

TSG-RAN Meeting #21
Frankfurt, Germany, 16-19 September 2003

RP-030484

Title: CRs (R'99 and linked Rel-4/Rel-5) to TS 25.331 (1)

Source: TSG-RAN WG2

Agenda item: 7.3.3

Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level	Workitem
25.331	1991	-	R99	Handling of key sets at Inter-RAT Handover to UTRAN	F	3.15.0	3.16.0	R2-031856	TEI
25.331	1992	-	Rel-4	Handling of key sets at Inter-RAT Handover to UTRAN	A	4.10.0	4.11.0	R2-031857	TEI
25.331	1993	-	Rel-5	Handling of key sets at Inter-RAT Handover to UTRAN	A	5.5.0	5.6.0	R2-031858	TEI
25.331	1994	-	R99	Correction to UE Positioning privacy procedures	F	3.15.0	3.16.0	R2-031866	TEI
25.331	1995	-	Rel-4	Correction to UE Positioning privacy procedures	A	4.10.0	4.11.0	R2-031867	TEI
25.331	1996	-	Rel-5	Correction to UE Positioning privacy procedures	A	5.5.0	5.6.0	R2-031868	TEI
25.331	2001	1	R99	START calculation	F	3.15.0	3.16.0	R2-032034	TEI
25.331	2002	1	Rel-4	START calculation	A	4.10.0	4.11.0	R2-032035	TEI
25.331	2003	1	Rel-5	START calculation	F	5.5.0	5.6.0	R2-032036	TEI
25.331	2004	-	R99	PRACH channelisation code list limitation to align with TS 25.221	F	3.15.0	3.16.0	R2-031898	TEI
25.331	2005	-	Rel-4	PRACH channelisation code list limitation to align with TS 25.221	A	4.10.0	4.11.0	R2-031899	TEI
25.331	2006	-	Rel-5	PRACH channelisation code list limitation to align with TS 25.221	A	5.5.0	5.6.0	R2-031900	TEI
25.331	2007	-	R99	Handling of transport channel information at radio bearer release	F	3.15.0	3.16.0	R2-031901	TEI
25.331	2008	-	Rel-4	Handling of transport channel information at radio bearer release	A	4.10.0	4.11.0	R2-031902	TEI
25.331	2009	-	Rel-5	Handling of transport channel information at radio bearer release	A	5.5.0	5.6.0	R2-031903	TEI
25.331	2010	-	R99	Reconfiguration with transition to CELL_PCH or URA_PCH	F	3.15.0	3.16.0	R2-031904	TEI
25.331	2011	-	Rel-4	Reconfiguration with transition to CELL_PCH or URA_PCH	A	4.10.0	4.11.0	R2-031905	TEI
25.331	2012	-	Rel-5	Reconfiguration with transition to CELL_PCH or URA_PCH	A	5.5.0	5.6.0	R2-031906	TEI

TSG-RAN Working Group 2 meeting #37
Budapest, Hungary 25th-29th Aug 2003

R2-031856

CR-Form-v7

CHANGE REQUEST

⌘ **25.331 CR 1991** ⌘ rev **3.f.0** ⌘ Current version: **3.f.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Handling of key sets at Inter-RAT Handover to UTRAN		
Source:	⌘ RAN WG2		
Work item code:	⌘ TEI	Date:	⌘ Aug 2003
Category:	⌘ F	Release:	⌘ R99
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)		2 (GSM Phase 2)
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)
	B (addition of feature),		R97 (Release 1997)
	C (functional modification of feature)		R98 (Release 1998)
	D (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change: ⌘ 1. It is currently not clear that UE shall consider a key set as 'new' only in case UE receives the key set for the ongoing signalling connection while in UMTS. This clarification is needed in order to prevent the UE from assuming that a key set received in another RAT is 'new' at a subsequent reception of a SECURITY MODE CONTROL message (and initialise the HFNs to zero), instead of assuming that the key set is 'not new' (and initialise HFNs to the values send to UTRAN in HANDOVER TO UTRAN COMPLETE).

2. It is currently not clear what key set UE shall use after Inter-RAT handover to UTRAN, in case the key set stored on USIM/SIM is different from the key set currently in use for ciphering of the connection in the other RAT.

Summary of change: ⌘ Section 8.1.12.3.1:
It is clarified in a note that the actions in this section are performed only in case UE receives a new key set for the ongoing signalling connection while in UTRA.

Section 8.3.6.3:
It is clarified in a note that keys received while in another RAT shall not be regarded as 'new'.

It is added in a note that UE (after handover from another RAT) at a subsequent security mode control procedure, activates ciphering and/or integrity protection using the key set stored in USIM/SIM.

It is corrected that UE shall, after the Inter-RAT handover to UTRAN, use the ciphering key set stored in the USIM/SIM, not the key set that was in use prior to the handover.

T1 impact:

<p>No impact on T1 specifications is foreseen</p> <p>Backward compatibility:</p> <p>Backwards compatible for a UE and UTRAN/CN that have assumed the indicated behaviour. In case either UE or UTRAN/CN are not complying with the correction, ciphering and/or integrity protection will fail after an Inter-RAT handover to UTRAN, in case the key set stored on USIM/SIM is different from the key set in use prior to the handover.</p>	
<p>Consequences if not approved:</p>	<p>⌘ Ciphering and/or integrity protection might fail after an Inter-RAT handover to UTRAN, in case the key set stored on USIM/SIM is different from the key set in use prior to the handover.</p>

<p>Clauses affected:</p>	<p>⌘ 8.1.12.3.1, 8.3.6.3</p>																
<p>Other specs affected:</p>	<table border="1"> <thead> <tr> <th>Y</th> <th>N</th> <th></th> <th>⌘</th> </tr> </thead> <tbody> <tr> <td></td> <td>X</td> <td>Other core specifications</td> <td></td> </tr> <tr> <td></td> <td>X</td> <td>Test specifications</td> <td></td> </tr> <tr> <td></td> <td>X</td> <td>O&M Specifications</td> <td></td> </tr> </tbody> </table>	Y	N		⌘		X	Other core specifications			X	Test specifications			X	O&M Specifications	
Y	N		⌘														
	X	Other core specifications															
	X	Test specifications															
	X	O&M Specifications															
<p>Other comments:</p>	<p>⌘</p>																

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.1.12.3.1 New ciphering and integrity protection keys

NOTE: The actions in this subclause are to be performed only if the new keys were received for an ongoing signalling connection [while in UTRA](#).

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

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

- 4> set the IE "Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the uplink COUNT-I to zero.
- 1> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
 - 2> for each signalling radio bearer and for each radio bearer for the CN domain indicated in the variable LATEST_CONFIGURED_CN_DOMAIN:
 - 3> if the IE "Status" in the variable CIPHERING_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers using RLC-TM:
 - 4> at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info":
 - 5> start using the new key in uplink and downlink;
 - 5> set the HFN component of the COUNT-C to zero.
 - 3> if the IE "Status" in the variable CIPHERING_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers and signalling radio bearers using RLC-AM and RLC-UM:
 - 4> in the downlink, at the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info":
 - 5> start using the new key;
 - 5> set the HFN component of the downlink COUNT-C to zero.
 - 4> in the uplink, at the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info":
 - 5> start using the new key;
 - 5> set the HFN component of the uplink COUNT-C to zero.
 - 1> consider the value of the latest transmitted START value to be zero.

8.3.6.3 Reception of HANDOVER TO UTRAN COMMAND message by the UE

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

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

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

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

- 2> set the IE "RAB Info Post" in the variable ESTABLISHED_RABS and the IE "Re-establishment timer" in the IE "RAB Info" in the variable ESTABLISHED_RABS to "useT314".
- 1> if IE "Specification mode" is set to "Preconfiguration":
 - 2> use the following values for parameters that are neither signalled within the HANDOVER TO UTRAN COMMAND message nor included within pre-defined or default configuration:
 - 3> 0 dB for the power offset $P_{\text{Pilot-DPCH}}$ bearer in FDD;
 - 3> calculate the Default DPCH Offset Value using the following formula:
 - 3> in FDD:

$$\text{Default DPCH Offset Value} = (\text{SRNTI 2 mod } 600) * 512$$
 - 3> in TDD:

Default DPCH Offset Value = (SRNTI 2 mod 7)

3> handle the above Default DPCH Offset Value as if an IE with that value was included in the message, as specified in subclause 8.6.6.21.

1> if IE "Specification mode" is set to "Complete specification":

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

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

1> set the IE "START" for each CN domain, in the IE "START list" in the HANDOVER TO UTRAN COMPLETE message equal to the START value for each CN domain stored in the USIM if the USIM is present, or as stored in the UE for each CN domain if the SIM is present;

NOTE: ~~Reception of new keys~~ Keys received while in another RAT shall not be regarded as 'new' (i.e. ~~does~~ not trigger the actions in subclause 8.1.12.3.1) in a subsequent security control procedure in UTRAN, irrespective of whether the keys are already being used in the other RAT or not. If the UE has received new keys in the other RAT before handover, then the START values in the USIM (sent in the HANDOVER TO UTRAN COMPLETE message and in the INTER_RAT_HANDOVER_INFO sent to the BSS while in the other RAT) will not reflect the receipt of these new keys. At a subsequent security mode control procedure in UTRA, UE activates ciphering and/or integrity protection using the key set stored in USIM/SIM.

1> set the value of "THRESHOLD" in the variable "START_THRESHOLD" equal to the 20 MSBs of the value stored in the USIM [50] for the maximum value of START for each CN Domain, or to the default value in [40] if the SIM is present;

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

2> for the CN domain included in the IE "CN domain identity" which is included in the IE "RAB info" of the IE "RAB information to setup", or the CS domain when these IEs are not present:

3> set the variable LATEST_CONFIGURED_CN_DOMAIN to the value indicated in the IE "CN domain identity", or to the CS domain when this IE is not present;

3> set the 20 MSB of the HFN component of the COUNT-C variable for all radio bearers using RLC-TM and all signalling radio bearers to the "START" value included in the IE "UE security information" in the variable "INTER_RAT_HANDOVER_INFO_TRANSFERRED";

3> set the remaining LSBs of the HFN component of COUNT-C for all radio bearers using RLC-TM and all signalling radio bearers to zero;

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

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

3> set the IE "Status" in the variable CIPHERING_STATUS to "Started";

3> apply the algorithm according to IE "Ciphering Algorithm" with the ciphering key set stored in the USIM/SIM ~~used while in the other radio access technology prior to handover~~ and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND.

NOTE: If ciphering has been activated and ongoing in the radio access technology from which inter RAT handover is performed, UTRAN should not include the IE "Ciphering mode info" in the SECURITY MODE COMMAND message that starts Integrity protection, and should not send a SECURITY MODE COMMAND including IE "Ciphering mode info" and IE "CN domain identity" set to the same value as UE variable LATEST_CONFIGURED_CN_DOMAIN until all pending ciphering activation times have been reached for the radio bearers using RLC-TM.

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

- 2> for the CN domain included in the IE "CN domain identity" which is included in the IE "RAB info" of the IE "RAB information to setup", or the CS domain when these IEs are not present:
- 3> set the IE "Status" in the variable CIPHERING_STATUS to "Not Started".

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

- 1> if the IE "Status" in the variable CIPHERING_STATUS of a CN domain is set to "Started" and transparent mode radio bearers have been established by this procedure for that CN domain:
 - 2> 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;
 - 2> include the IE "COUNT-C activation time" in the response message and specify a CFN value other than the default, "Now", that is a multiple of 8 frames (CFN mod 8 =0) and lies at least 200 frames ahead of the CFN in which the response message is first transmitted;
 - 2> at the CFN value as indicated in the response message in the IE "COUNT-C activation time" for radio bearers using RLC-TM:
 - 3> set the 20 MSB of the HFN component of the COUNT-C variable common for all transparent mode radio bearers of this CN domain to the START value as indicated in the IE "START list" of the response message for the relevant CN domain; and
 - 3> set the remaining LSBs of the HFN component of COUNT-C to zero;
 - 3> increment the HFN component of the COUNT-C variable by one even if the "COUNT-C activation time" is equal to zero;
 - 3> set the CFN component of the COUNT-C to the value of the IE "COUNT-C activation time" of the response message. The HFN component and the CFN component completely initialise the COUNT-C variable;
 - 3> step the COUNT-C variable, as normal, at each CFN value. The HFN component is no longer fixed in value but incremented at each CFN cycle.
- 1> if the IE "Status" in the variable CIPHERING_STATUS of a CN domain is set to "Not Started" and transparent mode radio bearers have been established by this procedure for that CN domain:
 - 2> initialise the 20 MSB of the HFN component of COUNT-C common for all transparent mode radio bearers of this CN domain with the START value as indicated in the IE "START list" of the response message for the relevant CN domain;
 - 2> set the remaining LSBs of the HFN component of COUNT-C to zero;
 - 2> do not increment the COUNT-C value common for all transparent mode radio bearers for this CN domain.
- 1> transmit a HANDOVER TO UTRAN COMPLETE message on the uplink DCCH, using, if ciphering has been started, the new ciphering configuration;
- 1> when the HANDOVER TO UTRAN COMPLETE message has been submitted to lower layers for transmission:
 - 2> enter UTRA RRC connected mode in state CELL_DCH;
 - 2> initialise variables upon entering UTRA RRC connected mode as specified in subclause 13.4;
 - 2> update the variable UE_CAPABILITY_TRANSFERRED with the UE capabilities stored in the variable INTER_RAT_HANDOVER_INFO_TRANSFERRED;
 - 2> for all radio bearers using RLC-AM or RLC-UM:
 - 3> set the 20 MSB of the HFN component of the uplink and downlink COUNT-C variable to the START value indicated in the IE "START list" of the response message for the relevant CN domain; and
 - 3> set the remaining LSBs of the HFN component of COUNT-C to zero;
 - 3> increment the HFN component of the COUNT-C variable by one;

3> start incrementing the COUNT-C values.

1> and the procedure ends.

TSG-RAN Working Group 2 meeting #37
Budapest, Hungary 25th-29th Aug 2003

R2-031857

CR-Form-v7

CHANGE REQUEST

⌘ **25.331 CR 1992** ⌘ rev ⌘ Current version: **4.10.0** ⌘

For [HELP](#) on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Handling of key sets at Inter-RAT Handover to UTRAN		
Source:	⌘ RAN WG2		
Work item code:	⌘ TEI	Date:	⌘ Aug 2003
Category:	⌘ A Use <u>one</u> 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 .	Release:	⌘ Rel-4 Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)

Reason for change: ⌘ 1. It is currently not clear that UE shall consider a key set as 'new' only in case UE receives the key set for the ongoing signalling connection while in UMTS. This clarification is needed in order to prevent the UE from assuming that a key set received in another RAT is 'new' at a subsequent reception of a SECURITY MODE CONTROL message (and initialise the HFNs to zero), instead of assuming that the key set is 'not new' (and initialise HFNs to the values send to UTRAN in HANDOVER TO UTRAN COMPLETE).

2. It is currently not clear what key set UE shall use after Inter-RAT handover to UTRAN, in case the key set stored on USIM/SIM is different from the key set currently in use for ciphering of the connection in the other RAT.

Summary of change: ⌘ Section 8.1.12.3.1:
It is clarified in a note that the actions in this section are performed only in case UE receives a new key set for the ongoing signalling connection while in UTRA.

Section 8.3.6.3:
It is clarified in a note that keys received while in another RAT shall not be regarded as 'new'.

It is added in a note that UE (after handover from another RAT) at a subsequent security mode control procedure, activates ciphering and/or integrity protection using the key set stored in USIM/SIM.

It is corrected that UE shall, after the Inter-RAT handover to UTRAN, use the ciphering key set stored in the USIM/SIM, not the key set that was in use prior to the handover.

T1 impact:

No impact on T1 specifications is foreseen

Backward compatibility:

Backwards compatible for a UE and UTRAN/CN that have assumed the indicated behaviour. In case either UE or UTRAN/CN are not complying with the correction, ciphering and/or integrity protection will fail after an Inter-RAT handover to UTRAN, in case the key set stored on USIM/SIM is different from the key set in use prior to the handover.

Consequences if not approved:

⌘ Ciphering and/or integrity protection might fail after an Inter-RAT handover to UTRAN, in case the key set stored on USIM/SIM is different from the key set in use prior to the handover.

Clauses affected:

⌘ 8.1.12.3.1, 8.3.6.3

Other specs affected:

Y	N		⌘
	X	Other core specifications	
	X	Test specifications	
	X	O&M Specifications	

Other comments:

⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/>. For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.1.12.3.1 New ciphering and integrity protection keys

NOTE: The actions in this subclause are to be performed only if the new keys were received for an ongoing signalling connection.

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

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

- 4> set the IE "Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the uplink COUNT-I to zero.
- 1> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
 - 2> for each signalling radio bearer and for each radio bearer for the CN domain indicated in the variable LATEST_CONFIGURED_CN_DOMAIN:
 - 3> if the IE "Status" in the variable CIPHERING_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers using RLC-TM:
 - 4> at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info":
 - 5> start using the new key in uplink and downlink;
 - 5> set the HFN component of the COUNT-C to zero.
 - 3> if the IE "Status" in the variable CIPHERING_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers and signalling radio bearers using RLC-AM and RLC-UM:
 - 4> in the downlink, at the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info":
 - 5> start using the new key;
 - 5> set the HFN component of the downlink COUNT-C to zero.
 - 4> in the uplink, at the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info":
 - 5> start using the new key;
 - 5> set the HFN component of the uplink COUNT-C to zero.
 - 1> consider the value of the latest transmitted START value to be zero.

8.3.6.3 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 may:

- 1> maintain a list of the set of cells to which the UE has Radio Links if the IE "Cell ID" is present.

The UE shall:

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

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

- 2> set the IE "RAB Info Post" in the variable ESTABLISHED_RABS and the IE "Re-establishment timer" in the IE "RAB Info" in the variable ESTABLISHED_RABS to "useT314".
- 1> if IE "Specification mode" is set to "Preconfiguration":
 - 2> use the following values for parameters that are neither signalled within the HANDOVER TO UTRAN COMMAND message nor included within pre-defined or default configuration:
 - 3> 0 dB for the power offset $P_{\text{Pilot-DPDCH}}$ bearer in FDD;
 - 3> calculate the Default DPCH Offset Value using the following formula:

3> in FDD:

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

3> in TDD:

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

3> handle the above Default DPCH Offset Value as if an IE with that value was included in the message, as specified in subclause 8.6.6.21.

1> if IE "Specification mode" is set to "Complete specification":

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

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

1> set the IE "START" for each CN domain, in the IE "START list" in the HANDOVER TO UTRAN COMPLETE message equal to the START value for each CN domain stored in the USIM if the USIM is present, or as stored in the UE for each CN domain if the SIM is present;

NOTE: Reception of new keys while in another RAT does not trigger the actions in subclause 8.1.12.3.1 in a subsequent security control procedure in UTRAN, irrespective of whether the keys are already being used in the other RAT or not. If the UE has received new keys in the other RAT before handover, then the START values in the USIM (sent in the HANDOVER TO UTRAN COMPLETE message and in the INTER_RAT_HANDOVER_INFO sent to the BSS while in the other RAT) will not reflect the receipt of these new keys.

1> set the value of "THRESHOLD" in the variable "START_THRESHOLD" to the 20 MSBs of the value stored in the USIM [50] for the maximum value of START for each CN Domain, or to the default value in [40] if the SIM is present;

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

2> for the CN domain included in the IE "CN domain identity" which is included in the IE "RAB info" of the IE "RAB information to setup", or the CS domain when these IEs are not present:

3> set the variable LATEST_CONFIGURED_CN_DOMAIN to the value indicated in the IE "CN domain identity", or to the CS domain when this IE is not present;

3> set the 20 MSB of the HFN component of the COUNT-C variable for all radio bearers using RLC-TM and all signalling radio bearers to the "START" value included in the IE "UE security information" in the variable "INTER_RAT_HANDOVER_INFO_TRANSFERRED";

3> set the remaining LSBs of the HFN component of COUNT-C for all radio bearers using RLC-TM and all signalling radio bearers to zero;

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

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

3> set the IE "Status" in the variable CIPHERING_STATUS to "Started";

3> apply the algorithm according to IE "Ciphering Algorithm" with the ciphering key set used while in the other radio access technology prior to handover and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND.

