TSG-RAN Meeting #28
Quebec, Canada, 01-03 June 2005

RP-050304
agenda item 7.3.5

Source: TSG-RAN WG2

Title: 25.331 CRs (Rel-5 & Rel-6) on handling of keys at inter-RAT handover

The following CRs are in RP-050304:

Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level	Workitem
25.331	2567	-	Rel-5	Correction to handling of keys at inter-RAT handover	F	5.12.1	5.13.0	R2-051527	TEI5
25.331	2568	-	Rel-6	Correction to handling of keys at inter-RAT handover	A	6.5.0	6.6.0	R2-051528	TEI5

3GPP TSG RAN2#47
Athens, Greece, 9-13 May 2005

Tdoc ⌘R2-051527

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **2567** ⌘**rev** **-** ⌘ Current version: **5.12.1** ⌘

*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 handling of keys at inter-RAT handover
Source:	⌘	RAN WG2
Work item code:	⌘	TEI5
Date:	⌘	09/05/2005
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*

Reason for change: ⌘

1) Current key set handling at Inter-RAT handover to UTRAN is not inline with either the CN1 or SA3 specifications. This has been discussed in a series of LSs between the WGs, e.g. R2-041261, R2-042072 and R2-050996

According to Draft Report of TSG SA meeting #27, "TSG SA asked TSG RAN WGs to align their specifications to the work done in the other WGs for Rel-5 onwards".

If the UE has received new keys in the other RAT, but not activated them, then the UE will according to current text activate the new keys upon the reception of the HANDOVER TO UTRAN COMMAND message and not consider them as "new". However, this leads to the following problems:

i) If an AKA procedure is initiated between a UE and anchor MSC after an inter-MSC handover then this is done transparently to MSC-B which is currently serving the UE.
The new keys generated during this AKA exchange are only passed from MSC-A to MSC-B using MAP after the exchange is complete, and so if, during or shortly after this AKA procedure the UE is handed over to UTRAN the MSC-B will provide the keys belonging to the key set used in the old RAT to the target RNC rather than the new keys being negotiated during the AKA exchange between the UE and MSC-A. Thus, when the UE responds to the HANDOVER TO UTRAN COMMAND message using the ciphering key stored on the USIM rather than the one belonging to the key set used in the previous RAT, the RNC will be unable to decode the HANDOVER TO UTRAN COMPLETE message and the handover will fail.

ii) It possible that MSC omits authentication for a specific access, because subscriber was authenticated in a previous access. When MSC then starts ciphering and algorithms supported in MSC and MS does not match, BSC then may choose 'no encryption' for the connection (GSM TS 12.03, chapter 4.3.1). In this case, MSC should do a 'late authentication' after it realizes that the connection will be unencrypted (GSM TS 12.03, chapter 6.2.1). In this case, after an Inter-RAT handover to UTRAN, UE and UTRAN will assume different key sets, due to the misalignment between specifications. Ciphering and/or integrity protection will fail.

2) The wording 'if ciphering has been activated and ongoing' could be misinterpreted in such a way that e.g.

a. after the ciphering has been switched off again in GERAN before the handover to UTRAN, or
b. the GERAN CIPHER MODE COMMAND indicates 'no ciphering',

the actions in 8.3.6.3 no longer apply.

In GERAN, after receipt of any 'valid' CIPHER MODE COMMAND, the key set is loaded from the USIM to the ME (see TS 44.018, section 3.4.7.2) and ciphering can be started during a handover (see TS 44.018, section 3.4.4.1). I.e. in GERAN, the state after receipt of a CIPHER MODE COMMAND indicating 'no ciphering' corresponds in UTRAN to the state after receipt of a SECURITY MODE COMMAND with ciphering algorithm UEA0 ('no encryption').

Summary of change: ⌘ The handling of the keys is corrected in section 8.3.6.3 so that the UE will use the keys belonging to the key set used in the previous RAT.

