TSG-RAN Meeting #20 *RP-030369*
Hämeenlinna, Finland, 03-06 June 2003

Title: **Revision of CRs 1976, 1977 and 1978 on Ciphering Mode info IE in 2G-3G Handover**

Source: **Ericsson, Motorola**

Agenda item: **7.2**

Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Version-New	Workitem
25.331	1976	4	R99	Ciphering Mode info IE in 2G-3G Handover	F	3.14.0	3.15.0	TEI
25.331	1977	4	Rel-4	Ciphering Mode info IE in 2G-3G Handover	A	4.9.0	4.10.0	TEI
25.331	1978	4	Rel-5	Ciphering Mode info IE in 2G-3G Handover	A	5.4.0	5.5.0	TEI

3GPP TSG RAN Meeting #20
Hämeenlinna, Finland, 3 - 6 June, 2003

Tdoc ⌘RP-030369

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1976**	⌘**rev**	**4**	⌘	Current version:	**3.e.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:	⌘ Ciphering Mode info IE in 2G-3G Handover		
Source:	⌘ Ericsson, Motorola		
Work item code:	⌘ TEI	***Date:*** ⌘	02/06/2003
Category:	⌘ **F**	***Release:*** ⌘	R99
	Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change: ⌘	Currently section 8.6.5-33.102 states that upon handover to 3G the Serving RNC sends the Security Mode Command to setup Integrity. However, it is not stated if the SMC should include ciphering information or not. The inclusion of ciphering information under these conditions is a potential problem for UE implementations. Currently, it is mandated that for the UE to set the ciphering activation time on the HANDOVER TO UTRAN COMPLETE message to a value that is at least 200 frames in advance and lies on an 80ms TTI boundary. If the activation time for TM bearers is chosen such that it would trigger the usage of a new ciphering configuration before the HFN starts being incremented, the UE actions are not defined in the current specification. Currently, in case UE receives a new security key set while connected via another RAT, it is not clear what START value that UE shall associate with this new key set. Currently, it is not clear that UE, after a handovr to UTRAN, shall continue to use the key set currently in use in the other RAT.
Summary of change: ⌘	It is clarified that the UTRAN should not send the Ciphering Mode Info IE again, until all ciphering activation times for RBs using RLC-TM of the concerned CN domain have expired. It is clarified that UTRAN should not include IE Ciphering Mode Info in the Security Mode Command to start Integrity Protection. It is clarified that UE shall associate the START values sent in HANDOVER TO UTRAN COMPLETE with the key set in use at the handover to UTRAN.

		It is clarified that UE, after a handover to UTRAN, shall continue to use the key set in use in the other RAT prior to handover. It is clarified that the actions for new keys is to be performed only in the case where the new keys are received (i.e. Authentication performed) for the on-going signaling connection. **Impact Analysis:** This CR only affects functionality covered by "Consequences if not approved"
Consequences if not approved:	⌘	The UTRAN may send a SECURITY MODE COMMAND message (e.g. when starting Integrity protection) which contains a ciphering reconfiguration. If this reconfiguration occurs before all the pending ciphering activation times have elapsed, it will have an unpredictable result (i.e. The UE behaviour is not specified) and loss of ciphering synchronisation between UE and UTRAN may occur. UE (or UTRAN) may apply the wrong START value for ciphering or ciphering key in UTRAN if new keys are received in GSM.

Clauses affected:	⌘	8.1.12.3.1, 8.3.6.3				
		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.

8.1.12.3.1 New ciphering and integrity protection keys

NOTE: The actions in this sub-clause are to be performed only if the new keys were received for an on-going 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 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: ~~New keys received~~Reception of new keys while in another RAT does not trigger the actions in 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> 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> 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.

3GPP TSG RAN Meeting #20
Hämeenlinna, Finland, 3 - 6 June, 2003

Tdoc ⌘RP-030369

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1977**	⌘**rev**	**4**	⌘	Current version:	**4.9.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☒ Core Network ☐

Title:	⌘ Ciphering Mode info IE in 2G-3G Handover			
Source:	⌘ Ericsson, Motorola			
Work item code:	⌘ TEI		***Date:*** ⌘	02/06/2003
Category:	⌘ **A**		***Release:*** ⌘	Rel-4

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

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘ Currently section 8.6.5-33.102 states that upon handover to 3G the Serving RNC sends the Security Mode Command to setup Integrity. However, it is not stated if the SMC should include ciphering information or not.

The inclusion of ciphering information under these conditions is a potential problem for UE implementations. Currently, it is mandated that for the UE to set the ciphering activation time on the HANDOVER TO UTRAN COMPLETE message to a value that is at least 200 frames in advance and lies on an 80ms TTI boundary. If the activation time for TM bearers is chosen such that it would trigger the usage of a new ciphering configuration before the HFN starts being incremented, the UE actions are not defined in the current specification.