NOTE: If ciphering has been activated and ongoing in the radio access technology from which inter RAT handover is performed, UTRAN should not include the IE "Ciphering mode info" in the SECURITY MODE COMMAND message that starts Integrity protection, and should not send a SECURITY MODE COMMAND including IE "Ciphering mode info" and IE "CN domain identity" set to the same value as UE variable LATEST_CONFIGURED_CN_DOMAIN until all pending ciphering activation times have been reached for the radio bearers using RLC-TM.

- 1> if ciphering has not been activated and ongoing in the radio access technology from which inter-RAT handover is performed:
 - 2> for the CN domain included in the IE "CN domain identity" which is included in the IE "RAB info" of the IE "RAB information to setup", or the CS domain when these IEs are not present:
 - 3> set the IE "Status" in the variable CIPHERING_STATUS to "Not Started".

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

- 1> if the IE "Status" in the variable CIPHERING_STATUS of a CN domain is set to "Started" and transparent mode radio bearers have been established by this procedure for that CN domain:
 - 2> 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;
 - 2> include the IE "COUNT-C activation time" in the response message and specify a CFN value for this IE other than the default, "Now", that is a multiple of 8 frames (CFN mod 8 =0) and lies at least 200 frames ahead of the CFN in which the response message is first transmitted;
 - 2> at the CFN value as indicated in the response message in the IE "COUNT-C activation time" for radio bearers using RLC-TM:
 - 3> set the 20 MSB of the HFN component of the COUNT-C variable common for all transparent mode radio bearers of this CN domain to the START value as indicated in the IE "START list" of the response message for the relevant CN domain; and
 - 3> set the remaining LSBs of the HFN component of COUNT-C to zero;
 - 3> increment the HFN component of the COUNT-C variable by one even if the "COUNT-C activation time" is equal to zero;
 - 3> set the CFN component of the COUNT-C to the value of the IE "COUNT-C activation time" of the response message. The HFN component and the CFN component completely initialise the COUNT-C variable;
 - 3> step the COUNT-C variable, as normal, at each CFN value. The HFN component is no longer fixed in value but incremented at each CFN cycle.
- 1> if the IE "Status" in the variable CIPHERING_STATUS of a CN domain is set to "Not Started" and transparent mode radio bearers have been established by this procedure for that CN domain:
 - 2> initialise the 20 MSB of the HFN component of COUNT-C common for all transparent mode radio bearers of this CN domain with the START value as indicated in the IE "START list" of the response message for the relevant CN domain;
 - 2> set the remaining LSBs of the HFN component of COUNT-C to zero;
 - 2> do not increment the COUNT-C value common for all transparent mode radio bearers for this CN domain.
- 1> transmit a HANDOVER TO UTRAN COMPLETE message on the uplink DCCH, using, if ciphering has been started, the new ciphering configuration;
- 1> when the HANDOVER TO UTRAN COMPLETE message has been submitted to lower layers for transmission:
 - 2> enter UTRA RRC connected mode in state CELL_DCH;
 - 2> initialise variables upon entering UTRA RRC connected mode as specified in subclause 13.4;

- 2> update the variable UE_CAPABILITY_TRANSFERRED with the UE capabilities stored in the variable INTER_RAT_HANDOVER_INFO_TRANSFERRED;
- 2> for all radio bearers using RLC-AM or RLC-UM:
 - 3> set the 20 MSB of the HFN component of the uplink and downlink COUNT-C variable to the START value indicated in the IE "START list" of the response message for the relevant CN domain; and
 - 3> set the remaining LSBs of the HFN component of COUNT-C to zero;
 - 3> increment the HFN component of the COUNT-C variable by one;
 - 3> start incrementing the COUNT-C values.
- 1> and the procedure ends.

TSG-RAN Working Group 2 meeting #37
Budapest, Hungary 25th-29th Aug 2003

R2-031858

CR-Form-v7

CHANGE REQUEST

⌘ **25.331 CR 1993** ⌘ rev ⌘ Current version: **5.5.0** ⌘

For [HELP](#) on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Handling of key sets at Inter-RAT Handover to UTRAN		
Source:	⌘ RAN WG2		
Work item code:	⌘ TEI	Date:	⌘ Aug 2003
Category:	⌘ A Use <u>one</u> 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 .	Release:	⌘ Rel-5 Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)

Reason for change: ⌘ 1. It is currently not clear that UE shall consider a key set as 'new' only in case UE receives the key set for the ongoing signalling connection while in UMTS. This clarification is needed in order to prevent the UE from assuming that a key set received in another RAT is 'new' at a subsequent reception of a SECURITY MODE CONTROL message (and initialise the HFNs to zero), instead of assuming that the key set is 'not new' (and initialise HFNs to the values send to UTRAN in HANDOVER TO UTRAN COMPLETE).

2. It is currently not clear what key set UE shall use after Inter-RAT handover to UTRAN, in case the key set stored on USIM/SIM is different from the key set currently in use for ciphering of the connection in the other RAT.

Summary of change: ⌘ Section 8.1.12.3.1:
It is clarified in a note that the actions in this section are performed only in case UE receives a new key set for the ongoing signalling connection while in UTRA.

Section 8.3.6.3:
It is clarified in a note that keys received while in another RAT shall not be regarded as 'new'.

It is added in a note that UE (after handover from another RAT) at a subsequent security mode control procedure, activates ciphering and/or integrity protection using the key set stored in USIM/SIM.

It is corrected that UE shall, after the Inter-RAT handover to UTRAN, use the ciphering key set stored in the USIM/SIM, not the key set that was in use prior to the handover.

T1 impact:

<p>No impact on T1 specifications is foreseen</p> <p>Backward compatibility:</p> <p>Backwards compatible for a UE and UTRAN/CN that have assumed the indicated behaviour. In case either UE or UTRAN/CN are not complying with the correction, ciphering and/or integrity protection will fail after an Inter-RAT handover to UTRAN, in case the key set stored on USIM/SIM is different from the key set in use prior to the handover.</p>	
<p>Consequences if not approved:</p>	<p>⌘ Ciphering and/or integrity protection might fail after an Inter-RAT handover to UTRAN, in case the key set stored on USIM/SIM is different from the key set in use prior to the handover.</p>

<p>Clauses affected:</p>	<p>⌘ 8.1.12.3.1, 8.3.6.3</p>																
<p>Other specs affected:</p>	<table border="1"> <thead> <tr> <th>Y</th> <th>N</th> <th></th> <th>⌘</th> </tr> </thead> <tbody> <tr> <td></td> <td>X</td> <td>Other core specifications</td> <td></td> </tr> <tr> <td></td> <td>X</td> <td>Test specifications</td> <td></td> </tr> <tr> <td></td> <td>X</td> <td>O&M Specifications</td> <td></td> </tr> </tbody> </table>	Y	N		⌘		X	Other core specifications			X	Test specifications			X	O&M Specifications	
Y	N		⌘														
	X	Other core specifications															
	X	Test specifications															
	X	O&M Specifications															
<p>Other comments:</p>	<p>⌘</p>																

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.1.12.3.1 New ciphering and integrity protection keys

NOTE: The actions in this subclause are to be performed only if the new keys were received for an ongoing signalling connection [while in UTRA](#).

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

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

- 4> set the IE "Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the uplink COUNT-I to zero.
- 1> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":
 - 2> for each signalling radio bearer and for each radio bearer for the CN domain indicated in the variable LATEST_CONFIGURED_CN_DOMAIN:
 - 3> if the IE "Status" in the variable CIPHERING_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers using RLC-TM:
 - 4> at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info":
 - 5> start using the new key in uplink and downlink;
 - 5> set the HFN component of the COUNT-C to zero.
 - 3> if the IE "Status" in the variable CIPHERING_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers and signalling radio bearers using RLC-AM and RLC-UM:
 - 4> in the downlink, at the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info":
 - 5> start using the new key;
 - 5> set the HFN component of the downlink COUNT-C to zero.
 - 4> in the uplink, at the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info":
 - 5> start using the new key;
 - 5> set the HFN component of the uplink COUNT-C to zero.
 - 1> consider the value of the latest transmitted START value to be zero.

8.3.6.3 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 may:

- 1> maintain a list of the set of cells to which the UE has Radio Links if the IE "Cell ID" is present.

The UE shall:

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

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

- 2> set the IE "RAB Info Post" in the variable ESTABLISHED_RABS and the IE "Re-establishment timer" in the IE "RAB Info" in the variable ESTABLISHED_RABS to "useT314".
- 1> if IE "Specification mode" is set to "Preconfiguration":
 - 2> use the following values for parameters that are neither signalled within the HANDOVER TO UTRAN COMMAND message nor included within pre-defined or default configuration:
 - 3> 0 dB for the power offset $P_{\text{Pilot-DPDCH}}$ bearer in FDD;
 - 3> calculate the Default DPCH Offset Value using the following formula:

3> in FDD:

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

3> in TDD:

Default DPCH Offset Value = (SRNTI 2 mod 7)

3> handle the above Default DPCH Offset Value as if an IE with that value was included in the message, as specified in subclause 8.6.6.21.

1> if IE "Specification mode" is set to "Complete specification":

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

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

1> set the IE "START" for each CN domain, in the IE "START list" in the HANDOVER TO UTRAN COMPLETE message equal to the START value for each CN domain stored in the USIM if the USIM is present, or as stored in the UE for each CN domain if the SIM is present;

NOTE: ~~Reception of new keys~~ Keys received while in another RAT shall not be regarded as 'new' (i.e. ~~does~~ not trigger the actions in subclause 8.1.12.3.1) in a subsequent security control procedure in UTRAN, irrespective of whether the keys are already being used in the other RAT or not. If the UE has received new keys in the other RAT before handover, then the START values in the USIM (sent in the HANDOVER TO UTRAN COMPLETE message and in the INTER_RAT_HANDOVER_INFO sent to the BSS while in the other RAT) will not reflect the receipt of these new keys. At a subsequent security mode control procedure in UTRA, UE activates ciphering and/or integrity protection using the key set stored in USIM/SIM.

1> set the value of "THRESHOLD" in the variable "START_THRESHOLD" to the 20 MSBs of the value stored in the USIM [50] for the maximum value of START for each CN Domain, or to the default value in [40] if the SIM is present;

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

2> for the CN domain included in the IE "CN domain identity" which is included in the IE "RAB info" of the IE "RAB information to setup", or the CS domain when these IEs are not present:

3> set the variable LATEST_CONFIGURED_CN_DOMAIN to the value indicated in the IE "CN domain identity", or to the CS domain when this IE is not present;

3> set the 20 MSB of the HFN component of the COUNT-C variable for all radio bearers using RLC-TM and all signalling radio bearers to the "START" value included in the IE "UE security information" in the variable "INTER_RAT_HANDOVER_INFO_TRANSFERRED";

3> set the remaining LSBs of the HFN component of COUNT-C for all radio bearers using RLC-TM and all signalling radio bearers to zero;

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

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

3> set the IE "Status" in the variable CIPHERING_STATUS to "Started";

3> apply the algorithm according to IE "Ciphering Algorithm" with the ciphering key set stored in the USIM/SIM ~~used while in the other radio access technology prior to handover~~ and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND.

NOTE: If ciphering has been activated and ongoing in the radio access technology from which inter RAT handover is performed, UTRAN should not include the IE "Ciphering mode info" in the SECURITY MODE COMMAND message that starts Integrity protection, and should not send a SECURITY MODE COMMAND including IE "Ciphering mode info" and IE "CN domain identity" set to the same value as UE variable LATEST_CONFIGURED_CN_DOMAIN until all pending ciphering activation times have been reached for the radio bearers using RLC-TM.

- 1> if ciphering has not been activated and ongoing in the radio access technology from which inter-RAT handover is performed:
 - 2> for the CN domain included in the IE "CN domain identity" which is included in the IE "RAB info" of the IE "RAB information to setup", or the CS domain when these IEs are not present:
 - 3> set the IE "Status" in the variable CIPHERING_STATUS to "Not Started".

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

- 1> if the IE "Status" in the variable CIPHERING_STATUS of a CN domain is set to "Started" and transparent mode radio bearers have been established by this procedure for that CN domain:
 - 2> 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;
 - 2> include the IE "COUNT-C activation time" in the response message and specify a CFN value for this IE other than the default, "Now", that is a multiple of 8 frames (CFN mod 8 =0) and lies at least 200 frames ahead of the CFN in which the response message is first transmitted;
 - 2> at the CFN value as indicated in the response message in the IE "COUNT-C activation time" for radio bearers using RLC-TM:
 - 3> set the 20 MSB of the HFN component of the COUNT-C variable common for all transparent mode radio bearers of this CN domain to the START value as indicated in the IE "START list" of the response message for the relevant CN domain; and
 - 3> set the remaining LSBs of the HFN component of COUNT-C to zero;
 - 3> increment the HFN component of the COUNT-C variable by one even if the "COUNT-C activation time" is equal to zero;
 - 3> set the CFN component of the COUNT-C to the value of the IE "COUNT-C activation time" of the response message. The HFN component and the CFN component completely initialise the COUNT-C variable;
 - 3> step the COUNT-C variable, as normal, at each CFN value. The HFN component is no longer fixed in value but incremented at each CFN cycle.
- 1> if the IE "Status" in the variable CIPHERING_STATUS of a CN domain is set to "Not Started" and transparent mode radio bearers have been established by this procedure for that CN domain:
 - 2> initialise the 20 MSB of the HFN component of COUNT-C common for all transparent mode radio bearers of this CN domain with the START value as indicated in the IE "START list" of the response message for the relevant CN domain;
 - 2> set the remaining LSBs of the HFN component of COUNT-C to zero;
 - 2> do not increment the COUNT-C value common for all transparent mode radio bearers for this CN domain.
- 1> transmit a HANDOVER TO UTRAN COMPLETE message on the uplink DCCH, using, if ciphering has been started, the new ciphering configuration;
- 1> when the HANDOVER TO UTRAN COMPLETE message has been submitted to lower layers for transmission:
 - 2> enter UTRA RRC connected mode in state CELL_DCH;
 - 2> initialise variables upon entering UTRA RRC connected mode as specified in subclause 13.4;

- 2> update the variable UE_CAPABILITY_TRANSFERRED with the UE capabilities stored in the variable INTER_RAT_HANDOVER_INFO_TRANSFERRED;
- 2> for all radio bearers using RLC-AM or RLC-UM:
 - 3> set the 20 MSB of the HFN component of the uplink and downlink COUNT-C variable to the START value indicated in the IE "START list" of the response message for the relevant CN domain; and
 - 3> set the remaining LSBs of the HFN component of COUNT-C to zero;
 - 3> increment the HFN component of the COUNT-C variable by one;
 - 3> start incrementing the COUNT-C values.
- 1> and the procedure ends.

CHANGE REQUEST

25.331 CR 1994 # rev - # Current version: **3.15.0**

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

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# Correction to UE Positioning privacy procedures.		
Source:	# RAN WG2		
Work item code:	# TEI	Date:	# 07/07/2003
Category:	# F	Release:	# R99
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)		2 (GSM Phase 2)
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)
	B (addition of feature),		R97 (Release 1997)
	C (functional modification of feature)		R98 (Release 1998)
	D (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	# In 2 places the RRC specification indicates that a UE only performs UP measurements if permitted to do so by upper layers. The specification also defines errors cause values to return to the UTRAN in the case that the upper layers do not permit the UE to perform the measurements. This behaviour is not aligned with the privacy procedures described in the location services stage 2 in 23.171. The privacy procedures allow the user to reject a position request from an external party or application. The procedures use NAS signalling and following this signalling it is the responsibility of the core network to ensure that position information is provided only to authorised parties or applications. The RRC UP procedures have no part to play in the privacy process and the UE has no knowledge about why UP measurements are being requested by UTRAN. Therefore, the UE should never refuse to perform UP measurements based on indications from upper layers.
Summary of change:	# The incorrect sentences saying that the UE only performs UP measurements if permitted to do so by upper layers are deleted. It is stated that the UE shall never set the error cause values relating to upper layers denying the measurements. The actual cause values are left in the tabular and ASN.1 in order to avoid making any change to the ASN.1. Isolated Impact Analysis Functionality corrected: UE Positioning - all methods Isolated impact statement: Correction to a function where specification was containing a contradiction with the stage 2. Would not affect implementations

	behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.																		
Consequences if not approved:	⌘	If the CR is not approved then some UE implementations may not perform UE positioning measurements in some situations. The worst case situation would be if the UE refused to perform UP measurements when the network is actually requested the measurements due to an emergency call.																	
Clauses affected:	⌘	8.6.7.19.1a, 8.6.7.19.1b, 8.6.7.19.5																	
Other specs affected:	<table border="1"> <tr> <td>Y</td> <td>N</td> </tr> <tr> <td>X</td> <td></td> </tr> <tr> <td></td> <td>X</td> </tr> <tr> <td></td> <td>X</td> </tr> </table>	Y	N	X			X		X	<table> <tr> <td>Other core specifications</td> <td>⌘</td> <td>25.305 CR 090</td> </tr> <tr> <td>Test specifications</td> <td></td> <td></td> </tr> <tr> <td>O&M Specifications</td> <td></td> <td></td> </tr> </table>	Other core specifications	⌘	25.305 CR 090	Test specifications			O&M Specifications		
Y	N																		
X																			
	X																		
	X																		
Other core specifications	⌘	25.305 CR 090																	
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/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.6.7.19.1a UE positioning reporting for UE assisted methods

The UE shall:

- 1> when a measurement report is triggered;~~;-and~~
~~1> if higher layers indicated that the positioning request is permitted;~~
- 2> if the UE was able to perform measurements on at least one neighbour cell included in the variable UE_POSITIONING_OTDOA_DATA_UE_ASSISTED in case of OTDOA or one satellite included in the variable UE_POSITIONING_GPS_DATA in case of GPS positioning:
 - 3> if the IE "Vertical Accuracy" is included:
 - 4> interpret the presence of this IE to indicate that the UTRAN desires to compute a 3-dimensional position estimate.
 - 3> if the IE "Positioning Methods" is set to "GPS":
 - 4> include the IE "UE positioning GPS measured results" in the measurement report and set the contents of the IE as follows:
 - 5> if the UE supports the capability to provide the GPS timing of the cell frames measurement:
 - 6> if the IE "GPS timing of Cell wanted" is set to TRUE:
 - 7> perform the UE GPS timing of cell frames measurement on the serving cell or on one cell of the active set.
 - 7> include the IE "Primary CPICH Info" for FDD or the IE "cell parameters id" for TDD; and
 - 7> include the IE "Reference SFN" and the IE "UE GPS timing of cell frames".
 - 6> if the UE does not support the capability to provide the GPS timing of the cell; or
 - 6> if the IE "GPS timing of Cell wanted" is set to FALSE:
 - 7> include the IE "GPS TOW msec".
 - 3> if the IE "Positioning Methods" is set to "OTDOA":
 - 4> include the IE "UE positioning OTDOA measured results" in the measurement report and set the contents of the IE as follows:
 - 5> set IE "SFN" to the SFN when the last measurement was performed;
 - 5> if the UE supports the capability to perform the Rx-Tx time difference type 2 measurement:
 - 6> if the UE is in CELL_DCH state:
 - 7> if the measured value is equal to "1279.9375":
 - 8> set the IE "Rx-Tx time difference type 2" in IE "UE positioning OTDOA measured results" for the reference cell to "1279.8750".
 - 7> otherwise:
 - 8> set the IE "Rx-Tx time difference type 2" in IE "UE positioning OTDOA measured results" for the reference cell to the measured value.
 - 7> include the IE group "Rx-Tx time difference type 2 info" for the reference cell and for each neighbour cell listed in variable UE_POSITIONING_OTDOA_DATA_UE_ASSISTED that belongs to the active set.
 - 5> if the UE does not support the capability to perform the Rx-Tx time difference type 2 measurement:

- 6> set the IE "Rx-Tx time difference type 2" in IE "UE positioning OTDOA measured results" for the reference cell to value "1279.9375" to indicate that the measurement is not supported.
- 4> include IE group "Neighbour" for all neighbour cells listed in variable UE_POSITIONING_OTDOA_DATA_UE_ASSISTED on which the SFN-SFN observed time difference type 2 measurement could be performed.
- 3> if IE "Positioning Methods" in the MEASUREMENT CONTROL message has been assigned to value "OTDOA or GPS":
 - 4> the UE may choose to either act as if IE "Positioning Methods" is set to "GPS" or "OTDOA" depending on the method chosen by the UE.
- 3> if the IE "Positioning Methods" is set to "CELL ID":
 - 4> if the UE supports the capability to perform the Rx-Tx time difference type 2 measurement; and
 - 4> if the UE is in CELL_DCH state:
 - 5> perform the Rx-Tx time difference type 2 measurement on the cells in the active set; and
 - 5> report the measurement results back to the network in the MEASUREMENT REPORT by using IE "UE positioning OTDOA measured results" including measurements on the cells in the active set; and
 - 5> report Rx-Tx time difference type 2 measurement of the reference cell (as designated by the UE); and
 - 5> for all reported neighbour cells:
 - 6> report Rx-Tx time difference type 2 measurement; and
 - 6> set the IE "SFN-SFN observed time difference type 2" and all IEs within the corresponding IE "UE positioning OTDOA quality" in IE "UE positioning OTDOA measured results" to value "0".
- 1> if the UE is not able to report the requested measurement results;~~;-or~~
 - ~~1> if higher layers have indicated that the positioning request is not permitted;-or~~
 - ~~1> if the positioning request was not processed by higher layers and timed out;~~
- 2> include IE "UE positioning error" in the MEASUREMENT REPORT and set the contents of this IE as specified in subclause 8.6.7.19.5.