Notes are added to section 8.3.6.3 to clarify the term "used key set".

The wording '…if ciphering has been activated and ongoing…' is changed to '…if ciphering has been activated…'.

Notes are added to sections 8.1.12.2.2 and 8.6.3.5.1 to clarify the handling of the security mode control procedure to start integrity protection after Inter-RAT handover to UTRAN.

Isolated Impact Analysis
Functionality corrected: Security after Inter-RAT handover to UTRAN

Isolated impact statement: Correction to a function where UE and CN specifications are not aligned. Currently specified UE behaviour will lead to failed handover and call drop in certain scenarios.

Implementation of this CR by a R99/Rel-4 UE will not cause backwards compatibility issues with UTRAN and CN.

Consequences if not approved: ⌘ When the UE responds to the HANDOVER TO UTRAN COMMAND message using the ciphering key stored on the USIM rather than the one belonging to the keyset used in the previous RAT, the RNC will be unable to decode the HANDOVER TO UTRAN COMPLETE message and the handover will fail leading to call drop in certain scenarios.

Clauses affected: ⌘ 8.1.12.2.2, 8.3.6.3, 8.6.3.5.1

	Y	N		
Other specs ⌘			Other core specifications	⌘

affected:	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.

8.1.12.2.2 Integrity protection configuration change

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

In case of Inter-RAT handover to UTRAN, after the reception of the HANDOVER TO UTRAN COMPLETE message and a key set is received, UTRAN should transmit a SECURITY MODE COMMAND message containing IE "Integrity protection mode info" in order to initiate integrity protection with the integrity key of the key set used in the other RAT (see 8.3.6.3).

When configuring Integrity protection, UTRAN should:

1> ensure that the UE needs to store at most three different Integrity protection configurations (keysets) at any given time. This includes the total number of Integrity protection configurations for all signalling radio bearers;

1> if Ciphering has already been started for the UE for the CN domain to be set in the IE "CN domain identity" in the SECURITY MODE COMMAND:

2> if for the CN domain indicated in the IE "CN domain identity" in the SECURITY MODE COMMAND, a new security key set (new ciphering and integrity protection keys) has been received from upper layers since the transmission of the last SECURITY MODE COMMAND message for that CN domain:

3> include the IE "Ciphering mode info" in the SECURITY MODE COMMAND.

1> if Ciphering has already been configured for the UE for a CN domain different from the CN domain to be set in the IE "CN domain identity" in the SECURITY MODE COMMAND:

2> include the IE "Ciphering mode info" in the SECURITY MODE COMMAND.

Prior to sending the SECURITY MODE COMMAND, for the CN domain indicated in the IE "CN domain identity" in the SECURITY MODE COMMAND, UTRAN should:

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

2> if new keys have been received:

3> initialise the hyper frame numbers as follows:

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

2> else (if new keys have not been received):

3> use the value "START" in the most recently received IE "START list" or IE "START" that belongs to the CN domain indicated in the IE "CN domain identity" to initialise all hyper frame numbers of COUNT-I for all the signalling radio bearers by:

4> setting the 20 most significant bits of the hyper frame numbers for all signalling radio bearers to the value "START" in the most recently received IE "START list" or IE "START" for that CN domain;

4> setting the remaining bits of the hyper frame numbers equal to zero.

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

2> if new keys have been received:

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

4> set all bits of the HFN of the COUNT-I value for RB2 to zero.

2> if new keys have not been received:

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

4> set the 20 most significant bits of the HFN of the downlink and uplink COUNT-I to the value of the most recently received IE "START" or IE "START list" for the CN domain to be set in the IE "CN Domain Identity";

4> set the remaining bits of the HFN of the downlink and uplink COUNT-I to zero.

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

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

2> set the FRESH value in the IE "Integrity protection initialisation number", included in the IE "Integrity protection mode info".

