~response message, SECURITY MODE COMPLETE: ~~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 COMPLETEIE "Integrity protection mode info":~~

      ~~- for this signalling radio bearer,~~ 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;

      - set the remaining bits of the IE "Uplink RRC HFN" to zero;

- 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, the UE shall for each signalling radio bearer other than RB2:
  - if the IE "Integrity protection mode command" has the value "start":
    - in the downlink, for this signalling radio bearer, 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;
    - set the remaining bits of the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero;
  - else:
    - 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":
      - [HANS, I want this to be B6]for this signalling radio bearer, 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;
      - set the remaining bits of the IE "Downlink RRC HFN" to zero;
  - if new keys have been received perform the actions in subclause 8.1.12.3.1;
- start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;
- transmit the SECURITY MODE COMPLETE message on the uplink DCCH in AM RLC;

- when the successful delivery of the SECURITY MODE COMPLETE message has been confirmed by RLC:
  - if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - 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 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:~~
        - ~~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;~~
        - ~~set the remaining bits of the hyper frame numbers to zero;~~
      - 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:
        - 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.
        - set the remaining bits of the hyper frame numbers to zero;
    - if new keys have been received perform the actions in subclause 8.1.12.3.1.

- resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
- set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
- clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.

- if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":

- 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, the UE shall for each signalling radio bearer other than RB2:

- if the IE "Integrity protection mode command" has the value "start":

- in the ~~downlink~~uplink, for this signalling radio bearer, set the 20 most significant bits of IE "~~Down~~Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the ~~down~~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;

- set the remaining bits of the IE "~~Down~~Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the ~~down~~uplink COUNT-I to zero;

- else:

- ~~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":~~

- ~~[HANS, I want this to be B6]for this signalling radio bearer, 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;~~

- ~~set the remaining bits of the IE "Downlink RRC HFN" to zero;~~

- 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:

- [Hans - same here B6]for this signalling radio bearer, 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;

- set the remaining bits of the IE "Uplink RRC HFN" to zero;

- if new keys have been received perform the actions in subclause 8.1.12.3.1;
- allow the transmission of RRC messages on all signalling radio bearers with any RRC SN ~~greater than or equal to the value in the "RRC message sequence number list" indicated for each signalling radio bearer in the IE "Uplink integrity protection activation info" of the response message~~;
- 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;
- set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
- clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.

- clear the variable SECURITY_MODIFICATION;
- notify upper layers upon change of the security configuration;
- and the procedure ends.

- 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:
  - release all its radio resources;
  - 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;
  - clear the variable ESTABLISHED_SIGNALLING_CONNECTIONS;
  - clear the variable ESTABLISHED_RABS;
  - clear the variable SECURITY_MODIFICATION;
  - enter idle mode;
  - perform actions when entering idle mode as specified in subclause 8.5.2;
  - 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:

- set the START value for ~~this~~ the CN domain ~~as~~ indicated in the variable LATEST_CONFIGURED_CN_DOMAIN ~~CN domain~~ to zero;
- if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
  - ~~for each signalling radio bearer, except SRB2:~~
  - for integrity protection in the downlink on each signalling radio bearer except RB2:
    - if IE "Integrity protection mode command" has the value "start":
      - for the first received message on this signalling radio bearer:
        - start using the new integrity key;
        - for this signalling radio bearer, set the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero.
    - else:
      - for the first message for which ~~when~~ 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":
        - ~~use~~ start using the new integrity key;
        - for this signalling radio bearer, set the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero.
  - for integrity protection in the uplink on each signalling radio bearer except RB2:

- for the first message for which ~~when~~ 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 ~~IE "Integrity protection mode info~~transmitted SECURITY MODE COMPLETE message~~"~~:
  - ~~use~~ start using the new integrity key;
  - for this signalling radio bearer, set the IE "Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the uplink COUNT-I to zero~~.~~;

- for integrity protection in the downlink on signalling radio bearer RB2:
  - at the received SECURITY MODE ~~-~~COMMAND:
    - start using the new integrity key;
    - set the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero;
- for integrity protection in the uplink on signalling radio bearer RB2 :
  - at the transmitted SECURITY MODE COMPLETE:
    - start using the new integrity key;
    - set the IE "Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the uplink COUNT-I to zero;

- if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info": [INDENTATION CHANGED IN FOLLOWING]
  - for each signalling radio bearer and for each radio bearer for the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN ~~this CN domain~~:
    - 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:
      - at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info":
        - start using the ~~use~~ the new key in uplink and downlink;
        - set the HFN component of the COUNT-C to zero.
    - 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:
      - in the downlink, at ~~and after~~ the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info":
        - ~~use~~ start using the new key;
        - set the HFN component of the downlink COUNT-C to zero.
      - in the uplink, at ~~and after~~ the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info":
        - ~~use~~ start using the new key;
        - set the HFN component of the uplink COUNT-C to zero.
- 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:

- 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;
- 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
- clear that entry;
- set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";
- when the response message has been submitted to lower layers for transmission:
  - set the variable INCOMPATIBLE_SECURITY_RECONFIGURATION to FALSE;
  - continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - 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:

- abort the ongoing integrity and/or ciphering reconfiguration;
- resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
- allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- ~~[OI21] 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;~~
- ~~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~~
- ~~clear that entry;~~
- ~~set the IE "failure cause" to the cause value "cell update occurred";~~
- when the response message has been submitted to lower layers for transmission:
  - if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
    - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO;
  - if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":

- set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
- clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.

- continue with any ongoing processes and procedures as if the ~~invalid~~ SECURITY MODE COMMAND message has not been received; and
- clear the variable SECURITY_MODIFICATION;
- 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:

- transmit a SECURITY MODE FAILURE message on the DCCH using AM RLC after setting the IEs as specified below:
  - 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
  - clear that entry;
  - set the IE "failure cause" to the cause value "invalid configuration".
- when the response message has been submitted to lower layers for transmission:
  - set the variable INVALID_CONFIGURATION to FALSE;
  - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE;
  - continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - 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:

- if the IE “Ciphering mode info” was included in the SECURITY MODE COMMAND message:
  - if new keys were received for the CN domain set in the IE "CN Domain Identity" in the SECURITY MODE COMMAND:
    - at the downlink and uplink activation time set 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;
  - else (if new keys were not received)
    - at the downlink and uplink activation time use 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 ~~uplink and~~ downlink and uplink COUNT-C values respectively for all the signalling radio bearers~~; while~~by:
      - setting 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;
      - setting the remaining bits of the hyper frame numbers equal to zero.

- if the IE “Integrity protection mode info” was included in the SECURITY MODE COMMAND message; and
  - if this was not the first SECURITY MODE COMMAND message for this RRC connection:
    - 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:
      - at the downlink and uplink activation time 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:
        - set all bits of the hyper frame numbers of the uplink and downlink COUNT-I to zero;
    - 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:
      - at the downlink and uplink activation time use 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 ~~uplink and downlink~~downlink and uplink COUNT-I values respectively for all the signalling radio bearers other than RB2~~; while~~by:
        - setting 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;
        - setting the remaining bits of the hyper frame numbers equal to zero.
- send an indication to upper layers that the new ~~integrity protection~~security configuration has been activated;
- resume, in the downlink, all suspended radio bearers and all signalling radio bearers;
- allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- if the IE "Integrity protection mode command" included in the SECURITY MODE COMMAND had the value "Start":
  - start applying integrity protection in the downlink for all signalling radio bearers;
- if the IE "Integrity protection mode command" included in the SECURITY MODE COMMAND had the value "Modify":
  - 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";
  - continue applying the new integrity configuration for signalling radio bearer RB2~~start applying the new integrity protection configuration in the downlink at the RRC sequence number for signalling radio bearer RB2, from and including the SECURITY MODE COMMAND~~;
  - 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";
- 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";
- 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";
- 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";

- ~~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";~~

- for radio bearers using RLC-AM or RLC-UM:
  - 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;
  - 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;
  - 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.
- for radio bearers using RLC-TM:
  - 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;
  - 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.
- 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:

- transmit a SECURITY MODE FAILURE message on the uplink DCCH using AM RLC;
- 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
- clear that entry;
- set the IE "failure cause" to the cause value "protocol error";
- include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL_ERROR_INFORMATION;
- when the response message has been submitted to lower layers for transmission:
  - continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - and the procedure ends.

8.2.2.2 Initiation

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

- configure new radio links in any new physical channel configuration;
- start transmission and reception on the new radio links;
- for a radio bearer establishment procedure:

- transmit a RADIO BEARER SETUP message on the downlink DCCH using AM or UM RLC.

- if signaling radio bearer RB4 is setup with this procedure and signaling radio bearers RB1-RB3 were already established prior to the procedure:

  - if the variable "LATEST_CONFIGURED_CN_DOMAIN" has been initialised:

    - any radio bearers setup by the same message as signalling radio bearer RB4 should be connected to the CN domain indicated in the varable "LATEST CONFIGURED CN DOMAIN";

- for a radio bearer reconfiguration procedure:

  - transmit a RADIO BEARER RECONFIGURATION message on the downlink DCCH using AM or UM RLC.

- for a radio bearer release procedure:

  - transmit a RADIO BEARER RELEASE message on the downlink DCCH using AM or UM RLC.

- for a transport channel reconfiguration procedure:

  - transmit a TRANSPORT CHANNEL RECONFIGURATION message on the downlink DCCH using AM or UM RLC.

- for a physical channel reconfiguration procedure:

  - transmit a PHYSICAL CHANNEL RECONFIGURATION message on the downlink DCCH using AM or UM RLC.

- if the reconfiguration procedure is simultaneous with SRNS relocation procedure:

  - include the IE "Downlink counter synchronisation info"; and

  - if ciphering and/or integrity protection are activated:

    - include new ciphering and/or integrity protection configuration information to be used after reconfiguration.

  - use the downlink DCCH using AM RLC.

- if transport channels are added, reconfigured or deleted in uplink and/or downlink:

  - set TFCS according to the new transport channel(s).

- 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:

  - 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 common channel configuration of a given cell and C-RNTI to be used in that cell to the UE.

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:

- abort the ongoing integrity and/or ciphering reconfiguration;
- resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;

~~[OI21] - transmit a failure response message as specified in subclause 8.2.2.9, setting the information elements as specified below:~~

~~- include the IE "RRC transaction identifier"; and~~

~~- 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~~

~~- clear that entry;~~

~~- set the IE "failure cause" to the cause value "cell update occurred";~~

- if the received reconfiguration message contained the IE "Ciphering mode info":
  - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
  - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO;
- if the received reconfiguration message contained the IE "Integrity protection mode info":
  - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
  - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.
- continue with any ongoing processes and procedures as if the reconfiguration message was not received.

The procedure ends.

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:

- set the variable ORDERED_RECONFIGURATION to TRUE;
- perform the physical layer synchronisation procedure as specified in [29];
- 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:

- 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:
  - act upon the IE "PDSCH code mapping" as specified in subclause 8.6; and
  - infer that the PDSCH will be transmitted from the cell from which the downlink DPCH is transmitted.
- 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:

- 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:

- remove any C-RNTI from MAC;
- clear the variable C_RNTI.

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

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

- if the IE "Frequency info" is included in the received reconfiguration message:
  - select a suitable UTRA cell according to [4] on that frequency.
- if the IE "Frequency info" is not included in the received reconfiguration message:
  - select a suitable UTRA cell according to [4].
- 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):
  - initiate a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";
  - when the cell update procedure completed successfully:
    - if the UE is in CELL_PCH or URA_PCH state:
      - initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
      - proceed as below.
- 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;
- select PRACH according to subclause 8.5.17;
- select Secondary CCPCH according to subclause 8.5.19;
- use the transport format set given in system information;
- if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - ignore that IE and stop using DRX.
- if the contents of the variable C_RNTI is empty:
  - perform a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";
  - when the cell update procedure completed successfully:
    - if the UE is in CELL_PCH or URA_PCH state:
      - initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
      - 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:

- if the IE "Frequency info" is included in the received reconfiguration message:
  - select a suitable UTRA cell according to [4] on that frequency;
  - 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):
    - initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
    - when the cell update procedure completed successfully:
      - 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:

- if the received reconfiguration message included the IE "Downlink counter synchronisation info":
  - re-establish RB2;
  - set the new uplink and downlink HFN of RB2 to MAX(uplink HFN of RB2 | downlink HFN of RB2) + 1;
  - increment by one the downlink and uplink HFN values for RB2;
  - calculate the START value according to subclause 8.5.9;
  - include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
- if the received reconfiguration message did not include the IE "Downlink counter synchronisation info":
  - if the variable START_VALUE_TO_TRANSMIT is set:
    - include and set the IE "START" to the value of that variable.
  - if the variable START_VALUE_TO_TRANSMIT is not set and the IE "New U-RNTI" is included:
    - calculate the START value according to subclause 8.5.9;
    - include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
  - if the received reconfiguration message caused a change in the RLC size for any RB using RLC-AM:
    - calculate the START value according to subclause 8.5.9;
    - 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".
- if the received reconfiguration message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - set the IE “Status” in the variable SECURITY_MODIFICATION for all the CN domains ~~as indicated in the IE "CN domain identity"~~ in the variable SECURITY_MODIFICATION to “Affected”;
- if the received reconfiguration message contained the IE "Ciphering mode info":
  - include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.

~~- if the received reconfiguration message contained the IE "Integrity protection mode info" with the IE "Integrity protection mode command" set to "Modify":~~

- ~~include and set the IE "Uplink integrity protection activation info" to the value of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.~~

- if the received reconfiguration message did not contain the IE "Ciphering activation time for DPCH" in IE "Ciphering mode info":
  - if prior to this procedure there exist no transparent mode RLC radio bearers:
    - if, at the conclusion of this procedure, the UE will be in CELL_DCH state; and
    - if, at the conclusion of this procedure, at least one transparent mode RLC radio bearer exists:
      - include the IE "COUNT-C activation time" and specify a CFN value for this IE.
  - if prior to this procedure there exists at least one transparent mode RLC radio bearer:
    - if, at the conclusion of this procedure, no transparent mode RLC radio bearers exist:
      - include the IE "COUNT-C activation time" and specify a CFN value for this IE.
- 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
- clear that entry;
- if the variable PDCP_SN_INFO is not empty:
  - include the IE "RB with PDCP information list" and set it to the value of the variable PDCP_SN_INFO.
- 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):
  - set the IE "Uplink Timing Advance" according to subclause 8.6.6.26.
- if the IE "Integrity protection mode info" was present in the received reconfiguration message:
  - 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:

- if the IE "Frequency info" is included in the received reconfiguration message:
  - select a suitable UTRA cell according to [4] on that frequency.
- if the IE "Frequency info" is not included in the received reconfiguration message:
  - select a suitable UTRA cell according to [4].
- prohibit periodical status transmission in RLC;
- remove any C-RNTI from MAC;
- clear the variable C_RNTI;
- 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;
- select Secondary CCPCH according to subclause 8.5.19;
- if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 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.
- if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:

- set the variable INVALID_CONFIGURATION to TRUE.

- 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):
  - initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
  - when the cell update procedure completed successfully:
    - the procedure ends.
- 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:
  - initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
  - when the cell update procedure is successfully completed:
    - the procedure ends.
- 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:
  - initiate a URA update procedure according to subclause 8.3.1 using the cause "URA reselection";
  - when the URA update procedure is successfully completed:
    - 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:

- 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:

- 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:

- 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:

- 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:

- 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:

- if the IE "Downlink counter synchronization info" was included in the reconfiguration message:
  - when RLC has confirmed the successful transmission of the response message:

- 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;
- 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;
- set the remaining bits of the HFN values of all AM and UM RLC entities with RB identities different from 2 to zero.

- if the variable PDCP_SN_INFO is empty:
  - if the received reconfiguration message contained the IE "Ciphering mode info":
    - when RLC has confirmed the successful transmission of the response message:
      - notify upper layers upon change of the security configuration;
      - perform the actions below.
  - if the received reconfiguration message did not contain the IE "Ciphering mode info":
    - when RLC has been requested to transmit the response message:
      - perform the actions below.
- if the variable PDCP_SN_INFO is non-empty:
  - when RLC has confirmed the successful transmission of the response message:
    - for each radio bearer in the variable PDCP_SN_INFO:
      - if the IE "RB started" in the variable ESTABLISHED_RABS is set to "started":
        - configure the RLC entity for that radio bearer to "continue".
    - 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:

- when RLC has confirmed the successful transmission of the response message:
  - for each radio bearer in the variable PDCP_SN_INFO:
    - if the IE "RB started" in the variable ESTABLISHED_RABS is set to "started":
      - configure the RLC entity for that radio bearer to "continue".
  - enter the new state (CELL_PCH or URA_PCH, respectively);
  - perform the actions below.

The UE shall:

- set the variable ORDERED_RECONFIGURATION to FALSE;
- if the received reconfiguration message contained the IE "Ciphering mode info":
  - resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
  - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
  - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.

- if the received reconfiguration message contained the IE "Integrity protection mode info":
  - allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
  - 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;
  - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
  - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.
- clear the variable PDCP_SN_INFO;
- clear the variable START_VALUE_TO_TRANSMIT.
- 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:

- abort the ongoing integrity and/or ciphering reconfiguration;
- resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
- allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- transmit a failure response message as specified in subclause 8.2.2.9, setting the information elements as specified below:
  - include the IE "RRC transaction identifier"; and
  - 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
  - clear that entry;
  - set the IE "failure cause" to the cause value "cell update occurred";
  - if the received reconfiguration message contained the IE "Ciphering mode info":
    - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
    - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO;
  - if the received reconfiguration message contained the IE "Integrity protection mode info":
    - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
    - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.
- 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:

- transmit a failure response message as specified in subclause 8.2.2.9, setting the information elements as specified below:
  - include the IE "RRC transaction identifier"; and
  - 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
  - clear that entry;
  - set the IE "failure cause" to the cause value "protocol error";
  - include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL_ERROR_INFORMATION.

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, it may either:

- in case the procedure was triggered by reception of a CELL UPDATE:
  - 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";
  - 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":
    - set the 20 MSB of the MAC-d HFN with the corresponding START value in the IE "START list";
    - set the remaining LSB of the MAC-d HFN to zero.
  - transmit a CELL UPDATE CONFIRM message on the downlink DCCH or optionally on the CCCH but only if ciphering is not required; and
  - optionally include the IE "RLC re-establish indicator" to request a RLC re-establishment in the UE, in which case the corresponding RLC entities should also be re-established in UTRAN; or
- in case the procedure was triggered by reception of a URA UPDATE:
  - transmit a URA UPDATE CONFIRM message to the lower layers for transmission on the downlink CCCH or DCCH in which case the UTRAN should include the IE "URA identity" in the URA UPDATE CONFIRM message in a cell where multiple URA identifiers are broadcast; or
- 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:
  - if the CELL UPDATE message was sent because of an unrecoverable error in RB2, RB3 or RB4:
    - 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:

- stop timer T302;
- in case of a cell update procedure and the CELL UPDATE CONFIRM message:
  - includes "RB information elements"; and/or
  - includes "Transport channel information elements"; and/or
  - includes "Physical channel information elements"; and
  - if the variable ORDERED_RECONFIGURATION is set to FALSE:
    - set the variable ORDERED_RECONFIGURATION to TRUE;
- act upon all received information elements as specified in subclause 8.6, unless specified otherwise in the following:
  - if the IE "Frequency info" is included in the message:
    - if the IE "RRC State Indicator" is set to the value "CELL_FACH" or "CELL_PCH" or URA_PCH":
      - select a suitable UTRA cell according to [4] on that frequency;
      - act as specified in subclause 8.3.1.12.
    - if the IE "RRC State Indicator" is set to the value "CELL_DCH":
      - act on the IE "Frequency info" as specified in subclause 8.6.6.1.
  - use the transport channel(s) applicable for the physical channel types that is used; and
  - if the IE "TFS" is neither included nor previously stored in the UE for that transport channel(s):
    - use the TFS given in system information.
  - if none of the TFS stored is compatible with the physical channel:
    - delete the stored TFS;
    - use the TFS given in system information.
  - perform the physical layer synchronisation procedure as specified in [29];
  - if the CELL UPDATE CONFIRM message includes the IE "RLC re-establish indicator (RB2, RB3 and RB4)":
    - re-establish the RLC entities for signalling radio bearer RB2, signalling radio bearer RB3 and signalling radio bearer RB4 (if established);
    - 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":
      - 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;
  - if the CELL UPDATE CONFIRM message includes the IE "RLC re-establish indicator (RB5 and upwards)":
    - for radio bearers with RB identity 5 and upwards:
      - re-establish the AM RLC entities;

- 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":
  - 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;

- if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - set the IE “Status” in the variable SECURITY_MODIFICATION for all the CN domains ~~as indicated~~ in the ~~IE "CN domain identity"~~variable SECURITY_MODIFICATION to “Affected”;

- 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:

- not prohibit periodical status transmission in RLC;
- 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:
  - 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";
  - set the 20 MSB of the MAC-d HFN with the corresponding START value in the most recently sent IE "START list";
  - set the remaining LSB of the MAC-d HFN to zero;
  - apply ciphering on the transparent mode radio bearers;
  - 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

- 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";
- select PRACH according to subclause 8.5.17;
- select Secondary CCPCH according to subclause 8.5.19;
- not prohibit periodical status transmission in RLC;
- if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - ignore that IE and stop using DRX.