8.6.7.19.1b UE positioning reporting for UE based methods

The UE shall:

- 1> when a measurement report is triggered;~~;-and~~
 - ~~1> if higher layers indicated that the positioning request is permitted;~~
- 2> if the UE has been able to calculate a position after performing measurements on the cells included in the variable UE_POSITIONING_OTDOA_DATA_UE_BASED in case of OTDOA or on the list of satellites included in the variable UE_POSITIONING_GPS_DATA in case of GPS positioning;
- 3> include IE "UE positioning Position Estimate Info" in the MEASUREMENT REPORT and set the contents of the IE as follows:
 - 4> if the UE supports the capability to perform the UE GPS timing of cell frames measurement and UTRAN has requested to report the GPS timing of cell frames:
 - 5> perform the UE GPS timing of cell frames measurement on the serving cell or on one cell of the active set.

- 5> include the IE "Primary CPICH Info" for FDD or the IE "cell parameters id" for TDD;
- 5> include the SFN when the position was determined;
- 5> include the IE "UE GPS timing of cell frames".
- 4> if the UE does not support the capability to perform the UE GPS timing of cell frames measurement;
or
- 4> if the IE "GPS timing of Cell wanted" is set to FALSE:
 - 5> include the IE "GPS TOW msec".
- 4> if IE "Vertical Accuracy" has been included in IE "UE positioning reporting quantity":
 - 5> if the IE "Vertical Accuracy" has been assigned to value "0":
 - 6> if the IE "Horizontal Accuracy" has been assigned a value "0":
 - 7> may include IE "Ellipsoid point with altitude".
 - 6> if the IE "Horizontal Accuracy" has been assigned a value unequal to "0"; and
 - 6> if the UE has been able to calculate a 3-dimensional position
 - 7> include IE "Ellipsoid point with altitude" or IE "Ellipsoid point with altitude and uncertainty ellipsoid" as the position estimate.
 - 6> if the UE has not been able to calculate a 3-dimensional position:
 - 7> may act as if IE "Vertical Accuracy" was not included in IE "UE positioning reporting quantity".
 - 5> if the IE "Vertical Accuracy" has been assigned to a value unequal to "0":
 - 6> if the UE has been able to calculate a 3-dimensional position:
 - 7> include IE "Ellipsoid point with altitude and uncertainty ellipsoid" as the position estimate.
 - 6> if the UE has not been able to calculate a 3-dimensional position:
 - 7> act as if IE "Vertical Accuracy" has not been included in IE "UE positioning reporting quantity".
- 4> if IE "Vertical Accuracy" has not been included in IE "UE positioning reporting quantity":
 - 5> if IE "Horizontal Accuracy" in IE "UE positioning reporting quantity" has been assigned to value "0":
 - 6> may include IE "Ellipsoid point".
 - 5> if IE "Horizontal Accuracy" in IE "UE positioning reporting quantity" has been assigned to a value unequal to 0:
 - 6> include either IE "Ellipsoid point with uncertainty circle" or IE "Ellipsoid point with uncertainty ellipse" or IE "Ellipsoid point with altitude and uncertainty ellipsoid" as the position estimate.
- 1> if the UE was not able to calculate a position;~~;- or~~
- ~~1> if higher layers have indicated that the positioning request is not permitted; or~~
- ~~2> if the positioning request was not processed by higher layers and timed out;~~
- 23> include IE "UE positioning error" in the MEASUREMENT REPORT and set the contents of this IE as specified in subclause 8.6.7.19.5.

8.6.7.19.5 UE positioning Error

The UE shall set the contents of the IE "UE positioning Error" as follows:

- 1> if the IE "Positioning Methods" in IE "UE positioning reporting quantity" has been assigned to value "OTDOA" and no neighbour cells could be received,
 - 2> set IE "Error reason" to "Not Enough OTDOA Cells";
- 1> if the IE "Positioning Methods" in IE "UE positioning reporting quantity" has been assigned to value "GPS":
 - 2> if there were not enough GPS satellites to be received:
 - 3> set IE "Error reason" to "Not Enough GPS Satellites".
 - 2> if some GPS assistance data was missing:
 - 3> set IE "Error reason" to "Assistance Data Missing"; and
 - 3> if the IE ""Additional Assistance Data Request" included in the IE "UE positioning reporting quantity" stored in the variable MEASUREMENT_IDENTITY is set to TRUE:
 - 4> include the IE GPS Additional Assistance Data Request".
 - 2> if the UE was not able to read the SFN of the reference cell included in the IE "UE positioning GPS reference time" or in the IE "UE positioning acquisition assistance":
 - 3> set IE "Error reason" to "Reference Cell Not Serving Cell".
 - 2> if the UE was not able to measure the requested GPS timing of cell frames measurement:
 - 3> set IE "Error reason" to "Not Accomplished GPS Timing Of Cell Frames".

~~1> if higher layers have indicated that the positioning request is not permitted:~~

 - ~~2> set IE "Error reason" to "Request Denied By User".~~

~~1> if the positioning request was not processed by higher layers and timed out:~~

 - ~~2> set IE "Error reason" to "Not Processed And Timeout".~~
 - 1> if none of the conditions above are fulfilled:
 - 2> set IE "Error reason" to "Undefined Error".

1> the UE shall not set the IE "Error reason" to "Request Denied By User" or "Not Processed and Timeout".

10.3.7.87 UE positioning Error

Information Element/Group name	Need	Multi	Type and Reference	Semantics description
Error reason	MP		Enumerated(Not Enough OTDOA Cells, Not Enough GPS Satellites, Assistance Data Missing, Not Accomplished GPS Timing Of Cell Frames, Undefined Error, Request Denied By User, Not Processed And Timeout, Reference Cell Not Serving Cell)	Note 1
GPS Additional Assistance Data Request	CV- <i>GPSdataMissing</i>		UE positioning GPS Additional Assistance Data Request 10.3.7.88a	

NOTE 1: The following table describes each value of the IE "Error reason".

Value	Indication
Not Enough OTDOA Cells	There were not enough cells to be received.
Not Enough GPS Satellites	There were not enough GPS satellites to be received.
Assistance Data Missing	UE positioning GPS assistance data missing.
Not Accomplished GPS Timing Of Cell Frames	UE was not able to accomplish the GPS timing of cell frames measurement.
Undefined Error	Undefined error.
Request Denied By User	UE positioning request denied by upper layers.
Not Processed And Timeout	UE positioning request not processed by upper layers and timeout.
Reference Cell Not Serving Cell	UE was not able to read the SFN of the reference cell.

Condition	Explanation
<i>GPSdataMissing</i>	The IE is optional if the IE "Error reason" is "ER3" and not needed otherwise.

11.3 Information element definitions

```
UE-Positioning-ErrorCause ::=
    ENUMERATED {
        notEnoughOTDOA-Cells,
        notEnoughGPS-Satellites,
        assistanceDataMissing,
        notAccomplishedGPS-TimingOfCellFrames,
        undefinedError,
        requestDeniedByUser,
        notProcessedAndTimeout,
        referenceCellNotServingCell }

```

CHANGE REQUEST

25.331 CR 1995 # rev - # Current version: 4.10.0

For [HELP](#) on using this form, see bottom of this page or look at the pop-up text over the # symbols.

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# Correction to UE Positioning privacy procedures.
Source:	# RAN WG2
Work item code:	# TEI Date: # 07/07/2003
Category:	# A Release: # Rel-4
<p>Use <u>one</u> of the following categories:</p> <p>F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p>	
<p>Use <u>one</u> of the following releases:</p> <p>2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)</p>	

Reason for change: #	<p>In 2 places the RRC specification indicates that a UE only performs UP measurements if permitted to do so by upper layers. The specification also defines errors cause values to return to the UTRAN in the case that the upper layers do not permit the UE to perform the measurements. This behaviour is not aligned with the privacy procedures described in the location services stage 2 in 23.171.</p> <p>The privacy procedures allow the user to reject a position request from an external party or application. The procedures use NAS signalling and following this signalling it is the responsibility of the core network to ensure that position information is provided only to authorised parties or applications. The RRC UP procedures have no part to play in the privacy process and the UE has no knowledge about why UP measurements are being requested by UTRAN. Therefore, the UE should never refuse to perform UP measurements based on indications from upper layers.</p>
Summary of change: #	<p>The incorrect sentences saying that the UE only performs UP measurements if permitted to do so by upper layers are deleted.</p> <p>It is stated that the UE shall never set the error cause values relating to upper layers denying the measurements. The actual cause values are left in the tabular and ASN.1 in order to avoid making any change to the ASN.1.</p> <p>Isolated Impact Analysis Functionality corrected: UE Positioning - all methods</p> <p>Isolated impact statement: Correction to a function where specification was containing a contradiction with the stage 2. Would not affect implementations</p>

	behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.																		
Consequences if not approved:	⌘	If the CR is not approved then some UE implementations may not perform UE positioning measurements in some situations. The worst case situation would be if the UE refused to perform UP measurements when the network is actually requested the measurements due to an emergency call.																	
Clauses affected:	⌘	8.6.7.19.1a, 8.6.7.19.1b, 8.6.7.19.5																	
Other specs affected:	<table border="1"> <tr> <td>Y</td> <td>N</td> </tr> <tr> <td>X</td> <td></td> </tr> <tr> <td></td> <td>X</td> </tr> <tr> <td></td> <td>X</td> </tr> </table>	Y	N	X			X		X	<table> <tr> <td>Other core specifications</td> <td>⌘</td> <td>25.305 CR 091</td> </tr> <tr> <td>Test specifications</td> <td></td> <td></td> </tr> <tr> <td>O&M Specifications</td> <td></td> <td></td> </tr> </table>	Other core specifications	⌘	25.305 CR 091	Test specifications			O&M Specifications		
Y	N																		
X																			
	X																		
	X																		
Other core specifications	⌘	25.305 CR 091																	
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/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.6.7.19.1a UE positioning reporting for UE assisted methods

The UE shall:

1> when a measurement report is triggered;~~and~~

~~1> if higher layers indicated that the positioning request is permitted;~~

2> if the UE was able to perform measurements on at least one neighbour cell included in the variable UE_POSITIONING_OTDOA_DATA_UE_ASSISTED in case of OTDOA or one satellite included in the variable UE_POSITIONING_GPS_DATA in case of GPS positioning:

3> if the IE "Vertical Accuracy" is included:

4> interpret the presence of this IE to indicate that the UTRAN desires to compute a 3-dimensional position estimate.

3> if the IE "Positioning Methods" is set to "GPS":

4> include the IE "UE positioning GPS measured results" in the measurement report and set the contents of the IE as follows:

5> if the UE supports the capability to provide the GPS timing of the cell frames measurement:

6> if the IE "GPS timing of Cell wanted" is set to TRUE:

7> perform the UE GPS timing of cell frames measurement on the serving cell or on one cell of the active set.

7> include the IE "Primary CPICH Info" for FDD or the IE "cell parameters id" for TDD; and

7> include the IE "Reference SFN" and the IE "UE GPS timing of cell frames".

6> if the UE does not support the capability to provide the GPS timing of the cell; or

6> if the IE "GPS timing of Cell wanted" is set to FALSE:

7> include the IE "GPS TOW msec".

3> if the IE "Positioning Methods" is set to "OTDOA":

4> include the IE "UE positioning OTDOA measured results" in the measurement report and set the contents of the IE as follows:

5> set IE "SFN" to the SFN when the last measurement was performed;

5> if the UE supports the capability to perform the Rx-Tx time difference type 2 measurement:

6> if the UE is in CELL_DCH state:

7> if the measured value is equal to "1279.9375":

8> set the IE "Rx-Tx time difference type 2" in IE "UE positioning OTDOA measured results" for the reference cell to "1279.8750".

7> otherwise:

8> set the IE "Rx-Tx time difference type 2" in IE "UE positioning OTDOA measured results" for the reference cell to the measured value.

7> include the IE group "Rx-Tx time difference type 2 info" for the reference cell and for each neighbour cell listed in variable UE_POSITIONING_OTDOA_DATA_UE_ASSISTED that belongs to the active set.

5> if the UE does not support the capability to perform the Rx-Tx time difference type 2 measurement:

- 6> set the IE "Rx-Tx time difference type 2" in IE "UE positioning OTDOA measured results" for the reference cell to value "1279.9375" to indicate that the measurement is not supported.
- 4> include IE group "Neighbour" for all neighbour cells listed in variable UE_POSITIONING_OTDOA_DATA_UE_ASSISTED on which the SFN-SFN observed time difference type 2 measurement could be performed.
- 3> if IE "Positioning Methods" in the MEASUREMENT CONTROL message has been assigned to value "OTDOA or GPS":
 - 4> the UE may choose to either act as if IE "Positioning Methods" is set to "GPS" or "OTDOA" depending on the method chosen by the UE.
- 3> if the IE "Positioning Methods" is set to "CELL ID":
 - 4> if the UE supports the capability to perform the Rx-Tx time difference type 2 measurement; and
 - 4> if the UE is in CELL_DCH state:
 - 5> perform the Rx-Tx time difference type 2 measurement on the cells in the active set; and
 - 5> report the measurement results back to the network in the MEASUREMENT REPORT by using IE "UE positioning OTDOA measured results" including measurements on the cells in the active set; and
 - 5> report Rx-Tx time difference type 2 measurement of the reference cell (as designated by the UE); and
 - 5> for all reported neighbour cells:
 - 6> report Rx-Tx time difference type 2 measurement; and
 - 6> set the IE "SFN-SFN observed time difference type 2" and all IEs within the corresponding IE "UE positioning OTDOA quality" in IE "UE positioning OTDOA measured results" to value "0".
- 1> if the UE is not able to report the requested measurement results;~~;-or~~
 - ~~1> if higher layers have indicated that the positioning request is not permitted;-or~~
 - ~~1> if the positioning request was not processed by higher layers and timed out;~~
- 2> include IE "UE positioning error" in the MEASUREMENT REPORT and set the contents of this IE as specified in subclause 8.6.7.19.5.

8.6.7.19.1b UE positioning reporting for UE based methods

The UE shall:

- 1> when a measurement report is triggered;~~;-and~~
 - ~~1> if higher layers indicated that the positioning request is permitted;~~
- 2> if the UE has been able to calculate a position after performing measurements on the cells included in the variable UE_POSITIONING_OTDOA_DATA_UE_BASED in case of OTDOA or on the list of satellites included in the variable UE_POSITIONING_GPS_DATA in case of GPS positioning;
- 3> include IE "UE positioning Position Estimate Info" in the MEASUREMENT REPORT and set the contents of the IE as follows:
 - 4> if the UE supports the capability to perform the UE GPS timing of cell frames measurement and UTRAN has requested to report the GPS timing of cell frames:
 - 5> perform the UE GPS timing of cell frames measurement on the serving cell or on one cell of the active set.

- 5> include the IE "Primary CPICH Info" for FDD or the IE "cell parameters id" for TDD;
- 5> include the SFN when the position was determined;
- 5> include the IE "UE GPS timing of cell frames".
- 4> if the UE does not support the capability to perform the UE GPS timing of cell frames measurement;
or
- 4> if the IE "GPS timing of Cell wanted" is set to FALSE:
 - 5> include the IE "GPS TOW msec".
- 4> if IE "Vertical Accuracy" has been included in IE "UE positioning reporting quantity":
 - 5> if the IE "Vertical Accuracy" has been assigned to value "0":
 - 6> if the IE "Horizontal Accuracy" has been assigned a value "0":
 - 7> may include IE "Ellipsoid point with altitude".
 - 6> if the IE "Horizontal Accuracy" has been assigned a value unequal to "0"; and
 - 6> if the UE has been able to calculate a 3-dimensional position
 - 7> include IE "Ellipsoid point with altitude" or IE "Ellipsoid point with altitude and uncertainty ellipsoid" as the position estimate.
 - 6> if the UE has not been able to calculate a 3-dimensional position:
 - 7> may act as if IE "Vertical Accuracy" was not included in IE "UE positioning reporting quantity".
 - 5> if the IE "Vertical Accuracy" has been assigned to a value unequal to "0":
 - 6> if the UE has been able to calculate a 3-dimensional position:
 - 7> include IE "Ellipsoid point with altitude and uncertainty ellipsoid" as the position estimate.
 - 6> if the UE has not been able to calculate a 3-dimensional position:
 - 7> act as if IE "Vertical Accuracy" has not been included in IE "UE positioning reporting quantity".
- 4> if IE "Vertical Accuracy" has not been included in IE "UE positioning reporting quantity":
 - 5> if IE "Horizontal Accuracy" in IE "UE positioning reporting quantity" has been assigned to value "0":
 - 6> may include IE "Ellipsoid point".
 - 5> if IE "Horizontal Accuracy" in IE "UE positioning reporting quantity" has been assigned to a value unequal to 0:
 - 6> include either IE "Ellipsoid point with uncertainty circle" or IE "Ellipsoid point with uncertainty ellipse" or IE "Ellipsoid point with altitude and uncertainty ellipsoid" as the position estimate.
- 1> if the UE was not able to calculate a position;~~;- or~~
- ~~1> if higher layers have indicated that the positioning request is not permitted; or~~
- ~~2> if the positioning request was not processed by higher layers and timed out;~~
- 23> include IE "UE positioning error" in the MEASUREMENT REPORT and set the contents of this IE as specified in subclause 8.6.7.19.5.

8.6.7.19.5 UE positioning Error

The UE shall set the contents of the IE "UE positioning Error" as follows:

- 1> if the IE "Positioning Methods" in IE "UE positioning reporting quantity" has been assigned to value "OTDOA" and no neighbour cells could be received,
 - 2> set IE "Error reason" to "Not Enough OTDOA Cells";
- 1> if the IE "Positioning Methods" in IE "UE positioning reporting quantity" has been assigned to value "GPS":
 - 2> if there were not enough GPS satellites to be received:
 - 3> set IE "Error reason" to "Not Enough GPS Satellites".
 - 2> if some GPS assistance data was missing:
 - 3> set IE "Error reason" to "Assistance Data Missing"; and
 - 3> if the IE "Additional Assistance Data Request" included in the IE "UE positioning reporting quantity" stored in the variable MEASUREMENT_IDENTITY is set to TRUE:
 - 4> include the IE GPS Additional Assistance Data Request".
 - 2> if the UE was not able to read the SFN of the reference cell included in the IE "UE positioning GPS reference time" or in the IE "UE positioning acquisition assistance":
 - 3> set IE "Error reason" to "Reference Cell Not Serving Cell".
 - 2> if the UE was not able to measure the requested GPS timing of cell frames measurement:
 - 3> set IE "Error reason" to "Not Accomplished GPS Timing Of Cell Frames".
 - ~~1> if higher layers have indicated that the positioning request is not permitted:
 - 2> set IE "Error reason" to "Request Denied By User".~~
 - ~~1> if the positioning request was not processed by higher layers and timed out:
 - 2> set IE "Error reason" to "Not Processed And Timeout".~~
 - 1> if none of the conditions above are fulfilled:
 - 2> set IE "Error reason" to "Undefined Error".