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

2> for each signalling radio bearer RBn, except RB2:

3> prohibit the transmission of signalling messages with RRC SN greater or equal to the RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info".

2> consider an integrity protection activation time in downlink to be pending until the selected activation time is equal to the next RRC sequence number to be used, which means that the last RRC message using the old integrity protection configuration has been submitted to lower layers;

2> set, for each signalling radio bearer RBn, that has no pending integrity protection activation time set by a previous security mode control procedure, an RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info", at which time the new integrity protection configuration shall be applied;

2> set, for each signalling radio bearer RBn, that has a pending integrity protection activation time set by a previous security mode control procedure, the RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info", to the value used in the previous security mode control procedure, at which time the latest integrity protection configuration shall be applied.

1> transmit the SECURITY MODE COMMAND message on RB2 using the new integrity protection configuration.

NOTE1: In the case of re-initialisation of Integrity Protection at HFN wrap around, the network should take into account the UE actions as described in subclauses 8.5.10.1 and 8.5.10.2.

NOTE2: After the SECURITY MODE COMMAND message is transmitted, the network should ensure that it can revert back to old integrity protection until it receives the SECURITY MODE COMPLETE message, to take into account the UE actions when security mode control procedure is unsuccessful. The network should also be aware that the UE may revert to old configuration when waiting for the acknowledgement from L2 for the SECURITY MODE COMPLETE message, and act accordingly.

NOTE3: In the case of the first SECURITY MODE COMMAND message following an SRNS relocation, the network should set the IE "Downlink integrity protection activation info" for SRB3 and SRB4 to at least "the current downlink RRC sequence number +2". As a consequence, at least the first message sent on SRB3 and SRB4 by the Target RNC will use the old integrity protection configuration.

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 $P_{Pilot\text{-}DPDCH}$ 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: Keys received while in another RAT are not regarded as "new" (i.e.do not trigger the actions in subclause 8.1.12.3.1) in a subsequent security mode 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.
If ciphering has been activated in the other RAT, then during the first security mode control procedure following the Inter-RAT handover to UTRAN procedure, UE activates integrity protection using the integrity key of the same key set as used in the other RAT. The term “used key set” denotes the key set that was stored on USIM/SIM at the last successfully completed RRC Security Mode Control (UTRAN) or RR Cipher Mode Control procedures (GERAN) after entering connected mode in UTRAN or GERAN.
If ciphering has not been activated in the other RAT, then ~~A~~at a subsequent security mode control procedure in UTRAN, UE activates ciphering and/or integrity protection using the key set stored in the 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 of the key set ~~stored in the USIM/SIM~~used in the other RAT prior to handover and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND.

NOTE: The term "used key set" denotes the key set that was stored on USIM/SIM at the last successfully completed RRC Security Mode Control (UTRAN) or RR Cipher Mode Control procedures (GERAN) after entering connected mode in UTRAN or GERAN.
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.

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> indicate to upper layers that no CN system information is available for any domain other then the CS domain;

1> if the USIM or SIM is present:

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.

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 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.

8.6.3.5.1 Initialisation of Integrity Protection

The UE shall:

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

2> initialise the information for all signalling radio bearers in the variable INTEGRITY_PROTECTION_INFO according to the following:

3> set the IE "Uplink RRC Message sequence number" in the variable INTEGRITY_PROTECTION_INFO to zero;

3> do not set the IE "Downlink RRC Message sequence number" in the variable INTEGRITY_PROTECTION_INFO;

3> set the variable INTEGRITY_PROTECTION_ACTIVATION_INFO to zero for each signalling radio bearer in the IE "ESTABLISHED_RABS".

NOTE: The IEs "Integrity protection activation info" and "RRC Message sequence number"included in the IE "Integrity Check Info" in the transmitted message do not have identical values, but integrity protection is applied from the first transmitted message.