If the UE after state transition enters URA_PCH or CELL_PCH state, it shall:

- prohibit periodical status transmission in RLC;
- clear the variable C_RNTI;
- stop using that C_RNTI just cleared from the variable C_RNTI in MAC;
- 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";
- select Secondary CCPCH according to subclause 8.5.19;

- if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 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.
- if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:
  - set the variable INVALID_CONFIGURATION to TRUE.

If the UE after the state transition remains in CELL_FACH state; and

- the contents of the variable C_RNTI are empty:

it shall check the value of V302; and:

- if V302 is equal to or smaller than N302:
  - 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:
      - abort the ongoing integrity and/or ciphering reconfiguration;
      - if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
        - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
        - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.
      - if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
        - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
        - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.
  - in case of a URA update procedure:
    - stop the URA update procedure; and
    - continue with a cell update procedure.
  - 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";
  - submit the CELL UPDATE message for transmission on the uplink CCCH;
  - increment counter V302;
  - restart timer T302 when the MAC layer indicates success or failure to transmit the message.
- if V302 is greater than N302:
  - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO;
  - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO;
  - in case of a cell update procedure:
    - clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - in case of a URA update procedure:

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

- release all its radio resources;
- 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;
- clear the variable ESTABLISHED_SIGNALLING_CONNECTIONS;
- clear the variable ESTABLISHED_RABS;
- enter idle mode;
- other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
- 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:

- if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
  - 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.

- ~~if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Integrity protection mode info" with the IE "Integrity protection mode command" set to "Modify":~~
  - ~~include the IE "Uplink integrity protection activation info" in any response message transmitted below; and~~
  - ~~set this IE to the value of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO~~.

- in case of a cell update procedure:
  - 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
  - clear that entry.
- in case of a URA update procedure:
  - 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
  - clear that entry;
- if the variable PDCP_SN_INFO is non-empty:
  - 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.
- if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message included the IE "Downlink counter synchronisation info":
  - calculate the START value according to subclause 8.5.9;

- 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.

- transmit a response message as specified in subclause 8.3.1.7;
- if the IE "Integrity protection mode info" was present in the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:
  - start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.
  - ~~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;~~
- if the variable ORDERED_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:
  - set the variable ORDERED_RECONFIGURATION to FALSE.
- clear the variable PDCP_SN_INFO;
- when the response message transmitted per subclause 8.3.1.7 to the UTRAN has been confirmed by RLC:

  /* Indentation below has been changed*/
  - if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
    - resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
    - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
    - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.
  - if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
    - 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;
    - allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
    - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and

  /* Indentation above has been changed*/
  - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.
- in case of a cell update procedure:
  - clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- in case of a URA update procedure:
  - clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- set the variable CELL_UPDATE_STARTED to FALSE;~~.~~
- clear the variable SECURITY_MODIFICATION.

The procedure ends.

8.3.3.3 Reception of UTRAN MOBILITY INFORMATION message by the UE

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

- act on received information elements as specified in subclause 8.6;
- if the IE "UE Timers and constants in connected mode" is present:
  - 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
  - for each updated timer value:
    - start using the new value next time the timer is started;
  - for each updated constant value:
    - start using the new value directly;
- 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
- clear that entry;
- if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - set the IE "Status" in the variable SECURITY_MODIFICATION for all the CN domains ~~as indicated~~ in the ~~IE "CN domain identity"~~ variable SECURITY_MODIFICATION to "Affected";
- if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
  - include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.
- ~~if the UTRAN MOBILITY INFORMATION message contained the IE "Integrity protection mode info" with the IE "Integrity protection mode command" set to "Modify":~~
  - ~~include and set the IE "Uplink integrity protection activation info" to the value of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.~~
- if the variable PDCP_SN_INFO is non-empty:
  - 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.
- if the received UTRAN MOBILITY INFORMATION message included the IE "Downlink counter synchronisation info":
  - calculate the START value according to subclause 8.5.9;
  - 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.
- transmit a UTRAN MOBILITY INFORMATION CONFIRM message on the uplink DCCH using AM RLC;
- if the IE "Integrity protection mode info" was present in the UTRAN MOBILITY INFORMATION message:
  - 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.
- if the variable PDCP_SN_INFO is empty; and
  - if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":

- when RLC has confirmed the successful transmission of the UTRAN MOBILITY INFORMATION CONFIRM message, perform the actions below.

- if the UTRAN MOBILITY INFORMATION message did not contain the IE "Ciphering mode info":

- when RLC has been requested to transmit the UTRAN MOBILITY INFORMATION CONFIRM message, perform the actions below.

- if the variable PDCP_SN_INFO is non-empty:

- when RLC has confirmed the successful transmission of the UTRAN MOBILITY INFORMATION CONFIRM message:

- for each radio bearer in the variable PDCP_SN_INFO:

- if the IE "RB started" in the variable ESTABLISHED_RABS is set to "started":

- configure the RLC entity for that radio bearer to "continue".

- clear the variable PDCP_SN_INFO.

- if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":

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

- set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and

- clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.

- if the UTRAN MOBILITY INFORMATION message contained the IE "Integrity protection mode info":

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

- set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and

- clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.

- clear the variable SECURITY_MODIFICATION.

The procedure ends.

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:

- first add the RLs indicated in the IE "Radio Link Addition Information";

- 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;

- perform the physical layer synchronisation procedure as specified in [29];

- if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":

- set the IE “Status” in the variable SECURITY_MODIFICATION for all the CN domains ~~as indicated~~ in the ~~IE "CN domain identity"~~ variable SECURITY_MODIFICATION to “Affected”;

- if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":

- include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.

~~- if the ACTIVE SET UPDATE message contained the IE "Integrity protection mode info" with the IE "Integrity protection mode command" set to "Modify":~~

~~- include and set the IE "Uplink integrity protection activation info" to the value of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO~~.

- if the variable PDCP_SN_INFO is non-empty:
  - include the IE "RB with PDCP information list" in the ACTIVE SET UPDATE COMPLETE message; and
  - set it to the value of the variable PDCP_SN_INFO.
- if the IE "TFCI combining indicator" associated with a radio link to be added is set to TRUE:
  - if a DSCH transport channel is assigned and there is a 'hard' split in the TFCI field:
    - configure Layer 1 to soft-combine TFCI (field 2) of this new link with those links already in the TFCI (field 2) combining set.
- if the received ACTIVE SET UPDATE message included the IE "Downlink counter synchronisation info":
  - calculate the START value according to subclause 8.5.9;
  - 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.
- 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
- clear that entry;
- transmit an ACTIVE SET UPDATE COMPLETE message on the uplink DCCH using AM RLC without waiting for the Physical Layer synchronization;
- if the IE "Integrity protection mode info" was present in the ACTIVE SET UPDATE message:
  - 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.
- if the variable PDCP_SN_INFO is empty:
  - if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":
    - when RLC has confirmed the successful transmission of the ACTIVE SET UPDATE COMPLETE message:
      - perform the actions below.
  - if the ACTIVE SET UPDATE message did not contain the IE "Ciphering mode info":
    - when RLC has been requested to transmit the ACTIVE SET UPDATE COMPLETE message:
      - perform the actions below.
- if the variable PDCP_SN_INFO is non-empty:
  - when RLC has confirmed the successful transmission of the ACTIVE SET UPDATE COMPLETE message:
    - for each radio bearer in the variable PDCP_SN_INFO:
      - if the IE "RB started" in the variable ESTABLISHED_RABS is set to "started":
        - configure the RLC entity for that radio bearer to "continue".

- clear the variable PDCP_SN_INFO.

- if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":
  - resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
  - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
  - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.
- if the ACTIVE SET UPDATE message contained the IE "Integrity protection mode info":
  - allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
  - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
  - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.
- clear the variable SECURITY_MODIFICATION;
- the procedure ends on the UE side.

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:

- 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
- initialise the variable ESTABLISHED_SIGNALLING_CONNECTIONS with the signalling connections that remains after the handover according to the specifications of the source RAT;
- 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;
- initialise the variable TIMERS_AND_CONSTANTS to the default values and start to use those timer and constants values;
- if IE "Specification mode" is set to "Preconfiguration" and IE "Preconfiguration mode" is set to "Predefined configuration":
  - initiate the radio bearer and transport channel configuration in accordance with the predefined parameters identified by the IE "Predefined configuration identity";
  - 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;
  - store information about the established radio access bearers and radio bearers according to the IE "Predefined configuration identity"; and
  - 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".

- if IE "Specification mode" is set to "Preconfiguration" and IE "Preconfiguration mode" is set to "Default configuration":
  - 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";
  - 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

  - 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".

- if IE "Specification mode" is set to "Preconfiguration":
  - 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:
    - 0 dB for the power offset $P_{Pilot\text{-}DPDCH}$ bearer in FDD;
    - calculate the Default DPCH Offset Value using the following formula:
      - in FDD:

$$\text{Default DPCH Offset Value} = (\text{SRNTI } 2 \bmod 600) * 512$$

      - in TDD:

$$\text{Default DPCH Offset Value} = (\text{SRNTI } 2 \bmod 7)$$

    - 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.

- if IE "Specification mode" is set to "Complete specification":
  - initiate the radio bearer, transport channel and physical channel configuration in accordance with the received radio bearer, transport channel and physical channel information elements.

- perform an open loop estimation to determine the UL transmission power according to subclause 8.5.3;

~~- calculate START according to subclause 8.5.9 for all CN domains~~

- 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~~with the calculated START value~~ ;

- if ciphering has been activated and ongoing in the radio access technology from which inter- RAT handover is performed:
  - 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":

    ~~- set the HFN component of the COUNT-C variable for all UL and DL radio bearers and all UL and DL signalling radio bearers that use RLC-AM and RLC-UM to the START value as stored in the USIM for that CN domain, if present or as stored in the UE if the USIM is not present; and~~

    ~~- if a "START" value was transferred prior to the handover according to the IE "UE security information" in the IEvariable " INTER_RAT_HANDOVER_INFO_TRANSFERRED";~~

    - set the 20 MSB of the HFN component of the COUNT-C variable for all ~~TM~~ 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" ;/*CHANGED TO B3*/

    ~~else:~~

- ~~set the 20 MSB of the HFN component of the COUNT-C variable for all TM radio bearers to zero;~~
- 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;
- not increment the HFN component of COUNT-C for ~~TM~~ radio bearers using RLC-TM, i.e. keep the HFN value fixed without incrementing every CFN cycle;
- set the CFN component of the COUNT-C variable to the value of the CFN as calculated in subclause 8.5.15;
- ~~set the HFN component of the COUNT-C variable for all UL and DL radio bearers and all UL and DL signalling radio bearers that use the transparent mode of RLC to zero, while not incrementing the value of the HFN component of the COUNT-C variable at each CFN cycle; and~~
- ~~set the CFN component of the COUNT-C variable to the value of the CFN as calculated in subclause 8.5.15;~~
- set the IE "Status" in the variable CIPHERING_STATUS to "Started";
- ~~apply the same ciphering status (ciphered/unciphered) as prior to inter-RAT handover;~~
- ~~if the change of algorithm is requested by means of the IE "Ciphering algorithm":~~
- apply ~~this~~ the algorithm according to IE "Ciphering Algorithm" and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND. /*CHANGED TO B3*/

- if ciphering has not been activated and ongoing in the radio access technology from which inter- RAT handover is performed:
  - 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":
    - set the IE "Status" in the variable CIPHERING_STATUS to "Not Started";

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

- 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:
  - include the IE "COUNT-C activation time" in the response message and specify a CFN value other than the default, "Now" for this IE;
  - at the CFN value as indicated in the response message in the IE "COUNT-C activation time" for radio bearers using RLC-TM:
    - 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
    - set the remaining LSBs of the HFN component of COUNT-C to zero;
    - increment the HFN component of the COUNT-C variable by one;
    - 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;
    - 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.
- transmit a HANDOVER TO UTRAN COMPLETE message on the uplink DCCH, using, if ciphering has been started, the new ciphering configuration~~, only if ciphering has been started~~;
- when the HANDOVER TO UTRAN COMPLETE message has been submitted to lower layers for transmission:
  - initialise variables upon entering UTRA RRC connected mode as specified in subclause 13.4~~.~~;

- for all radio bearers using RLC-AM or RLC-UM:
  - 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
  - set the remaining LSBs of the HFN component of COUNT-C to zero;
  - increment the HFN component of the COUNT-C variable by one;
  - start incrementing the COUNT-C values;
- and the procedure ends.

8.3.7.4 Successful completion of the inter-RAT handover

Upon successfully completing the handover, UTRAN should:

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

Upon successfully completing the handover, the UE shall:

- if the USIM is present:
  - store the current START value for every CN domain in the USIM [50];
  - 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:
    - delete the ciphering and integrity keys that are stored in the USIM for that CN domain;
    - inform the deletion of these keys to upper layers.
- if the SIM is present:
  - store the current START value for every CN domain in the UE;
  - 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:
    - delete the ciphering and integrity keys that are stored in the SIM for that CN domain;
    - inform the deletion of these keys to upper layers.
- 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.

8.5.2 Actions when entering idle mode from connected mode

When entering idle mode from connected mode, the UE shall:

- clear or set variables upon leaving UTRA RRC connected mode as specified in subclause 13.4;
- attempt to select a suitable cell to camp on.

When leaving connected mode according to [4], the UE shall:

- perform cell selection.

While camping on a cell, the UE shall:

- acquire system information according to the system information procedure in subclause 8.1;

- perform measurements according to the measurement control procedure specified in subclause 8.4; and
- if the UE is registered:
  - be prepared to receive paging messages according to the paging procedure in subclause 8.2.

If IE "PLMN identity" within variable SELECTED_PLMN has the value "GSM-MAP", the UE shall:

- delete any NAS system information received in connected mode;
- acquire the NAS system information in system information block type 1; and
- proceed according to subclause 8.6.1.2.

When entering idle mode, the UE shall:

- if the USIM is present, for each CN domain:
  - if a new security key set was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:
    - set the START value for this domain to ~~0~~zero and;
    - store this START value for this domain in the USIM;
  - else:
  - if the current "START" value, according to chapter 8.5.9~~,~~ for a CN domain, is greater than or equal to the value "THRESHOLD" of the variable START_THRESHOLD:
    - delete the ciphering and integrity keys that are stored in the USIM for that CN domain;
    - inform the deletion of these keys to upper layers.
  - else
    - store the current "START" value for this CN domain on the USIM.
- else, if the SIM is present:
  - if the current "START" value, according to ~~chapter~~subclause 8.5.9~~,~~ for a CN domain, is greater than or equal to the value "THRESHOLD" of the variable START_THRESHOLD:
    - delete the Kc key that is stored in the SIM;
    - set the "START" values for both CN domains to zero and store them in the UE;
    - inform the deletion of these keys to upper layers.
  - else
    - store the current "START" value for every CN domain in the UE~~.~~

~~- if the USIM is present:~~

~~- store the current START value for every CN domain in the USIM [50];~~

~~- 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:~~

~~- delete the ciphering and integrity keys that are stored in the USIM for that CN domain;~~

~~- set the value of START value to THRESHOLD;~~

~~- inform the deletion of these keys to upper layers.~~

8.5.8 Maintenance of Hyper Frame Numbers

The MSBs of both the ciphering sequence numbers (COUNT-C) and integrity sequence numbers (COUNT-I), for the ciphering and integrity protection algorithms, respectively [40], are called the Hyper Frame Numbers (HFN).

For integrity protection, the UE shall:

- maintain COUNT-I as specified in subclause 8.5.10.

The following hyper frame numbers types are defined:

MAC-d HFN:
24 MSB of COUNT-C for data sent over RLC TM

RLC UM HFN:
25 MSB of COUNT-C for data sent over RLC UM

RLC AM HFN:
20 MSB of COUNT-C for data sent over RLC AM

RRC HFN:
28 MSB of COUNT-I

For non-transparent mode RLC signalling radio bearers and radio bearers, the UE shall:

- maintain one uplink and one d~~o~~wnlink COUNT-C per signalling radio bearer and per radio bearer and one uplink and one downlink COUNT-I per signalling radio bearer.

For all transparent mode RLC signalling radio bearers and radio bearers of each CN domain, the UE shall:

- maintain one COUNT-C, common for all signalling radio bearers and radio bearers in uplink and downlink;
- maintain one uplink and one downlink COUNT-I per signalling radio bearer.

NOTE: In this release of the specification there is only an uplink transparent mode COUNT-I, which is used for signalling radio bearer RB0.

COUNT-C and COUNT-I are defined in [40], with the following supplement for COUNT-C: for transparent mode RLC radio bearers with a transmission time interval of x radio frames (x = 2, 4, 8), the MAC PDU is carried by L1 in x consecutive radio frames due to radio frame segmentation. In this case, ~~the CFN of the first segment of the MAC PDU is used as the CFN component of COUNT-C.~~the CFN of the first radio frame in the TTI shall be used as the CFN component of COUNT-C for ciphering of all data ~~all radio frames~~ in the TTI [15].

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 | radio bearers and signalling radio bearers using the most recently configured CK_X and IK_X}) + 2~~1~~.

- 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~~1~~: 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 $START_X'$.

~~NOTE2: COUNT-C corresponding to non-ciphered radio bearers using RLC-AM or RLC-UM shall not be included in the calculation of the START$_X$'. If Ciphering is stopped on one RB, the values of the COUNT-C at the time ciphering is stopped shall remain in the calculation of the START$_X$'.~~

COUNT-C corresponding to non-ciphered radio bearers 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 ~~remain~~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:

- 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.

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:

- check the value of the IE "RRC message sequence number" included in the IE "Integrity check info";
  - if the "Downlink RRC Message sequence number" is not present in the variable INTEGRITY_PROTECTION_INFO:
    - 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.
  - if the "Downlink RRC Message sequence number" is present in the variable INTEGRITY_PROTECTION_INFO:
    - 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:
      - increment "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with one.
    - 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:
      - discard the message.
- calculate an expected message authentication code in accordance with subclause 8.5.10.3;
- compare the expected message authentication code with the value of the received IE "message authentication code" contained in the IE "Integrity check info";
  - if the expected message authentication code and the received message authentication code are the same, the integrity check is successful:
    - 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.
  - if the calculated expected message authentication code and the received message authentication code differ:
    - 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):
      - decrement "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO by one.
    - 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:

- discard the message.

8.5.10.2 Integrity protection in uplink

Prior to sending an RRC message using the signalling radio bearer with radio bearer identity n, and the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" the UE shall:

- increment "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with 1. When "Uplink RRC Message sequence number" for signalling

radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO becomes 0, the UE shall increment "Uplink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with 1;

- calculate the message authentication code in accordance with subclause 8.5.10.3;
- replace the "Message authentication code" in the IE "Integrity check info" in the message with the calculated message authentication code;
- replace the "RRC Message sequence number" in the IE "Integrity check info" in the message with contents set to the new value of the "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO.

In the response message for the procedure ordering the security reconfiguration, the UE indicates the activation time, for each signalling radio bearer except for the signalling radio bearer that was used for this security reconfiguration procedure. When the new integrity configuration is to be applied in uplink, UTRAN should start to apply the new integrity protection configuration according to the activation time for each signalling radio bearer (except for the signalling radio bearer which is used to send the message that is reconfiguring the security configuration) where the new configuration is to be applied starting from and including reception of the response message).

8.5.10.3 Calculation of message authentication code

The UE shall calculate the message authentication code in accordance with [40]. The input parameter MESSAGE [40] for the integrity algorithm shall be constructed by:

- setting the "Message authentication code" in the IE "Integrity check info" in the message to the value of the IE "RB identity" ~~the radio bearer identity~~ for the signalling radio bearer;
- setting the "RRC Message sequence number" in the IE "Integrity check info" in the message to zero;
- encoding the message;
- appending RRC padding (if any) as a bit string to the encoded bit string as the least significant bits.

For usage on an RRC message transmitted or received on the radio bearer with identity n, the UE shall:

- construct the input parameter COUNT-I [40] by appending the following IEs from the IE "Signalling radio bearer specific integrity protection information" for radio bearer n in the variable INTEGRITY_PROTECTION_INFO:
  - for uplink:
    - "Uplink RRC HFN", as the MSB, and "Uplink RRC Message sequence number", as LSB.
  - for downlink:
    - "Downlink RRC HFN", as the MSB, and the IE "RRC message sequence number" included in the IE "Integrity check info", as LSB.

8.6.3.4 Ciphering mode info

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

If the IE "Ciphering mode info" is present and if the IE "Reconfiguration" in the variable CIPHERING_STATUS is set to TRUE, the UE shall:

- ignore this second attempt to change the ciphering configuration; and
- set the variable INCOMPATIBLE_SECURITY_RECONFIGURATION to TRUE.