1> the UE shall not set the IE "Error reason" to "Request Denied By User" or "Not Processed and Timeout".

10.3.7.87 UE positioning Error

Information Element/Group name	Need	Multi	Type and Reference	Semantics description
Error reason	MP		Enumerated(Not Enough OTDOA Cells, Not Enough GPS Satellites, Assistance Data Missing, Not Accomplished GPS Timing Of Cell Frames, Undefined Error, Request Denied By User, Not Processed And Timeout, Reference Cell Not Serving Cell)	Note 1
GPS Additional Assistance Data Request	CV- <i>GPSdataMissing</i>		UE positioning GPS Additional Assistance Data Request 10.3.7.88a	

NOTE 1: The following table describes each value of the IE "Error reason".

Value	Indication
Not Enough OTDOA Cells	There were not enough cells to be received.
Not Enough GPS Satellites	There were not enough GPS satellites to be received.
Assistance Data Missing	UE positioning GPS assistance data missing.
Not Accomplished GPS Timing Of Cell Frames	UE was not able to accomplish the GPS timing of cell frames measurement.
Undefined Error	Undefined error.
Request Denied By User	UE positioning request denied by upper layers.
Not Processed And Timeout	UE positioning request not processed by upper layers and timeout.
Reference Cell Not Serving Cell	UE was not able to read the SFN of the reference cell.

Condition	Explanation
<i>GPSdataMissing</i>	The IE is optional if the IE "Error reason" is "ER3" and not needed otherwise.

11.3 Information element definitions

```
UE-Positioning-ErrorCause ::=
    ENUMERATED {
        notEnoughOTDOA-Cells,
        notEnoughGPS-Satellites,
        assistanceDataMissing,
        notAccomplishedGPS-TimingOfCellFrames,
        undefinedError,
        requestDeniedByUser,
        notProcessedAndTimeout,
        referenceCellNotServingCell }

```

CHANGE REQUEST

25.331 CR 1996 # rev - # Current version: 5.5.0

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

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# Correction to UE Positioning privacy procedures.
Source:	# RAN WG2
Work item code:	# TEI Date: # 07/07/2003
Category:	# A Release: # Rel-5
<p>Use <u>one</u> of the following categories:</p> <p>F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p>	
<p>Use <u>one</u> of the following releases:</p> <p>2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)</p>	

Reason for change:	# In 2 places the RRC specification indicates that a UE only performs UP measurements if permitted to do so by upper layers. The specification also defines errors cause values to return to the UTRAN in the case that the upper layers do not permit the UE to perform the measurements. This behaviour is not aligned with the privacy procedures described in the location services stage 2 in 23.171.
	The privacy procedures allow the user to reject a position request from an external party or application. The procedures use NAS signalling and following this signalling it is the responsibility of the core network to ensure that position information is provided only to authorised parties or applications. The RRC UP procedures have no part to play in the privacy process and the UE has no knowledge about why UP measurements are being requested by UTRAN. Therefore, the UE should never refuse to perform UP measurements based on indications from upper layers.
Summary of change:	# The incorrect sentences saying that the UE only performs UP measurements if permitted to do so by upper layers are deleted.
	It is stated that the UE shall never set the error cause values relating to upper layers denying the measurements. The actual cause values are left in the tabular and ASN.1 in order to avoid making any change to the ASN.1.
	Isolated Impact Analysis Functionality corrected: UE Positioning - all methods
	Isolated impact statement: Correction to a function where specification was containing a contradiction with the stage 2. Would not affect implementations

	behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.																		
Consequences if not approved:	⌘	If the CR is not approved then some UE implementations may not perform UE positioning measurements in some situations. The worst case situation would be if the UE refused to perform UP measurements when the network is actually requested the measurements due to an emergency call.																	
Clauses affected:	⌘	8.6.7.19.1a, 8.6.7.19.1b, 8.6.7.19.5																	
Other specs affected:	<table border="1"> <tr> <td>Y</td> <td>N</td> </tr> <tr> <td>X</td> <td></td> </tr> <tr> <td></td> <td>X</td> </tr> <tr> <td></td> <td>X</td> </tr> </table>	Y	N	X			X		X	<table> <tr> <td>Other core specifications</td> <td>⌘</td> <td>25.305 CR 092</td> </tr> <tr> <td>Test specifications</td> <td></td> <td></td> </tr> <tr> <td>O&M Specifications</td> <td></td> <td></td> </tr> </table>	Other core specifications	⌘	25.305 CR 092	Test specifications			O&M Specifications		
Y	N																		
X																			
	X																		
	X																		
Other core specifications	⌘	25.305 CR 092																	
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/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.6.7.19.1a UE positioning reporting for UE assisted methods

The UE shall:

- 1> when a measurement report is triggered;~~and~~
~~1> if higher layers indicated that the positioning request is permitted;~~
- 2> if the UE was able to perform measurements on at least one neighbour cell included in the variable UE_POSITIONING_OTDOA_DATA_UE_ASSISTED in case of OTDOA or one satellite included in the variable UE_POSITIONING_GPS_DATA in case of GPS positioning:
 - 3> if the IE "Vertical Accuracy" is included:
 - 4> interpret the presence of this IE to indicate that the UTRAN desires to compute a 3-dimensional position estimate.
 - 3> if the IE "Positioning Methods" is set to "GPS":
 - 4> include the IE "UE positioning GPS measured results" in the measurement report and set the contents of the IE as follows:
 - 5> if the UE supports the capability to provide the GPS timing of the cell frames measurement:
 - 6> if the IE "GPS timing of Cell wanted" is set to TRUE:
 - 7> perform the UE GPS timing of cell frames measurement on the serving cell or on one cell of the active set.
 - 7> include the IE "Primary CPICH Info" for FDD or the IE "cell parameters id" for TDD; and
 - 7> include the IE "Reference SFN" and the IE "UE GPS timing of cell frames".
 - 6> if the UE does not support the capability to provide the GPS timing of the cell; or
 - 6> if the IE "GPS timing of Cell wanted" is set to FALSE:
 - 7> include the IE "GPS TOW msec".
 - 3> if the IE "Positioning Methods" is set to "OTDOA":
 - 4> include the IE "UE positioning OTDOA measured results" in the measurement report and set the contents of the IE as follows:
 - 5> set IE "SFN" to the SFN when the last measurement was performed;
 - 5> if the UE supports the capability to perform the Rx-Tx time difference type 2 measurement:
 - 6> if the UE is in CELL_DCH state:
 - 7> if the measured value is equal to "1279.9375":
 - 8> set the IE "Rx-Tx time difference type 2" in IE "UE positioning OTDOA measured results" for the reference cell to "1279.8750".
 - 7> otherwise:
 - 8> set the IE "Rx-Tx time difference type 2" in IE "UE positioning OTDOA measured results" for the reference cell to the measured value.
 - 7> include the IE group "Rx-Tx time difference type 2 info" for the reference cell and for each neighbour cell listed in variable UE_POSITIONING_OTDOA_DATA_UE_ASSISTED that belongs to the active set.
 - 5> if the UE does not support the capability to perform the Rx-Tx time difference type 2 measurement:

- 6> set the IE "Rx-Tx time difference type 2" in IE "UE positioning OTDOA measured results" for the reference cell to value "1279.9375" to indicate that the measurement is not supported.
- 4> include IE group "Neighbour" for all neighbour cells listed in variable UE_POSITIONING_OTDOA_DATA_UE_ASSISTED on which the SFN-SFN observed time difference type 2 measurement could be performed.
- 3> if IE "Positioning Methods" in the MEASUREMENT CONTROL message has been assigned to value "OTDOA or GPS":
 - 4> the UE may choose to either act as if IE "Positioning Methods" is set to "GPS" or "OTDOA" depending on the method chosen by the UE.
- 3> if the IE "Positioning Methods" is set to "CELL ID":
 - 4> if the UE supports the capability to perform the Rx-Tx time difference type 2 measurement; and
 - 4> if the UE is in CELL_DCH state:
 - 5> perform the Rx-Tx time difference type 2 measurement on the cells in the active set; and
 - 5> report the measurement results back to the network in the MEASUREMENT REPORT by using IE "UE positioning OTDOA measured results" including measurements on the cells in the active set; and
 - 5> report Rx-Tx time difference type 2 measurement of the reference cell (as designated by the UE); and
 - 5> for all reported neighbour cells:
 - 6> report Rx-Tx time difference type 2 measurement; and
 - 6> set the IE "SFN-SFN observed time difference type 2" and all IEs within the corresponding IE "UE positioning OTDOA quality" in IE "UE positioning OTDOA measured results" to value "0".
- 1> if the UE is not able to report the requested measurement results;~~;-or~~
 - ~~1> if higher layers have indicated that the positioning request is not permitted;-or~~
 - ~~1> if the positioning request was not processed by higher layers and timed out;~~
- 2> include IE "UE positioning error" in the MEASUREMENT REPORT and set the contents of this IE as specified in subclause 8.6.7.19.5.

8.6.7.19.1b UE positioning reporting for UE based methods

The UE shall:

- 1> when a measurement report is triggered;~~;-and~~
 - ~~1> if higher layers indicated that the positioning request is permitted;~~
- 2> if the UE has been able to calculate a position after performing measurements on the cells included in the variable UE_POSITIONING_OTDOA_DATA_UE_BASED in case of OTDOA or on the list of satellites included in the variable UE_POSITIONING_GPS_DATA in case of GPS positioning;
- 3> include IE "UE positioning Position Estimate Info" in the MEASUREMENT REPORT and set the contents of the IE as follows:
 - 4> if the UE supports the capability to perform the UE GPS timing of cell frames measurement and UTRAN has requested to report the GPS timing of cell frames:
 - 5> perform the UE GPS timing of cell frames measurement on the serving cell or on one cell of the active set.

- 5> include the IE "Primary CPICH Info" for FDD or the IE "cell parameters id" for TDD;
- 5> include the SFN when the position was determined;
- 5> include the IE "UE GPS timing of cell frames".
- 4> if the UE does not support the capability to perform the UE GPS timing of cell frames measurement;
or
- 4> if the IE "GPS timing of Cell wanted" is set to FALSE:
 - 5> include the IE "GPS TOW msec".
- 4> if IE "Vertical Accuracy" has been included in IE "UE positioning reporting quantity":
 - 5> if the IE "Vertical Accuracy" has been assigned to value "0":
 - 6> if the IE "Horizontal Accuracy" has been assigned a value "0":
 - 7> may include IE "Ellipsoid point with altitude".
 - 6> if the IE "Horizontal Accuracy" has been assigned a value unequal to "0"; and
 - 6> if the UE has been able to calculate a 3-dimensional position
 - 7> include IE "Ellipsoid point with altitude" or IE "Ellipsoid point with altitude and uncertainty ellipsoid" as the position estimate.
 - 6> if the UE has not been able to calculate a 3-dimensional position:
 - 7> may act as if IE "Vertical Accuracy" was not included in IE "UE positioning reporting quantity".
 - 5> if the IE "Vertical Accuracy" has been assigned to a value unequal to "0":
 - 6> if the UE has been able to calculate a 3-dimensional position:
 - 7> include IE "Ellipsoid point with altitude and uncertainty ellipsoid" as the position estimate.
 - 6> if the UE has not been able to calculate a 3-dimensional position:
 - 7> act as if IE "Vertical Accuracy" has not been included in IE "UE positioning reporting quantity".
- 4> if IE "Vertical Accuracy" has not been included in IE "UE positioning reporting quantity":
 - 5> if IE "Horizontal Accuracy" in IE "UE positioning reporting quantity" has been assigned to value "0":
 - 6> may include IE "Ellipsoid point".
 - 5> if IE "Horizontal Accuracy" in IE "UE positioning reporting quantity" has been assigned to a value unequal to 0:
 - 6> include either IE "Ellipsoid point with uncertainty circle" or IE "Ellipsoid point with uncertainty ellipse" or IE "Ellipsoid point with altitude and uncertainty ellipsoid" as the position estimate.
- 1> if the UE was not able to calculate a position;~~;- or~~
- ~~1> if higher layers have indicated that the positioning request is not permitted; or~~
- ~~2> if the positioning request was not processed by higher layers and timed out;~~
- 23> include IE "UE positioning error" in the MEASUREMENT REPORT and set the contents of this IE as specified in subclause 8.6.7.19.5.

8.6.7.19.5 UE positioning Error

The UE shall set the contents of the IE "UE positioning Error" as follows:

- 1> if the IE "Positioning Methods" in IE "UE positioning reporting quantity" has been assigned to value "OTDOA" and no neighbour cells could be received,
 - 2> set IE "Error reason" to "Not Enough OTDOA Cells";
- 1> if the IE "Positioning Methods" in IE "UE positioning reporting quantity" has been assigned to value "GPS":
 - 2> if there were not enough GPS satellites to be received:
 - 3> set IE "Error reason" to "Not Enough GPS Satellites".
 - 2> if some GPS assistance data was missing:
 - 3> set IE "Error reason" to "Assistance Data Missing"; and
 - 3> if the IE "Additional Assistance Data Request" included in the IE "UE positioning reporting quantity" stored in the variable MEASUREMENT_IDENTITY is set to TRUE:
 - 4> include the IE GPS Additional Assistance Data Request".
 - 2> if the UE was not able to read the SFN of the reference cell included in the IE "UE positioning GPS reference time" or in the IE "UE positioning acquisition assistance":
 - 3> set IE "Error reason" to "Reference Cell Not Serving Cell".
 - 2> if the UE was not able to measure the requested GPS timing of cell frames measurement:
 - 3> set IE "Error reason" to "Not Accomplished GPS Timing Of Cell Frames".
 - ~~1> if higher layers have indicated that the positioning request is not permitted:
 - 2> set IE "Error reason" to "Request Denied By User".~~
 - ~~1> if the positioning request was not processed by higher layers and timed out:
 - 2> set IE "Error reason" to "Not Processed And Timeout".~~
 - 1> if none of the conditions above are fulfilled:
 - 2> set IE "Error reason" to "Undefined Error".

1> the UE shall not set the IE "Error reason" to "Request Denied By User" or "Not Processed and Timeout".

10.3.7.87 UE positioning Error

Information Element/Group name	Need	Multi	Type and Reference	Semantics description
Error reason	MP		Enumerated(Not Enough OTDOA Cells, Not Enough GPS Satellites, Assistance Data Missing, Not Accomplished GPS Timing Of Cell Frames, Undefined Error, Request Denied By User, Not Processed And Timeout, Reference Cell Not Serving Cell)	Note 1
GPS Additional Assistance Data Request	CV- <i>GPSdataMissing</i>		UE positioning GPS Additional Assistance Data Request 10.3.7.88a	

NOTE 1: The following table describes each value of the IE "Error reason".

Value	Indication
Not Enough OTDOA Cells	There were not enough cells to be received.
Not Enough GPS Satellites	There were not enough GPS satellites to be received.
Assistance Data Missing	UE positioning GPS assistance data missing.
Not Accomplished GPS Timing Of Cell Frames	UE was not able to accomplish the GPS timing of cell frames measurement.
Undefined Error	Undefined error.
Request Denied By User	UE positioning request denied by upper layers.
Not Processed And Timeout	UE positioning request not processed by upper layers and timeout.
Reference Cell Not Serving Cell	UE was not able to read the SFN of the reference cell.

Condition	Explanation
<i>GPSdataMissing</i>	The IE is optional if the IE "Error reason" is "ER3" and not needed otherwise.

11.3 Information element definitions

```
UE-Positioning-ErrorCause ::=
    ENUMERATED {
        notEnoughOTDOA-Cells,
        notEnoughGPS-Satellites,
        assistanceDataMissing,
        notAccomplishedGPS-TimingOfCellFrames,
        undefinedError,
        requestDeniedByUser,
        notProcessedAndTimeout,
        referenceCellNotServingCell }

```

3GPP TSG-RAN2 Meeting #37
Budapest, Hungary 25th to 29th August 2003

Tdoc #R2-032034

CR-Form-v7	
<h2 style="margin: 0;">CHANGE REQUEST</h2>	
# 25.331 CR 2001 # rev 1 #	Current version: 3.15.0 #

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	# START calculation		
Source:	# RAN WG2		
Work item code:	# TEI	Date:	# August 2003
Category:	# F	Release:	# R99
	Use <u>one</u> 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 <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)

Reason for change:	#
	<ol style="list-style-type: none"> 1 The calculation of START is defined to be valid in connected mode (Section 8.5.9). However, in some situations (e.g. transmission of the first INITIAL DIRECT TRANSFER of a signaling connection) the calculation can not be performed since COUNT-C and COUNT-I has not been initialised. In this scenario, the UE should use the START value stored on USIM/SIM. The COUNT-C and COUNT-I values are initialised at SECURITY MODE COMMAND which is potentially received quite some time after entering connected mode. This also means that the START value will be the same in RRC CONNECTION SETUP COMPLETE and INITIAL DIRECT TRANSFER which is the intended behaviour. 2 Currently, it is not clear if UE, when storing START values on USIM (or in ME in case of SIM) calculates a 'new' START value, hereby avoiding that HFN values are not reused for the next RRC connection.
Summary of change:	#
	<ol style="list-style-type: none"> 1 Sections 8.5.9: It is clarified when COUNT-I and/or COUNT-C has not been initialised, the START value calculation in 8.5.9 is not performed and instead the UE should use the START value stored on the USIM (or in ME in case of SIM). The Rel-5 implementation is different than the R'99/Rel-4. 2 Sections 8.5.2 and 8.5.22: It is added that UE should perform a START value calculation prior to storing the START value on USIM (or in ME in case of SIM).
Consequences if not approved:	#
	<ol style="list-style-type: none"> 1 If the CR is not implemented the START value calculation in 8.5.9 can not be

performed as specified in cases where the COUNT-I/ COUNT-C has not been initialised. If this undefined COUNT calculation results in a value, and the message IDT and RRC Connection setup complete are received in the wrong order, there might be ciphering and/or integrity protection failures.

2 Security principles are broken, since UE might reuse the same HFN values after setup of the next RRC connection.

Impact analysis:

Impacted functionality: Handling of START value

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent.

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- No interoperability problems are foreseen.

Clauses affected: ⌘ 8.5.2, 8.5.9, 8.5.22

	Y	N	
Other specs affected:	⌘	X	Other core specifications ⌘
		X	Test specifications
		X	O&M Specifications

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.5.2 Actions when entering idle mode from connected mode

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

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

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

- 1> perform cell selection.

While camping on a cell, the UE shall:

- 1> acquire system information according to the system information procedure in subclause 8.1;
- 1> perform measurements according to the measurement control procedure specified in subclause 8.4; and
- 1> if the UE is registered:
 - 2> 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:

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

When entering idle mode, the UE shall:

- 1> if the USIM is present, for each CN domain:
 - 2> 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:
 - 3> set the START value for this domain to zero; and
 - 3> store this START value for this domain in the USIM.
 - 2> else:
 - 3> 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:
 - 4> delete the ciphering and integrity keys that are stored in the USIM for that CN domain;
 - 4> inform the deletion of these keys to upper layers.
 - 3> else:
 - 4> store the current "START" value for this CN domain on the USIM.

NOTE: Prior to storing the "START" value, UE should calculate the "START" according to subclause 8.5.9.

- 1> else:
 - 2> if the SIM is present, for each CN domain:
 - 3> 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, the UE should:
 - 4> set the START value for this domain to zero; and
 - 4> store this START value for this domain in the UE.
 - 3> else, the UE shall:

- 4> if the current "START" value, according to subclause 8.5.9 for this CN domain, is greater than or equal to the value "THRESHOLD" of the variable START_THRESHOLD:
 - 5> delete the Kc key for this CN domain;
 - 5> delete the ciphering and integrity keys that are stored in the UE for that CN domain;
 - 5> set the "START" values for this CN domain to zero and store it in the UE;
 - 5> inform the deletion of the key to upper layers.
- 4> else:
 - 5> store the current "START" value for this CN domain in the UE.

NOTE: Prior to storing the "START" value, UE should calculate the "START" according to subclause 8.5.9.

