TSG-RAN Meeting #21 **RP-030520**
Frankfurt, Germany, 16 - 19 September 2003

Title: **CR (R99) to TS 25.331**

Source: **Ericsson**

Agenda item: **7.3.3**

TS 25.331 **(RP-030520)**

RP Tdoc #	WG Toc#	Spec	CR	R	Subject	Phase	Cat	Current
RP-030520		25.331	2001	2	START calculation in connected mode	R99	F	3.16.0
RP-030520		25.331	2002	2	START calculation in connected mode	Rel-4	A	4.11.0
RP-030520		25.331	2003	2	START calculation in connected mode	Rel-5	A	5.6.0

3GPP TSG-RAN Meeting #21
Frankfurt, Germany 16th to 19th September 2003

Tdoc ⌘RP-030520

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **2001** ⌘**rev** **2** ⌘ Current version: **3.15.0** ⌘

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

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

Title:	⌘	START calculation in connected mode
Source:	⌘	Ericsson
Work item code:	⌘	TEI
Date:	⌘	August 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: ⌘

1 The calculation of START is defined to be valid in connected mode (Section 8.5.9). However, in some situations (e.g. transmission of the first INITIAL DIRECT TRANSFER of a signaling connection) the calculation can not be performed since COUNT-C and COUNT-I has not been initialised. In this scenario, the UE should use the START value stored on USIM/SIM. The COUNT-C and COUNT-I values are initialised at SECURITY MODE COMMAND which is potentially received quite some time after entering connected mode.
This also means that the START value will be the same in RRC CONNECTION SETUP COMPLETE and INITIAL DIRECT TRANSFER which is the intended behaviour.

2 Currently, it is not clear if UE, when storing START values on USIM (or in ME in case of SIM) calculates a 'new' START value, hereby avoiding that HFN values are not reused for the next RRC connection.

Summary of change: ⌘

1 Sections 8.5.9: It is clarified when COUNT-I and/or COUNT-C has not been initialised, the START value calculation in 8.5.9 is not performed and instead the UE **should** use the START value stored on the USIM (or in ME in case of SIM). **The Rel-5 implementation is different than the R'99/Rel-4.**

2 Sections 8.5.2 and 8.5.22: It is added that UE should peform a START value calculation prior to storing the START value on USIM (or in ME in case of SIM).

3 In revision 2 of the CR, the wording in 8.5.9 is changed since the first IDT of a signalling connection should contain the same START value as the RRC

CONNECTION SETUP COMPLETE and not the value "THRESHOLD" (which at this stage is stored in the START field in USIM)
Also, other procedures could require a calculation of the START value before the security mode command procedure is successfully completed (e.g. CELL UPDATE, SRNS relocation). In all these cases, the START value in any transmitted UL message **should** have the same value as the RRC CONNECTIONSETUP COMPLETE.

Consequences if not approved: ⌘

1 If the CR is not implemented the START value calculation in 8.5.9 can not be performed as specified in cases where the COUNT-I/ COUNT-C has not been initialised. If this undefined COUNT calculation results in a value, and the message IDT and RRC Connection setup complete are received in the wrong order, there might be ciphering and/or integrity protection failures.

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

Impact analysis:

Impacted functionality: Handling of START value

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

Interoperability:

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

Clauses affected: ⌘ 8.5.2, 8.5.9, 8.5.22

Other specs affected: ⌘

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

Other comments: ⌘

How to create CRs using this form:

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

8.5.2 Actions when entering idle mode from connected mode

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

1> clear or set variables upon leaving UTRA RRC connected mode as specified in subclause 13.4;

1> attempt to select a suitable cell to camp on.

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

1> perform cell selection.

While camping on a cell, the UE shall:

1> acquire system information according to the system information procedure in subclause 8.1;

1> perform measurements according to the measurement control procedure specified in subclause 8.4; and

1> if the UE is registered:

2> be prepared to receive paging messages according to the paging procedure in subclause 8.2.

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

1> delete any NAS system information received in connected mode;

1> acquire the NAS system information in system information block type 1; and

1> proceed according to subclause 8.6.1.2.

When entering idle mode, the UE shall:

1> if the USIM is present, for each CN domain:

2> if a new security key set was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:

3> set the START value for this domain to zero; and

3> store this START value for this domain in the USIM.

2> else:

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

4> delete the ciphering and integrity keys that are stored in the USIM for that CN domain;

4> inform the deletion of these keys to upper layers.

3> else:

4> store the current "START" value for this CN domain on the USIM.

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

1> else:

2> if the SIM is present, for each CN domain:

3> if a new security key set was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection, the UE should:

4> set the START value for this domain to zero; and

4> store this START value for this domain in the UE.

3> else, the UE shall:

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

5> delete the Kc key for this CN domain;

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

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

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

4> else:

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

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

8.5.9 START value calculation

In connected mode~~, if COUNT-C and/or COUNT-I has been initialised for a CN domain 'X'~~if a security mode command procedure has been successfully completed for a CN domain during the current RRC connection, the START value for that CN domain ~~'X'~~ is calculated as:

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

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

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

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

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

If a security mode command procedure has not been successfully completed for a CN domain during the current RRC connection, the UE should use the latest transmitted START value for this CN domain.

8.5.22 Actions when entering another RAT from connected mode

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

1> if the USIM is present, for each CN domain:

2> if a new security key set was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:

3> set the START value for this domain to zero and;

3> store this START value for this domain in the USIM.

2> else:

3> store the current START value for this CN domain in the USIM [50].

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

1> if the SIM is present, for each CN domain:

2> if a new security key was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:

3> set the START value for this domain to zero and;

3> store this START value for this domain in the UE.