If the IE "Ciphering mode info" is present and if the IE "Reconfiguration" in the variable CIPHERING_STATUS is set to FALSE, the UE shall:

- ~~if the IE "Status" in the variable CIPHERING_STATUS of the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN has the value "Not Started", and if the IE "Ciphering mode command" has the value "stop"; or~~

- 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

- if there does not exist exactly one ciphering activation time in the IE "Radio bearer downlink ciphering 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

- ~~if there does not exist exactly one ciphering activation time in the IE "Ciphering activation time for DPCH" for each established RLC-TM 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~~

- if the IE "Ciphering activation time for DPCH" is not included in message ACTIVE SET UPDATE or SECURITY MODE COMMAND, and there exist ~~RLC-TM~~ 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

- 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":

  - ignore this attempt to change the ciphering configuration;

  - set the variable INVALID_CONFIGURATION to TRUE;

  - perform the actions as specified in subclause 8.1.12.4c.

- set the IE "Reconfiguration" in the variable CIPHERING_STATUS to TRUE;

- ~~if IE "Ciphering mode command" has the value "start/restart":~~

- set the IE "Status" in the variable CIPHERING_STATUS of the~~this~~ CN domains for which the IE “Status” of the variable SECURITY_MODIFICATION is set to “Affected”~~domain~~ to "Started";

- ~~start or restart~~apply the new ciphering configuration in the lower layers for all RBs ~~and SRBs~~ 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:

  - using the ciphering algorithm (UEA [40]) indicated by the IE "Ciphering algorithm" as part of the new ciphering configuration;

  - for each radio bearer ~~and signalling 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:

    - use the value of the IE "RB identity" in the variable ESTABLISHED_RABS minus one as the value of BEARER [40] in the ciphering algorithm.

    - ~~start incrementing the COUNT-C values for all RLC-AM and RLC-UM signalling radio bearers and continue incrementing the COUNT-C values for all RLC-AM and RLC-UM radio bearers;~~

    - ~~if at least one transparent mode radio bearer exists for this CN domain and ciphering was started for this CN domain;~~

      - ~~continue incrementing the COUNT-C value for this CN domain.~~

    - ~~else:~~

~~- start incrementing the COUNT-C values for that CN domain at the ciphering activation time as specified in the procedure.~~

~~NOTE: If the ciphering activation time for transparent mode radio bearers was specified in the downlink then the IE "Ciphering activation time for DPCH" is included (e.g. for the SECURITY MODE COMMAND), otherwise, this ciphering activation time is specified in the IE "COUNT-C activation time" in the uplink response message.~~

~~- if the IE "Ciphering mode command" has the value "stop":~~

~~- when the new ciphering configuration is applied at the time as specified below:~~

~~- stop ciphering for all radio bearers for this CN domain and all signalling radio bearers;~~

~~- stop incrementing COUNT-C values for all UL and DL signalling radio bearers and also for UL and DL radio bearers using RLC-TM;~~

~~- continue incrementing COUNT-C values for all UL and DL radio bearers using RLC-UM or RLC-AM.~~

~~- set the IE "Status" in the variable CIPHERING_STATUS of the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN to "Not started".~~

- ~~in case the IE "Ciphering mode command" has the value "start/restart", or "stop",~~ the new ciphering configuration shall be applied as follows:

~~- store the (oldest currently used) ciphering configuration until activation times have elapsed for the new ciphering configuration to be applied on all signalling radio bearers and radio bearers;~~

- consider an activation time in downlink to be pending:

  - for UM-RLC until an UMD PDU with sequence number equal to or larger than activation time –1 has been received;

  - for AM-RLC until all AMD PDUs with sequence numbers up to and including activation time –1 have been received;

  - for TM-RLC until the CFN indicated in the activation time has been reached;

- if there are pending activation times in downlink set for ciphering by a previous procedure changing the ciphering configuration:

  - apply the ciphering configuration included in the current message at this pending activation time.

- 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:

  - for radio bearers using RLC-TM:

  - apply the old ciphering configuration for CFN less than the number indicated in the IE "Ciphering activation time for DPCH";

  - apply the new ciphering configuration for CFN greater than or equal to the number indicated in IE "Ciphering activation time for DPCH".

- 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":

  - for radio bearers using RLC-TM:

  - apply the old ciphering configuration for CFN less than the number as indicated in the transmitted uplink response message for the ciphering activation time for this radio bearer;

  - 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.

- if the IE "Radio bearer downlink ciphering activation time info" is present:
  - apply the following procedure for each radio bearer and signalling radio bearers using RLC-AM or RLC-UM indicated by the IE "RB identity":
    - ~~suspend uplink transmission on the radio bearer or the signalling radio bearer (except for that SRBm that the message was used~~);
    - 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:
      - do not transmit RLC PDUs with sequence number greater than or equal to the uplink activation time, where the uplink activation time is seclected according to the rules below;
    - 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:
      - for each radio bearer and signalling radio bearer that has no pending ciphering activation time in the uplink as set by a previous procedure changing the security configuration:
        - set a suitable value that would ensure a minimised delay in the change to the latest security configuration.
      - 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:
        - set the same value as the pending ciphering activation time.
      - consider this activation time in uplink to be elapsed when the selected activation time (as above) is equal to the "RLC send sequence number";
    - 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;
    - ~~when the data transmission of that radio bearer or signalling radio bearer is resumed:~~

    /* Indentation has been changed in the following bullets*/
    - switch to the new ciphering configuration according to the following:
      - 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;
      - 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;
      - 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;
      - 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.

    /* Indentation has been changed in the above bullets*/

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

- 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 ~~two~~ three different integrity protection configurations (keysets) in total for all signalling radio bearers for all CN domains.~~, the old and newest integrity protection configurations, per CN domain~~.

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:

- ignore this second attempt to change the integrity protection configuration; and
- 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:

- set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to TRUE;
- 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:
  - initialise the information for all signalling radio bearers in the variable INTEGRITY_PROTECTION_INFO according to the following:
    - set the IE "Uplink RRC Message sequence number" in the variable INTEGRITY_PROTECTION_INFO to zero;
    - do not ~~include~~ set the IE "Downlink RRC Message sequence number" ~~which is included~~ in the variable INTEGRITY_PROTECTION_INFO;~~.~~
    - set the variable INTEGRITY_PROTECTION_ACTIVATION_INFO to zero for each signalling radio berer in the IE "ESTABLISHED_RABS".
  - set the IE "Status" in the variable INTEGRITY_PROTECTION_INFO to the value "Started";
  - perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:
    - using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";
    - using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].
    - 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;
    - start applying the new integrity protection configuration in the downlink for signalling radio bearer RB2 from and including the received SECURITY MODE COMMAND message;
    - start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;
    - 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".
- 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

- perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:
  - using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";
  - using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].
  - let RBm be the signalling radio bearer where the reconfiguration message was received and let RBn be the signalling radio bearer where the response message is transmitted;
- 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;
- ~~apply the new integrity protection configuration in the downlink for the first message expected to be received and all subsequent messages;~~
- ~~apply the new integrity protection configuration in the uplink for the first message transmitted and all subsequent messages;~~
  - 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;
  - start applying the new integrity protection configuration in the downlink for signalling radio bearer RBm from and including the received configuration message;
  - start applying the new integrity protection configuration in the uplink for signalling radio bearer RBn from and including the transmitted response message;
  - 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".

- 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:
  - 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;
  - if there are pending activation times set for integrity protection by a previous procedure changing the integrity protection configuration:
    - apply the integrity protection configuration at this pending activation time as indicated in this procedure.
  - 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";
  - perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1;
    - if present, use the algorithm indicated by the IE "Integrity protection algorithm" (UIA [40]);
  - ~~let RBm be the signalling radio bearer on which the message containing the IE "integrity protection mode info" was received;~~
  - set the content of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO according to the following:
    - for each established signalling radio bearer, stored in the variable ESTABLISHED_RABS:

- 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:
  - 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:
    - set a suitable value that would ensure a minimised delay in the change to the latest integrity protection configuration.
  - for signalling radio bearer that has a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
    - set the same value as the pending activation time for integrity protection;
  - 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.
- for signalling radio bearer RB0:
  - 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.
- prohibit the transmission of RRC messages on all signalling radio bearers, except for RB2~~m~~, 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.

- start applying the new integrity protection configuration in the uplink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2~~m~~, 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;
- start applying the new integrity protection configuration in the uplink at the RRC sequence number for signalling radio bearer RB2~~m~~, as specified for the procedure initiating the integrity protection reconfiguration;
- start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2~~m~~, 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".

- start applying the new integrity protection configuration in the downlink at the RRC sequence number for signalling radio bearer RB2~~m~~, 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:

- ignore this attempt to change the integrity protection configuration; and
- set the variable INVALID_CONFIGURATION to TRUE.

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

- not change the integrity protection configuration.

8.6.4.1 Signalling RB information to setup list

If the IE "Signalling RB information to setup list" is included the UE shall:

- use the same START value to initialise the COUNT-C and COUNT-I variables for all the signalling radio bearers in the list;
- if the IE "Signalling RB information to setup list" was included in the RADIO BEARER SETUP message:
  - if the variable "LATEST_CONFIGURED_CN_DOMAIN" has been initialised:
    - calculate the START value only once during this procedure according to subclause 8.5.9 for the CN domain indicated in the variable "LATEST_CONFIGURED_CN_DOMAIN";
    - store the calculated START value in the variable START_VALUE_TO_TRANSMIT;
- for each occurrence of the IE "Signalling RB information to setup":
  - use the value of the IE "RB identity" as the identity of the signalling radio bearer to setup;
  - if the signalling radio bearer identified with the IE "RB identity" does not exist in the variable ESTABLISHED_RABS:
    - create a new entry for the signalling radio bearer in the variable ESTABLISHED_RABS;
  - if the variable LATEST_CONFIGURED_CN_DOMAIN has been initialised and the value "STATUS" of the variable "CIPHERING_STATUS" of the CN domain stored in this variable is "Started":
    - if the IE "Uplink RLC mode" or the IE "Downlink RLC mode" either in the IE "RLC info" or referenced by the RB identity in the IE "Same as RB" is set to "AM RLC" or "UM RLC":
      - initialise the 20 MSB of the hyper frame number component of COUNT-C for this signalling radio bearer with the START value in the variable START_VALUE_TO_TRANSMIT~~for the CN domain as indicated in the variable "LATEST_CONFIGURED_CN_DOMAIN";~~
      - set the remaining LSB of the hyper frame number component of COUNT-C for this signalling radio bearer to zero.
      - start to perform ciphering on this signaling radio bearer, using the value of the IE "RB identity" minus one as the value of BEARER in the ciphering algorithm.
  - if the variable LATEST_CONFIGURED_CN_DOMAIN has been initialised and the value "Status" of the variable "INTEGRITY_PROTECTION_INFO" of the CN domain stored in this variable is "Started":

- initialise the 20 MSB of the hyper frame number component of COUNT-I for this signalling radio bearer with the START value in the variable START_VALUE_TO_TRANSMIT~~for the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN~~;

- set the remaining LSB of the hyper frame number component of COUNT-I for this signalling radio bearer to zero;

- for this signalling radio bearer, set the IE "Uplink RRC Message sequence number" in the variable INTEGRITY_PROTECTION_INFO to zero.

- start performing integrity protection according to subclause 8.5.10.1 and 8.5.10.2

- perform the actions for the IE "RLC info" as specified in subclause 8.6.4.9, applied for that signalling radio bearer;

- perform the actions for the IE "RB mapping info" as specified in subclause 8.6.4.8, applied for that signalling radio bearer.

- apply a default value of the IE "RB identity" equal to 1 for the first IE "Signalling RB information to setup"; and

- increase the default value by 1 for each occurrence.

8.6.4.2 RAB information for setup

If the IE "RAB information for setup" is included, the procedure is used to establish radio bearers belonging to a radio access bearer, and the UE shall:

- if several IEs "RAB information for setup" are included and the included IEs "CN domain identity" in the IE "RAB info" does not all have the same value:

  - set the variable INVALID_CONFIGURATION to TRUE.

- if the radio access bearer identified with the IE "RAB info" does not exist in the variable ESTABLISHED_RABS:

  - create a new entry for the radio access bearer in the variable ESTABLISHED_RABS;

  - store the content of the IE "RAB info" in the entry for the radio access bearer in the variable ESTABLISHED_RABS;

  - indicate the establishment of the radio access bearer to the upper layer entity using the IE "CN domain identity", forwarding the content of the IE "RAB identity";

  - if prior to this procedure there exists no transparent mode radio bearer for the CN domain included in the IE "CN domain identity" and at least one transparent mode radio bearer is included in the IE "RB information to setup"; or

  - if at least one RLC-AM or RLC-UM radio bearer is included in the IE "RB information to setup":

    - calculate the START value only once during this procedure (the same START value shall be used on all new radio bearers created for this radio access bearer) according to subclause 8.5.9 for the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" part of the IE "RAB information to setup";

    - store the calculated START value in the variable START_VALUE_TO_TRANSMIT.

- for each radio bearer in the IE "RB information to setup":

  - if the radio bearer identified with the IE "RB identity" does not exist in the variable ESTABLISHED_RABS:

    - perform the actions specified in subclause 8.6.4.3;

    - store information about the new radio bearer in the entry for the radio access bearer identified by "RAB info" in the variable ESTABLISHED_RABS;

    - create a new RAB subflow for the radio access bearer;

- number the RAB subflow in ascending order, assigning the smallest number to the RAB subflow corresponding to the first radio bearer in the list;
- if the IE "CN domain identity" in the IE "RAB info" is set to "PS domain" and the number of RAB subflows for the radio access bearer is greater than 1:
  - set the variable INVALID_CONFIGURATION to TRUE.

- if the radio bearer identified with the IE "RB identity" already exists in the variable ESTABLISHED_RABS:
  - set the variable INVALID_CONFIGURATION to TRUE.

8.6.4.2a RAB information to reconfigure

If the IE "RAB information to reconfigure" is included then the UE shall:

- if the entry for the radio access bearer identified by the IE "CN domain identity" together with the IE "RAB Identity" in the variable ESTABLISHED_RABS already exists:
  - perform the action for the IE "NAS Synchronization Indicator", according to subclause 8.6.4.12.
- else:
  - set the variable INVALID_CONFIGURATION to TRUE.

8.6.4.3 RB information to setup

If the IE "RB information to setup" is included, the UE shall apply the following actions on the radio bearer identified with the value of the IE "RB identity". The UE shall:

- use the same START value to initialise the hyper frame number components of COUNT-C variables for all the new radio bearers to setup;
- perform the actions for the IE "PDCP info", if present, according to subclause 8.6.4.10, applied for the radio bearer;
- perform the actions for the IE "RLC info", according to subclause 8.6.4.9, applied for the radio bearer;
- perform the actions for the IE "RB mapping info", according to subclause 8.6.4.8, applied for the radio bearer;
- if the IE "Downlink RLC mode" either in the IE "RLC info" or referenced by the RB identity in the IE "Same as RB" is set to "TM RLC":
  - configure delivery of erroneous SDUs in lower layers according to indication from upper layer [5].
- if the IE "Uplink RLC mode" or the IE "Downlink RLC mode" either in the IE "RLC info" or referenced by the RB identity in the IE "Same as RB" is set to "AM RLC" or "UM RLC":
  - initialise the 20 MSB of the hyper frame number component of COUNT-C for this radio bearer with the START value in the variable START_VALUE_TO_TRANSMIT;
  - set the remaining LSB of the hyper frame number component of COUNT-C for this radio bearer to zero;
  - start incrementing the COUNT-C values.
- if the IE "Uplink RLC mode" and the IE "Downlink RLC mode" either in the IE "RLC info" or referenced by the RB identity in the IE "Same as RB" is set to "TM RLC":
  - if prior to this procedure there exists no transparent mode radio bearer for the CN domain included in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED_RABS and at least one transparent mode radio bearer is included in the IE "RB information to setup":
    - ~~A~~at the activation time as specified in the IE "Ciphering activation time for DPCH" if included in the IE "Ciphering mode info" in the command message or, if this IE is not included, as specified in the IE "COUNT-C activation time" included in the response message:

- initialise the 20 ~~MSB~~most significant bits of the hyper frame number component of COUNT-C common for all transparent mode radio bearers of this CN domain with the START value in the variable START_VALUE_TO_TRANSMIT;
- set the remaining LSB of the hyper frame number component of COUNT-C to zero;
- if 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 "Not Started":
  - do not increment the COUNT-C value for this CN domain;
- else, if 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":
  - start increment the COUNT-C value for this CN domain;

- if prior to this procedure there exists at least one transparent mode radio bearer for the CN domain included in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED_RABS:
  - continue incrementing the COUNT-C value common for all transparent mode radio bearers of this CN domain.

~~- if no other transparent mode RLC radio bearers and signalling radio bearers exist in the variable ESTABLISHED_RABS:~~

~~- initialise the 20 MSB of the hyper frame number component of COUNT-C for this radio bearer with the START value in the variable START_VALUE_TO_TRANSMIT;~~

~~- set the remaining LSB of the hyper frame number component of COUNT-C for this radio bearer to zero.~~

~~- if at least one transparent mode RLC radio bearers or signalling radio bearers exist in the variable ESTABLISHED_RABS:~~

~~- set the MAC-d HFN component of the COUNT-C for this radio bearer with the MAC-d HFN that is common (refer to subclause 8.5.8) for the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" part of the IE "RAB information for setup".~~

- if 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":
  - start to perform ciphering on the radio bearer in lower layers, using the value of the IE "RB identity" minus one as the value of BEARER in the ciphering algorithm.

NOTE: UTRAN should not use the IE "RB information to setup" to setup radio bearers with RB identity in the range 1-4.

8.6.4.8 RB mapping info

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

- for each multiplexing option of the RB:
  - 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:
    - set the variable INVALID_CONFIGURATION to TRUE.
  - if a multiplexing option that maps a logical channel corresponding to a TM-RLC entity onto RACH, CPCH, FACH or DSCH is included:
    - set the variable INVALID_CONFIGURATION to TRUE.
  - 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"):

- set the variable INVALID_CONFIGURATION to TRUE.

- 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:
  - set the variable INVALID_CONFIGURATION to TRUE.
- 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:
  - set the variable INVALID_CONFIGURATION to TRUE.
- if that RB is using UM or TM and the multiplexing option realises it using two logical channels:
  - set the variable INVALID_CONFIGURATION to TRUE.
- for each logical channel in that multiplexing option:
  - if the value of the IE "RLC size list" is set to "Explicit list":
    - 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
    - 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
    - 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
    - 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":
      - set the variable INVALID_CONFIGURATION to TRUE.
  - if the value of the IE "RLC size list" is set to "All":
    - 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
    - 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":
      - set the variable INVALID_CONFIGURATION to TRUE.
  - if the value of the IE "RLC size list" is set to "Configured":
    - 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
    - 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:

- set the variable INVALID_CONFIGURATION to TRUE.

- 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:
  - set the variable INVALID_CONFIGURATION to TRUE.
- delete all previously stored multiplexing options for that radio bearer;
- store each new multiplexing option for that radio bearer;
- select and configure the multiplexing options applicable for the transport channels to be used;
- if the IE "Uplink transport channel type" is set to the value "RACH":
  - 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.
- 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
- in case the selected multiplexing option is a multiplexing option on RACH:
  - ignore the RLC size indexes that do not correspond to any RLC size within the Transport Format Set stored for RACH.
- 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:
  - 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.
- 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:
  - re-establish the corresponding RLC entity;
  - configure the corresponding RLC entity with the new RLC size;
  - 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
  - for each AM RLC signalling radio bearer in the the CN domain as indicated in the IE "CN domain identity" in the variable LATEST_CONFIGURED_CN_DOMAIN whose RLC size is changed:
  - ~~for the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED_RABS for all radio bearers; and~~
  - ~~for the CN domain as indicated in the IE "CN domain identity" in the variable LATEST_CONFIGURED_CN_DOMAIN for all signalling radio bearers:~~
    - if the IE "Status" in the variable CIPHERING_STATUS of this CN domain is set to "Started":
      - if this IE was included in system information:
        - 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.
      - if this IE was included in CELL UPDATE CONFIRM:
        - 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.

- if this IE was included in a reconfiguration message:
  - 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.

- if that RB is using UM:
  - indicate the largest applicable RLC size to the corresponding RLC entity.
- 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);
- configure the MAC with the logical channel priorities according to selected multiplexing option;
- configure the MAC with the set of applicable RLC Sizes for each of the logical channels used for that RB;
- if there is no multiplexing option applicable for the transport channels to be used:
  - set the variable INVALID_CONFIGURATION to TRUE.
- if there is more than one multiplexing option applicable for the transport channels to be used:
  - set the variable INVALID_CONFIGURATION to TRUE.