8.5.22 Actions when entering another RAT from connected mode

When entering another RAT from connected mode (due to Inter-RAT handover from UTRAN, Inter-RAT cell change order from UTRAN or Inter-RAT cell reselection from UTRAN), after successful completion of the procedure causing the transition to the other RAT, the UE shall:

- 1> if the USIM is present, for each CN domain:
 - 2> 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:
 - 3> set the START value for this domain to zero and;
 - 3> store this START value for this domain in the USIM.
 - 2> else:
 - 3> store the current START value for this CN domain in the USIM [50].

[NOTE: Prior to storing the START value, UE should calculate the START according to subclause 8.5.9.](#)

- 1> if the SIM is present, for each CN domain:
 - 2> if a new security key was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:
 - 3> set the START value for this domain to zero and;
 - 3> store this START value for this domain in the UE.
 - 2> else:
 - 3> store the current START value for this CN domain in the UE.

[NOTE: Prior to storing the START value, UE should calculate the START according to subclause 8.5.9.](#)

8.5.9 START value calculation

In connected mode, if COUNT-C and/or COUNT-I has been initialised for a CN domain 'X', the START value for that CN domain is calculated as:

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

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

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

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

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

If neither COUNT-I nor COUNT-C has been initialised for a CN domain, the START value stored in USIM (or stored in ME in case SIM is present) should be used as calculated START value.

3GPP TSG-RAN2 Meeting #37
Budapest, Hungary 25th to 29th August 2003

Tdoc #R2-032035

CR-Form-v7

CHANGE REQUEST

⌘ **25.331 CR 2002** ⌘ rev **1** ⌘ Current version: **4.10.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ START calculation
Source:	⌘ RAN WG2
Work item code:	⌘ TEI
Date:	⌘ August 2003
Category:	⌘ A
<p>Use <u>one</u> of the following categories:</p> <p>F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p>	
Release:	⌘ Rel-4
<p>Use <u>one</u> of the following releases:</p> <p>2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)</p>	

Reason for change:	⌘
<ol style="list-style-type: none"> The calculation of START is defined to be valid in connected mode (Section 8.5.9). However, in some situations (e.g. transmission of the first INITIAL DIRECT TRANSFER of a signaling connection) the calculation can not be performed since COUNT-C and COUNT-I has not been initialised. In this scenario, the UE should use the START value stored on USIM/SIM. The COUNT-C and COUNT-I values are initialised at SECURITY MODE COMMAND which is potentially received quite some time after entering connected mode. This also means that the START value will be the same in RRC CONNECTION SETUP COMPLETE and INITIAL DIRECT TRANSFER which is the intended behaviour. Currently, it is not clear if UE, when storing START values on USIM (or in ME in case of SIM) calculates a 'new' START value, hereby avoiding that HFN values are not reused for the next RRC connection. 	
Summary of change:	⌘
<ol style="list-style-type: none"> Sections 8.5.9: It is clarified when COUNT-I and/or COUNT-C has not been initialised, the START value calculation in 8.5.9 is not performed and instead the UE should use the START value stored on the USIM (or in ME in case of SIM). The Rel-5 implementation is different than the R'99/Rel-4. Sections 8.5.2 and 8.5.22: It is added that UE should perform a START value calculation prior to storing the START value on USIM (or in ME in case of SIM). 	
Consequences if not approved:	⌘
<ol style="list-style-type: none"> If the CR is not implemented the START value calculation in 8.5.9 can not be performed as specified in cases where the COUNT-I/ COUNT-C has not been 	

initialised. If this undefined COUNT calculation results in a value, and the message IDT and RRC Connection setup complete are received in the wrong order, there might be ciphering and/or integrity protection failures.

2 Security principles are broken, since UE might reuse the same HFN values after setup of the next RRC connection.

Impact analysis:

Impacted functionality: Handling of START value

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent.

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- No interoperability problems are foreseen.

Clauses affected: ⌘ 8.5.2, 8.5.9, 8.5.22

	Y	N	
Other specs affected:	⌘	X	Other core specifications ⌘
		X	Test specifications
		X	O&M Specifications

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.5.2 Actions when entering idle mode from connected mode

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

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

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

- 1> perform cell selection.

While camping on a cell, the UE shall:

- 1> acquire system information according to the system information procedure in subclause 8.1;
- 1> perform measurements according to the measurement control procedure specified in subclause 8.4; and
- 1> if the UE is registered:
 - 2> 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:

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

When entering idle mode, the UE shall:

- 1> if the USIM is present, for each CN domain:
 - 2> 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:
 - 3> set the START value for this domain to zero; and
 - 3> store this START value for this domain in the USIM.
 - 2> else:
 - 3> 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:
 - 4> delete the ciphering and integrity keys that are stored in the USIM for that CN domain;
 - 4> inform the deletion of these keys to upper layers.
 - 3> else:
 - 4> store the current "START" value for this CN domain on the USIM.

NOTE: [Prior to storing the "START" value, UE should calculate the "START" according to subclause 8.5.9.](#)

1> else:

- 2> if the SIM is present, for each CN domain:
 - 3> 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:
 - 4> set the START value for this domain to zero; and
 - 4> store this START value for this domain in the UE

3> else:

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

5> delete the Kc key for this CN domain;

5> delete the ciphering and integrity keys that are stored in the UE for that CN domain;

5> set the "START" values for this CN domain to zero and store it the UE;

5> inform the deletion of the key to upper layers.

4> else:

5> store the current "START" value for this CN domain in the UE.

NOTE: Prior to storing the "START" value, UE should calculate the "START" according to subclause 8.5.9.

8.5.9 START value calculation

In connected mode, if COUNT-C and/or COUNT-I has been initialised for a CN domain 'X', the START value for that CN domain is calculated as:

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

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

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

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

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

If neither COUNT-I or COUNT-C has been initialised for a CN domain, the START value stored in the USIM (or stored in ME in case SIM is present) should be used instead of the calculated value.

8.5.22 Actions when entering another RAT from connected mode

When entering another RAT from connected mode (due to Inter-RAT handover from UTRAN, Inter-RAT cell change order from UTRAN or Inter-RAT cell reselection from UTRAN), after successful completion of the procedure causing the transition to the other RAT, the UE shall:

- 1> if the USIM is present, for each CN domain:
 - 2> 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:
 - 3> set the START value for this domain to zero and;
 - 3> store this START value for this domain in the USIM;
 - 2> else:
 - 3> store the current START value for every CN domain in the USIM [50].

[NOTE: Prior to storing the “START” value, UE should calculate the “START” according to subclause 8.5.9.](#)

- 1> if the SIM is present, for each CN domain:
 - 2> if a new security key was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:
 - 3> set the START value for this domain to zero and;
 - 3> store this START value for this domain in the USIM.
 - 2> else:
 - 3> store the current START value for this CN domain in the UE.

[NOTE: Prior to storing the “START” value, UE should calculate the “START” according to subclause 8.5.9.](#)

3GPP TSG-RAN2 Meeting #37
Budapest, Hungary 25th to 29th August 2003

Tdoc #R2-032036

CR-Form-v7
CHANGE REQUEST
25.331 CR 2003 # rev 1 # Current version: 5.5.0

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

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# START calculation		
Source:	# RAN WG2		
Work item code:	# TEI	Date:	# August 2003
Category:	# F	Release:	# Rel-5
	Use <u>one</u> 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 <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)

Reason for change: #	<ol style="list-style-type: none"> 1 The calculation of START is defined to be valid in connected mode (Section 8.5.9). However, in some situations (e.g. transmission of the first INITIAL DIRECT TRANSFER of a signaling connection) the calculation can not be performed since COUNT-C and COUNT-I has not been initialised. In this scenario, the UE shall use the START value stored on USIM/SIM. The COUNT-C and COUNT-I values are initialised at SECURITY MODE COMMAND which is potentially received quite some time after entering connected mode. This also means that the START value will be the same in RRC CONNECTION SETUP COMPLETE and INITIAL DIRECT TRANSFER which is the intended behaviour. 2 Currently, it is not clear if UE, when storing START values on USIM (or in ME in case of SIM) calculates a 'new' START value, hereby avoiding that HFN values are not reused for the next RRC connection.
Summary of change: #	<ol style="list-style-type: none"> 1 Sections 8.5.9: It is clarified when COUNT-I and/or COUNT-C has not been initialised, the START value calculation in 8.5.9 is not performed and instead the UE shall use the START value stored on the USIM (or in ME in case of SIM). The Rel-5 implementation is different than the R'99/Rel-4. 2 Sections 8.5.2 and 8.5.22: It is added that UE should perform a START value calculation prior to storing the START value on USIM (or in ME in case of SIM).
Consequences if not approved: #	<ol style="list-style-type: none"> 1 If the CR is not implemented the START value calculation in 8.5.9 can not be performed as specified in cases where the COUNT-I/ COUNT-C has not been

initialised. If this undefined COUNT calculation results in a value, and the message IDT and RRC Connection setup complete are received in the wrong order, there might be ciphering and/or integrity protection failures.

2 Security principles are broken, since UE might reuse the same HFN values after setup of the next RRC connection.

Impact analysis:

Impacted functionality: Handling of START value

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent.

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- No interoperability problems are foreseen.

Clauses affected: ⌘ 8.5.2, 8.5.9, 8.5.22

	Y	N	
Other specs affected:	⌘	X	Other core specifications ⌘
		X	Test specifications
		X	O&M Specifications

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.5.2 Actions when entering idle mode from connected mode

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

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

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

- 1> perform cell selection.

While camping on a cell, the UE shall:

- 1> acquire system information according to the system information procedure in subclause 8.1;
- 1> perform measurements according to the measurement control procedure specified in subclause 8.4; and
- 1> if the UE is registered:
 - 2> 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:

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

When entering idle mode, the UE shall:

- 1> if the USIM is present, for each CN domain:
 - 2> 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:
 - 3> set the START value for this domain to zero; and
 - 3> store this START value for this domain in the USIM.
 - 2> else:
 - 3> 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:
 - 4> delete the ciphering and integrity keys that are stored in the USIM for that CN domain;
 - 4> inform the deletion of these keys to upper layers.
 - 3> else:
 - 4> store the current "START" value for this CN domain on the USIM.

[NOTE: Prior to storing the "START" value, UE should calculate the "START" according to subclause 8.5.9.](#)

1> else:

- 2> if the SIM is present, for each CN domain:
 - 3> 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:
 - 4> set the START value for this domain to zero; and
 - 4> store this START value for this domain in the UE

3> else:

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

5> delete the Kc key for this CN domain;

5> delete the ciphering and integrity keys that are stored in the UE for that CN domain;

5> set the "START" values for this CN domain to zero and store it the UE;

5> inform the deletion of the key to upper layers.

4> else:

5> store the current "START" value for this CN domain in the UE.

NOTE: Prior to storing the "START" value, UE should calculate the "START" according to subclause 8.5.9.

8.5.9 START value calculation

In connected mode, if COUNT-C and/or COUNT-I has been initialised for a CN domain 'X', the START value for that CN domain is calculated as:

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

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

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

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

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

If neither COUNT-I or COUNT-C has been initialised for a CN domain, the START value stored in the USIM (or stored in ME in case SIM is present) shall be used instead of the calculated value.

8.5.22 Actions when entering another RAT from connected mode

When entering another RAT from connected mode (due to Inter-RAT handover from UTRAN, Inter-RAT cell change order from UTRAN or Inter-RAT cell reselection from UTRAN), after successful completion of the procedure causing the transition to the other RAT, the UE shall:

- 1> if the USIM is present, for each CN domain:
 - 2> 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:
 - 3> set the START value for this domain to zero and;
 - 3> store this START value for this domain in the USIM;

NOTE: Prior to storing the “START” value, UE should calculate the “START” according to subclause 8.5.9.

- 2> else:
 - 3> store the current START value for every CN domain in the USIM [50].

- 1> if the SIM is present, for each CN domain:
 - 2> if a new security key was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:
 - 3> set the START value for this domain to zero and;
 - 3> store this START value for this domain in the USIM.

NOTE: Prior to storing the “START” value, UE should calculate the “START” according to subclause 8.5.9.

- 2> else:
 - 3> store the current START value for this CN domain in the UE.

CR-Form-v7

CHANGE REQUEST

25.331 CR 2004 # rev - # Current version: **3.15.0**

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	# PRACH channelisation code list limitation to align with TS 25.221		
Source:	# RAN WG2		
Work item code:	# TEI	Date:	# 19/08/2003
Category:	# F	Release:	# R99
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)	2	(GSM Phase 2)
	A (corresponds to a correction in an earlier release)	R96	(Release 1996)
	B (addition of feature),	R97	(Release 1997)
	C (functional modification of feature)	R98	(Release 1998)
	D (editorial modification)	R99	(Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .	Rel-4	(Release 4)
		Rel-5	(Release 5)
		Rel-6	(Release 6)

Reason for change:	# Currently the PRACH channelisation code list allows all 16 SF16 channelisation codes to be specified in SIB5/6. However in section 5.3.3.5 of 25.221 only channelisation codes 16/1 to 16/8 are specified and have an associated midamble shift defined. Therefore if the PRACH channelisation code list contains channelisation codes 16/9 to 16/16 then the UE operation is undefined and PRACH operation will fail.
Summary of change:	# Notes are added into both tabular and ASN.1 which specify that channelisation code 16/9 to 16/16 are not allowed. Also an example of PRACH channelisation in section 8.6.6..29 dealing with access service class is modified so that only valid channelisation are used.
Consequences if not approved:	# PRACH channelisation codes can be specified which will cause PRACH to fail. Isolated impact analysis: this CR corrects errors in the PRACH channelisation codes defined in TDD (only). Without this change channelisation codes can be specified in system information which do not have a specific associated midamble shift defined in 25.221.

Clauses affected:	# 8.6.6.29, 10.3.6.51, 11.3										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	#	X	#	X	#	X	Other core specifications	#
Y	N										
#	X										
#	X										
#	X										
		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/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ☹ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/>. For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.6.6.29 ASC setting

If the IE "ASC setting" is included, the UE shall:

- 1> establish the available signatures for this ASC as specified in the following:
 - 2> renumber the list of available signatures specified in the IE "Available signature" included in the IE "PRACH info" from signature index 0 to signature index N-1, where N is the number of available signatures, starting with the lowest available signature number and continuing in sequence, in the order of increasing signature numbers;
 - 2> consider as available signatures for this ASC the signatures included in this renumbered list from the index specified by the IE "Available signature Start Index" to the index specified by the IE "Available signature End Index".
- 1> establish the available access slot sub-channels for this ASC as specified in the following:
 - 2> if the IE "AICH transmission timing" included in the IE "AICH Info" is set to '0':
 - 3> ignore the leftmost (most significant) bit (bit b3) of the bit string specified by the IE "Assigned Sub-Channel Number";
 - 3> repeat 4 times the 3 rightmost (least significant) bits (bits b2-b0) of the bit string specified by the IE "Assigned Sub-Channel Number" to form a resulting bit string 'b2 b1 b0 b2 b1 b0 b2 b1 b0 b2 b1 b0' of length 12 bits, where the leftmost bit is the most significant.
 - 2> if the IE "AICH transmission timing" included in the IE "AICH Info" is set to '1':
 - 3> repeat 3 times the bit string (bits b3-b0) specified by the IE "Assigned Sub-Channel Number" to form a bit string 'b3 b2 b1 b0 b3 b2 b1 b0 b3 b2 b1 b0' of length 12 bits, where the leftmost bit is the most significant.
 - 2> perform in both cases, for the resulting bit string (that includes the repetitions) bit-wise logical AND operation with the IE "Available Sub Channel number" included in IE "PRACH info (for RACH)";
 - 2> consider as available sub-channels for this ASC the available sub-channels indicated in the resulting bit string, after logical AND operation i.e. each bit set to 1 or 0 indicates availability or non-availability, respectively, of sub-channel number x , with x from 0 to 11, for the respective ASC.

NOTE 1: In FDD, the list of available signatures is renumbered from signature index 0 to signature index N-1, where N is the number of available signatures, starting with the lowest available signature number and continuing in sequence, in the order of increasing signature numbers.

- List of available signatures: 16 or fewer signatures are available.
- Example: only signatures 0, 5, 10 and 15 are available, then :
- Signature 0 is: available signature index 0
- Signature 5 is: available signature index 1
- Signature 10 is: available signature index 2
- Signature 15 is: available signature index 3

NOTE 2: In TDD, the list of available channelisation codes (defined in PRACH info) is renumbered from channelisation code index 0 to channelisation code index N-1, where N is the number of available channelisation codes, starting with the lowest available channelisation code number and continuing in sequence, in the order of increasing channelisation code numbers

List of available channelisation codes : 8 or less channelisation codes are available.

The i-th bit of the bitmap defined in the IE "Available Channelisation Code indices" defines whether the channelisation code with the available channelisation code index i is to be used for this ASC (bit set means used, bit unset means not used). Only the low N bits shall be used in the bitmap, where N is the number of available channelisation codes defined in PRACH info.

Ex : spreading factor 16, channelisation codes 16/1, 16/2, 16/5, ~~16/10~~ 16/8 are available :

- Channelisation code 16/1 is: available channelisation code index 0
- Channelisation code 16/2 is: available channelisation code index 1
- Channelisation code 16/5 is: available channelisation code index 2
- Channelisation code ~~16/10~~ 16/8 is: available channelisation code index 3

Available Channelisation Code indices has the value '00001100' means: Channelisation Codes 16/5 and ~~16/10~~ 16/8 are available for this ASC.

NOTE 3: In TDD, the subchannel description is found in [33].

10.3.6.51 PRACH Channelisation Code List

NOTE: Only for TDD.

Information Element/Group name	Need	Multi	Type and reference	Semantics description
CHOICE SF	MP			
>SF16				
>>Channelisation Code List	MP	1 to 8		
>>>Channelisation code	MP		Enumerated ((16/1)...(16/16))	There is a 1:1 mapping between spreading code and midamble shift defined in [30] for channelisation codes (16/1) to (16/8). Note: channelisation codes (16/9) to (16/16) shall not be used.
>SF8				
>>Channelisation Code List	MP	1 to 8		
>>>Channelisation Code	MP		Enumerated((8/1)..(8/8))	

11.3 Information element definitions

```
TDD-PRACH-CCodeList ::= CHOICE {
    sf8 SEQUENCE (SIZE (1..8)) OF
```

```
TDD-PRACH-CCode8,  
-- Channelisation codes cc16-9, cc16-10, cc16-11, cc16-12, cc16-13, cc16-14, cc16-15 and cc16-16  
shall not be used  
sf16 SEQUENCE (SIZE (1..8)) OF  
TDD-PRACH-CCode16  
}
```


CR-Form-v7

CHANGE REQUEST

25.331 CR 2005 # rev - # Current version: **4.10.0**

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	# PRACH channelisation code list limitation to align with TS 25.221		
Source:	# RAN WG2		
Work item code:	# TEI	Date:	# 19/08/2003
Category:	# A	Release:	# Rel-4
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)		2 (GSM Phase 2)
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)
	B (addition of feature),		R97 (Release 1997)
	C (functional modification of feature)		R98 (Release 1998)
	D (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	# Currently the PRACH channelisation code list allows all 16 SF16 channelisation codes to be specified in SIB5/6. However in section 5.3.3.5 of 25.221 only channelisation codes 16/1 to 16/8 are specified and have an associated midamble shift defined. Therefore if the PRACH channelisation code list contains channelisation codes 16/9 to 16/16 then the UE operation is undefined and PRACH operation will fail.
Summary of change:	# Notes are added into both tabular and ASN.1 which specify that channelisation code 16/9 to 16/16 are not allowed. Also an example of PRACH channelisation in section 8.6.6..29 dealing with access service class is modified so that only valid channelisation are used.
Consequences if not approved:	# PRACH channelisation codes can be specified which will cause PRACH to fail. Isolated impact analysis: this CR corrects errors in the PRACH channelisation codes defined in TDD (only). Without this change channelisation codes can be specified in system information which do not have a specific associated midamble shift defined in 25.221.