2> set the IE "Status" in the variable INTEGRITY_PROTECTION_INFO to the value "Started";

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

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

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

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

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

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

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

NOTE: After Inter-RAT handover to UTRAN, and ciphering was activated in the other RAT, then during the first security mode control procedure following the handover, UE activates integrity protection using the integrity key of the same key set as used in the other RAT (see.8.3.6.3).

3GPP TSG RAN2#47
Athens, Greece, 9-13 May 2005

Tdoc ⌘R2-051528

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **2568** ⌘**rev** **-** ⌘ Current version: **6.5.0** ⌘

*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 handling of keys at inter-RAT handover
Source:	⌘	RAN WG2
Work item code:	⌘	TEI5
Date:	⌘	09/05/2005
Category:	⌘	**A**
Release:	⌘	Rel-6

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

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*

Reason for change: ⌘

1) Current key set handling at Inter-RAT handover to UTRAN is not inline with either the CN1 or SA3 specifications. This has been discussed in a series of LSs between the WGs, e.g. R2-041261, R2-042072 and R2-050996

According to Draft Report of TSG SA meeting #27, "TSG SA asked TSG RAN WGs to align their specifications to the work done in the other WGs for Rel-5 onwards".

If the UE has received new keys in the other RAT, but not activated them, then the UE will according to current text activate the new keys upon the reception of the HANDOVER TO UTRAN COMMAND message and not consider them as "new". However, this leads to the following problems:

i) If an AKA procedure is initiated between a UE and anchor MSC after an inter-MSC handover then this is done transparently to MSC-B which is currently serving the UE.
The new keys generated during this AKA exchange are only passed from MSC-A to MSC-B using MAP after the exchange is complete, and so if, during or shortly after this AKA procedure the UE is handed over to UTRAN the MSC-B will provide the keys belonging to the key set used in the old RAT to the target RNC rather than the new keys being negotiated during the AKA exchange between the UE and MSC-A. Thus, when the UE responds to the HANDOVER TO UTRAN COMMAND message using the ciphering key stored on the USIM rather than the one belonging to the key set used in the previous RAT, the RNC will be unable to decode the HANDOVER TO UTRAN COMPLETE message and the handover will fail.

ii) It possible that MSC omits authentication for a specific access, because subscriber was authenticated in a previous access. When MSC then starts ciphering and algorithms supported in MSC and MS does not match, BSC then may choose 'no encryption' for the connection (GSM TS 12.03, chapter 4.3.1). In this case, MSC should do a 'late authentication' after it realizes that the connection will be unencrypted (GSM TS 12.03, chapter 6.2.1). In this case, after an Inter-RAT handover to UTRAN, UE and UTRAN will assume different key sets, due to the misalignment between specifications. Ciphering and/or integrity protection will fail.

2) The wording 'if ciphering has been activated and ongoing' could be misinterpreted in such a way that e.g.

a. after the ciphering has been switched off again in GERAN before the handover to UTRAN, or
b. the GERAN CIPHER MODE COMMAND indicates 'no ciphering',

the actions in 8.3.6.3 no longer apply.

In GERAN, after receipt of any 'valid' CIPHER MODE COMMAND, the key set is loaded from the USIM to the ME (see TS 44.018, section 3.4.7.2) and ciphering can be started during a handover (see TS 44.018, section 3.4.4.1). I.e. in GERAN, the state after receipt of a CIPHER MODE COMMAND indicating 'no ciphering' corresponds in UTRAN to the state after receipt of a SECURITY MODE COMMAND with ciphering algorithm UEA0 ('no encryption').

Summary of change: ⌘ The handling of the keys is corrected in section 8.3.6.3 so that the UE will use the keys belonging to the key set used in the previous RAT.

Notes are added to section 8.3.6.3 to clarify the term "used key set".

The wording '…if ciphering has been activated and ongoing…' is changed to '…if ciphering has been activated…'.

Notes are added to sections 8.1.12.2.2 and 8.6.3.5.1 to clarify the handling of the security mode control procedure to start integrity protection after Inter-RAT handover to UTRAN.