In case IE "RB mapping info" includes IE "Downlink RLC logical channel info" but IE "Number of downlink RLC logical channels" is absent, 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:

- 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":
  - ignore that System Information Block.
- 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’:
  - ignore that System Information Block.
- 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’:
  - keep the transport format set if this exists for that transport channel;
  - set the variable INVALID_CONFIGURATION to TRUE.
- 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

- 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
- 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
- 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
- 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
- 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
- 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":
  - keep the transport format set if this exists for that transport channel;
  - set the variable INVALID_CONFIGURATION to TRUE.
- if the total number of configured transport formats for the transport channel exceeds maxTF:
  - keep the transport format set if this exists for that transport channel;
  - set the variable INVALID_CONFIGURATION to TRUE.
- if the IE "Transport format set" is considered as valid according to the rules above:
  - remove a previously stored transport format set if this exists for that transport channel;
  - store the transport format set for that transport channel;
  - 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;
  - if the IE "Transport format Set" has the choice "Transport channel type" set to "Dedicated transport channel":
    - calculate the transport block size for all transport formats in the TFS using the following

      TB size = RLC size + 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.
  - if the IE "Transport format Set" has the choice "Transport channel type" set to "Common transport channel":
    - calculate the transport block size for all transport formats in the TFS using the following:

      TB size = RLC size.
  - if the IE "Number of Transport blocks" <> 0 and IE "RLC size" = 0, no RLC PDU data exists but only parity bits exist for that transport format;
  - if the IE "Number of Transport blocks" = 0, neither RLC PDU neither data nor parity bits exist for that transport format;

- configure the MAC with the new transport format set (with computed transport block sizes) for that transport channel;
- 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:
  - 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.
  - if the IE "Transport Format Set" was received within the IE "PRACH system information list":
    - 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.
  - 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:
    - 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.
  - 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:
    - set the variable INVALID_CONFIGURATION to true.
  - 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:
    - re-establish the corresponding RLC entity;
    - configure the corresponding RLC entity with the new RLC size;
    - 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
    - for each AM RLC signalling radio bearer in the the CN domain as indicated in the IE "CN domain identity" in the variable LATEST_CONFIGURED_CN_DOMAIN whose RLC size is changed: ~~- for the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED_RABS for all radio bearers; and~~

      ~~- for the CN domain as indicated in the IE "CN domain identity" in the variable LATEST_CONFIGURED_CN_DOMAIN for all signalling radio bearers:~~
      - 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":
        - 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.
      - 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":
        - 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.
      - 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":
        - 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.
    - 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":

- 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.

- if that RB is using UM:
  - indicate the largest applicable RLC size to the corresponding RLC entity.
- 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].

8.6.6.28 Downlink DPCH info common for all radio links

If the IE "Downlink DPCH info common for all RL" is included the UE shall:

- perform actions for the IE "Timing indication" as specified in subclause 8.5.15.2;
- ignore the value received in IE "CFN-targetSFN frame offset";
- if the IE "Downlink DPCH power control information" is included:
  - perform actions for the IE "DPC Mode" according to [29].
- if the IE choice "mode" is set to 'FDD':
  - if the IE "Downlink rate matching restriction information" is included:
    - set the variable INVALID_CONFIGURATION to TRUE.
  - perform actions for the IE "spreading factor";
  - perform actions for the IE "Fixed or Flexible position";
  - perform actions for the IE "TFCI existence";
  - if the IE choice "SF" is set to 256:
    - store the value of the IE "Number of bits for pilot bits".
  - if the IE choice "SF" set to 128:
    - store the value of the IE "Number of bits for pilot bits".
- if the IE choice "mode" is set to 'TDD':
  - perform actions for the IE "Common timeslot info".

If the IE "Downlink DPCH info common for all RL" is included in a message used to perform a Timing re-initialised hard handover or the IE "Downlink DPCH info common for all RL" is included in a message used to transfer the UE from a state different ~~than~~from Cell_DCH to the Cell_DCH state, and ciphering is active for any radio bearer using RLC-TM, the UE shall, after having activated the dedicated physical channels indicated by that IE:

~~- increment HFN for RLC-TM by '1'.~~

- set the 20 MSB of the HFN component of COUNT-C for TM-RLC to the value of the latest transmitted IE "START" or "START List" for this CN domain, while not incrementing the value of the HFN component of COUNT-C at each CFN cycle; and

- set the remaining LSBs of the HFN component of COUNT-C to zero;

~~- include the IE "COUNT-C activation time" in the response message and specify a CFN value other than the default, "Now" for this IE;~~

~~- set the CFN component of the COUNT-C variable to the value of the CFN as calculated in subclause 8.5.15;~~

- include the IE "COUNT-C activation time" in the response message and specify a CFN value other than the default, "Now" for this IE;
- calculate the START value according to subclause 8.5.9;
- include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the response message;
- at the CFN value as indicated in the response message in the IE "COUNT-C activation time":
  - 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
  - set the remaining LSBs of the HFN component of COUNT-C to zero;
  - increment the HFN component of the COUNT-C variable by one;
  - 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;
  - step the COUNT-C variable, as normal, at each CFN value,~~. The~~ i.e. the HFN component is no longer fixed in value but incremented at each CFN cycle.

10.2.16b HANDOVER TO UTRAN COMPLETE

This message is sent by the UE when a handover to UTRAN 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	
UE Information elements				
START list	CH	1 to <maxCNdomains>		START [40] values for all CN domains. ~~The IE is mandatory if it has not been transferred prior to the handover.~~
>CN domain identity	MP		CN domain identity 10.3.1.1	
>START	MP		START 10.3.3.38	
RB Information elements				
COUNT-C activation time	OP		Activation time 10.3.3.1	Used for radio bearers mapped on RLC-TM.

10.2.16c INITIAL DIRECT TRANSFER

This message is used to initiate a signalling connection based on indication from the upper layers, and to transfer a NAS message.

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	
UE information elements				
Integrity check info	CH		Integrity check info 10.3.3.16	
CN information elements				
CN domain identity	MP		CN domain identity 10.3.1.1	
Intra Domain NAS Node Selector	MP		Intra Domain NAS Node Selector 10.3.1.6	
NAS message	MP		NAS message 10.3.1.8	
START	~~OP~~-OP		START 10.3.3.38	START value to be used in the CN domain as indicated in the IE CN domain identity. This IE shall always be present inthis version of the protocol.
Measurement information elements				
Measured results on RACH	OP		Measured results on RACH 10.3.7.45	

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)	The command "stop" is not used in this version of the protocol
Ciphering algorithm	CV-*notStop*		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
notStop	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.

10.3.3.16 Integrity check info

The Integrity check info contains the RRC message sequence number needed in the calculation of XMAC-I [40] and the calculated MAC-I.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message authentication code	MP		bit string(32)	MAC-I [40]. The Message Authentication Code bits are numbered b0-b31, where b0 is the least significant bit. The 27 MSB of the IE shall be set to zero and the 5 LSB of the IE shall be set to the value of the IE "RB identity" for the used signalling radio bearer ~~identity~~when the encoded RRC message is used as the MESSAGE parameter in the integrity protection algorithm.
RRC Message sequence number	MP		Integer (0..15)	The local RRC hyper frame number (RRC HFN) is concatenated with the RRC message sequence number to form the input parameter COUNT-I for the integrity protection algorithm. The IE value shall be set to zero when the encoded RRC message is used as the MESSAGE parameter in the integrity protection algorithm.

13.4.x SECURITY_MODIFICATION

This variable contains information on which CN domain is affected by the ongoing security reconfiguration

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Status for each CN domain	MP	<1 to maxCNDomains>		
>CN domain identity	MP		CN domain identity 10.3.1.1	
>Status	MP		Enumerated(Affected, Not Affected)	

11.2 PDU definitions

```
-- **************************************************
--
-- INITIAL DIRECT TRANSFER
--
```

```
-- **************************************************

InitialDirectTransfer ::= SEQUENCE {
    -- Core network IEs
        cn-DomainIdentity               CN-DomainIdentity,
        intraDomainNasNodeSelector      IntraDomainNasNodeSelector,
        nas-Message                     NAS-Message,
    -- Measurement IEs
        measuredResultsOnRACH           MeasuredResultsOnRACH               OPTIONAL,
        v3a0NonCriticalExtensions       SEQUENCE {
        initialDirectTransfer-v3a0ext   InitialDirectTransfer-v3a0ext,
        -- Extension mechanism for non- release99 information
            nonCriticalExtensions           SEQUENCE {}     OPTIONAL
        }       OPTIONAL
}


InitialDirectTransfer-v3a0ext ::= SEQUENCE {
        -- the START value shall always be included in this version of the protocol
        start-Value             START-Value                                 OPTIONAL
            }
```

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,
    START-Value,
    U-RNTI,
    UE-RadioAccessCapability,
    UE-RadioAccessCapability-v370ext,
    UE-RadioAccessCapability-v380ext,
-- Radio Bearer IEs :
    PredefinedConfigStatusList,
    PredefinedConfigValueTag,
    RAB-InformationSetupList,
    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;


-- 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 {
    interRAThandover                    InterRATHandoverInfoWithInterRATCapabilities,
    srncRelocation                      SRNC-RelocationInfo,
    extension                           NULL
}

-- **************************************************
--
-- RRC information, target RNC to source RNC
--
-- **************************************************


TargetRNC-ToSourceRNC-Container::= CHOICE {
    radioBearerSetup                    RadioBearerSetup,
    radioBearerReconfiguration          RadioBearerReconfiguration,
    radioBearerRelease                  RadioBearerRelease,
    transportChannelReconfiguration     TransportChannelReconfiguration,
    physicalChannelReconfiguration      PhysicalChannelReconfiguration,
    rrc-FailureInfo                     RRC-FailureInfo,
    extension                           NULL
}

-- Part2: Container definitions, similar to the PDU definitions in 11.2 for RRC messages
-- In alphabetical order


-- **************************************************
--
-- Handover to UTRAN information
--
-- **************************************************

InterRATHandoverInfoWithInterRATCapabilities ::= CHOICE {
    r3                              SEQUENCE {
        interRAThandoverInfo-r3         InterRATHandoverInfoWithInterRATCapabilities-r3-IEs,
    -- IE InterRATHandoverInfoWithInterRATCapabilities-r3-IEs also
    -- includes non critical extensions
        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 (SIZE (0..255))
        -- 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
}

InterRATHandoverInfoWithInterRATCapabilities-v390ext-IEs ::= SEQUENCE {
    -- User equipment IEs
        failureCauseWithProtErr             FailureCauseWithProtErr                 OPTIONAL
}

-- **************************************************
--
-- 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,
                    -- 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
}

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{
        StartValueForCIphering-v3a0ext      START-Value
}