Clauses affected:	# 8.6.6.29, 10.3.6.51, 11.3												
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">#</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	#	#	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	#
Y	N												
#	#												
<input type="checkbox"/>	<input checked="" type="checkbox"/>												
<input type="checkbox"/>	<input checked="" type="checkbox"/>												
<input type="checkbox"/>	<input checked="" type="checkbox"/>												
		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/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ☹ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/>. For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.6.6.29 ASC setting

If the IE "ASC setting" is included, the UE shall:

- 1> establish the available signatures for this ASC as specified in the following:
 - 2> renumber the list of available signatures specified in the IE "Available signature" included in the IE "PRACH info" from signature index 0 to signature index N-1, where N is the number of available signatures, starting with the lowest available signature number and continuing in sequence, in the order of increasing signature numbers;
 - 2> consider as available signatures for this ASC the signatures included in this renumbered list from the index specified by the IE "Available signature Start Index" to the index specified by the IE "Available signature End Index".
- 1> establish the available access slot sub-channels for this ASC as specified in the following:
 - 2> if the IE "AICH transmission timing" included in the IE "AICH Info" is set to '0':
 - 3> ignore the leftmost (most significant) bit (bit b3) of the bit string specified by the IE "Assigned Sub-Channel Number";
 - 3> repeat 4 times the 3 rightmost (least significant) bits (bits b2-b0) of the bit string specified by the IE "Assigned Sub-Channel Number" to form a resulting bit string 'b2 b1 b0 b2 b1 b0 b2 b1 b0 b2 b1 b0' of length 12 bits, where the leftmost bit is the most significant.
 - 2> if the IE "AICH transmission timing" included in the IE "AICH Info" is set to '1':
 - 3> repeat 3 times the bit string (bits b3-b0) specified by the IE "Assigned Sub-Channel Number" to form a bit string 'b3 b2 b1 b0 b3 b2 b1 b0 b3 b2 b1 b0' of length 12 bits, where the leftmost bit is the most significant.
 - 2> perform in both cases, for the resulting bit string (that includes the repetitions) bit-wise logical AND operation with the IE "Available Sub Channel number" included in IE "PRACH info (for RACH)";
 - 2> consider as available sub-channels for this ASC the available sub-channels indicated in the resulting bit string, after logical AND operation i.e. each bit set to 1 or 0 indicates availability or non-availability, respectively, of sub-channel number x , with x from 0 to 11, for the respective ASC.

NOTE 1: In FDD, the list of available signatures is renumbered from signature index 0 to signature index N-1, where N is the number of available signatures, starting with the lowest available signature number and continuing in sequence, in the order of increasing signature numbers.

- List of available signatures: 16 or fewer signatures are available.
- Example: only signatures 0, 5, 10 and 15 are available, then :
- Signature 0 is: available signature index 0
- Signature 5 is: available signature index 1
- Signature 10 is: available signature index 2
- Signature 15 is: available signature index 3

NOTE 2: In 3.84 Mcps TDD, the list of available channelisation codes (defined in PRACH info) is renumbered from channelisation code index 0 to channelisation code index N-1, where N is the number of available channelisation codes, starting with the lowest available channelisation code number and continuing in sequence, in the order of increasing channelisation code numbers

List of available channelisation codes : 8 or less channelisation codes are available.

The i-th bit of the bitmap defined in the IE "Available Channelisation Code indices" defines whether the channelisation code with the available channelisation code index i is to be used for this ASC (bit set means used, bit unset means not used). Only the low N bits shall be used in the bitmap, where N is the number of available channelisation codes defined in PRACH info.

Ex : spreading factor 16, channelisation codes 16/1, 16/2, 16/5, ~~16/10~~16/8 are available :

- Channelisation code 16/1 is: available channelisation code index 0
- Channelisation code 16/2 is: available channelisation code index 1
- Channelisation code 16/5 is: available channelisation code index 2
- Channelisation code ~~16/10~~16/8 is: available channelisation code index 3

Available Channelisation Code indices has the value '00001100' means: Channelisation Codes 16/5 and ~~16/10~~16/8 are available for this ASC.

NOTE 3: In TDD, the subchannel description is found in [33].

NOTE 4: In 1.28 Mcps TDD, the list of available SYNC_UL codes (defined in PRACH info) is numbered from SYNC_UL code index 0 to SYNC_UL code index N-1, where N is the number of available SYNC_UL codes, starting with the lowest available SYNC_UL code number and continuing in sequence, in the order of increasing SYNC_UL code numbers

The i-th bit of the bitmap defined in the IE "Available SYNC_UL codes indices" defines whether the SYNC_UL code with the available SYNC_UL code index i is to be used for this ASC (bit set means used, bit unset means not used). Only the low N bits shall be used in the bitmap, where N is the number of available SYNC_UL codes defined in PRACH info.

- List of available SYNC_UL codes: 8 or fewer SYNC_UL codes are available.

Example: only signatures 0, 5, 6 and 7 are available, then:

- SYNC_UL codes 0 is: available SYNC_UL codes index 0
- SYNC_UL codes 5 is: available SYNC_UL codes index 1
- SYNC_UL codes 6 is: available SYNC_UL codes index 2
- SYNC_UL codes 7 is: available SYNC_UL codes index 3

Available SYNC_UL codes indices has the value '00001100' means: SYNC_UL codes 6 and 7 are available for this ASC.

10.3.6.51 PRACH Channelisation Code List

NOTE: Only for 3.84 Mcps TDD.

Information Element/Group name	Need	Multi	Type and reference	Semantics description	Version
CHOICE SF	MP				
>SF16					
>>Channelisation Code List	MP	1 to 8			
>>>Channelisation code	MP		Enumerated ((16/1)...(16/16))	There is a 1:1 mapping between spreading code and midamble	

Information Element/Group name	Need	Multi	Type and reference	Semantics description	Version
				shift defined in [30] for channelisation codes (16/1) to (16/8). Note: channelisation codes (16/9) to (16/16) shall not be used.	
>SF8					
>>Channelisation Code List	MP	1 to 8			
>>>Channelisation Code	MP		Enumerated(8/1)..(8/8)		

11.3 Information element definitions

```

TDD-PRACH-CCodeList ::= CHOICE {
    sf8 SEQUENCE (SIZE (1..8)) OF
        TDD-PRACH-CCode8,
    -- Channelisation codes cc16-9, cc16-10, cc16-11, cc16-12, cc16-13, cc16-14, cc16-15 and cc16-16
    -- shall not be used
    sf16 SEQUENCE (SIZE (1..8)) OF
        TDD-PRACH-CCode16
}
    
```

CR-Form-v7

CHANGE REQUEST

25.331 CR 2006 # rev - # Current version: **5.5.0**

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	# PRACH channelisation code list limitation to align with TS 25.221		
Source:	# RAN WG2		
Work item code:	# TEI	Date:	# 19/08/2003
Category:	# A	Release:	# Rel-5
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)	2	(GSM Phase 2)
	A (corresponds to a correction in an earlier release)	R96	(Release 1996)
	B (addition of feature),	R97	(Release 1997)
	C (functional modification of feature)	R98	(Release 1998)
	D (editorial modification)	R99	(Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .	Rel-4	(Release 4)
		Rel-5	(Release 5)
		Rel-6	(Release 6)

Reason for change:	# Currently the PRACH channelisation code list allows all 16 SF16 channelisation codes to be specified in SIB5/6. However in section 5.3.3.5 of 25.221 only channelisation codes 16/1 to 16/8 are specified and have an associated midamble shift defined. Therefore if the PRACH channelisation code list contains channelisation codes 16/9 to 16/16 then the UE operation is undefined and PRACH operation will fail.
Summary of change:	# Notes are added into both tabular and ASN.1 which specify that channelisation code 16/9 to 16/16 are not allowed. Also an example of PRACH channelisation in section 8.6.6..29 dealing with access service class is modified so that only valid channelisation are used.
Consequences if not approved:	# PRACH channelisation codes can be specified which will cause PRACH to fail. Isolated impact analysis: this CR corrects errors in the PRACH channelisation codes defined in TDD (only). Without this change channelisation codes can be specified in system information which do not have a specific associated midamble shift defined in 25.221.

Clauses affected:	# 8.6.6.29, 10.3.6.51, 11.3										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	#	X	#	X	#	X	Other core specifications	#
Y	N										
#	X										
#	X										
#	X										
		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/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ☹ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/>. For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.6.6.29 ASC setting

If the IE "ASC setting" is included, the UE shall:

- 1> establish the available signatures for this ASC as specified in the following:
 - 2> renumber the list of available signatures specified in the IE "Available signature" included in the IE "PRACH info" from signature index 0 to signature index N-1, where N is the number of available signatures, starting with the lowest available signature number and continuing in sequence, in the order of increasing signature numbers;
 - 2> consider as available signatures for this ASC the signatures included in this renumbered list from the index specified by the IE "Available signature Start Index" to the index specified by the IE "Available signature End Index".
- 1> establish the available access slot sub-channels for this ASC as specified in the following:
 - 2> if the IE "AICH transmission timing" included in the IE "AICH Info" is set to '0':
 - 3> ignore the leftmost (most significant) bit (bit b3) of the bit string specified by the IE "Assigned Sub-Channel Number";
 - 3> repeat 4 times the 3 rightmost (least significant) bits (bits b2-b0) of the bit string specified by the IE "Assigned Sub-Channel Number" to form a resulting bit string 'b2 b1 b0 b2 b1 b0 b2 b1 b0 b2 b1 b0' of length 12 bits, where the leftmost bit is the most significant.
 - 2> if the IE "AICH transmission timing" included in the IE "AICH Info" is set to '1':
 - 3> repeat 3 times the bit string (bits b3-b0) specified by the IE "Assigned Sub-Channel Number" to form a bit string 'b3 b2 b1 b0 b3 b2 b1 b0 b3 b2 b1 b0' of length 12 bits, where the leftmost bit is the most significant.
 - 2> perform in both cases, for the resulting bit string (that includes the repetitions) bit-wise logical AND operation with the IE "Available Sub Channel number" included in IE "PRACH info (for RACH)";
 - 2> consider as available sub-channels for this ASC the available sub-channels indicated in the resulting bit string, after logical AND operation i.e. each bit set to 1 or 0 indicates availability or non-availability, respectively, of sub-channel number x , with x from 0 to 11, for the respective ASC.

NOTE 1: In FDD, the list of available signatures is renumbered from signature index 0 to signature index N-1, where N is the number of available signatures, starting with the lowest available signature number and continuing in sequence, in the order of increasing signature numbers.

- List of available signatures: 16 or fewer signatures are available.
- Example: only signatures 0, 5, 10 and 15 are available, then :
 - Signature 0 is: available signature index 0
 - Signature 5 is: available signature index 1
 - Signature 10 is: available signature index 2
 - Signature 15 is: available signature index 3

NOTE 2: In 3.84 Mcps TDD, the list of available channelisation codes (defined in PRACH info) is renumbered from channelisation code index 0 to channelisation code index N-1, where N is the number of available channelisation codes, starting with the lowest available channelisation code number and continuing in sequence, in the order of increasing channelisation code numbers

List of available channelisation codes : 8 or less channelisation codes are available.

The i-th bit of the bitmap defined in the IE "Available Channelisation Code indices" defines whether the channelisation code with the available channelisation code index i is to be used for this ASC (bit set means used, bit unset means not used). Only the low N bits shall be used in the bitmap, where N is the number of available channelisation codes defined in PRACH info.

Ex : spreading factor 16, channelisation codes 16/1, 16/2, 16/5, ~~16/10~~16/8 are available :

- Channelisation code 16/1 is: available channelisation code index 0
- Channelisation code 16/2 is: available channelisation code index 1
- Channelisation code 16/5 is: available channelisation code index 2
- Channelisation code ~~16/10~~16/8 is: available channelisation code index 3

Available Channelisation Code indices has the value '00001100' means: Channelisation Codes 16/5 and ~~16/10~~16/8 are available for this ASC.

NOTE 3: In TDD, the subchannel description is found in [33].

NOTE 4: In 1.28 Mcps TDD, the list of available SYNC_UL codes (defined in PRACH info) is numbered from SYNC_UL code index 0 to SYNC_UL code index N-1, where N is the number of available SYNC_UL codes, starting with the lowest available SYNC_UL code number and continuing in sequence, in the order of increasing SYNC_UL code numbers

The i-th bit of the bitmap defined in the IE "Available SYNC_UL codes indices" defines whether the SYNC_UL code with the available SYNC_UL code index i is to be used for this ASC (bit set means used, bit unset means not used). Only the low N bits shall be used in the bitmap, where N is the number of available SYNC_UL codes defined in PRACH info.

- List of available SYNC_UL codes: 8 or fewer SYNC_UL codes are available.

Example: only signatures 0, 5, 6 and 7 are available, then:

- SYNC_UL codes 0 is: available SYNC_UL codes index 0
- SYNC_UL codes 5 is: available SYNC_UL codes index 1
- SYNC_UL codes 6 is: available SYNC_UL codes index 2
- SYNC_UL codes 7 is: available SYNC_UL codes index 3

Available SYNC_UL codes indices has the value '00001100' means: SYNC_UL codes 6 and 7 are available for this ASC.

10.3.6.51 PRACH Channelisation Code List

NOTE: Only for 3.84 Mcps TDD.

Information Element/Group name	Need	Multi	Type and reference	Semantics description	Version
CHOICE SF	MP				
>SF16					
>>Channelisation Code List	MP	1 to 8			
>>>Channelisation code	MP		Enumerated ((16/1)...(16/16))	There is a 1:1 mapping between spreading code and midamble	

Information Element/Group name	Need	Multi	Type and reference	Semantics description	Version
				shift defined in [30] for channelisation codes (16/1) to (16/8). Note: channelisation codes (16/9) to (16/16) shall not be used.	
>SF8					
>>Channelisation Code List	MP	1 to 8			
>>>Channelisation Code	MP		Enumerated(8/1)..(8/8)		

11.3 Information element definitions

```

TDD-PRACH-CCodeList ::= CHOICE {
    sf8 SEQUENCE (SIZE (1..8)) OF
        TDD-PRACH-CCode8,
    -- Channelisation codes cc16-9, cc16-10, cc16-11, cc16-12, cc16-13, cc16-14, cc16-15 and cc16-16
    -- shall not be used
    sf16 SEQUENCE (SIZE (1..8)) OF
        TDD-PRACH-CCode16
}
    
```

CHANGE REQUEST

25.331 CR 2007 # rev - # Current version: **3.15.0**

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	# Handling of transport channel information at radio bearer release		
Source:	# RAN WG2		
Work item code:	# TEI	Date:	# 18/08/2003
Category:	# F	Release:	# R99
	<i>Use <u>one</u> of the following categories:</i> 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 .		<i>Use <u>one</u> of the following releases:</i> 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)

Reason for change:	# It is not sufficiently clear that the UE stores transport channel configurations until they are explicitly deleted by a message from the network, or the UE leaves RRC connected mode. In particular, some readers might assume that the transport channel configuration are explicitly deleted as radio bearer release or RRC state transition.
Summary of change:	# A note is added to clarify that the UE stores transport channel configurations until they explicitly deleted by a message containing the IE 'Deleted UL/DL TrCH information' or the UE leaves RRC connected mode. Isolated Impact Analysis: Functionality corrected: Handling of transport channel configurations Isolated impact statement: Correction to a function where specification was not sufficiently explicit. Would not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise. If either the UTRAN or the UE is not aligned to this CR then the UE and UTRAN can become de-synchronised with regard the to DCH transport channels that are currently configured for the UE. This will result in incompatible TFCS configurations at the UE and UTRAN and data loss.
Consequences if not approved:	# If the CR is not approved then UTRAN implementations may assume that when a RB is released the transport channels used by that RB are implicitly deleted and so the RB Release message does not need to delete them explicitly. This can lead to an incompatible TFCS configuration at the UE and UTRAN causing loss of data and ultimately a radio link failure.

Clauses affected:	⌘	8.6.5.5, 8.6.5.6										
Other specs affected:	⌘	<table border="1"><tr><th>Y</th><th>N</th></tr><tr><td>-</td><td>-</td></tr><tr><td>-</td><td>-</td></tr><tr><td>-</td><td>-</td></tr></table>	Y	N	-	-	-	-	-	-	Other core specifications	⌘
		Y	N									
		-	-									
-	-											
-	-											
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/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/>. For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.6.5.5 Added or Reconfigured UL TrCH information

If the IE "Added or Reconfigured UL TrCH information" is included then the UE shall:

- 1> for the transport channel identified by the IE "UL Transport Channel Identity" and IE "Uplink transport channel type":
 - 2> perform the actions for the IE "Transport Format Set" as specified in subclause 8.6.5.1.

Note: The UE stores the UL transport channel configuration until it is explicitly deleted by a message containing the IE "Deleted UL TrCH information" or the UE leaves RRC Connected mode.

8.6.5.6 Added or Reconfigured DL TrCH information

If the IE "Added or Reconfigured DL TrCH information" is included then for the transport channel identified by the IE "DL Transport Channel Identity" the UE shall:

- 1> if the choice "DL parameters" is set to 'explicit':
 - 2> perform the actions for the IE "Transport Format Set" as specified in subclause 8.6.5.1.
- 1> if the choice "DL parameters" is set to 'same as uplink':
 - 2> if the IE "UL Transport Channel Identity" indicates an existing or a new UL Transport Channel:
 - 3> store as transport format for this transport channel the transport format associated with the transport channel identified by the IE "UL Transport Channel Identity".
 - 2> else:
 - 3> set the variable INVALID_CONFIGURATION to TRUE.

1> if the IE "DCH quality target" is included:

- 2> perform the actions specified in subclause 8.6.5.4.

Note: The UE stores the DL transport channel configuration until it is explicitly deleted by a message containing the IE "Deleted DL TrCH information" or the UE leaves RRC connected mode.

8.6.5.7 Deleted UL TrCH information

If the IE "Deleted UL TrCH information" is included the UE shall:

- 1> delete any information about the transport channel identified by the IE "UL TrCH identity" and IE "Uplink transport channel type".

8.6.5.8 Deleted DL TrCH information

If the IE "Deleted DL TrCH information" is included the UE shall:

- 1> delete any information about the transport channel identified by the IE "DL TrCH identity".

CHANGE REQUEST

25.331 CR 2008 # rev - # Current version: **4.10.0**

For [HELP](#) on using this form, see bottom of this page or look at the pop-up text over the # symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	# Handling of transport channel information at radio bearer release		
Source:	# RAN WG2		
Work item code:	# TEI	Date:	# 18/08/2003
Category:	# A	Release:	# Rel-4
	<i>Use <u>one</u> of the following categories:</i> 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 .		<i>Use <u>one</u> of the following releases:</i> 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)

Reason for change:	# It is not sufficiently clear that the UE stores transport channel configurations until they are explicitly deleted by a message from the network, or the UE leaves RRC connected mode. In particular, some readers might assume that the transport channel configuration are explicitly deleted as radio bearer release or RRC state transition.
Summary of change:	# A note is added to clarify that the UE stores transport channel configurations until they explicitly deleted by a message containing the IE 'Deleted UL/DL TrCH information' or the UE leaves RRC connected mode. Isolated Impact Analysis: Functionality corrected: Handling of transport channel configurations Isolated impact statement: Correction to a function where specification was not sufficiently explicit. Would not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise. If either the UTRAN or the UE is not aligned to this CR then the UE and UTRAN can become de-synchronised with regard the to DCH transport channels that are currently configured for the UE. This will result in incompatible TFCS configurations at the UE and UTRAN and data loss.
Consequences if not approved:	# If the CR is not approved then UTRAN implementations may assume that when a RB is released the transport channels used by that RB are implicitly deleted and so the RB Release message does not need to delete them explicitly. This can lead to an incompatible TFCS configuration at the UE and UTRAN causing loss of data and ultimately a radio link failure.

Clauses affected:	⌘	8.6.5.5, 8.6.5.6										
Other specs affected:	⌘	<table border="1"><tr><th>Y</th><th>N</th></tr><tr><td>-</td><td>-</td></tr><tr><td>-</td><td>-</td></tr><tr><td>-</td><td>-</td></tr></table>	Y	N	-	-	-	-	-	-	Other core specifications	⌘
		Y	N									
		-	-									
-	-											
-	-											
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/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/>. For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.6.5.5 Added or Reconfigured UL TrCH information

If the IE "Added or Reconfigured UL TrCH information" is included then the UE shall:

- 1> for the transport channel identified by the IE "UL Transport Channel Identity" and IE "Uplink transport channel type":
 - 2> perform the actions for the IE "Transport Format Set" as specified in subclause 8.6.5.1.

Note: The UE stores the UL transport channel configuration until it is explicitly deleted by a message containing the IE "Deleted UL TrCH information" or the UE leaves RRC Connected mode.