Isolated Impact Analysis
Functionality corrected: Security after Inter-RAT handover to UTRAN

Isolated impact statement: Correction to a function where UE and CN specifications are not aligned. Currently specified UE behaviour will lead to failed handover and call drop in certain scenarios.

Implementation of this CR by a R99/Rel-4 UE will not cause backwards compatibility issues with UTRAN and CN.

Consequences if not approved: ⌘ When the UE responds to the HANDOVER TO UTRAN COMMAND message using the ciphering key stored on the USIM rather than the one belonging to the keyset used in the previous RAT, the RNC will be unable to decode the HANDOVER TO UTRAN COMPLETE message and the handover will fail leading to call drop in certain scenarios.

Clauses affected: ⌘ 8.1.12.2.2, 8.3.6.3, 8.6.3.5.1

	Y	N		
Other specs ⌘			Other core specifications	⌘

affected:	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.

8.1.12.2.2 Integrity protection configuration change

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

In case of Inter-RAT handover to UTRAN, after the reception of the HANDOVER TO UTRAN COMPLETE message and a key set is received, UTRAN should transmit a SECURITY MODE COMMAND message containing IE “Integrity protection mode info" in order to initiate integrity protection with the integrity key of the key set used in the other RAT (see 8.3.6.3).

When configuring Integrity protection, UTRAN should:

1> ensure that the UE needs to store at most three different Integrity protection configurations (keysets) at any given time. This includes the total number of Integrity protection configurations for all signalling radio bearers;

1> if Ciphering has already been started for the UE for the CN domain to be set in the IE "CN domain identity" in the SECURITY MODE COMMAND:

2> if for the CN domain indicated in the IE "CN domain identity" in the SECURITY MODE COMMAND, a new security key set (new ciphering and integrity protection keys) has been received from upper layers since the transmission of the last SECURITY MODE COMMAND message for that CN domain:

3> include the IE "Ciphering mode info" in the SECURITY MODE COMMAND.

1> if Ciphering has already been configured for the UE for a CN domain different from the CN domain to be set in the IE "CN domain identity" in the SECURITY MODE COMMAND:

2> include the IE "Ciphering mode info" in the SECURITY MODE COMMAND.

Prior to sending the SECURITY MODE COMMAND, for the CN domain indicated in the IE "CN domain identity" in the SECURITY MODE COMMAND, UTRAN should:

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

2> if new keys have been received:

3> initialise the hyper frame numbers as follows:

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

2> else (if new keys have not been received):

3> use the value "START" in the most recently received IE "START list" or IE "START" that belongs to the CN domain indicated in the IE "CN domain identity" to initialise all hyper frame numbers of COUNT-I for all the signalling radio bearers by:

4> setting the 20 most significant bits of the hyper frame numbers for all signalling radio bearers to the value "START" in the most recently received IE "START list" or IE "START" for that CN domain;

4> setting the remaining bits of the hyper frame numbers equal to zero.

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

2> if new keys have been received:

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

4> set all bits of the HFN of the COUNT-I value for RB2 to zero.

2> if new keys have not been received:

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

4> set the 20 most significant bits of the HFN of the downlink and uplink COUNT-I to the value of the most recently received IE "START" or IE "START list" for the CN domain to be set in the IE "CN Domain Identity";

4> set the remaining bits of the HFN of the downlink and uplink COUNT-I to zero.

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

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

2> set the FRESH value in the IE "Integrity protection initialisation number", included in the IE "Integrity protection mode info".

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

2> for each signalling radio bearer RBn, except RB2:

3> prohibit the transmission of signalling messages with RRC SN greater or equal to the RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info".