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: 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,
    measurementCommandWithType          MeasurementCommandWithType,
    -- TABULAR: The CHOICE Measurement in the tabular description is included
    -- in the IE above.
    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
```

13.4.11a LATEST_CONFIGURED_CN_DOMAIN

This variable stores the CN-domain that was most recently configured to be used for ciphering and integrity protection.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Latest configured CN domain	OP		CN domain identity 10.3.1.1	Cleared when entering UTRA RRC connected mode when not stated otherwise in the procedure. Cleared when leaving UTRA RRC connected mode.

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
Non RRC IEs				
>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 Complete, await Active Set Update Complete, await Handover Complete, send Cell Update Confirm, send URA Update Confirm, , others)	
Ciphering related information				
>Ciphering status for each CN domain	MP	<1 to maxCNDomains>		
>>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-*Ciphering*			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

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
>>SFN	MP		Integer(0..4095)	
>COUNT-C list	CV-*Ciphering*	1 to <maxCNdomains>		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)
>>Uplink HFN	MP		Bit string(20..25)	This IE is either RLC AM HFN (20 bits) or RLC UM HFN (25 bits)
Integrity protection related information				
>Integrity protection status	MP		Enumerated(Not started, Started)	
>Signalling radio bearer specific integrity protection information	CV-*IP*	4 to <maxSRBsetup>		
>>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)	
RRC IEs				
UE Information elements				
>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 *Position estimate*	MP			
>>>Ellipsoid Point			Ellipsoid Point; 10.3.8.4a	
>>>Ellipsoid point with uncertainty circle			Ellipsoid point with uncertainty circle	

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
			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	
Other Information elements				
>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	
UTRAN Mobility Information elements				
>URA Identifier	OP		URA identity 10.3.2.6	
CN Information Elements				
>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	
Measurement Related Information elements				
>For each ongoing measurement reporting	OP	1 to <MaxNoOfMeas>		
>>Measurement Identity	MP		Measurement identity 10.3.7.48	
>>Measurement Command	MP		Measurement command 10.3.7.46	
>>Measurement Type	CV-*Setup*		Measurement type 10.3.7.50	
>>Measurement Reporting Mode	OP		Measurement reporting mode	

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
			10.3.7.49	
>>Additional Measurements list	OP		Additional measurements list 10.3.7.1	
>>CHOICE *Measurement*	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 10.3.7.51	
>>>>CHOICE *report criteria*	OP			
>>>>>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 *report criteria*	OP			
>>>>>Inter-frequency measurement reporting criteria			Inter-frequency measurement reporting	

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
			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 measuremen t 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		Measuremen t validity 10.3.7.51	
>>>>CHOICE *report criteria*	OP			
>>>>>Inter-RAT measurement reporting criteria			Inter-RAT measuremen t 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 measuremen t object 10.3.7.70	
>>>>Traffic volume measurement quantity	OP		Traffic volume measuremen t quantity 10.3.7.71	
>>>>Traffic volume reporting quantity	OP		Traffic volume reporting quantity 10.3.7.74	
>>>>CHOICE *report criteria*	OP			
>>>>>Traffic volume measurement reporting criteria			Traffic volume measuremen t reporting criteria 10.3.7.72	
>>>>>Periodical reporting			Periodical reporting criteria 10.3.7.53	
>>>>>No reporting			NULL	
>>>Quality				

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
>>>>Quality measurement Object	OP		Quality measurement object	
>>>>CHOICE *report criteria*	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 *report criteria*	OP			
>>>>>UE internal measurement reporting criteria			UE internal measurement 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 *report criteria*	OP			
>>>>>LCS reporting criteria			LCS reporting criteria 10.3.7.110	
>>>>>Periodical reporting			Periodical reporting criteria 10.3.7.53	
>>>>>No reporting				
Radio Bearer Information Elements				
>Pre-defined configuration status information	OP		Pre-defined configuration status information 14.13.2.3	
>Signalling RB information list	MP	1 to <maxSRBsetup>		For each signalling radio bearer
>>Signalling RB information	MP		Signalling RB information to setup 10.3.4.24	
>RAB information list	OP	1 to		Information for each RAB

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
		<maxRABsetup>		
>>RAB information	MP		RAB information to setup 10.3.4.10	
Transport Channel Information Elements				
Uplink transport channels				
>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 *mode*	OP			
>>FDD				
>>>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)
Downlink transport channels				
>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	
Other Information elements				
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
Setup	The IE is mandatory present when the IE Measurement command has the value "Setup", otherwise the IE is not needed.
Ciphering	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.
IP	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.
ProtErr	This IE is mandatory present if the IE "Protocol error indicator" is included and has the value "TRUE". Otherwise it is not needed.

3GPP TSG-RAN2 Meeting #27
Orlando, USA, 18-22 of February

R2-020583

CR-Form-v5

CHANGE REQUEST

⌘ **25.331** **CR** **1283** ⌘ **rev** **1** ⌘ Current version: **4.3.0** ⌘

*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:	⌘	Security clarifications
Source:	⌘	Alcatel, Ericsson, Nortel, Motorola
Work item code:	⌘	***Date:*** ⌘ 2002-02-22
Category:	⌘	**F** ***Release:*** ⌘ REL-4

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change: ⌘ The current specification is unclear on a number of points and require clarification.

Shadow R4 CR of CR1282r5~~3~~.

Incorrect procedure for UE actions on receipt of HO TO UTRAN COMMAND.

Changes in this revision, r1, are highlighted in blue in subclause 8.3.6.3 - the only subclause affected in this revision.

Summary of change: ⌘

[A] 8.1.12.2.1 (and other)

It is clarified that "suspend" means that PDUs with SN>X shall not be transmitted.

8.1.12.2.1, 8.1.12.2.2, 8.1.12.5

OI 2.38 UTRAN procedures completed/corrected.

8.1.3.6 (and other)

[B] For integrity protection RRC messages with RRC SN >X are allowed to transmit when the integrity configuration has been changed. This is missing in some procedures, i.e. Cell update, at reception of security mode complete, transmission of response messages in normal case.

8.2.2.3

[C] / OI 2.41: The IE "Integrity protection mode info" with the IE "Integrity protection mode command" set to "modify" can only be received in SECURITY MODE COMMAND. This is removed from other reconfiguration messages.

8.5.8

[D] The first CFN of the TTI shall be used for ciphering in the whole TTI. This is clarified in 8.5.8. (See also CR to 25.321).

8.5.9

OI 2.25: It needs to be clarified that COUNT-C corresponding to non ciphered RB should NOT be included in the START value calculation.

8.6.3.4

[E] "Pending activation time" is clarified for downlink. This is needed as the UE in some cases shall apply a new configuration at a pending activation time.

8.6.3.5

OI 2.49: Added missing Integrity Protection invalid configuration check.

8.6.4.1

[F] The start of ciphering is missing when an SRB is setup (SRB4) and ciphering is already started for the CN domain (see similar text in RB setup, 8.6.4.3).

8.3.6.3 and 10.2.16.b

[G] UE shall, in case USIM is present, include in the HANDOVER TO UTRAN COMPLETE message the START values that were not transferred to the network via the other RAT. The specification is clarified, by referring to UE variable INTER_RAT_HANDOVER_INFO_TRANSFERRED.

8.6.4.1 (and others)

OI 2.37. The variable START_VALUE_TO_TRANSMIT needs to be set when SRB4 is setup in RB SETUP. It is also clarified that SRB4 and any RB needs to be from the same CN domain.

In revision2:

OI 21 (8.1.12.4.b and 8.2.2.12b)

Failure message when security procedure is interruped by cell update. UE shall not send failure message after having sent the SECURITY MODE COMPLETE message (see R2-020348)

Section 8.1.12.2.1 and 8.1.12.2.2: The restriction on the number of ciphering configurations and integrity protection algorithms that the UE needs to store is clarified.

8.5.9. The START value calculation is changed from MAX(HFN)+1 to MAX(HFN)+2 in order to avoid reuse in case of loss of data in UM before RB release.

In revision 3:

- ASN.1 changes added

- STARTlist is added in the inter node containers

- SIM handling

- Timing initialised HHO

		- HO from GSM - ASN change for inter node containers
Consequences if not approved:	⌘	Potential misinterpretation of security functionality. Unclear behavior. Risk for ciphering failure in case of RB setup of SRB4 and other scenarios.

Clauses affected:	⌘	8.1.3.6, 8.1.8.2, 8.1.8.3, 8.1.12.2, 8.1.12.2.1, 8.1.12.2.2, 8.1.12.3, 8.1.12.3.1, 8.1.12.4, 8.1.12.4a, 8.1.12.4b, 8.1.12.5, 8.2.2.2, 8.2.2.3, 8.2.2.4, 8.2.2.12b, 8.3.1.5, 8.3.1.6, 8.3.3.3, 8.3.4.3, 8.3.6.3, 8.6.7.4, 8.5.2, 8.5.8, 8.5.9, 8.5.10.3, 8.6.3.4, 8.6.3.5, 8.6.4.1, 8.6.4.3, 8.6.4.8, 8.6.6.28, 10.2.16b, 10.2.16c, 10.3.3.5, 10.3.3.16, 11.2, 11.5, 13.4.x (new section), 13.4.11b (new section), 14.12.4.2		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/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.

8.1.3.6 Reception of an RRC CONNECTION SETUP message by the UE

The UE shall compare the value of the IE "Initial UE identity" in the received RRC CONNECTION SETUP message with the value of the variable INITIAL_UE_IDENTITY.

If the values are different, the UE shall:

- ignore the rest of the message.

If the values are identical, the UE shall:

- stop timer T300, and act upon all received information elements as specified in subclause 8.6, unless specified otherwise in the following:
  - if the UE will be in the CELL_FACH state at the conclusion of this procedure:
    - if the IE "Frequency info" is included:
      - select a suitable UTRA cell according to [4] on that frequency;
    - select PRACH according to subclause 8.5.17;
    - select Secondary CCPCH according to subclause 8.5.19;
    - ignore the IE "UTRAN DRX cycle length coefficient" and stop using DRX.
- perform the physical layer synchronisation procedure as specified in [29];
- enter a state according to subclause 8.6.3.3;
- submit an RRC CONNECTION SETUP COMPLETE message to the lower layers on the uplink DCCH after successful state transition per subclause 8.6.3.3, with the contents set as specified below:
  - set the IE "RRC transaction identifier" to:
    - the value of "RRC transaction identifier" in the entry for the RRC CONNECTION SETUP message in the table "Accepted transactions" in the variable TRANSACTIONS; and
    - clear that entry.
  - if the USIM or SIM is present:
    - set the "START" for each CN domain in the IE "START list" in the RRC CONNECTION SETUP COMPLETE message with the corresponding START value that is stored in the USIM [50], if present, or as stored in the UE if the SIM is present; and then
    - set the START value stored in the USIM [50] if present, and as stored in the UE if the SIM is present, for any CN domain to the value "THRESHOLD" of the variable START_THRESHOLD.
  - if neither the USIM nor SIM is not present:
    - set the "START" for each CN domain in the IE "START list" in the RRC CONNECTION SETUP COMPLETE message to zero;
    - set the value of "THRESHOLD" in the variable "START_THRESHOLD" to the default value [40].
  - retrieve its UTRA UE radio access capability information elements from variable UE_CAPABILITY_REQUESTED; and then
  - include this in IE "UE radio access capability" and IE "UE radio access capability extension", provided this IE is included in variable UE_CAPABILITY_REQUESTED;
  - retrieve its inter-RAT-specific UE radio access capability information elements from variable UE_CAPABILITY_REQUESTED; and then
  - include this in IE "UE system specific capability".

When the RRC CONNECTION SETUP COMPLETE message has been submitted to lower layers for transmission the UE shall:

- if the UE has entered CELL_FACH state:
  - start timer T305 using its initial value 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.
- store the contents of the variable UE_CAPABILITY_REQUESTED in the variable UE_CAPABILITY_TRANSFERRED;
- initialise variables upon entering UTRA RRC connected mode as specified in subclause 13.4;
- consider the procedure to be successful;

And the procedure ends.

8.1.8.2 Initiation of Initial direct transfer procedure in the UE

In the UE, the initial direct transfer procedure shall be initiated, when the upper layers request establishment of a signalling connection. This request also includes a request for the transfer of a NAS message.

Upon initiation of the initial direct transfer procedure when the UE is in idle mode, the UE shall:

- set the variable ESTABLISHMENT_CAUSE to the cause for establishment indicated by upper layers;
- perform an RRC connection establishment procedure, according to subclause 8.1.3;
- if the RRC connection establishment procedure was not successful:
  - indicate failure to establish the signalling connection to upper layers and end the procedure.
- when the RRC connection establishment procedure is completed successfully:
  - continue with the initial direct transfer procedure as below.

Upon initiation of the initial direct transfer procedure when the UE is in CELL_PCH or URA_PCH state, the UE shall:

- perform a cell update procedure, according to subclause 8.3.1, using the cause "uplink data transmission";
- when the cell update procedure completed successfully:
  - continue with the initial direct transfer procedure as below.

The UE shall, in the INITIAL DIRECT TRANSFER message:

- set the IE "NAS message" as received from upper layers; and
- set the IE "CN domain identity" as indicated by the upper layers; and
- set the IE "Intra Domain NAS Node Selector" as follows:
  - derive the IE "Intra Domain NAS Node Selector" from TMSI/PMTSI, IMSI, or IMEI; and
  - provide the coding of the IE "Intra Domain NAS Node Selector" according to the following priorities:
    1. derive the routing parameter for IDNNS from TMSI (CS domain) or PTMSI (PS domain) whenever a valid TMSI/PTMSI is available;
    2. base the routing parameter for IDNNS on IMSI when no valid TMSI/PTMSI is available;
    3. base the routing parameter for IDNNS on IMEI only if no (U)SIM is inserted in the UE.
- calculate the START according to subclause 8.5.9 for the CN domain set in the IE "CN Domain Identity"; and
  - include the calculated START value for that CN domain in the IE “START”;

In CELL_FACH state, the UE shall:

- include a 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);

- include in the IE "Measured results on RACH" all requested reporting quantities for cells for which measurements are reported.

The UE shall:

- transmit the INITIAL DIRECT TRANSFER message on the uplink DCCH using AM RLC on signalling radio bearer RB3;

- when the INITIAL DIRECT TRANSFER message has been submitted to lower layers for transmission:

  - confirm the establishment of a signalling connection to upper layers; and

  - add the signalling connection with the identity indicated by the IE "CN domain identity" in the variable ESTABLISHED_SIGNALLING_CONNECTIONS; and

  - the procedure ends.

When not stated otherwise elsewhere, the UE may also initiate the initial direct transfer procedure when another procedure is ongoing, and in that case the state of the latter procedure shall not be affected.

A new signalling connection request may be received from upper layers during transition to idle mode. In those cases, from the time of the indication of release to upper layers until the UE has entered idle mode, any such upper layer request to establish a new signalling connection shall be queued. This request shall be processed after the UE has entered idle mode.

8.1.8.3 Reception of INITIAL DIRECT TRANSFER message by the UTRAN

On reception of the INITIAL DIRECT TRANSFER message the NAS message should be routed using the IE "CN Domain Identity". UTRAN may also use the IE "Intra Domain NAS Node Selector" for routing among the CN nodes for the addressed CN domain.

If no signalling connection exists towards the chosen node, then a signalling connection is established.

If the IE "Measured results on RACH" is present in the message, the UTRAN should extract the contents to be used for radio resource control.

When the UTRAN receives an INITIAL DIRECT TRANSFER message, it shall not affect the state of any other ongoing RRC procedures, when not stated otherwise elsewhere.

The UTRAN should:

- set the START value for the CN domain indicated in the IE "CN domain identity" to the value of the IE "START";

8.1.12.2 Initiation

8.1.12.2.1 Ciphering configuration change

To ~~stop or~~ 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.

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:

- ~~if this is the first SECURITY MODE COMMAND sent for this RRC connection:~~

  - ~~use 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 for all the signalling radio bearers; while:~~

    - ~~setting the 20 most significant bits of the hyper frame numbers for all signalling radio bearers to the START for that CN domain;~~

    - ~~setting the remaining bits of the hyper frame numbers equal to zero.~~

- (INDENTATION) suspend all radio bearers using RLC-AM or RLC-UM and suspend 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:~~;~~

- ~~suspend 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;~~

  - (INDENTATION)do 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; /* Indentation changed to B~~3~~2*/

- ~~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";~~

- ~~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";~~

- 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;

- if a transparent mode radio bearer for this CN domain exists:

  - include the IE "Ciphering activation time for DPCH" in IE "Ciphering mode info", at which time the new ciphering configuration shall be applied;

- 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;

- 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;

- if Integrity protection has already been started for the UE; and

  - 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:

    - include the IE “Integrity protection mode info” in the SECURITY MODE COMMAND

- if Integrity protection has already been started for the UE; and

  - 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:

    - include the IE “Integrity protection mode info” in the SECURITY MODE COMMAND

- transmit the SECURITY MODE COMMAND message on RB2~~the downlink DCCH in AM RLC~~.

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.

When configuring Integrity protection, UTRAN should:

- 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.
- 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; and
  - 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:
    - include the IE “Ciphering mode info” in the SECURITY MODE COMMAND;
- 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;
  - 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:

- if this is the first SECURITY MODE COMMAND sent for this RRC connection:
  - if new keys have been received:
    - initialise the hyper frame numbers as follows:
      - set all bits of the hyper frame numbers of the COUNT-I values for all signalling radio bearers to zero;
  - else (if new keys have not been received):
    - 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:
      - 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;
      - setting the remaining bits of the hyper frame numbers equal to zero;
- else (this is not the first SECURITY MODE COMMAND sent for this RRC connection):
  - if new keys have been received;
    - initialise the hyper frame number for COUNT-I for RB2 as follows:
      - set all bits of the HFN of the COUNT-I value for RB2 to zero;
  - if new keys have not been received;
    - initialize the hyper frame number for COUNT-I for RB2 as follows:
      - 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 the IE "CN Domain Identity";
      - set the remaining bits of the HFN of the downlink and uplink COUNT-I to zero;
- if the IE "Integrity protection mode command" has the value "Start":

- prohibit the transmission of signalling messages with any RRC SN on all signalling radio bearers, except RB2;

- set the FRESH value in the IE "Integrity protection initialisation number", included in the IE "Integrity protection mode info";

- if the IE "Integrity protection mode command" has the value "Modify":

- for each signalling radio bearer RBn, except RB2:

- 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";

- 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;

- 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;

- 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:

- if ~~the~~ neither IE~~s~~ "Ciphering mode info" ~~and the~~nor IE ~~IE~~ "Integrity protection mode info" is ~~are both not~~ included in the SECURITY MODE COMMAND:

  - set the variable INVALID_CONFIGURATION to TRUE.

- 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:

  - set the variable LATEST_CONFIGURED_CN_DOMAIN equal to the IE "CN domain identity";

  - 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”;

  - 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”

  - ~~if the value of the IE "Status" in the variable "INTEGRITY_PROTECTION_INFO" is "Not started":~~

    - ~~use the value "START" in the most recently sent 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 for all the signalling radio bearers; while~~

      - ~~setting the 20 most significant bits of the hyper frame numbers for all signalling radio bearers to the START for that CN domain;~~

      - ~~setting the remaining bits of the hyper frame numbers equal to zero.~~

  - 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

  - clear that entry;

- if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
  - perform the actions as specified in subclause 8.6.3.4.
- if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
  - perform the actions as specified in subclause 8.6.3.5.

- prior to sending the SECURITY MODE COMPLETE message:
  - use the old ciphering configuration for this message;
  - if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO
    - for each radio bearer and signalling radio bearer that belongs to the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN:
      - 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;
      - continue incrementing the COUNT-C values for all RLC-AM and RLC-UM radio bearers;
    - 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 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:
        - 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;
        - set the remaining bits of the hyper frame numbers to zero;
    - if new keys have been received perform the actions in subclause 8.1.12.3.1.
  - if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
    - 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;.
    - 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:
      - in the downlink, for the received SECURITY MODE COMMAND message :
        - 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;
        - set the remaining bits of the IE "Downlink RRC HFN" to zero;
      - in the uplink, for the transmitted response message, SECURITY MODE COMPLETE:
        - 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;
        - set the remaining bits of the IE "Uplink RRC HFN" to zero;

- 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, the UE shall for each signalling radio bearer other than RB2:
  - if the IE "Integrity protection mode command" has the value "start":
    - in the downlink, for this signalling radio bearer, 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;
    - set the remaining bits of the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero;
  - else:
    - 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":
      - [HANS, I want this to be B6]for this signalling radio bearer, 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;
      - set the remaining bits of the IE "Downlink RRC HFN" to zero;
  - if new keys have been received perform the actions in subclause 8.1.12.3.1;
- start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;
- transmit the SECURITY MODE COMPLETE message on the uplink DCCH in AM RLC;

- when the successful delivery of the SECURITY MODE COMPLETE message has been confirmed by RLC:
  - if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - 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 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:
        - 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.
        - set the remaining bits of the hyper frame numbers to zero;
    - if new keys have been received perform the actions in subclause 8.1.12.3.1.
    - resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
    - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
    - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.
  - if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":

- 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, the UE shall for each signalling radio bearer other than RB2:
  - if the IE "Integrity protection mode command" has the value "start":
    - in the uplink, for this signalling radio bearer, 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;
    - set the remaining bits of the IE "Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the uplink COUNT-I to zero;
  - else:
    - 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:
      - [Hans - same here B6]for this signalling radio bearer, 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;
      - set the remaining bits of the IE "Uplink RRC HFN" to zero;
  - if new keys have been received perform the actions in subclause 8.1.12.3.1;
  - allow the transmission of RRC messages on all signalling radio bearers with any RRC SN ~~greater than or equal to the value in the "RRC message sequence number list" indicated for each signalling radio bearer in the IE "Uplink integrity protection activation info" of the response message~~;
  - 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;
  - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
  - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.
- clear the variable SECURITY_MODIFICATION;
- notify upper layers upon change of the security configuration;
- and the procedure ends.

- 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:
  - release all its radio resources;
  - 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;
  - clear the variable ESTABLISHED_SIGNALLING_CONNECTIONS;
  - clear the variable ESTABLISHED_RABS;
  - clear the variable SECURITY_MODIFICATION;

- enter idle mode;
- perform actions when entering idle mode as specified in subclause 8.5.2;
- 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:

- set the START value for ~~this~~ the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN ~~CN domain~~ to zero;

- if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":

~~- for each signalling radio bearer:~~

  - for integrity protection in the downlink on each signalling radio bearer except RB2:

    - if IE "Integrity protection mode command" has the value "start":

      - for the first received message on this signalling radio bearer:

        - start using the new integrity key;

        - for this signalling radio bearer, set the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero.

    - else:

      - for the first message for which~~when~~ 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":

        - ~~use~~ start using the new integrity key;

        - for this signalling radio bearer, set the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero.

  - for integrity protection in the uplink on each signalling radio bearer except RB2:

    - for the first message for which~~when~~ 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 IE "Integrity protection mode info":

      - ~~use~~start using the new integrity key;

      - for this signalling radio bearer, set the IE "Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the uplink COUNT-I to zero.;

    - for integrity protection in the downlink on signalling radio bearer RB2:- at the received SECURITY MODECOMMAND:

      - start using the new integrity key;

      - set the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero;

    - for integrity protection in the uplink on signalling radio bearer RB2 :- at the transmitted SECURITY MODE COMPLETE:

      - start using the new integrity key;

      - set the IE "Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the uplink COUNT-I to zero;

- if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
  - for each signalling radio bearer and for each radio bearer for ~~this CN domain~~the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN:
    - 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:
      - at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info":
        - ~~use~~ start using the new key in uplink and downlink;
        - set the HFN component of the COUNT-C to zero.
    - 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:
      - in the downlink, at ~~and after~~ the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info":
        - ~~use~~ start using the new key;
        - set the HFN component of the downlink COUNT-C to zero.
      - in the uplink, at ~~and after~~ the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info":
        - ~~use~~ start using the new key;
        - set the HFN component of the uplink COUNT-C to zero;
- 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:

- 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;
- 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
- clear that entry;
- set the IE "failure cause" to the cause value "incompatible simultaneous reconfiguration";
- when the response message has been submitted to lower layers for transmission:
  - set the variable INCOMPATIBLE_SECURITY_RECONFIGURATION to FALSE;
  - continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - 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:

- abort the ongoing integrity and/or ciphering reconfiguration;
- resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
- allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- ~~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;~~
- ~~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~~
- ~~clear that entry;~~
- ~~set the IE "failure cause" to the cause value "cell update occurred";~~
- when the response message has been submitted to lower layers for transmission:
  - if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
    - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
    - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO;
  - if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":
    - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
    - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.
  - continue with any ongoing processes and procedures as if the ~~invalid~~ SECURITY MODE COMMAND message has not been received; and
  - clear the variable SECURITY_MODIFICATION;
  - 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:

- transmit a SECURITY MODE FAILURE message on the DCCH using AM RLC after setting the IEs as specified below:
  - 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
  - clear that entry;

- set the IE "failure cause" to the cause value "invalid configuration".

- when the response message has been submitted to lower layers for transmission:
  - set the variable INVALID_CONFIGURATION to FALSE;
  - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE;
  - continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - 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:

- if the IE “Ciphering mode info” was included in the SECURITY MODE COMMAND message:
  - if new keys were received for the CN domain set in the IE "CN Domain Identity" in the SECURITY MODE COMMAND:
    - at the downlink and uplink activation time set 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;
  - else (if new keys were not received)
    - at the downlink and uplink activation time use 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 by:
      - setting 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;
      - setting the remaining bits of the hyper frame numbers equal to zero.
- if the IE “Integrity protection mode info” was included in the SECURITY MODE COMMAND message; and
  - if this was not the first SECURITY MODE COMMAND message for this RRC connection:
    - 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:
      - at the downlink and uplink activation time 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:
        - set all bits of the hyper frame numbers of the uplink and downlink COUNT-I to zero;
    - 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:
      - at the downlink and uplink activation time use 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 by:
        - setting 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;
        - setting the remaining bits of the hyper frame numbers equal to zero.

- send an indication to upper layers that the new ~~integrity protection~~security configuration has been activated;
- resume, in the downlink, all suspended radio bearers and all signalling radio bearers;
- allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- if the IE "Integrity protection mode command" included in the SECURITY MODE COMMAND had the value "Start":
  - start applying integrity protection in the downlink for all signalling radio bearers;
- if the IE "Integrity protection mode command" included in the SECURITY MODE COMMAND had the value "Modify":
  - 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";
  - continue applying the new integrity configuration for signalling radio bearer RB2;
  - 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";
- 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";
- 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";
- 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";
- for radio bearers using RLC-AM or RLC-UM:
  - 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;
  - 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;
  - 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.
- for radio bearers using RLC-TM:
  - 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;
  - 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.
- 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:

- transmit a SECURITY MODE FAILURE message on the uplink DCCH using AM RLC;
- 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
- clear that entry;
- set the IE "failure cause" to the cause value "protocol error";
- include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL_ERROR_INFORMATION;
- when the response message has been submitted to lower layers for transmission:
  - continue with any ongoing processes and procedures as if the invalid SECURITY MODE COMMAND message has not been received;
  - and the procedure ends.

8.2.2.2 Initiation

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

- configure new radio links in any new physical channel configuration;
- start transmission and reception on the new radio links;
- for a radio bearer establishment procedure:
  - transmit a RADIO BEARER SETUP message on the downlink DCCH using AM or UM RLC.
  - if signaling radio bearer RB4 is setup with this procedure and signaling radio bearers RB1-RB3 were already established prior to the procedure:
    - if the variable "LATEST_CONFIGURED_CN_DOMAIN" has been initialised:
      - any radio bearers setup by the same message as signalling radio bearer RB4 should be connected to the CN domain indicated in the varable "LATEST CONFIGURED CN DOMAIN";
- for a radio bearer reconfiguration procedure:
  - transmit a RADIO BEARER RECONFIGURATION message on the downlink DCCH using AM or UM RLC.
- for a radio bearer release procedure:
  - transmit a RADIO BEARER RELEASE message on the downlink DCCH using AM or UM RLC.
- for a transport channel reconfiguration procedure:
  - transmit a TRANSPORT CHANNEL RECONFIGURATION message on the downlink DCCH using AM or UM RLC.
- for a physical channel reconfiguration procedure:
  - transmit a PHYSICAL CHANNEL RECONFIGURATION message on the downlink DCCH using AM or UM RLC.
- if the reconfiguration procedure is simultaneous with SRNS relocation procedure:

- include the IE "Downlink counter synchronisation info"; and
- if ciphering and/or integrity protection are activated:
  - include new ciphering and/or integrity protection configuration information to be used after reconfiguration.
- use the downlink DCCH using AM RLC.

- if transport channels are added, reconfigured or deleted in uplink and/or downlink:
  - set TFCS according to the new transport channel(s).
- 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:
  - 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 common channel configuration of a given cell and C-RNTI to be used in that cell to 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:

- set the variable ORDERED_RECONFIGURATION to TRUE;
- perform the physical layer synchronisation procedure as specified in [29];
- 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:

- 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:
  - act upon the IE "PDSCH code mapping" as specified in subclause 8.6; and
  - infer that the PDSCH will be transmitted from the cell from which the downlink DPCH is transmitted.
- 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:

- 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:

- remove any C-RNTI from MAC;
- clear the variable C_RNTI.

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

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

- if the IE "Frequency info" is included in the received reconfiguration message:
  - select a suitable UTRA cell according to [4] on that frequency.
- if the IE "Frequency info" is not included in the received reconfiguration message:
  - select a suitable UTRA cell according to [4].
- 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):
  - initiate a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";

- when the cell update procedure completed successfully:
  - if the UE is in CELL_PCH or URA_PCH state:
    - initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
    - proceed as below.
- 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;
- select PRACH according to subclause 8.5.17;
- select Secondary CCPCH according to subclause 8.5.19;
- use the transport format set given in system information;