8.6.5.6 Added or Reconfigured DL TrCH information

If the IE "Added or Reconfigured DL TrCH information" is included then for the transport channel identified by the IE "DL Transport Channel Identity" the UE shall:

- 1> if the choice "DL parameters" is set to 'explicit':
 - 2> perform the actions for the IE "Transport Format Set" as specified in subclause 8.6.5.1.
- 1> if the choice "DL parameters" is set to 'same as uplink':
 - 2> if the IE "UL Transport Channel Identity" indicates an existing or a new UL Transport Channel:
 - 3> store as transport format for this transport channel the transport format associated with the transport channel identified by the IE "UL Transport Channel Identity".
 - 2> else:
 - 3> set the variable INVALID_CONFIGURATION to TRUE.

1> if the IE "DCH quality target" is included:

- 2> perform the actions specified in subclause 8.6.5.4.

Note: The UE stores the DL transport channel configuration until it is explicitly deleted by a message containing the IE "Deleted DL TrCH information" or the UE leaves RRC connected mode.

8.6.5.7 Deleted UL TrCH information

If the IE "Deleted UL TrCH information" is included the UE shall:

- 1> delete any information about the transport channel identified by the IE "UL TrCH identity" and IE "Uplink transport channel type".

8.6.5.8 Deleted DL TrCH information

If the IE "Deleted DL TrCH information" is included the UE shall:

- 1> delete any information about the transport channel identified by the IE "DL TrCH identity".

CHANGE REQUEST

25.331 CR 2009 # rev - # Current version: **5.5.0**

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	# Handling of transport channel information at radio bearer release		
Source:	# RAN WG2		
Work item code:	# TEI	Date:	# 18/08/2003
Category:	# A	Release:	# Rel-5
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)		2 (GSM Phase 2)
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)
	B (addition of feature),		R97 (Release 1997)
	C (functional modification of feature)		R98 (Release 1998)
	D (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	# It is not sufficiently clear that the UE stores transport channel configurations until they are explicitly deleted by a message from the network, or the UE leaves RRC connected mode. In particular, some readers might assume that the transport channel configuration are explicitly deleted as radio bearer release or RRC state transition.
Summary of change:	# A note is added to clarify that the UE stores transport channel configurations until they explicitly deleted by a message containing the IE 'Deleted UL/DL TrCH information' or the UE leaves RRC connected mode.
	<p>Isolated Impact Analysis:</p> <p>Functionality corrected: Handling of transport channel configurations</p> <p>Isolated impact statement: Correction to a function where specification was not sufficiently explicit. Would not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.</p> <p>If either the UTRAN or the UE is not aligned to this CR then the UE and UTRAN can become de-synchronised with regard the to DCH transport channels that are currently configured for the UE. This will result in incompatible TFCS configurations at the UE and UTRAN and data loss.</p>
Consequences if not approved:	# If the CR is not approved then UTRAN implementations may assume that when a RB is released the transport channels used by that RB are implicitly deleted and so the RB Release message does not need to delete them explicitly. This can lead to an incompatible TFCS configuration at the UE and UTRAN causing loss of data and ultimately a radio link failure.

Clauses affected:	⌘	8.6.5.5, 8.6.5.6										
Other specs affected:	⌘	<table border="1"><tr><th>Y</th><th>N</th></tr><tr><td>-</td><td>-</td></tr><tr><td>-</td><td>-</td></tr><tr><td>-</td><td>-</td></tr></table>	Y	N	-	-	-	-	-	-	Other core specifications	⌘
		Y	N									
		-	-									
-	-											
-	-											
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/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/>. For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.6.5.5 Added or Reconfigured UL TrCH information

If the IE "Added or Reconfigured UL TrCH information" is included then the UE shall:

- 1> for the transport channel identified by the IE "UL Transport Channel Identity" and IE "Uplink transport channel type":
 - 2> perform the actions for the IE "Transport Format Set" as specified in subclause 8.6.5.1.

Note: The UE stores the UL transport channel configuration until it is explicitly deleted by a message containing the IE "Deleted UL TrCH information" or the UE leaves RRC Connected mode.

8.6.5.6 Added or Reconfigured DL TrCH information

If the IE "Added or Reconfigured DL TrCH information" is included then for the transport channel identified by the IE "DL Transport Channel Identity" the UE shall:

- 1> if the choice "DL parameters" is set to 'explicit':
 - 2> perform the actions for the IE "Transport Format Set" as specified in subclause 8.6.5.1.
- 1> if the choice "DL parameters" is set to 'same as uplink':
 - 2> if the IE "UL Transport Channel Identity" indicates an existing or a new UL Transport Channel:
 - 3> store as transport format for this transport channel the transport format associated with the transport channel identified by the IE "UL Transport Channel Identity".
 - 2> else:
 - 3> set the variable INVALID_CONFIGURATION to TRUE.
- 1> if the choice "DL parameters" is set to 'HSDSCH':
 - 2> if the IE "HARQ Info" is included:
 - 3> perform the actions specified in subclause 8.6.5.6b.
 - 2> if the IE "MAC-hs reset indicator" is present:
 - 3> reset the MAC-hs entity[15].
- 1> if the IE "DCH quality target" is included:
 - 2> perform the actions specified in subclause 8.6.5.4.

Note: The UE stores the DL transport channel configuration until it is explicitly deleted by a message containing the IE "Deleted DL TrCH information" or the UE leaves RRC connected mode.

8.6.5.7 Deleted UL TrCH information

If the IE "Deleted UL TrCH information" is included the UE shall:

- 1> delete any information about the transport channel identified by the IE "UL TrCH identity" and IE "Uplink transport channel type".

8.6.5.8 Deleted DL TrCH information

If the IE "Deleted DL TrCH information" is included the UE shall:

- 1> delete any information about the transport channel identified by the IE "DL TrCH identity".

CHANGE REQUEST

⌘ **25.331 CR 2010** ⌘ rev - ⌘ Current version: **3.15.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Reconfiguration with transition to CELL_PCH or URA_PCH		
Source:	⌘ RAN WG2		
Work item code:	⌘ TEI	Date:	⌘ August 25 2003
Category:	⌘ F Use <u>one</u> 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 .	Release:	⌘ R99 Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)

Reason for change:	⌘ In the current definition of the reconfiguration procedure with transition to CELL_PCH or URA_PCH two aspects seem incorrectly specified. 1. The UE is required to check if the IE "UTRAN DRX cycle length coefficient" is present in the message only after the state transition. In this case the UE is required to set the variable INVALID_CONFIGURATION to TRUE, but it is not clear how this variable will be used, since the complete message has already been sent. 2. In some circumstances the UE is required to send a CELL UPDATE/URA UPDATE message immediately after the state transition. Only after the completion of the cell update/ura update procedure the reconfiguration procedure can be considered completed. The cell update procedure, though, could result in a subsequent reconfiguration via the CELL UPDATE CONFIRM message. If the original reconfiguration procedure is still outstanding, the UE may have problems accepting a new reconfiguration from the CELL UPDATE CONFIRM message.
Summary of change:	⌘ It is proposed to correct the specification as follows: 1. The check on the presence of the IE "UTRAN DRX cycle length coefficient" shall be performed before the complete message is sent. If the IE is not present and the UE is required to transition to CELL_PCH or URA_PCH, the variable INVALID_CONFIGURATION shall be set to TRUE. 2. If a cell update is required immediately after the state transition, the reconfiguration procedure shall be considered completed after the cell update has been sent.

Isolated Impact Change Analysis.

This change clarifies the reconfiguration procedure with transition to CELL_PCH/URA_PCH.

Only the UE implementation is affected.

It would not affect implementations behaving like indicated in the CR, it would affect implementations supporting the corrected functionality otherwise.

Consequences if not approved:

- ⌘ 1. If the IE "UTRAN DRX cycle length coefficient" is not included in the reconfiguration message that sends the UE to CELL_PCH or URA_PCH, The UE will not be able to correctly complete the state transition and will not send a failure message leaving the UE in an unpredictable state. The subsequent procedure may also be affected due to the fact that the variable INVALID_CONFIGURATION is set to TRUE after the complete message is sent.
2. If UTRAN tries to perform a new reconfiguration with the CELL UPDATE CONFIRM message sent immediately after a message ordering a state transition to CELL_PCH, the UE may reject the new configuration, since the old one is not yet completed.

Clauses affected:

⌘ 8.2.2.3

Other specs affected:

Y	N		
	X	Other core specifications	⌘
	X	Test specifications	
	X	O&M Specifications	

Other comments:

⌘

How to create CRs using this form:

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

Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

[...]

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.

In case the reconfiguration procedure is used to remove all existing RL(s) in the active set while new RL(s) are established the UE shall:

- 1> perform the physical layer synchronisation procedure A as specified in [29] (FDD only);
- 1> apply the hard handover procedure as specified in subclause 8.3.5;
- 1> be able to perform this procedure even if no prior UE measurements have been performed on the target cell and/or frequency.

If the UE receives:

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

it shall:

- 1> set the variable ORDERED_RECONFIGURATION to TRUE;
- 1> if the UE will enter the CELL_DCH state from any state other than CELL_DCH state at the conclusion of this procedure:
 - 2> perform the physical layer synchronisation procedure A as specified in [29] (FDD only).
- 1> act upon all received information elements as specified in subclause 8.6, unless specified in the following and perform the actions below.

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

- 1> in FDD, if the IE "PDSCH code mapping" is included but the IE "PDSCH with SHO DCH Info" is not included and if the DCH has only one link in its active set:
 - 2> act upon the IE "PDSCH code mapping" as specified in subclause 8.6; and
 - 2> infer that the PDSCH will be transmitted from the cell from which the downlink DPCH is transmitted.
- 1> enter a state according to subclause 8.6.3.3.

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

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

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

If after state transition the UE enters CELL_DCH state, the UE shall, after the state transition:

1> in FDD; or

1> in TDD when "Primary CCPCH Info" is included indicating a new target cell and "New C-RNTI" is not specified:

2> remove any C-RNTI from MAC;

2> clear the variable C_RNTI.

In FDD, if after state transition the UE leaves CELL_DCH state, the UE shall, after the state transition:

1> remove any DSCH-RNTI from MAC;

1> clear the variable DSCH_RNTI.

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

1> if the IE "Uplink DPCH Info" is absent:

2> not change its current UL Physical channel configuration.

1> in TDD:

2> if "Primary CCPCH Info" is included indicating a new target cell and "New C-RNTI" is not specified:

3> remove any C-RNTI from MAC;

3> clear the variable C_RNTI.

If after state transition the UE enters CELL_FACH state, the UE shall, after the state transition:

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

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

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

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

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

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

2> when the cell update procedure completed successfully:

3> if the UE is in CELL_PCH or URA_PCH state:

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

4> proceed as below.

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

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

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

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

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

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

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

- 1> if the received reconfiguration message included the IE "Downlink counter synchronisation info"; or
- 1> if the received reconfiguration message is a RADIO BEARER RECONFIGURATION and the IE "New U-RNTI" is included:
 - 2> if the variable PDCP_SN_INFO is empty:
 - 3> configure the corresponding RLC entity for all AM and UM radio bearers and AM and UM signalling radio bearers except RB2 to "stop".
 - 2> else:
 - 3> configure the RLC entity for signalling radio bearers RB1, RB3 and RB4 to "stop";
 - 3> configure the RLC entity for UM and AM radio bearers for which the IE "PDCP SN Info" is not included to "stop".
- 2> re-establish RB2;

- 2> for the downlink and the uplink, apply the ciphering configuration as follows:
 - 3> if the received re-configuration message included the IE "Ciphering Mode Info":
 - 4> use the ciphering configuration in the received message when transmitting the response message.
 - 3> if the ciphering configuration for RB2 from a previously received SECURITY MODE COMMAND has not yet been applied because the activation times not having been reached:
 - 4> if the previous SECURITY MODE COMMAND was received due to new keys being received:
 - 5> consider the new ciphering configuration to include the received new keys.
 - 4> if the ciphering configuration for RB2 from a previously received SECURITY MODE COMMAND has not yet been applied because of the corresponding activation times not having been reached and the previous SECURITY MODE COMMAND caused a change in LATEST_CONFIGURED_CN_DOMAIN:
 - 5> consider the new ciphering configuration to include the keys associated with the LATEST_CONFIGURED_CN_DOMAIN.
 - 4> apply the new ciphering configuration immediately following RLC re-establishment.
 - 3> else:
 - 4> continue using the current ciphering configuration.
- 2> set the new uplink and downlink HFN component of COUNT-C of RB2 to MAX(uplink HFN component of COUNT-C of RB2, downlink HFN component of COUNT-C of RB2);
- 2> increment by one the downlink and uplink values of the HFN component of COUNT-C for RB2;
- 2> calculate the START value according to subclause 8.5.9;
- 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message did not include the IE "Downlink counter synchronisation info":
 - 2> if the variable START_VALUE_TO_TRANSMIT is set:
 - 3> include and set the IE "START" to the value of that variable.
 - 2> if the variable START_VALUE_TO_TRANSMIT is not set and the IE "New U-RNTI" is included:
 - 3> calculate the START value according to subclause 8.5.9;
 - 3> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
- 2> if the received reconfiguration message caused a change in the RLC size for any RB using RLC-AM:
 - 3> calculate the START value according to subclause 8.5.9;
 - 3> include the calculated START values for the CN domain associated with the corresponding RB identity in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
 - 2> set the IE "Status" in the variable SECURITY_MODIFICATION for all the CN domains in the variable SECURITY_MODIFICATION to "Affected".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info":
 - 2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.

- 1> if the received reconfiguration message did not contain the IE "Ciphering activation time for DPCH":
 - 2> if prior to this procedure there exist no transparent mode RLC radio bearers for the CN domain indicated in the IE "CN domain identity" in the IE "RAB info":
 - 3> if, at the conclusion of this procedure, the UE will be in CELL_DCH state; and
 - 3> if, at the conclusion of this procedure, at least one transparent mode RLC radio bearer exists for the CN domain indicated in the IE "CN domain identity" in the IE "RAB info":
 - 4> include the IE "COUNT-C activation time" and specify a CFN value for this IE that is a multiple of 8 frames ($CFN \bmod 8 = 0$) and lies at least 200 frames ahead of the CFN in which the response message is first transmitted.

NOTE: UTRAN should not include the IE "Ciphering mode info" in any reconfiguration message unless it is also used to perform an SRNS relocation with change of ciphering algorithm.

- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the received message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> if the variable PDCP_SN_INFO is not empty:
 - 2> include the IE "RB with PDCP information list" and set it to the value of the variable PDCP_SN_INFO.
- 1> in TDD, if the procedure is used to perform a handover to a cell where timing advance is enabled, and the UE can calculate the timing advance value in the new cell (i.e. in a synchronous TDD network):
 - 2> set the IE "Uplink Timing Advance" according to subclause 8.6.6.26.
- 1> if the IE "Integrity protection mode info" was present in the received reconfiguration message:
 - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.

If after state transition the UE enters CELL_PCH or URA_PCH state, the UE shall, after the state transition and transmission of the response message:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
 - 2> select a suitable UTRA cell according to [4] on that frequency.
- 1> if the IE "Frequency info" is not included in the received reconfiguration message:
 - 2> select a suitable UTRA cell according to [4].
- 1> prohibit periodical status transmission in RLC;
- 1> remove any C-RNTI from MAC;
- 1> clear the variable C_RNTI;
- 1> start timer T305 using its initial value if timer T305 is not running and if periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" in the variable TIMERS_AND_CONSTANTS;
- 1> select Secondary CCPCCH according to subclause 8.5.19;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
 - 2> use the value in the IE "UTRAN DRX Cycle length coefficient" for calculating Paging occasion and PICH Monitoring Occasion as specified in subclause 8.6.3.2.

~~1> if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:~~

~~2> set the variable INVALID_CONFIGURATION to TRUE.~~

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

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

~~2> when the cell update procedure completed successfully:~~

~~32>~~ the procedure ends. [\[Editor's note: Style changed to B2\]](#)

1> if the UE enters CELL_PCH state from CELL_FACH state, and the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE:

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

~~2> when the cell update procedure is successfully completed:~~

~~32>~~ the procedure ends. [\[Editor's note: Style changed to B2\]](#)

1> if the UE enters URA_PCH state, and after cell selection the criteria for URA update caused by "URA reselection" according to subclause 8.3.1 is fulfilled:

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

2> when the URA update procedure is successfully completed:

3> the procedure ends.

[...]

CHANGE REQUEST

25.331 CR 2011 # rev - # Current version: 4.10.0

For [HELP](#) on using this form, see bottom of this page or look at the pop-up text over the # symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	# Reconfiguration with transition to CELL_PCH or URA_PCH		
Source:	# RAN WG2		
Work item code:	# TEI	Date:	# August 25 2003
Category:	# A	Release:	# Rel-4
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)		2 (GSM Phase 2)
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)
	B (addition of feature),		R97 (Release 1997)
	C (functional modification of feature)		R98 (Release 1998)
	D (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	# In the current definition of the reconfiguration procedure with transition to CELL_PCH or URA_PCH two aspects seem incorrectly specified.
	<p>1. The UE is required to check if the IE "UTRAN DRX cycle length coefficient" is present in the message only after the state transition. In this case the UE is required to set the variable INVALID_CONFIGURATION to TRUE, but it is not clear how this variable will be used, since the complete message has already been sent.</p> <p>2. In some circumstances the UE is required to send a CELL UPDATE/URA UPDATE message immediately after the state transition. Only after the completion of the cell update/ura update procedure the reconfiguration procedure can be considered completed. The cell update procedure, though, could result in a subsequent reconfiguration via the CELL UPDATE CONFIRM message. If the original reconfiguration procedure is still outstanding, the UE may have problems accepting a new reconfiguration from the CELL UPDATE CONFIRM message.</p>
Summary of change:	# It is proposed to correct the specification as follows:
	<p>1. The check on the presence of the IE "UTRAN DRX cycle length coefficient" shall be performed before the complete message is sent. If the IE is not present and the UE is required to transition to CELL_PCH or URA_PCH, the variable INVALID_CONFIGURATION shall be set to TRUE.</p> <p>2. If a cell update is required immediately after the state transition, the reconfiguration procedure shall be considered completed after the cell update has been sent.</p>

Isolated Impact Change Analysis.

This change clarifies the reconfiguration procedure with transition to CELL_PCH/URA_PCH.
Only the UE implementation is affected.
It would not affect implementations behaving like indicated in the CR, it would affect implementations supporting the corrected functionality otherwise.

Consequences if not approved:

- ⌘ 1. If the IE "UTRAN DRX cycle length coefficient" is not included in the reconfiguration message that sends the UE to CELL_PCH or URA_PCH, The UE will not be able to correctly complete the state transition and will not send a failure message leaving the UE in an unpredictable state. The subsequent procedure may also be affected due to the fact that the variable INVALID_CONFIGURATION is set to TRUE after the complete message is sent.
- 2. If UTRAN tries to perform a new reconfiguration with the CELL UPDATE CONFIRM message sent immediately after a message ordering a state transition to CELL_PCH, the UE may reject the new configuration, since the old one is not yet completed.

Clauses affected:

⌘ 8.2.2.3

Other specs affected:

Y	N	
	X	Other core specifications
	X	Test specifications
	X	O&M Specifications

⌘

Other comments:

⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

[...]

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;

In case the reconfiguration procedure is used to remove all existing RL(s) in the active set while new RL(s) are established the UE shall:

- 1> perform the physical layer synchronisation procedure A as specified in [29] (FDD only);
- 1> apply the hard handover procedure as specified in subclause 8.3.5;
- 1> be able to perform this procedure even if no prior UE measurements have been performed on the target cell and/or frequency.

If the UE receives:

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

it shall:

- 1> set the variable ORDERED_RECONFIGURATION to TRUE;
- 1> if the UE will enter the CELL_DCH state from any state other than CELL_DCH state at the conclusion of this procedure:
 - 2> perform the physical layer synchronisation procedure A as specified in [29] (FDD only).
- 1> act upon all received information elements as specified in subclause 8.6, unless specified in the following and perform the actions below.

The UE may:

- 1> maintain a list of the set of cells to which the UE has Radio Links if the IE "Cell ID" is present.