2> consider an integrity protection activation time in downlink to be pending until the selected activation time is equal to the next RRC sequence number to be used, which means that the last RRC message using the old integrity protection configuration has been submitted to lower layers;

2> set, for each signalling radio bearer RBn, that has no pending integrity protection activation time set by a previous security mode control procedure, an RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info", at which time the new integrity protection configuration shall be applied;

2> set, for each signalling radio bearer RBn, that has a pending integrity protection activation time set by a previous security mode control procedure, the RRC sequence number in entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info", to the value used in the previous security mode control procedure, at which time the latest integrity protection configuration shall be applied.

1> transmit the SECURITY MODE COMMAND message on RB2 using the new integrity protection configuration.

NOTE1: In the case of re-initialisation of Integrity Protection at HFN wrap around, the network should take into account the UE actions as described in subclauses 8.5.10.1 and 8.5.10.2.

NOTE2: After the SECURITY MODE COMMAND message is transmitted, the network should ensure that it can revert back to old integrity protection until it receives the SECURITY MODE COMPLETE message, to take into account the UE actions when security mode control procedure is unsuccessful. The network should also be aware that the UE may revert to old configuration when waiting for the acknowledgement from L2 for the SECURITY MODE COMPLETE message, and act accordingly.

NOTE3: In the case of the first SECURITY MODE COMMAND message following an SRNS relocation, the network should set the IE "Downlink integrity protection activation info" for SRB3 and SRB4 to at least "the current downlink RRC sequence number +2". As a consequence, at least the first message sent on SRB3 and SRB4 by the Target RNC will use the old integrity protection configuration.

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 $P_{Pilot\text{-}DPDCH}$ 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: Keys received while in another RAT are not regarded as "new" (i.e.do not trigger the actions in subclause 8.1.12.3.1) in a subsequent security mode 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.
If ciphering has been activated in the other RAT, then during the first security mode control procedure following the Inter-RAT handover to UTRAN procedure, UE activates integrity protection using the integrity key of the same key set as used in the other RAT. The term “used key set” denotes the key set that was stored on USIM/SIM at the last successfully completed RRC Security Mode Control (UTRAN) or RR Cipher Mode Control procedures (GERAN) after entering connected mode in UTRAN or GERAN.
If ciphering has not been activated in the other RAT, then ~~At~~ at a subsequent security mode control procedure in UTRAN, UE activates ciphering and/or integrity protection using the key set stored in the 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 of the key set ~~stored in the USIM/SIM~~ used in the other RAT prior to handover and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND.

NOTE: The term "used key set" denotes the key set that was stored on USIM/SIM at the last successfully completed RRC Security Mode Control (UTRAN) or RR Cipher Mode Control procedures (GERAN) after entering connected mode in UTRAN or GERAN.
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.

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> indicate to upper layers that no CN system information is available for any domain other then the CS domain;

1> if the USIM or SIM is present:

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.

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 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.

8.6.3.5.1 Initialisation of Integrity Protection

The UE shall:

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

2> initialise the information for all signalling radio bearers in the variable INTEGRITY_PROTECTION_INFO according to the following:

3> set the IE "Uplink RRC Message sequence number" in the variable INTEGRITY_PROTECTION_INFO to zero;

3> do not set the IE "Downlink RRC Message sequence number" in the variable INTEGRITY_PROTECTION_INFO;

3> set the variable INTEGRITY_PROTECTION_ACTIVATION_INFO to zero for each signalling radio bearer in the IE "ESTABLISHED_RABS".

NOTE: The IEs "Integrity protection activation info" and "RRC Message sequence number"included in the IE "Integrity Check Info" in the transmitted message do not have identical values, but integrity protection is applied from the first transmitted message.

2> set the IE "Status" in the variable INTEGRITY_PROTECTION_INFO to the value "Started";

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

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

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

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

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

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

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

NOTE: After Inter-RAT handover to UTRAN, and ciphering was activated in the other RAT, then during the first security mode control procedure following the handover, UE activates integrity protection using the integrity key of the same key set as used in the other RAT (see.8.3.6.3).