- if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - ignore that IE and stop using DRX.
- if the contents of the variable C_RNTI is empty:
  - perform a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";
  - when the cell update procedure completed successfully:
    - if the UE is in CELL_PCH or URA_PCH state:
      - initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
      - 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:

- if the IE "Frequency info" is included in the received reconfiguration message:
  - select a suitable UTRA cell according to [4] on that frequency;
  - 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):
    - initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";
    - when the cell update procedure completed successfully:
      - 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:

- if the received reconfiguration message included the IE "Downlink counter synchronisation info":
  - re-establish RB2;
  - set the new uplink and downlink HFN of RB2 to MAX(uplink HFN of RB2 | downlink HFN of RB2) + 1;
  - increment by one the downlink and uplink HFN values for RB2;
  - calculate the START value according to subclause 8.5.9;

- include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".

- if the received reconfiguration message did not include the IE "Downlink counter synchronisation info":
  - if the variable START_VALUE_TO_TRANSMIT is set:
    - include and set the IE "START" to the value of that variable.
  - if the variable START_VALUE_TO_TRANSMIT is not set and the IE "New U-RNTI" is included:
    - calculate the START value according to subclause 8.5.9;
    - include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
  - if the received reconfiguration message caused a change in the RLC size for any RB using RLC-AM:
    - calculate the START value according to subclause 8.5.9;
    - 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".
- if the received reconfiguration message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - set the IE “Status” in the variable SECURITY_MODIFICATION for all the CN domains in the variable SECURITY_MODIFICATION to “Affected”;
- if the received reconfiguration message contained the IE "Ciphering mode info":
  - include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.
- ~~if the received reconfiguration message contained the IE "Integrity protection mode info" with the IE "Integrity protection mode command" set to "Modify":~~
  - ~~include and set the IE "Uplink integrity protection activation info" to the value of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.~~
- if the received reconfiguration message did not contain the IE "Ciphering activation time for DPCH" in IE "Ciphering mode info":
  - if prior to this procedure there exist no transparent mode RLC radio bearers:
    - if, at the conclusion of this procedure, the UE will be in CELL_DCH state; and
    - if, at the conclusion of this procedure, at least one transparent mode RLC radio bearer exists:
      - include the IE "COUNT-C activation time" and specify a CFN value for this IE.
  - if prior to this procedure there exists at least one transparent mode RLC radio bearer:
    - if, at the conclusion of this procedure, no transparent mode RLC radio bearers exist:
      - include the IE "COUNT-C activation time" and specify a CFN value for this IE.
- 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
- clear that entry;
- if the variable PDCP_SN_INFO is not empty:
  - include the IE "RB with PDCP information list" and set it to the value of the variable PDCP_SN_INFO.
- 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):

- set the IE "Uplink Timing Advance" according to subclause 8.6.6.26.

- if the IE "Integrity protection mode info" was present in the received reconfiguration message:

  - 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:

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

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

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

  - select a suitable UTRA cell according to [4].

- prohibit periodical status transmission in RLC;

- remove any C-RNTI from MAC;

- clear the variable C_RNTI;

- 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;

- select Secondary CCPCH according to subclause 8.5.19;

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

  - 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.

- if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:

  - set the variable INVALID_CONFIGURATION to TRUE.

- 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):

  - initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";

  - when the cell update procedure completed successfully:

    - the procedure ends.

- 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:

  - initiate a cell update procedure according to subclause 8.3.1 using the cause "cell reselection";

  - when the cell update procedure is successfully completed:

    - the procedure ends.

- 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:

  - initiate a URA update procedure according to subclause 8.3.1 using the cause "URA reselection";

  - when the URA update procedure is successfully completed:

    - 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:

- 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:

- 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:

- 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:

- 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:

- 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:

- if the IE "Downlink counter synchronization info" was included in the reconfiguration message:
  - when RLC has confirmed the successful transmission of the response message:
    - 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;
    - 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;
    - set the remaining bits of the HFN values of all AM and UM RLC entities with RB identities different from 2 to zero.
- if the variable PDCP_SN_INFO is empty:
  - if the received reconfiguration message contained the IE "Ciphering mode info":
    - when RLC has confirmed the successful transmission of the response message:
      - notify upper layers upon change of the security configuration;
      - perform the actions below.
  - if the received reconfiguration message did not contain the IE "Ciphering mode info":
    - when RLC has been requested to transmit the response message:
      - perform the actions below.
- if the variable PDCP_SN_INFO is non-empty:
  - when RLC has confirmed the successful transmission of the response message:
    - for each radio bearer in the variable PDCP_SN_INFO:

- if the IE "RB started" in the variable ESTABLISHED_RABS is set to "started":
  - configure the RLC entity for that radio bearer to "continue".
- 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:

- when RLC has confirmed the successful transmission of the response message:
  - for each radio bearer in the variable PDCP_SN_INFO:
    - if the IE "RB started" in the variable ESTABLISHED_RABS is set to "started":
      - configure the RLC entity for that radio bearer to "continue".
  - enter the new state (CELL_PCH or URA_PCH, respectively);
  - perform the actions below.

The UE shall:

- set the variable ORDERED_RECONFIGURATION to FALSE;
- if the received reconfiguration message contained the IE "Ciphering mode info":
  - resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
  - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
  - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.
- if the received reconfiguration message contained the IE "Integrity protection mode info":
  - allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
  - 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;
  - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
  - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.
- clear the variable PDCP_SN_INFO;
- clear the variable START_VALUE_TO_TRANSMIT;- /*Itentation to be changed to B1 (this was not alligned with R99*/
- 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:

- abort the ongoing integrity and/or ciphering reconfiguration;
- resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
- allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- ~~transmit a failure response message as specified in subclause 8.2.2.9, setting the information elements as specified below:~~
  - ~~include the IE "RRC transaction identifier"; and~~
  - ~~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~~
  - ~~clear that entry;~~
  - ~~set the IE "failure cause" to the cause value "cell update occurred";~~
  - if the received reconfiguration message contained the IE "Ciphering mode info":
    - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
    - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO;
  - if the received reconfiguration message contained the IE "Integrity protection mode info":
    - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
    - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.
- 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:

- transmit a failure response message as specified in subclause 8.2.2.9, setting the information elements as specified below:
  - include the IE "RRC transaction identifier"; and
  - 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
  - clear that entry;
  - set the IE "failure cause" to the cause value "protocol error";
  - include the IE "Protocol error information" with contents set to the value of the variable PROTOCOL_ERROR_INFORMATION.

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, it may either:

- in case the procedure was triggered by reception of a CELL UPDATE:
  - 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";
  - 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":
    - set the 20 MSB of the MAC-d HFN with the corresponding START value in the IE "START list";
    - set the remaining LSB of the MAC-d HFN to zero.
  - transmit a CELL UPDATE CONFIRM message on the downlink DCCH or optionally on the CCCH but only if ciphering is not required; and
  - optionally include the IE "RLC re-establish indicator" to request a RLC re-establishment in the UE, in which case the corresponding RLC entities should also be re-established in UTRAN; or
- in case the procedure was triggered by reception of a URA UPDATE:
  - transmit a URA UPDATE CONFIRM message to the lower layers for transmission on the downlink CCCH or DCCH in which case the UTRAN should include the IE "URA identity" in the URA UPDATE CONFIRM message in a cell where multiple URA identifiers are broadcast; or
- 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:
  - if the CELL UPDATE message was sent because of an unrecoverable error in RB2, RB3 or RB4:
    - 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:

- stop timer T302;
- in case of a cell update procedure and the CELL UPDATE CONFIRM message:
  - includes "RB information elements"; and/or
  - includes "Transport channel information elements"; and/or
  - includes "Physical channel information elements"; and
  - if the variable ORDERED_RECONFIGURATION is set to FALSE:
    - set the variable ORDERED_RECONFIGURATION to TRUE;
- act upon all received information elements as specified in subclause 8.6, unless specified otherwise in the following:

- if the IE "Frequency info" is included in the message:
  - if the IE "RRC State Indicator" is set to the value "CELL_FACH" or "CELL_PCH" or URA_PCH":
    - select a suitable UTRA cell according to [4] on that frequency;
    - act as specified in subclause 8.3.1.12.
  - if the IE "RRC State Indicator" is set to the value "CELL_DCH":
    - act on the IE "Frequency info" as specified in subclause 8.6.6.1.
- use the transport channel(s) applicable for the physical channel types that is used; and
- if the IE "TFS" is neither included nor previously stored in the UE for that transport channel(s):
  - use the TFS given in system information.
- if none of the TFS stored is compatible with the physical channel:
  - delete the stored TFS;
  - use the TFS given in system information.
- perform the physical layer synchronisation procedure as specified in [29];
- if the CELL UPDATE CONFIRM message includes the IE "RLC re-establish indicator (RB2, RB3 and RB4)":
  - re-establish the RLC entities for signalling radio bearer RB2, signalling radio bearer RB3 and signalling radio bearer RB4 (if established);
  - 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":
    - 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;
- if the CELL UPDATE CONFIRM message includes the IE "RLC re-establish indicator (RB5 and upwards)":
  - for radio bearers with RB identity 5 and upwards:
    - re-establish the AM RLC entities;
    - 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":
      - 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;

- if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - set the IE “Status” in the variable SECURITY_MODIFICATION for all the CN domains in the variable SECURITY_MODIFICATION to “Affected”;
- 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:

- not prohibit periodical status transmission in RLC;
- 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:

- 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";
- set the 20 MSB of the MAC-d HFN with the corresponding START value in the most recently sent IE "START list";
- set the remaining LSB of the MAC-d HFN to zero;
- apply ciphering on the transparent mode radio bearers;
- 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

- 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";
- select PRACH according to subclause 8.5.17;
- select Secondary CCPCH according to subclause 8.5.19;
- not prohibit periodical status transmission in RLC;
- if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - ignore that IE and stop using DRX.

If the UE after state transition enters URA_PCH or CELL_PCH state, it shall:

- prohibit periodical status transmission in RLC;
- clear the variable C_RNTI;
- stop using that C_RNTI just cleared from the variable C_RNTI in MAC;
- 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";
- select Secondary CCPCH according to subclause 8.5.19;
- if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
  - 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.
- if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:
  - set the variable INVALID_CONFIGURATION to TRUE.

If the UE after the state transition remains in CELL_FACH state; and

- the contents of the variable C_RNTI are empty:

it shall check the value of V302; and:

- if V302 is equal to or smaller than N302:
  - 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:
      - abort the ongoing integrity and/or ciphering reconfiguration;

- if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
  - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
  - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.
- if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
  - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
  - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.

- in case of a URA update procedure:
  - stop the URA update procedure; and
  - continue with a cell update procedure.
- 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";
- submit the CELL UPDATE message for transmission on the uplink CCCH;
- increment counter V302;
- restart timer T302 when the MAC layer indicates success or failure to transmit the message.

- if V302 is greater than N302:
  - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO;
  - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO;
  - in case of a cell update procedure:
    - clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - in case of a URA update procedure:
    - clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
  - release all its radio resources;
  - 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;
  - clear the variable ESTABLISHED_SIGNALLING_CONNECTIONS;
  - clear the variable ESTABLISHED_RABS;
  - enter idle mode;
  - other actions the UE shall perform when entering idle mode from connected mode are specified in subclause 8.5.2;
  - 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:

- if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
  - 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.
- ~~if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Integrity protection mode info" with the IE "Integrity protection mode command" set to "Modify":~~
  - ~~include the IE "Uplink integrity protection activation info" in any response message transmitted below; and~~
  - ~~set this IE to the value of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.~~
- in case of a cell update procedure:
  - 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
  - clear that entry.
- in case of a URA update procedure:
  - 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
  - clear that entry;
- if the variable PDCP_SN_INFO is non-empty:
  - 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.
- if the received CELL UPDATE CONFIRM or URA UPDATE CONFIRM message included the IE "Downlink counter synchronisation info":
  - calculate the START value according to subclause 8.5.9;
  - 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.
- transmit a response message as specified in subclause 8.3.1.7;
- if the IE "Integrity protection mode info" was present in the CELL UPDATE CONFIRM or URA UPDATE CONFIRM message:
  - start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.
  - ~~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;~~
- if the variable ORDERED_RECONFIGURATION is set to TRUE caused by the received CELL UPDATE CONFIRM message in case of a cell update procedure:
  - set the variable ORDERED_RECONFIGURATION to FALSE.
- clear the variable PDCP_SN_INFO;
- when the response message transmitted per subclause 8.3.1.7 to the UTRAN has been confirmed by RLC:

/* Indentation below has been changed*/

- if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Ciphering mode info":
  - resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
  - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
  - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.
- if the CELL UPDATE CONFIRM / URA UPDATE CONFIRM message contained the IE "Integrity protection mode info":
  - 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;
  - allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
- set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and

/* Indentation above has been changed*/

- clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.

- in case of a cell update procedure:
  - clear the entry for the CELL UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- in case of a URA update procedure:
  - clear the entry for the URA UPDATE CONFIRM message in the table "Rejected transactions" in the variable TRANSACTIONS.
- set the variable CELL_UPDATE_STARTED to FALSE;
- clear the variable SECURITY_MODIFICATION.

The procedure ends.

8.3.3.3 Reception of UTRAN MOBILITY INFORMATION message by the UE

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

- act on received information elements as specified in subclause 8.6;
- if the IE "UE Timers and constants in connected mode" is present:
  - 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
  - for each updated timer value:
    - start using the new value next time the timer is started;
  - for each updated constant value:
    - start using the new value directly;
- 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
- clear that entry;

- if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
  - set the IE “Status” in the variable SECURITY_MODIFICATION for all the CN domains in the variable SECURITY_MODIFICATION to “Affected”;
- if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
  - include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.
- ~~if the UTRAN MOBILITY INFORMATION message contained the IE "Integrity protection mode info" with the IE "Integrity protection mode command" set to "Modify":~~
  - ~~include and set the IE "Uplink integrity protection activation info" to the value of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.~~
- if the variable PDCP_SN_INFO is non-empty:
  - 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.
- if the received UTRAN MOBILITY INFORMATION message included the IE "Downlink counter synchronisation info":
  - calculate the START value according to subclause 8.5.9;
  - 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.
- transmit a UTRAN MOBILITY INFORMATION CONFIRM message on the uplink DCCH using AM RLC;
- if the IE "Integrity protection mode info" was present in the UTRAN MOBILITY INFORMATION message:
  - 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.
- if the variable PDCP_SN_INFO is empty; and
  - if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
    - when RLC has confirmed the successful transmission of the UTRAN MOBILITY INFORMATION CONFIRM message, perform the actions below.
  - if the UTRAN MOBILITY INFORMATION message did not contain the IE "Ciphering mode info":
    - when RLC has been requested to transmit the UTRAN MOBILITY INFORMATION CONFIRM message, perform the actions below.
- if the variable PDCP_SN_INFO is non-empty:
  - when RLC has confirmed the successful transmission of the UTRAN MOBILITY INFORMATION CONFIRM message:
    - for each radio bearer in the variable PDCP_SN_INFO:
      - if the IE "RB started" in the variable ESTABLISHED_RABS is set to "started":
        - configure the RLC entity for that radio bearer to "continue".
    - clear the variable PDCP_SN_INFO.
- if the UTRAN MOBILITY INFORMATION message contained the IE "Ciphering mode info":
  - resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
  - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and

- clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.

- if the UTRAN MOBILITY INFORMATION message contained the IE "Integrity protection mode info":

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

  - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and

  - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.

- clear the variable SECURITY_MODIFICATION.

The procedure ends.

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:

- first add the RLs indicated in the IE "Radio Link Addition Information";

- 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;

- perform the physical layer synchronisation procedure as specified in [29];

- if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":

- set the IE “Status” in the variable SECURITY_MODIFICATION for all the CN domains in the variable SECURITY_MODIFICATION to “Affected”;

- if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":

  - include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.

- ~~if the ACTIVE SET UPDATE message contained the IE "Integrity protection mode info" with the IE "Integrity protection mode command" set to "Modify":~~

  - ~~include and set the IE "Uplink integrity protection activation info" to the value of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.~~

- if the variable PDCP_SN_INFO is non-empty:

  - include the IE "RB with PDCP information list" in the ACTIVE SET UPDATE COMPLETE message; and

  - set it to the value of the variable PDCP_SN_INFO.

- if the IE "TFCI combining indicator" associated with a radio link to be added is set to TRUE:

  - if a DSCH transport channel is assigned and there is a 'hard' split in the TFCI field:

    - configure Layer 1 to soft-combine TFCI (field 2) of this new link with those links already in the TFCI (field 2) combining set.

- if the received ACTIVE SET UPDATE message included the IE "Downlink counter synchronisation info":

  - calculate the START value according to subclause 8.5.9;

  - 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.

- 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

- clear that entry;
- transmit an ACTIVE SET UPDATE COMPLETE message on the uplink DCCH using AM RLC without waiting for the Physical Layer synchronization;
- if the IE "Integrity protection mode info" was present in the ACTIVE SET UPDATE message:
  - 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.
- if the variable PDCP_SN_INFO is empty:
  - if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":
    - when RLC has confirmed the successful transmission of the ACTIVE SET UPDATE COMPLETE message:
      - perform the actions below.
  - if the ACTIVE SET UPDATE message did not contain the IE "Ciphering mode info":
    - when RLC has been requested to transmit the ACTIVE SET UPDATE COMPLETE message:
      - perform the actions below.
- if the variable PDCP_SN_INFO is non-empty:
  - when RLC has confirmed the successful transmission of the ACTIVE SET UPDATE COMPLETE message:
    - for each radio bearer in the variable PDCP_SN_INFO:
      - if the IE "RB started" in the variable ESTABLISHED_RABS is set to "started":
        - configure the RLC entity for that radio bearer to "continue".
    - clear the variable PDCP_SN_INFO.
- if the ACTIVE SET UPDATE message contained the IE "Ciphering mode info":
  - resume data transmission on any suspended radio bearer and signalling radio bearer mapped on RLC-AM or RLC-UM;
  - set the IE "Reconfiguration" in the variable CIPHERING_STATUS to FALSE; and
  - clear the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.
- if the ACTIVE SET UPDATE message contained the IE "Integrity protection mode info":
  - allow the transmission of RRC messages on all signalling radio bearers with any RRC SN;
  - set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to FALSE; and
  - clear the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.
- clear the variable SECURITY_MODIFICATION;
- the procedure ends on the UE side.

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:

- 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
- initialise the variable ESTABLISHED_SIGNALLING_CONNECTIONS with the signalling connections that remains after the handover according to the specifications of the source RAT;
- 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;
- initialise the variable TIMERS_AND_CONSTANTS to the default values and start to use those timer and constants values;
- if IE "Specification mode" is set to "Preconfiguration" and IE "Preconfiguration mode" is set to "Predefined configuration":
  - initiate the radio bearer and transport channel configuration in accordance with the predefined parameters identified by the IE "Predefined configuration identity";
  - 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;
  - store information about the established radio access bearers and radio bearers according to the IE "Predefined configuration identity"; and
  - 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".
- if IE "Specification mode" is set to "Preconfiguration" and IE "Preconfiguration mode" is set to "Default configuration":
  - 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";
  - 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

  - 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".
- if IE "Specification mode" is set to "Preconfiguration":
  - 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:
    - 0 dB for the power offset $P_{Pilot\text{-}DPDCH}$ bearer in FDD;
    - calculate the Default DPCH Offset Value using the following formula:
      - in FDD:

        Default DPCH Offset Value = (SRNTI 2 mod 600) * 512

      - in TDD:

        Default DPCH Offset Value = (SRNTI 2 mod 7)

    - 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.
- if IE "Specification mode" is set to "Complete specification":

- initiate the radio bearer, transport channel and physical channel configuration in accordance with the received radio bearer, transport channel and physical channel information elements.

- perform an open loop estimation to determine the UL transmission power according to subclause 8.5.3;

- calculate START according to subclause 8.5.9 for all CN domains

- 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 presentwith the calculated START value ;

- if ciphering has been activated and ongoing in the radio access technology from which inter- RAT handover is performed:

  - 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":

    - set the HFN component of the COUNT-C variable for all UL and DL radio bearers that use RLC-AM and RLC-UM and all UL and DL signalling radio bearers that use RLC-AM and RLC-UM to the START value for that CN domain as stored in the USIM if present for that CN domain,; and

    - if a "START" value was transferred prior to the handover according to the IE "UE security information" in the variable " INTER_RAT_HANDOVER_INFO_TRANSFERRED":

    - set the 20 MSB of the HFN component of the COUNT-C variable for all TM 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" ; /*CHANGED TO B3*/

    - else:

      - set the 20 MSB of the HFN component of the COUNT-C variable for all TM radio bearers to zero;

    - 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;

    - not increment the HFN component of COUNT-C for TM radio bearers using RLC-TM, i.e. keep the HFN value fixed without incrementing every CFN cycle;

    - set the CFN component of the COUNT-C variable to the value of the CFN as calculated in subclause 8.5.15;

    - set the HFN component of the COUNT-C variable for all UL and DL radio bearers and all UL and DL signalling radio bearers that use the transparent mode of RLC to zero, while not incrementing the value of the HFN component of the COUNT-C variable at each CFN cycle; and

    - set the CFN component of the COUNT-C variable to the value of the CFN as calculated in subclause 8.5.15;

    - set the IE "Status" in the variable CIPHERING_STATUS to "Started";

    - apply the same ciphering status (ciphered/unciphered) as prior to inter-RAT handover;

    - if the change of algorithm is requested by means of the IE "Ciphering algorithm":

      - apply this the algorithm according to IE "Ciphering Algorithm" and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND. /*CHANGED TO B3*/

- if ciphering has not been activated and ongoing in the radio access technology from which inter- RAT handover is performed:

  - 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":

    - set the IE "Status" in the variable CIPHERING_STATUS to "Not Started";

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

- 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:
  - include the IE "COUNT-C activation time" in the response message and specify a CFN value other than the default, "Now" for this IE;
  - at the CFN value as indicated in the response message in the IE "COUNT-C activation time" for radio bearers using RLC-TM:
    - 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
    - set the remaining LSBs of the HFN component of COUNT-C to zero;
    - increment the HFN component of the COUNT-C variable by one;
    - 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;
    - 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.
- transmit a HANDOVER TO UTRAN COMPLETE message on the uplink DCCH, using, if ciphering has been started, the new ciphering configuration~~, only if ciphering has been started~~;
- when the HANDOVER TO UTRAN COMPLETE message has been submitted to lower layers for transmission:
  - initialise variables upon entering UTRA RRC connected mode as specified in subclause 13.4.;
  - for all radio bearers using RLC-AM or RLC-UM:
    - 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
    - set the remaining LSBs of the HFN component of COUNT-C to zero;
    - increment the HFN component of the COUNT-C variable by one;
    - start incrementing the COUNT-C values;
- and the procedure ends.

8.3.7.4 Successful completion of the inter-RAT handover

Upon successfully completing the handover, UTRAN should:

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

Upon successfully completing the handover, the UE shall:

- if the USIM is present:
  - store the current START value for every CN domain in the USIM [50];
  - 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:
    - delete the ciphering and integrity keys that are stored in the USIM for that CN domain;
    - inform the deletion of these keys to upper layers.
- if the SIM is present:
  - store the current START value for every CN domain in the UE;

- 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:
  - delete the ciphering and integrity keys that are stored in the SIM for that CN domain;
  - inform the deletion of these keys to upper layers.
- 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.

8.5.2 Actions when entering idle mode from connected mode

When entering idle mode from connected mode, the UE shall:

- clear or set variables upon leaving UTRA RRC connected mode as specified in subclause 13.4;
- attempt to select a suitable cell to camp on.

When leaving connected mode according to [4], the UE shall:

- perform cell selection.

While camping on a cell, the UE shall:

- acquire system information according to the system information procedure in subclause 8.1;
- perform measurements according to the measurement control procedure specified in subclause 8.4; and
- if the UE is registered:
  - be prepared to receive paging messages according to the paging procedure in subclause 8.2.

If IE "PLMN identity" within variable SELECTED_PLMN has the value "GSM-MAP", the UE shall:

- delete any NAS system information received in connected mode;
- acquire the NAS system information in system information block type 1; and
- proceed according to subclause 8.6.1.2.

When entering idle mode, the UE shall:

- if the USIM is present, for each CN domain:
  - if a new security key set was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:
    - set the START value for this domain to zero and;
    - store this START value for this domain in the USIM;
  - else:
  - if the current "START" value, according to chapter 8.5.9 for a CN domain, is greater than or equal to the value "THRESHOLD" of the variable START_THRESHOLD:
    - delete the ciphering and integrity keys that are stored in the USIM for that CN domain;
    - inform the deletion of these keys to upper layers.
  - else
    - store the current "START" value for this CN domain on the USIM.
- else, if the SIM is present:

- if the current "START" value, according to subclause 8.5.9 for a CN domain, is greater than or equal to the value "THRESHOLD" of the variable START_THRESHOLD:

  - delete the Kc key that is stored in the SIM;

  - set the "START" values for both CN domains to zero and store them in the UE;

  - inform the deletion of these keys to upper layers.

- else

  - store the current "START" value for every CN domain in the UE

~~- if the USIM is present:~~

~~- store the current START value for every CN domain in the USIM [50];~~

~~- 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:~~

~~- delete the ciphering and integrity keys that are stored in the USIM for that CN domain;~~

~~- set the value of START value to THRESHOLD;~~

~~- inform the deletion of these keys to upper layers.~~

8.5.8 Maintenance of Hyper Frame Numbers

The MSBs of both the ciphering sequence numbers (COUNT-C) and integrity sequence numbers (COUNT-I), for the ciphering and integrity protection algorithms, respectively [40], are called the Hyper Frame Numbers (HFN).

For integrity protection, the UE shall:

- maintain COUNT-I as specified in subclause 8.5.10.

The following hyper frame numbers types are defined:

MAC-d HFN:
24 MSB of COUNT-C for data sent over RLC TM

RLC UM HFN:
25 MSB of COUNT-C for data sent over RLC UM

RLC AM HFN:
20 MSB of COUNT-C for data sent over RLC AM

RRC HFN:
28 MSB of COUNT-I

For non-transparent mode RLC signalling radio bearers and radio bearers, the UE shall:

- maintain one uplink and one downlink COUNT-C per signalling radio bearer and per radio bearer and one uplink and one downlink COUNT-I per signalling radio bearer.

For all transparent mode RLC signalling radio bearers and radio bearers of each CN domain, the UE shall:

- maintain one COUNT-C, common for all signalling radio bearers and radio bearers in uplink and downlink;

- maintain one uplink and one downlink COUNT-I per signalling radio bearer.

NOTE: In this release of the specification there is only an uplink transparent mode COUNT-I, which is used for signalling radio bearer RB0.

COUNT-C and COUNT-I are defined in [40], with the following supplement for COUNT-C: for transparent mode RLC radio bearers with a transmission time interval of x radio frames (x = 2, 4, 8), the MAC PDU is carried by L1 in x consecutive radio frames due to radio frame segmentation. In this case, the CFN of the first radio frame in the TTI shall

be used as the CFN component of COUNT-C for ciphering of all data in the TTI [15].~~the CFN of the first segment of the MAC PDU is used as the CFN component of COUNT-C.~~

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 | radio bearers and signalling radio bearers using the most recently configured CK_X and IK_X}) + 2~~1~~.

- 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 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:

- 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.

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:

- check the value of the IE "RRC message sequence number" included in the IE "Integrity check info";
  - if the "Downlink RRC Message sequence number" is not present in the variable INTEGRITY_PROTECTION_INFO:
    - 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.
  - if the "Downlink RRC Message sequence number" is present in the variable INTEGRITY_PROTECTION_INFO:
    - 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:
      - increment "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with one.
    - 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:
      - discard the message.
- calculate an expected message authentication code in accordance with subclause 8.5.10.3;
- compare the expected message authentication code with the value of the received IE "message authentication code" contained in the IE "Integrity check info";
  - if the expected message authentication code and the received message authentication code are the same, the integrity check is successful:
    - 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.
  - if the calculated expected message authentication code and the received message authentication code differ:
    - 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):
      - decrement "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO by one.
    - 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:

- discard the message.

8.5.10.2 Integrity protection in uplink

Prior to sending an RRC message using the signalling radio bearer with radio bearer identity n, and the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" the UE shall:

- increment "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with 1. When "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO becomes 0, the UE shall increment "Uplink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with 1;
- calculate the message authentication code in accordance with subclause 8.5.10.3;
- replace the "Message authentication code" in the IE "Integrity check info" in the message with the calculated message authentication code;