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

- 1> in FDD, if the IE "PDSCH code mapping" is included but the IE "PDSCH with SHO DCH Info" is not included and if the DCH has only one link in its active set:
 - 2> act upon the IE "PDSCH code mapping" as specified in subclause 8.6; and
 - 2> infer that the PDSCH will be transmitted from the cell from which the downlink DPCH is transmitted.

1> enter a state according to subclause 8.6.3.3.

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

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

NOTE: The Release '99 RADIO BEARER RECONFIGURATION message always includes the IE "RB information to reconfigure". UTRAN has to include it even if it does not require the reconfiguration of any RB.

If after state transition the UE enters CELL_DCH state, the UE shall, after the state transition:

1> in FDD; or

1> in TDD when "Primary CCPCH Info" is included indicating a new target cell and "New C-RNTI" is not specified:

2> remove any C-RNTI from MAC;

2> clear the variable C_RNTI.

In FDD, if after state transition the UE leaves CELL_DCH state, the UE shall, after the state transition:

1> remove any DSCH-RNTI from MAC;

1> clear the variable DSCH_RNTI.

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

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

1> in TDD:

2> if "Primary CCPCH Info" is included indicating a new target cell and "New C-RNTI" is not specified:

3> remove any C-RNTI from MAC;

3> clear the variable C_RNTI. If after state transition the UE enters CELL_FACH state, the UE shall, after the state transition:

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

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

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

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

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

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

2> when the cell update procedure completed successfully:

3> if the UE is in CELL_PCH or URA_PCH state:

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

4> proceed as below.

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

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

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

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

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

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

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

- 1> if the received reconfiguration message included the IE "Downlink counter synchronisation info"; or
- 1> if the received reconfiguration message is a RADIO BEARER RECONFIGURATION and the IE "New U-RNTI" is included:
 - 2> if the variable PDCP_SN_INFO is empty:
 - 3> configure the corresponding RLC entity for all AM and UM radio bearers and AM and UM signalling radio bearers except RB2 to "stop".
 - 2> else:
 - 3> configure the RLC entity for signalling radio bearers RB1, RB3 and RB4 to "stop";
 - 3> configure the RLC entity for UM and AM radio bearers for which the IE "PDCP SN Info" is not included to "stop".
- 2> re-establish RB2;

- 2> for the downlink and the uplink, apply the ciphering configuration as follows:
 - 3> if the received re-configuration message included the IE "Ciphering Mode Info":
 - 4> use the ciphering configuration in the received message when transmitting the response message.
 - 3> if the ciphering configuration for RB2 from a previously received SECURITY MODE COMMAND has not yet been applied because the activation times not having been reached:
 - 4> if the previous SECURITY MODE COMMAND was received due to new keys being received:
 - 5> consider the new ciphering configuration to include the received new keys.
 - 4> if the ciphering configuration for RB2 from a previously received SECURITY MODE COMMAND has not yet been applied because of the corresponding activation times not having been reached and the previous SECURITY MODE COMMAND caused a change in LATEST_CONFIGURED_CN_DOMAIN:
 - 5> consider the new ciphering configuration to include the keys associated with the LATEST_CONFIGURED_CN_DOMAIN.
 - 4> apply the new ciphering configuration immediately following RLC re-establishment.
 - 3> else:
 - 4> continue using the current ciphering configuration.
- 2> set the new uplink and downlink HFN component of COUNT-C of RB2 to MAX(uplink HFN component of COUNT-C of RB2, downlink HFN component of COUNT-C of RB2);
- 2> increment by one the downlink and uplink values of the HFN component of COUNT-C for RB2;
- 2> calculate the START value according to subclause 8.5.9;
- 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message did not include the IE "Downlink counter synchronisation info":
 - 2> if the variable START_VALUE_TO_TRANSMIT is set:
 - 3> include and set the IE "START" to the value of that variable.
 - 2> if the variable START_VALUE_TO_TRANSMIT is not set and the IE "New U-RNTI" is included:
 - 3> calculate the START value according to subclause 8.5.9;
 - 3> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
- 2> if the received reconfiguration message caused a change in the RLC size for any RB using RLC-AM:
 - 3> calculate the START value according to subclause 8.5.9;
 - 3> include the calculated START values for the CN domain associated with the corresponding RB identity in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
 - 2> set the IE "Status" in the variable SECURITY_MODIFICATION for all the CN domains in the variable SECURITY_MODIFICATION to "Affected".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info":
 - 2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.

- 1> if the received reconfiguration message did not contain the IE "Ciphering activation time for DPCH":
 - 2> if prior to this procedure there exist no transparent mode RLC radio bearers for the CN domain indicated in the IE "CN domain identity" in the IE "RAB info":
 - 3> if, at the conclusion of this procedure, the UE will be in CELL_DCH state; and
 - 3> if, at the conclusion of this procedure, at least one transparent mode RLC radio bearer exists for the CN domain indicated in the IE "CN domain identity" in the IE "RAB info":
 - 4> include the IE "COUNT-C activation time" and specify a CFN value for this IE that is a multiple of 8 frames ($CFN \bmod 8 = 0$) and lies at least 200 frames ahead of the CFN in which the response message is first transmitted.

NOTE: UTRAN should not include the IE "Ciphering mode info" in any reconfiguration message unless it is also used to perform an SRNS relocation with change of ciphering algorithm.

- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the received message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> if the variable PDCP_SN_INFO is not empty:
 - 2> include the IE "RB with PDCP information list" and set it to the value of the variable PDCP_SN_INFO.
- 1> in TDD, if the procedure is used to perform a handover to a cell where timing advance is enabled, and the UE can calculate the timing advance value in the new cell (i.e. in a synchronous TDD network):
 - 2> set the IE "Uplink Timing Advance" according to subclause 8.6.6.26.
- 1> if the IE "Integrity protection mode info" was present in the received reconfiguration message:
 - 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.

If after state transition the UE enters CELL_PCH or URA_PCH state, the UE shall, after the state transition and transmission of the response message:

- 1> if the IE "Frequency info" is included in the received reconfiguration message:
 - 2> select a suitable UTRA cell according to [4] on that frequency.
- 1> if the IE "Frequency info" is not included in the received reconfiguration message:
 - 2> select a suitable UTRA cell according to [4].
- 1> prohibit periodical status transmission in RLC;
- 1> remove any C-RNTI from MAC;
- 1> clear the variable C_RNTI;
- 1> start timer T305 using its initial value if timer T305 is not running and if periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" in the variable TIMERS_AND_CONSTANTS;
- 1> select Secondary CCPCCH according to subclause 8.5.19;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
 - 2> use the value in the IE "UTRAN DRX Cycle length coefficient" for calculating Paging occasion and PICH Monitoring Occasion as specified in subclause 8.6.3.2.

~~1> if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:~~

~~2> set the variable INVALID_CONFIGURATION to TRUE.~~

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

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

~~2> when the cell update procedure completed successfully:~~

~~3>~~ the procedure ends. [\[Editor's note: Style changed to B2\]](#)

1> if the UE enters CELL_PCH state from CELL_FACH state, and the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE:

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

~~2> when the cell update procedure is successfully completed:~~

~~3>~~ the procedure ends. [\[Editor's note: Style changed to B2\]](#)

1> if the UE enters URA_PCH state, and after cell selection the criteria for URA update caused by "URA reselection" according to subclause 8.3.1 is fulfilled:

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

2> when the URA update procedure is successfully completed:

3> the procedure ends.

[...]

CHANGE REQUEST

25.331 CR 2012 # rev - # Current version: **5.5.0**

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

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# Reconfiguration with transition to CELL_PCH or URA_PCH		
Source:	# RAN WG2		
Work item code:	# TEI	Date:	# August 25 2003
Category:	# A	Release:	# Rel-5
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)		2 (GSM Phase 2)
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)
	B (addition of feature),		R97 (Release 1997)
	C (functional modification of feature)		R98 (Release 1998)
	D (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	# In the current definition of the reconfiguration procedure with transition to CELL_PCH or URA_PCH two aspects seem incorrectly specified.
	<p>1. The UE is required to check if the IE "UTRAN DRX cycle length coefficient" is present in the message only after the state transition. In this case the UE is required to set the variable INVALID_CONFIGURATION to TRUE, but it is not clear how this variable will be used, since the complete message has already been sent.</p> <p>2. In some circumstances the UE is required to send a CELL_UPDATE/URA_UPDATE message immediately after the state transition. Only after the completion of the cell update/ura update procedure the reconfiguration procedure can be considered completed. The cell update procedure, though, could result in a subsequent reconfiguration via the CELL_UPDATE_CONFIRM message. If the original reconfiguration procedure is still outstanding, the UE may have problems accepting a new reconfiguration from the CELL_UPDATE_CONFIRM message.</p>
Summary of change:	# It is proposed to correct the specification as follows:
	<p>1. The check on the presence of the IE "UTRAN DRX cycle length coefficient" shall be performed before the complete message is sent. If the IE is not present and the UE is required to transition to CELL_PCH or URA_PCH, the variable INVALID_CONFIGURATION shall be set to TRUE.</p> <p>2. If a cell update is required immediately after the state transition, the reconfiguration procedure shall be considered completed after the cell update has been sent.</p>

Isolated Impact Change Analysis.

This change clarifies the reconfiguration procedure with transition to CELL_PCH/URA_PCH.
Only the UE implementation is affected.
It would not affect implementations behaving like indicated in the CR, it would affect implementations supporting the corrected functionality otherwise.

Consequences if not approved:

- ⌘ 1. If the IE "UTRAN DRX cycle length coefficient" is not included in the reconfiguration message that sends the UE to CELL_PCH or URA_PCH, The UE will not be able to correctly complete the state transition and will not send a failure message leaving the UE in an unpredictable state. The subsequent procedure may also be affected due to the fact that the variable INVALID_CONFIGURATION is set to TRUE after the complete message is sent.
- 2. If UTRAN tries to perform a new reconfiguration with the CELL UPDATE CONFIRM message sent immediately after a message ordering a state transition to CELL_PCH, the UE may reject the new configuration, since the old one is not yet completed.

Clauses affected:

⌘ 8.2.2.3

Other specs affected:

Y	N	
	X	Other core specifications
	X	Test specifications
	X	O&M Specifications

⌘

Other comments:

⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

[...]

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:

- 1> be able to receive any of the following messages:
 - 2> RADIO BEARER SETUP message; or
 - 2> RADIO BEARER RECONFIGURATION message; or
 - 2> RADIO BEARER RELEASE message; or
 - 2> TRANSPORT CHANNEL RECONFIGURATION message; or
 - 2> PHYSICAL CHANNEL RECONFIGURATION message;
- 1> perform a hard handover and apply physical layer synchronisation procedure A as specified in [29], even if no prior UE measurements have been performed on the target cell and/or frequency.

If the UE receives:

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

it shall:

- 1> set the variable ORDERED_RECONFIGURATION to TRUE;
- 1> if the UE will enter the CELL_DCH state from any state other than CELL_DCH state at the conclusion of this procedure:
 - 2> perform the physical layer synchronisation procedure A as specified in [29] (FDD only).
- 1> act upon all received information elements as specified in subclause 8.6, unless specified in the following and perform the actions below.

The UE may:

- 1> maintain a list of the set of cells to which the UE has Radio Links if the IE "Cell ID" is present.

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

- 1> in FDD, if the IE "PDSCH code mapping" is included but the IE "PDSCH with SHO DCH Info" is not included and if the DCH has only one link in its active set:
 - 2> act upon the IE "PDSCH code mapping" as specified in subclause 8.6; and
 - 2> infer that the PDSCH will be transmitted from the cell from which the downlink DPCH is transmitted.
- 1> enter a state according to subclause 8.6.3.3.

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

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

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

If after state transition the UE enters CELL_DCH state, the UE shall, after the state transition:

1> remove any C-RNTI from MAC;

1> clear the variable C_RNTI.

If after state transition the UE leaves CELL_DCH state, the UE shall, after the state transition:

1> stop any HS-DSCH reception procedures according to the stored HS-PDSCH configuration;

1> clear any stored HS-PDSCH configuration;

1> remove any H-RNTI stored;

1> clear the variable H_RNTI;

1> set the variable HS_DSCH_RECEPTION to FALSE.

In FDD, if after state transition the UE leaves CELL_DCH state, the UE shall, after the state transition:

1> remove any DSCH-RNTI from MAC;

1> clear the variable DSCH_RNTI.

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

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

1> if "DPCH frame offset" is included for one or more RLS in the active set:

2> use its value to determine the beginning of the DPCH frame in accordance with the following:

3> if the received IE "DPCH frame offset" is across the value range border compared to the DPCH frame offset currently used by the UE:

4> consider it to be a request to adjust the timing with 256 chips across the frame border (e.g. if the UE receives value 0 while the value currently used is 38144 consider this as a request to adjust the timing with +256 chips).

3> if after taking into account value range borders, the received IE "DPCH frame offset" corresponds to a request to adjust the timing with a step exceeding 256 chips:

4> set the variable INVALID_CONFIGURATION to TRUE.

3> and the procedure ends.

2> adjust the radio link timing accordingly.

If after state transition the UE enters CELL_FACH state, the UE shall, after the state transition:

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

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

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

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

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

- 2> initiate a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";
- 2> when the cell update procedure completed successfully:
 - 3> if the UE is in CELL_PCH or URA_PCH state:
 - 4> initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
 - 4> proceed as below.
- 1> start timer T305 using its initial value if timer T305 is not running and if periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" in system information block type 1;
- 1> select PRACH according to subclause 8.5.17;
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> use the transport format set given in system information;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
 - 2> ignore that IE and stop using DRX.
- 1> if the contents of the variable C_RNTI is empty:
 - 2> perform a cell update procedure according to subclause 8.3.1 using the cause "Cell reselection";
 - 2> when the cell update procedure completed successfully:
 - 3> if the UE is in CELL_PCH or URA_PCH state:
 - 4> initiate a cell update procedure according to subclause 8.3.1 using the cause "Uplink data transmission";
 - 4> proceed as below.

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

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

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

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

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

- 1> if the received reconfiguration message included the IE "Downlink counter synchronisation info"; or

- 1> if the received reconfiguration message is a RADIO BEARER RECONFIGURATION and the IE "New U-RNTI" is included:
 - 2> if the variable PDCP_SN_INFO is empty:
 - 3> configure the corresponding RLC entity for all AM and UM radio bearers and AM and UM signalling radio bearers except RB2 to "stop".
 - 2> else:
 - 3> configure the RLC entity for signalling radio bearers RB1, RB3 and RB4 to "stop";
 - 3> configure the RLC entity for UM and AM radio bearers for which the IE "PDCP SN Info" is not included to "stop".
 - 2> re-establish RB2;
 - 2> for the downlink and the uplink, apply the ciphering configuration as follows:
 - 3> if the received re-configuration message included the IE "Ciphering Mode Info":
 - 4> use the ciphering configuration in the received message when transmitting the response message.
 - 3> if the ciphering configuration for RB2 from a previously received SECURITY MODE COMMAND has not yet been applied because the activation times not having been reached:
 - 4> if the previous SECURITY MODE COMMAND was received due to new keys being received:
 - 5> consider the new ciphering configuration to include the received new keys.
 - 4> if the ciphering configuration for RB2 from a previously received SECURITY MODE COMMAND has not yet been applied because of the corresponding activation times not having been reached and the previous SECURITY MODE COMMAND caused a change in LATEST_CONFIGURED_CN_DOMAIN:
 - 5> consider the new ciphering configuration to include the keys associated with the LATEST_CONFIGURED_CN_DOMAIN.
 - 4> apply the new ciphering configuration immediately following RLC re-establishment.
 - 3> else:
 - 4> continue using the current ciphering configuration.
 - 2> set the new uplink and downlink HFN component of COUNT-C of RB2 to MAX(uplink HFN component of COUNT-C of RB2, downlink HFN component of COUNT-C of RB2);
 - 2> increment by one the downlink and uplink values of the HFN component of COUNT-C for RB2;
 - 2> calculate the START value according to subclause 8.5.9;
 - 2> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message did not include the IE "Downlink counter synchronisation info":
 - 2> if the variable START_VALUE_TO_TRANSMIT is set:
 - 3> include and set the IE "START" to the value of that variable.
 - 2> if the variable START_VALUE_TO_TRANSMIT is not set and the IE "New U-RNTI" is included:
 - 3> calculate the START value according to subclause 8.5.9;
 - 3> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info".
 - 2> if the received reconfiguration message caused a change in the RLC size for any RB using RLC-AM:

- 3> calculate the START value according to subclause 8.5.9;
 - 3> include the calculated START values for the CN domain associated with the corresponding RB identity in the IE "START list" in the IE "Uplink counter synchronisation info".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info" or contained the IE "Integrity protection mode info":
- 2> set the IE "Status" in the variable SECURITY_MODIFICATION for all the CN domains in the variable SECURITY_MODIFICATION to "Affected".
- 1> if the received reconfiguration message contained the IE "Ciphering mode info":
- 2> include and set the IE "Radio bearer uplink ciphering activation time info" to the value of the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO.
- 1> if the received reconfiguration message did not contain the IE "Ciphering activation time for DPCH":
- 2> if prior to this procedure there exist no transparent mode RLC radio bearers for the CN domain indicated in the IE "CN domain identity" in the IE "RAB info":
 - 3> if, at the conclusion of this procedure, the UE will be in CELL_DCH state; and
 - 3> if, at the conclusion of this procedure, at least one transparent mode RLC radio bearer exists for the CN domain indicated in the IE "CN domain identity" in the IE "RAB info":
 - 4> include the IE "COUNT-C activation time" and specify a CFN value for this IE that is a multiple of 8 frames ($CFN \bmod 8 = 0$) and lies at least 200 frames ahead of the CFN in which the response message is first transmitted.

NOTE: UTRAN should not include the IE "Ciphering mode info" in any reconfiguration message unless it is also used to perform an SRNS relocation with change of ciphering algorithm.

- 1> set the IE "RRC transaction identifier" to the value of "RRC transaction identifier" in the entry for the received message in the table "Accepted transactions" in the variable TRANSACTIONS; and
- 1> clear that entry;
- 1> if the variable PDCP_SN_INFO is not empty:
- 2> include the IE "RB with PDCP information list" and set it to the value of the variable PDCP_SN_INFO.
- 1> in TDD, if the procedure is used to perform a handover to a cell where timing advance is enabled, and the UE can calculate the timing advance value in the new cell (i.e. in a synchronous TDD network):
- 2> set the IE "Uplink Timing Advance" according to subclause 8.6.6.26.
- 1> if the IE "Integrity protection mode info" was present in the received reconfiguration message:
- 2> start applying the new integrity protection configuration in the uplink for signalling radio bearer RB2 from and including the transmitted response message.

If after state transition the UE enters CELL_PCH or URA_PCH state, the UE shall, after the state transition and transmission of the response message:

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

- 1> clear the variable C_RNTI;
- 1> start timer T305 using its initial value if timer T305 is not running and if periodical update has been configured by T305 in the IE "UE Timers and constants in connected mode" set to any other value than "infinity" in the variable TIMERS_AND_CONSTANTS;
- 1> select Secondary CCPCH according to subclause 8.5.19;
- 1> if the IE "UTRAN DRX cycle length coefficient" is included in the same message:
 - 2> use the value in the IE "UTRAN DRX Cycle length coefficient" for calculating Paging occasion and PICH Monitoring Occasion as specified in subclause 8.6.3.2.

~~1> if the IE "UTRAN DRX cycle length coefficient" is not included in the same message:~~

~~2> set the variable INVALID_CONFIGURATION to TRUE.~~

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

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

~~2> when the cell update procedure completed successfully:~~

~~32> the procedure ends. [\[Editor's note: Style changed to B2\]](#)~~

- 1> if the UE enters CELL_PCH state from CELL_FACH state, and the received reconfiguration message included the IE "Primary CPICH info" (for FDD) or "Primary CCPCH info" (for TDD), and the UE selected another cell than indicated by this IE:

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

~~2> when the cell update procedure is successfully completed:~~

~~32> the procedure ends. [\[Editor's note: Style changed to B2\]](#)~~

- 1> if the UE enters URA_PCH state, and after cell selection the criteria for URA update caused by "URA reselection" according to subclause 8.3.1 is fulfilled:

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

- 2> when the URA update procedure is successfully completed:

- 3> the procedure ends.

[...]