Currently, in case UE receives a new security key set while connected via another RAT, it is not clear what START value that UE shall associate with this new key set.

Currently, it is not clear that UE, after a handovr to UTRAN, shall continue to use the key set currently in use in the other RAT.

Summary of change: ⌘ It is clarified that the UTRAN should not send the Ciphering Mode Info IE again, until all ciphering activation times for RBs using RLC-TM of the concerned CN domain have expired.

It is clarified that UTRAN should not include IE Ciphering Mode Info in the Security Mode Command to start Integrity Protection.

It is clarified that UE shall associate the START values sent in HANDOVER TO UTRAN COMPLETE with the key set in use at the handover to UTRAN.

It is clarified that UE, after a handover to UTRAN, shall continue to use the key set in use in the other RAT prior to handover.
It is clarified that the actions for new keys is to be performed only in the case where the new keys are received (i.e. Authentication performed) for the on-going signaling connection.

Impact Analysis:
This CR only affects UTRAN and its impact is covered by “Consequences if not approved”

Consequences if not approved: ⌘ The UTRAN may send a SECURITY MODE COMMAND message (e.g. when starting Integrity protection) which contains a ciphering reconfiguration. If this reconfiguration occurs before all the pending ciphering activation times have elapsed, it will have an unpredictable result (i.e. The UE behaviour is not specified) and loss of ciphering synchronisation between UE and UTRAN may occur.

UE (or UTRAN) may apply the wrong START value for ciphering or ciphering key in UTRAN if new keys are received in GSM.

Clauses affected: ⌘ 8.1.12.3.1, 8.3.6.3

	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.

8.1.12.3.1 New ciphering and integrity protection keys

NOTE: The actions in this sub-clause are to be performed only if the new keys were received for an on-going 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 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: ~~New keys received~~Reception of new keys while in another RAT does not trigger the actions in 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> 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> 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.

3GPP TSG RAN Meeting #20
Hämeenlinna, Finland, 3 - 6 June, 2003

Tdoc ⌘RP-030369

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1978**	⌘**rev**	**4**	⌘	Current version:	**5.4.0** ⌘

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

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network ☒ Core Network □

Title:	⌘ Ciphering Mode info IE in 2G-3G Handover		
Source:	⌘ Ericsson, Motorola		
Work item code:	⌘ TEI	***Date:*** ⌘	02/06/2003
Category:	⌘ **A**	***Release:*** ⌘	Rel-5

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘ Currently section 8.6.5-33.102 states that upon handover to 3G the Serving RNC sends the Security Mode Command to setup Integrity. However, it is not stated if the SMC should include ciphering information or not.

The inclusion of ciphering information under these conditions is a potential problem for UE implementations. Currently, it is mandated that for the UE to set the ciphering activation time on the HANDOVER TO UTRAN COMPLETE message to a value that is at least 200 frames in advance and lies on an 80ms TTI boundary. If the activation time for TM bearers is chosen such that it would trigger the usage of a new ciphering configuration before the HFN starts being incremented, the UE actions are not defined in the current specification.

Currently, in case UE receives a new security key set while connected via another RAT, it is not clear what START value that UE shall associate with this new key set.

Currently, it is not clear that UE, after a handovr to UTRAN, shall continue to use the key set currently in use in the other RAT.

Summary of change: ⌘ It is clarified that the UTRAN should not send the Ciphering Mode Info IE again, until all ciphering activation times for RBs using RLC-TM of the concerned CN domain have expired.

It is clarified that UTRAN should not include IE Ciphering Mode Info in the Security Mode Command to start Integrity Protection.

It is clarified that UE shall associate the START values sent in HANDOVER TO UTRAN COMPLETE with the key set in use at the handover to UTRAN.

		It is clarified that UE, after a handover to UTRAN, shall continue to use the key set in use in the other RAT prior to handover. It is clarified that the actions for new keys is to be performed only in the case where the new keys are received (i.e. Authentication performed) for the on-going signaling connection. **Impact Analysis:** This CR only affects UTRAN and its impact is covered by "Consequences if not approved"
Consequences if not approved:	⌘	The UTRAN may send a SECURITY MODE COMMAND message (e.g. when starting Integrity protection) which contains a ciphering reconfiguration. If this reconfiguration occurs before all the pending ciphering activation times have elapsed, it will have an unpredictable result (i.e. The UE behaviour is not specified) and loss of ciphering synchronisation between UE and UTRAN may occur. UE (or UTRAN) may apply the wrong START value for ciphering or ciphering key in UTRAN if new keys are received in GSM.

Clauses affected:	⌘	8.1.12.3.1, 8.3.6.3				
		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.

8.1.12.3.1 New ciphering and integrity protection keys

NOTE: The actions in this sub-clause are to be performed only if the new keys were received for an on-going 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 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: ~~New keys received~~Reception of new keys while in another RAT does not trigger the actions in 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> 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> 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.