- replace the "RRC Message sequence number" in the IE "Integrity check info" in the message with contents set to the new value of the "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO.

In the response message for the procedure ordering the security reconfiguration, the UE indicates the activation time, for each signalling radio bearer except for the signalling radio bearer that was used for this security reconfiguration procedure. When the new integrity configuration is to be applied in uplink, UTRAN should start to apply the new integrity protection configuration according to the activation time for each signalling radio bearer (except for the signalling radio bearer which is used to send the message that is reconfiguring the security configuration) where the new configuration is to be applied starting from and including reception of the response message).

8.5.10.3 Calculation of message authentication code

The UE shall calculate the message authentication code in accordance with [40]. The input parameter MESSAGE [40] for the integrity algorithm shall be constructed by:

- setting the "Message authentication code" in the IE "Integrity check info" in the message the value of the IE "RB identity" ~~to the radio bearer identity~~ for the signalling radio bearer;
- setting the "RRC Message sequence number" in the IE "Integrity check info" in the message to zero;
- encoding the message;
- appending RRC padding (if any) as a bit string to the encoded bit string as the least significant bits.

For usage on an RRC message transmitted or received on the radio bearer with identity n, the UE shall:

- construct the input parameter COUNT-I [40] by appending the following IEs from the IE "Signalling radio bearer specific integrity protection information" for radio bearer n in the variable INTEGRITY_PROTECTION_INFO:
  - for uplink:
    - "Uplink RRC HFN", as the MSB, and "Uplink RRC Message sequence number", as LSB.
  - for downlink:
    - "Downlink RRC HFN", as the MSB, and the IE "RRC message sequence number" included in the IE "Integrity check info", as LSB.

8.6.3.4 Ciphering mode info

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

~~signalling radio bearers and~~ radio bearers~~, the old and latest ciphering configurations~~ and three configurations in total for all signalling radio bearers.~~, per CN domain~~.

If the IE "Ciphering mode info" is present and if the IE "Reconfiguration" in the variable CIPHERING_STATUS is set to TRUE, the UE shall:

- ignore this second attempt to change the ciphering configuration; and
- set the variable INCOMPATIBLE_SECURITY_RECONFIGURATION to TRUE.

If the IE "Ciphering mode info" is present and if the IE "Reconfiguration" in the variable CIPHERING_STATUS is set to FALSE, the UE shall:

~~- if the IE "Status" in the variable CIPHERING_STATUS of the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN has the value "Not Started", and if the IE "Ciphering mode command" has the value "stop"; or~~

- 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
- if there does not exist exactly one ciphering activation time in the IE "Radio bearer downlink ciphering 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

~~- if there does not exist exactly one ciphering activation time in the IE "Ciphering activation time for DPCH" for each established RLC-TM 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~~

- 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
- 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":
  - ignore this attempt to change the ciphering configuration;
  - set the variable INVALID_CONFIGURATION to TRUE;
  - perform the actions as specified in subclause 8.1.12.4c.
- set the IE "Reconfiguration" in the variable CIPHERING_STATUS to TRUE;

~~- if IE "Ciphering mode command" has the value "start/restart":~~

- set the IE "Status" in the variable CIPHERING_STATUS of the~~this~~ CN domains for which the IE “Status” of the variable SECURITY_MODIFICATION is set to “Affected”~~domain~~ to "Started";
- ~~start or restart~~apply the new ciphering configuration in the lower layers for all RBs ~~and SRBs~~ 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:~~:~~
  - using the ciphering algorithm (UEA [40]) indicated by the IE "Ciphering algorithm" as part of the new ciphering configuration;
  - for each radio bearer ~~and signalling 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:~~:~~
    - use the value of the IE "RB identity" in the variable ESTABLISHED_RABS minus one as the value of BEARER [40] in the ciphering algorithm.

    ~~- start incrementing the COUNT-C values for all RLC-AM and RLC-UM signalling radio bearers and continue incrementing the COUNT-C values for all RLC-AM and RLC-UM radio bearers;~~

- ~~if at least one transparent mode radio bearer exists for this CN domain and ciphering was started for this CN domain;~~

  - ~~continue incrementing the COUNT-C value for this CN domain.~~

- ~~else:~~

  - ~~start incrementing the COUNT-C values for that CN domain at the ciphering activation time as specified in the procedure.~~

~~NOTE: If the ciphering activation time for transparent mode radio bearers was specified in the downlink then the IE "Ciphering activation time for DPCH" is included (e.g. for the SECURITY MODE COMMAND), otherwise, this ciphering activation time is specified in the IE "COUNT-C activation time" in the uplink response message.~~

- ~~if the IE "Ciphering mode command" has the value "stop":~~

  - ~~when the new ciphering configuration is applied at the time as specified below:~~

    - ~~stop ciphering for all radio bearers for this CN domain and all signalling radio bearers;~~

    - ~~stop incrementing COUNT-C values for all UL and DL signalling radio bearers and also for UL and DL radio bearers using RLC-TM;~~

    - ~~continue incrementing COUNT-C values for all UL and DL radio bearers using RLC-UM or RLC-AM.~~

  - ~~set the IE "Status" in the variable CIPHERING_STATUS of the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN to "Not started".~~

- ~~in case the IE "Ciphering mode command" has the value "start/restart" or "stop",~~ the new ciphering configuration shall be applied as follows:

  - ~~store the (oldest currently used) ciphering configuration until activation times have elapsed for the new ciphering configuration to be applied on all signalling radio bearers and radio bearers;~~

  - consider an activation time in downlink to be pending:

    - for UM-RLC until an UMD PDU with sequence number equal to or larger than activation time –1 has been received;

    - for AM-RLC until all AMD PDUs with sequence numbers up to and including activation time –1 have been received;

    - for TM-RLC until the CFN indicated in the activation time has been reached;

  - if there are pending activation times in downlimk set for ciphering by a previous procedure changing the ciphering configuration:

    - apply the ciphering configuration included in the present message at this pending activation time.

  - 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:

    - for radio bearers using RLC-TM:

      - apply the old ciphering configuration for CFN less than the number indicated in the IE "Ciphering activation time for DPCH";

      - apply the new ciphering configuration for CFN greater than or equal to the number indicated in IE "Ciphering activation time for DPCH".

  - 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":

    - for radio bearers using RLC-TM:

- apply the old ciphering configuration for CFN less than the number as indicated in the transmitted uplink response message for the ciphering activation time for this radio bearer;
- 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.

- if the IE "Radio bearer downlink ciphering activation time info" is present:
  - apply the following procedure for each radio bearer and signalling radio bearers using RLC-AM or RLC-UM indicated by the IE "RB identity":

    - ~~suspend uplink transmission on the radio bearer or the signalling radio bearer (except for that SRBm that the message was used);~~

    - 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:

      - do not transmit RLC PDUs with sequence number greater than or equal to the uplink activation time, where the uplink activation time is seclected according to the rules below;

    - 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:

      - for each radio bearer and signalling radio bearer that has no pending ciphering activation time in the uplink as set by a previous procedure changing the security configuration:

        - set a suitable value that would ensure a minimised delay in the change to the latest security configuration.

      - for each radio bearer and signalling radio bearer that has a pending ciphering activation time ~~as~~ in the uplink as set by a previous procedure changing the security configuration:

        - set the same value as the pending ciphering activation time.

      - consider this activation time in uplink to be elapsed when the selected activation time (as above) is equal to the "RLC send sequence number";

    - 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;

    - ~~when the data transmission of that radio bearer or signalling radio bearer is resumed:~~

    /* Indentation has been changed in the following bullets*/

    - switch to the new ciphering configuration according to the following:

      - 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;

      - 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;

      - 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;

- 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.

/* Indentation has been changed in the above bullets*/

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

- 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 threetwo different integrity protection configurations (keysets) in total for all signalling radio bearers for all CN domains., the old and newest integrity protection configurations, per CN domain.

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:

- ignore this second attempt to change the integrity protection configuration; and
- 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:

- set the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to TRUE;
- 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:
  - initialise the information for all signalling radio bearers in the variable INTEGRITY_PROTECTION_INFO according to the following:
    - set the IE "Uplink RRC Message sequence number" in the variable INTEGRITY_PROTECTION_INFO to zero;
    - do not include set the IE "Downlink RRC Message sequence number" which is included in the variable INTEGRITY_PROTECTION_INFO.;
    - set the variable INTEGRITY_PROTECTION_ACTIVATION_INFO to zero for each signalling radio berer in the IE "ESTABLISHED_RABS";
  - set the IE "Status" in the variable INTEGRITY_PROTECTION_INFO to the value "Started";
  - perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1 by:
    - using the algorithm (UIA [40]) indicated by the IE "Integrity protection algorithm" contained in the IE "Integrity protection mode info";
    - using the IE "Integrity protection initialisation number", contained in the IE "Integrity protection mode info" as the value of FRESH [40].
    - 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;
    - start applying the new integrity protection configuration in the downlink for signalling radio bearer RB2 from and including the received SECURITY MODE COMMAND message;
    - start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted SECURITY MODE COMPLETE message;
    - 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".

- 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

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

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

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

    - let RBm be the signalling radio bearer where the reconfiguration message was received and let RBn be the signalling radio bearer where the response message is transmitted;

  - 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;

    - 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;

    - start applying the new integrity protection configuration in the downlink for signalling radio bearer RBm from and including the received configuration message;

    - start applying the new integrity protection configuration in the uplink for signalling radio bearer RBn from and including the transmitted response message;

    - 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".

- 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:

  - 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;

  - if there are pending activation times set for integrity protection by a previous procedure changing the integrity protection configuration:

    - apply the integrity protection configuration at this pending activation time as indicated in this procedure.

  - 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";

  - perform integrity protection on the received message, applying the new integrity protection configuration, as described in subclause 8.5.10.1;

    - if present, use the algorithm indicated by the IE "Integrity protection algorithm" (UIA [40]);

  - ~~let RBm be the signalling radio bearer on which the message containing the IE "integrity protection mode info" was received;~~

  - set the content of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO according to the following:

    - for each established signalling radio bearer, stored in the variable ESTABLISHED_RABS:

      - 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:

- 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:
  - set a suitable value that would ensure a minimised delay in the change to the latest integrity protection configuration.
- for signalling radio bearer that has a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:
  - set the same value as the pending activation time for integrity protection;
- 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.

- for signalling radio bearer RB0:
  - 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.
- prohibit the transmission of RRC messages on all signalling radio bearers, except for RB2~~m~~, 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.

- start applying the new integrity protection configuration in the uplink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2~~m~~, 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;
- start applying the new integrity protection configuration in the uplink at the RRC sequence number for signalling radio bearer RB2~~m~~, as specified for the procedure initiating the integrity protection reconfiguration;
- start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2~~m~~, 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".

- start applying the new integrity protection configuration in the downlink at the RRC sequence number for signalling radio bearer RB2~~m~~, 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:

- ignore this attempt to change the integrity protection configuration; and
- set the variable INVALID_CONFIGURATION to TRUE.

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

- not change the integrity protection configuration.

8.6.4.1 Signalling RB information to setup list

If the IE "Signalling RB information to setup list" is included the UE shall:

- use the same START value to initialise the COUNT-C and COUNT-I variables for all the signalling radio bearers in the list;
- if the IE "Signalling RB information to setup list" was included in the RADIO BEARER SETUP message:
  - if the variable "LATEST_CONFIGURED_CN_DOMAIN" has been initialised:
    - calculate the START value only once during this procedure according to subclause 8.5.9 for the CN domain indicated in the variable "LATEST_CONFIGURED_CN_DOMAIN";
    - store the calculated START value in the variable START_VALUE_TO_TRANSMIT;
- for each occurrence of the IE "Signalling RB information to setup":
  - use the value of the IE "RB identity" as the identity of the signalling radio bearer to setup;
  - if the signalling radio bearer identified with the IE "RB identity" does not exist in the variable ESTABLISHED_RABS:
    - create a new entry for the signalling radio bearer in the variable ESTABLISHED_RABS;
  - if the variable LATEST_CONFIGURED_CN_DOMAIN has been initialised and the value "STATUS" of the variable "CIPHERING_STATUS" of the CN domain stored in this variable is "Started":
    - if the IE "Uplink RLC mode" or the IE "Downlink RLC mode" either in the IE "RLC info" or referenced by the RB identity in the IE "Same as RB" is set to "AM RLC" or "UM RLC":
      - initialise the 20 MSB of the hyper frame number component of COUNT-C for this signalling radio bearer with the START value in the variable START_VALUE_TO_TRANSMIT~~for the CN domain as indicated in the variable "LATEST_CONFIGURED_CN_DOMAIN"~~;
      - set the remaining LSB of the hyper frame number component of COUNT-C for this signalling radio bearer to zero.
      - start to perform ciphering on this signaling radio bearer, using the value of the IE "RB identity" minus one as the value of BEARER in the ciphering algorithm.
  - if the variable LATEST_CONFIGURED_CN_DOMAIN has been initialised and the value "Status" of the variable "INTEGRITY_PROTECTION_INFO" of the CN domain stored in this variable is "Started":
    - initialise the 20 MSB of the hyper frame number component of COUNT-I for this signalling radio bearer with the START value in the variable START_VALUE_TO_TRANSMIT;~~for the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN;~~

- set the remaining LSB of the hyper frame number component of COUNT-I for this signalling radio bearer to zero;
- for this signalling radio bearer, set the IE "Uplink RRC Message sequence number" in the variable INTEGRITY_PROTECTION_INFO to zero.
- start performing integrity protection according to subclause 8.5.10.1 and 8.5.10.2;

- perform the actions for the IE "RLC info" as specified in subclause 8.6.4.9, applied for that signalling radio bearer;
- perform the actions for the IE "RB mapping info" as specified in subclause 8.6.4.8, applied for that signalling radio bearer.

- apply a default value of the IE "RB identity" equal to 1 for the first IE "Signalling RB information to setup"; and
- increase the default value by 1 for each occurrence.

8.6.4.2 RAB information for setup

If the IE "RAB information for setup" is included, the procedure is used to establish radio bearers belonging to a radio access bearer, and the UE shall:

- if several IEs "RAB information for setup" are included and the included IEs "CN domain identity" in the IE "RAB info" does not all have the same value:
  - set the variable INVALID_CONFIGURATION to TRUE.
- if the radio access bearer identified with the IE "RAB info" does not exist in the variable ESTABLISHED_RABS:
  - create a new entry for the radio access bearer in the variable ESTABLISHED_RABS;
  - store the content of the IE "RAB info" in the entry for the radio access bearer in the variable ESTABLISHED_RABS;
  - indicate the establishment of the radio access bearer to the upper layer entity using the IE "CN domain identity", forwarding the content of the IE "RAB identity";
  - if prior to this procedure there exists no transparent mode radio bearer for the CN domain included in the IE "CN domain identity" and at least one transparent mode radio bearer is included in the IE "RB information to setup"; or
  - if at least one RLC-AM or RLC-UM radio bearer is included in the IE "RB information to setup":
    - calculate the START value only once during this procedure (the same START value shall be used on all new radio bearers created for this radio access bearer) according to subclause 8.5.9 for the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" part of the IE "RAB information to setup";
    - store the calculated START value in the variable START_VALUE_TO_TRANSMIT.
- for each radio bearer in the IE "RB information to setup":
  - if the radio bearer identified with the IE "RB identity" does not exist in the variable ESTABLISHED_RABS:
    - perform the actions specified in subclause 8.6.4.3;
    - store information about the new radio bearer in the entry for the radio access bearer identified by "RAB info" in the variable ESTABLISHED_RABS;
    - create a new RAB subflow for the radio access bearer;
    - number the RAB subflow in ascending order, assigning the smallest number to the RAB subflow corresponding to the first radio bearer in the list;

- if the IE "CN domain identity" in the IE "RAB info" is set to "PS domain" and the number of RAB subflows for the radio access bearer is greater than 1:
  - set the variable INVALID_CONFIGURATION to TRUE.
- if the radio bearer identified with the IE "RB identity" already exists in the variable ESTABLISHED_RABS:
  - set the variable INVALID_CONFIGURATION to TRUE.

8.6.4.2a RAB information to reconfigure

If the IE "RAB information to reconfigure" is included then the UE shall:

- if the entry for the radio access bearer identified by the IE "CN domain identity" together with the IE "RAB Identity" in the variable ESTABLISHED_RABS already exists:
  - perform the action for the IE "NAS Synchronization Indicator", according to subclause 8.6.4.12.
- else:
  - set the variable INVALID_CONFIGURATION to TRUE.

8.6.4.3 RB information to setup

If the IE "RB information to setup" is included, the UE shall apply the following actions on the radio bearer identified with the value of the IE "RB identity". The UE shall:

- use the same START value to initialise the hyper frame number components of COUNT-C variables for all the new radio bearers to setup;
- perform the actions for the IE "PDCP info", if present, according to subclause 8.6.4.10, applied for the radio bearer;
- perform the actions for the IE "RLC info", according to subclause 8.6.4.9, applied for the radio bearer;
- perform the actions for the IE "RB mapping info", according to subclause 8.6.4.8, applied for the radio bearer;
- if the IE "Downlink RLC mode" either in the IE "RLC info" or referenced by the RB identity in the IE "Same as RB" is set to "TM RLC":
  - configure delivery of erroneous SDUs in lower layers according to indication from upper layer [5].
- if the IE "Uplink RLC mode" or the IE "Downlink RLC mode" either in the IE "RLC info" or referenced by the RB identity in the IE "Same as RB" is set to "AM RLC" or "UM RLC":
  - initialise the 20 MSB of the hyper frame number component of COUNT-C for this radio bearer with the START value in the variable START_VALUE_TO_TRANSMIT;
  - set the remaining LSB of the hyper frame number component of COUNT-C for this radio bearer to zero;
  - start incrementing the COUNT-C values.
- if the IE "Uplink RLC mode" and the IE "Downlink RLC mode" either in the IE "RLC info" or referenced by the RB identity in the IE "Same as RB" is set to "TM RLC":
  - if prior to this procedure there exists no transparent mode radio bearer for the CN domain included in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED_RABS and at least one transparent mode radio bearer is included in the IE "RB information to setup":
    - - at the activation time as specified in the IE "Ciphering activation time for DPCH" if included in the IE "Ciphering mode info" in the command message or, if this IE is not included, as specified in the IE "COUNT-C activation time" included in the response message:
      - initialise the 20 most significant bits of the hyper frame number component of COUNT-C common for all transparent mode radio bearers of this CN domain with the START value in the variable START_VALUE_TO_TRANSMIT;

- set the remaining LSB of the hyper frame number component of COUNT-C to zero;
- if 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 "Not Started":
  - do not increment the COUNT-C value for this CN domain;
- else, if 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":
  - start increment the COUNT-C value for this CN domain;

- if prior to this procedure there exists at least one transparent mode radio bearer for the CN domain included in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED_RABS:
  - continue incrementing the COUNT-C value common for all transparent mode radio bearers of this CN domain.

~~- if no other transparent mode RLC radio bearers and signalling radio bearers exist in the variable ESTABLISHED_RABS:~~

~~- initialise the 20 MSB of the hyper frame number component of COUNT-C for this radio bearer with the START value in the variable START_VALUE_TO_TRANSMIT;~~

~~- set the remaining LSB of the hyper frame number component of COUNT-C for this radio bearer to zero.~~

~~- if at least one transparent mode RLC radio bearers or signalling radio bearers exist in the variable ESTABLISHED_RABS:~~

~~- set the MAC-d HFN component of the COUNT-C for this radio bearer with the MAC-d HFN that is common (refer to subclause 8.5.8) for the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" part of the IE "RAB information for setup".~~

- if 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":
  - start to perform ciphering on the radio bearer in lower layers, using the value of the IE "RB identity" minus one as the value of BEARER in the ciphering algorithm.

NOTE: UTRAN should not use the IE "RB information to setup" to setup radio bearers with RB identity in the range 1-4.

8.6.4.8 RB mapping info

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

- for each multiplexing option of the RB:
  - 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:
    - set the variable INVALID_CONFIGURATION to TRUE.
  - if a multiplexing option that maps a logical channel corresponding to a TM-RLC entity onto RACH, CPCH, FACH or DSCH is included:
    - set the variable INVALID_CONFIGURATION to TRUE.
  - 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"):
    - set the variable INVALID_CONFIGURATION to TRUE.

- 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:
  - set the variable INVALID_CONFIGURATION to TRUE.
- 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:
  - set the variable INVALID_CONFIGURATION to TRUE.
- if that RB is using UM or TM and the multiplexing option realises it using two logical channels:
  - set the variable INVALID_CONFIGURATION to TRUE.
- for each logical channel in that multiplexing option:
  - if the value of the IE "RLC size list" is set to "Explicit list":
    - 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
    - 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
    - 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
    - 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":
      - set the variable INVALID_CONFIGURATION to TRUE.
  - if the value of the IE "RLC size list" is set to "All":
    - 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
    - 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":
      - set the variable INVALID_CONFIGURATION to TRUE.
  - if the value of the IE "RLC size list" is set to "Configured":
    - 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
    - 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:
      - set the variable INVALID_CONFIGURATION to TRUE.

- 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:
  - set the variable INVALID_CONFIGURATION to TRUE.
- delete all previously stored multiplexing options for that radio bearer;
- store each new multiplexing option for that radio bearer;
- select and configure the multiplexing options applicable for the transport channels to be used;
- if the IE "Uplink transport channel type" is set to the value "RACH":
  - in FDD:
    - 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.
  - in TDD:
    - 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".
- 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
- in case the selected multiplexing option is a multiplexing option on RACH:
  - ignore the RLC size indexes that do not correspond to any RLC size within the Transport Format Set stored for RACH.
- 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:
  - 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.
- 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:
  - re-establish the corresponding RLC entity;
  - configure the corresponding RLC entity with the new RLC size;
  - 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
  - for each AM RLC signalling radio bearer in the the CN domain as indicated in the IE "CN domain identity" in the variable LATEST_CONFIGURED_CN_DOMAIN whose RLC size is changed:
  - ~~for the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED_RABS for all radio bearers; and~~
  - ~~for the CN domain as indicated in the IE "CN domain identity" in the variable LATEST_CONFIGURED_CN_DOMAIN for all signalling radio bearers:~~
    - if the IE "Status" in the variable CIPHERING_STATUS of this CN domain is set to "Started":
      - if this IE was included in system information:
        - 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.

- if this IE was included in CELL UPDATE CONFIRM:
  - 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.
- if this IE was included in a reconfiguration message:
  - 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.

- if that RB is using UM:
  - indicate the largest applicable RLC size to the corresponding RLC entity.
- 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);
- configure the MAC with the logical channel priorities according to selected multiplexing option;
- configure the MAC with the set of applicable RLC Sizes for each of the logical channels used for that RB;
- if there is no multiplexing option applicable for the transport channels to be used:
  - set the variable INVALID_CONFIGURATION to TRUE.
- if there is more than one multiplexing option applicable for the transport channels to be used:
  - set the variable INVALID_CONFIGURATION to TRUE.

In case IE "RB mapping info" includes IE "Downlink RLC logical channel info" but IE "Number of downlink RLC logical channels" is absent, 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:

- 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":
  - ignore that System Information Block.
- 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':
  - ignore that System Information Block.
- 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':
  - keep the transport format set if this exists for that transport channel;
  - set the variable INVALID_CONFIGURATION to TRUE.

- 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

- 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

- 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

- 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

- 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

- 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

- 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":

  - keep the transport format set if this exists for that transport channel;

  - set the variable INVALID_CONFIGURATION to TRUE.

- if the total number of configured transport formats for the transport channel exceeds maxTF:

  - keep the transport format set if this exists for that transport channel;

  - set the variable INVALID_CONFIGURATION to TRUE.

- if the IE "Transport format set" is considered as valid according to the rules above:

  - remove a previously stored transport format set if this exists for that transport channel;

  - store the transport format set for that transport channel;

  - 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;

  - if the IE "Transport format Set" has the choice "Transport channel type" set to "Dedicated transport channel":

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

      TB size = RLC size + 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.

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

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

      TB size = RLC size.

- if the IE "Number of Transport blocks" <> 0 and IE "RLC size" = 0, no RLC PDU data exists but only parity bits exist for that transport format;
- if the IE "Number of Transport blocks" = 0, neither RLC PDU neither data nor parity bits exist for that transport format;
- configure the MAC with the new transport format set (with computed transport block sizes) for that transport channel;
- 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:
  - 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.
  - if the IE "Transport Format Set" was received within the IE "PRACH system information list":
    - 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.
  - 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:
    - 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.
  - 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:
    - set the variable INVALID_CONFIGURATION to true.
  - 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:
    - re-establish the corresponding RLC entity;
    - configure the corresponding RLC entity with the new RLC size;
    - 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
    - for each AM RLC signalling radio bearer in the the CN domain as indicated in the IE "CN domain identity" in the variable LATEST_CONFIGURED_CN_DOMAIN whose RLC size is changed:~~for the CN domain as indicated in the IE "CN domain identity" in the IE "RAB info" in the variable ESTABLISHED_RABS for all radio bearers; and~~
    - ~~for the CN domain as indicated in the IE "CN domain identity" in the variable LATEST_CONFIGURED_CN_DOMAIN for all signalling radio bearers:~~
      - 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":
        - 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.
      - 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":
        - 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.
      - 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":

- 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.

- 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":

- 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.

- if that RB is using UM:

- indicate the largest applicable RLC size to the corresponding RLC entity.

- 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].

8.6.6.28 Downlink DPCH info common for all radio links

If the IE "Downlink DPCH info common for all RL" is included the UE shall:

- perform actions for the IE "Timing indication" as specified in subclause 8.5.15.2;
- ignore the value received in IE "CFN-targetSFN frame offset";
- if the IE "Downlink DPCH power control information" is included:
  - perform actions for the IE "DPC Mode" according to [29].
- if the IE choice "mode" is set to 'FDD':
  - if the IE "Downlink rate matching restriction information" is included:
    - set the variable INVALID_CONFIGURATION to TRUE.
  - perform actions for the IE "spreading factor";
  - perform actions for the IE "Fixed or Flexible position";
  - perform actions for the IE "TFCI existence";
  - if the IE choice "SF" is set to 256:
    - store the value of the IE "Number of bits for pilot bits".
  - if the IE choice "SF" set to 128:
    - store the value of the IE "Number of bits for pilot bits".
- if the IE choice "mode" is set to 'TDD':
  - perform actions for the IE "Common timeslot info".

If the IE "Downlink DPCH info common for all RL" is included in a message used to perform a Timing re-initialised hard handover or the IE "Downlink DPCH info common for all RL" is included in a message used to transfer the UE from a state different from Cell_DCH to the Cell_DCH state, and ciphering is active for any radio bearer using RLC-TM, the UE shall, after having activated the dedicated physical channels indicated by that IE:

- set the 20 MSB of the HFN component of COUNT-C for TM-RLC to the value of the latest transmitted IE "START" or "START List" for this CN domain, while not incrementing the value of the HFN component of COUNT-C at each CFN cycle; and

- set the remaining LSBs of the HFN component of COUNT-C to zero;

- include the IE "COUNT-C activation time" in the response message and specify a CFN value other than the default, "Now" for this IE;
- calculate the START value according to subclause 8.5.9;
- include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the response message;
- at the CFN value as indicated in the response message in the IE "COUNT-C activation time":
  - 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
  - set the remaining LSBs of the HFN component of COUNT-C to zero;
  - increment the HFN component of the COUNT-C variable by one;
  - 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;
  - step the COUNT-C variable, as normal, at each CFN value, i.e. the HFN component is no longer fixed in value but incremented at each CFN cycle.

~~- increment HFN for RLC-TM by '1'.~~

10.2.16b HANDOVER TO UTRAN COMPLETE

This message is sent by the UE when a handover to UTRAN 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	
UE Information elements				
START list	CH	1 to <maxCNdomains>		START [40] values for all CN domains. ~~The IE is mandatory if it has not been transferred prior to the handover.~~
>CN domain identity	MP		CN domain identity 10.3.1.1	
>START	MP		START 10.3.3.38	
RB Information elements				
COUNT-C activation time	OP		Activation time 10.3.3.1	Used for radio bearers mapped on RLC-TM.

10.2.16c INITIAL DIRECT TRANSFER

This message is used to initiate a signalling connection based on indication from the upper layers, and to transfer a NAS message.

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	
UE information elements				
Integrity check info	CH		Integrity check info 10.3.3.16	
CN information elements				
CN domain identity	MP		CN domain identity 10.3.1.1	
Intra Domain NAS Node Selector	MP		Intra Domain NAS Node Selector 10.3.1.6	
NAS message	MP		NAS message 10.3.1.8	
START	OP		START 10.3.3.38	START value to be used in the CN domain as indicated in the IE CN domain identity. This IE shall always be present inthis version of the protocol.
Measurement information elements				
Measured results on RACH	OP		Measured results on RACH 10.3.7.45	

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)	The command "stop" is not used in this version of the protocol
Ciphering algorithm	CV-*notStop*		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
notStop	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.

10.3.3.16 Integrity check info

The Integrity check info contains the RRC message sequence number needed in the calculation of XMAC-I [40] and the calculated MAC-I.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message authentication code	MP		bit string(32)	MAC-I [40]. The Message Authentication Code bits are numbered b0-b31, where b0 is the least significant bit. The 27 MSB of the IE shall be set to zero and the 5 LSB of the IE shall be set to the value of the IE "RB identity" for the used signalling radio bearer ~~identity~~ when the encoded RRC message is used as the MESSAGE parameter in the integrity protection algorithm.
RRC Message sequence number	MP		Integer (0..15)	The local RRC hyper frame number (RRC HFN) is concatenated with the RRC message sequence number to form the input parameter COUNT-I for the integrity protection algorithm. The IE value shall be set to zero when the encoded RRC message is used as the MESSAGE parameter in the integrity protection algorithm.

11.2 PDU definitions

```
-- **************************************************
--
-- INITIAL DIRECT TRANSFER
--
-- **************************************************

InitialDirectTransfer ::= SEQUENCE {
    -- Core network IEs
        cn-DomainIdentity               CN-DomainIdentity,
        intraDomainNasNodeSelector      IntraDomainNasNodeSelector,
        nas-Message                     NAS-Message,
    -- Measurement IEs
        measuredResultsOnRACH           MeasuredResultsOnRACH               OPTIONAL,
        v3a0NonCriticalExtensions       SEQUENCE {
        initialDirectTransfer-v3a0ext   InitialDirectTransfer-v3a0ext,
    -- Extension mechanism for non-     release99 information
        nonCriticalExtensions               SEQUENCE {}     OPTIONAL
        }       OPTIONAL
}


InitialDirectTransfer-v3a0ext ::= SEQUENCE {
        -- the START value shall always be included in this version of the protocol
        start-Value             START-Value                                 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,
    START-Value,
    U-RNTI,
    UE-RadioAccessCapability,
    UE-RadioAccessCapability-v370ext,
    UE-RadioAccessCapability-v380ext,
-- Radio Bearer IEs :
    PredefinedConfigStatusList,
    PredefinedConfigValueTag,
    RAB-InformationSetupList,
    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 {
        interRATHandoverInfo-r3         InterRATHandoverInfoWithInterRATCapabilities-r3-IEs,
    -- IE InterRATHandoverInfoWithInterRATCapabilities-r3-IEs also
    -- includes non critical extensions
        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 (SIZE (0..255))
        -- 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
}

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,
                        -- 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 this IE 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 {}                                 OPTIONAL
        }                                                                               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{
        StartValueForCIphering-v3a0ext      START-Value
}

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 this IE 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 {}                                 OPTIONAL
        }                                                                   OPTIONAL
}

-- 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: 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
}

MeasurementCommandWithType-r4 ::=   CHOICE {
    setup                               MeasurementType-r4,
    modify                              NULL,
    release                             NULL
}

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

OngoingMeasRep-r4 ::=               SEQUENCE {
    measurementIdentity         MeasurementIdentity,
    measurementCommandWithType          MeasurementCommandWithType-r4,
    -- TABULAR: The CHOICE Measurement in the tabular description is included
    -- in the IE above.
    measurementReportingMode            MeasurementReportingMode            OPTIONAL,
    additionalMeasurementID-List        AdditionalMeasurementID-List        OPTIONAL
}

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

OngoingMeasRepList-r4 ::=           SEQUENCE (SIZE (1..maxNoOfMeas)) OF
                                        OngoingMeasRep-r4

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
```

13.4.x SECURITY_MODIFICATION

This variable contains information on which CN domain is affected by the ongoing security reconfiguration

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Status for each CN domain	MP	<1 to maxCNDomains>		
>CN domain identity	MP		CN domain identity 10.3.1.1	
>Status	MP		Enumerated(Affected, Not Affected)	

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
Non RRC IEs				
>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,	

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
			await Transport CH Reconfiguration Complete, await Physical CH Reconfiguration Complete, await Active Set Update Complete, await Handover Complete, send Cell Update Confirm, send URA Update Confirm, , others)	
Ciphering related information				
>Ciphering status for each CN domain	MP	<1 to maxCNDomains>		
>>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-*Ciphering*			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-*Ciphering*	1 to <maxCNdomains>		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)
>>Uplink HFN	MP		Bit string(20..25)	This IE is either RLC AM HFN (20 bits) or RLC UM HFN (25 bits)

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
Integrity protection related information				
>Integrity protection status	MP		Enumerated(Not started, Started)	
>Signalling radio bearer specific integrity protection information	CV-*IP*	4 to <maxSRBsetup>		
>>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)	
RRC IEs				
UE Information elements				
>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 *Position estimate*	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	
Other Information elements				
>UE system specific capability	OP	1 to <maxSyste		

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
		mCapability>		
>>Inter-RAT UE radio access capability	MP		Inter-RAT UE radio access capability 10.3.8.7	
UTRAN Mobility Information elements				
>URA Identifier	OP		URA identity 10.3.2.6	
CN Information Elements				
>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	
Measurement Related Information elements				
>For each ongoing measurement reporting	OP	1 to <MaxNoOfMeas>		
>>Measurement Identity	MP		Measurement identity 10.3.7.48	
>>Measurement Command	MP		Measurement command 10.3.7.46	
>>Measurement Type	CV-*Setup*		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 *Measurement*	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	

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
			quantity 10.3.7.41	
>>>>Reporting cell status	OP		Reporting cell status 10.3.7.61	
>>>>Measurement validity	OP		Measurement validity 10.3.7.51	
>>>>CHOICE *report criteria*	OP			
>>>>>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 *report criteria*	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	

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
>>>>Reporting cell status	OP		Reporting cell status 10.3.7.61	
>>>>Measurement validity	OP		Measurement validity 10.3.7.51	
>>>>CHOICE *report criteria*	OP			
>>>>>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 *report criteria*	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 *report criteria*	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	

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
>>>>UE internal reporting quantity	OP		UE internal reporting quantity 10.3.7.82	
>>>>CHOICE *report criteria*	OP			
>>>>>UE internal measurement reporting criteria			UE internal measurement 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 *report criteria*	OP			
>>>>>LCS reporting criteria			LCS reporting criteria 10.3.7.110	
>>>>>Periodical reporting			Periodical reporting criteria 10.3.7.53	
>>>>>No reporting				
Radio Bearer Information Elements				
>Pre-defined configuration status information	OP		Pre-defined configuration status information 14.13.2.3	
>Signalling RB information list	MP	1 to <maxSRBsetup>		For each signalling radio bearer
>>Signalling RB information	MP		Signalling RB information to setup 10.3.4.24	
>RAB information list	OP	1 to <maxRABsetup>		Information for each RAB
>>RAB information	MP		RAB information to setup 10.3.4.10	
Transport Channel Information Elements				
Uplink transport channels				
>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>		

Information Element/Group Name	Need	Multi	Type and reference	Semantics description
>>UL transport channel information	MP		Added or reconfigured UL TrCH information 10.3.5.2	
>CHOICE *mode*	OP			
>>FDD				
>>>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)
Downlink transport channels				
>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	
Other Information elements				
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
Setup	The IE is mandatory present when the IE Measurement command has the value "Setup", otherwise the IE is not needed.
Ciphering	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.
IP	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.
ProtErr	This IE is mandatory present if the IE "Protocol error indicator" is included and has the value "TRUE". Otherwise it is not needed.