2> else:

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

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

3GPP TSG-RAN Meeting #21
Frankfurt, Germany 16th to 19th September 2003

Tdoc ⌘RP-030520

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **2002** ⌘**rev** **2** ⌘ Current version: **4.10.0** ⌘

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

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

Title:	⌘	START calculation in connected mode
Source:	⌘	Ericsson
Work item code:	⌘	TEI
Date:	⌘	August 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: ⌘

1 The calculation of START is defined to be valid in connected mode (Section 8.5.9). However, in some situations (e.g. transmission of the first INITIAL DIRECT TRANSFER of a signaling connection) the calculation can not be performed since COUNT-C and COUNT-I has not been initialised. In this scenario, the UE should use the START value stored on USIM/SIM. The COUNT-C and COUNT-I values are initialised at SECURITY MODE COMMAND which is potentially received quite some time after entering connected mode.
This also means that the START value will be the same in RRC CONNECTION SETUP COMPLETE and INITIAL DIRECT TRANSFER which is the intended behaviour.

2 Currently, it is not clear if UE, when storing START values on USIM (or in ME in case of SIM) calculates a 'new' START value, hereby avoiding that HFN values are not reused for the next RRC connection.

Summary of change: ⌘

1 Sections 8.5.9: It is clarified when COUNT-I and/or COUNT-C has not been initialised, the START value calculation in 8.5.9 is not performed and instead the UE **should** use the START value stored on the USIM (or in ME in case of SIM). **The Rel-5 implementation is different than the R'99/Rel-4.**

2 Sections 8.5.2 and 8.5.22: It is added that UE should peform a START value calculation prior to storing the START value on USIM (or in ME in case of SIM).

3 In revision 2 of the CR, the wording in 8.5.9 is changed since the first IDT of a signalling connection should contain the same START value as the RRC CONNECTION SETUP COMPLETE and not the value "THRESHOLD" (which at

this stage is stored in the START field in USIM)
Also, other procedures could require a calculation of the START value before the security mode command procedure is successfully completed (e.g. CELL UPDATE, SRNS relocation). In all these cases, the START value in any transmitted UL message **should** have the same value as the RRC CONNECTIONSETUP COMPLETE.

Consequences if not approved: ⌘

1 If the CR is not implemented the START value calculation in 8.5.9 can not be performed as specified in cases where the COUNT-I/ COUNT-C has not been initialised. If this undefined COUNT calculation results in a value, and the message IDT and RRC Connection setup complete are received in the wrong order, there might be ciphering and/or integrity protection failures.

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

Impact analysis:

Impacted functionality: Handling of START value

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

Interoperability:

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

Clauses affected: ⌘ 8.5.2, 8.5.9, 8.5.22

Other specs affected: ⌘

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

⌘

Other comments: ⌘

How to create CRs using this form:

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

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

8.5.2 Actions when entering idle mode from connected mode

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

1> clear or set variables upon leaving UTRA RRC connected mode as specified in subclause 13.4;

1> attempt to select a suitable cell to camp on.

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

1> perform cell selection.

While camping on a cell, the UE shall:

1> acquire system information according to the system information procedure in subclause 8.1;

1> perform measurements according to the measurement control procedure specified in subclause 8.4; and

1> if the UE is registered:

2> be prepared to receive paging messages according to the paging procedure in subclause 8.2.

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

1> delete any NAS system information received in connected mode;

1> acquire the NAS system information in system information block type 1; and

1> proceed according to subclause 8.6.1.2.

When entering idle mode, the UE shall:

1> if the USIM is present, for each CN domain:

2> if a new security key set was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:

3> set the START value for this domain to zero; and

3> store this START value for this domain in the USIM.

2> else:

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

4> delete the ciphering and integrity keys that are stored in the USIM for that CN domain;

4> inform the deletion of these keys to upper layers.

3> else:

4> store the current "START" value for this CN domain on the USIM.

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

1> else:

2> if the SIM is present, for each CN domain:

3> if a new security key set was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:

4> set the START value for this domain to zero; and

4> store this START value for this domain in the UE

3> else:

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

5> delete the Kc key for this CN domain;

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

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

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

4> else:

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

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

8.5.9 START value calculation

In connected mode, ~~if COUNT-C and/or COUNT-I has been initialised for a CN domain 'X'~~ if a security mode command procedure has been successfully completed for a CN domain during the current RRC connection, the START value for that CN domain ~~'X'~~ is calculated as:

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

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

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

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

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

If a security mode command procedure has not been successfully completed for a CN domain during the current RRC connection, the UE should use the latest transmitted START value for this CN domain.

8.5.22 Actions when entering another RAT from connected mode

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

1> if the USIM is present, for each CN domain:

2> if a new security key set was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:

3> set the START value for this domain to zero and;

3> store this START value for this domain in the USIM;

2> else:

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

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

1> if the SIM is present, for each CN domain:

2> if a new security key was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:

3> set the START value for this domain to zero and;

3> store this START value for this domain in the USIM.

2> else:

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

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

3GPP TSG-RAN Meeting #21
Frankfurt, Germany 16th to 19th September 2003

Tdoc ⌘RP-030520

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **2003** ⌘**rev** **2** ⌘ Current version: **5.5.0** ⌘

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

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

Title:	⌘	START calculation in connected mode
Source:	⌘	Ericsson
Work item code:	⌘	TEI
Date:	⌘	August 2003
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 The calculation of START is defined to be valid in connected mode (Section 8.5.9). However, in some situations (e.g. transmission of the first INITIAL DIRECT TRANSFER of a signaling connection) the calculation can not be performed since COUNT-C and COUNT-I has not been initialised. In this scenario, the UE shall use the START value stored on USIM/SIM. The COUNT-C and COUNT-I values are initialised at SECURITY MODE COMMAND which is potentially received quite some time after entering connected mode.
This also means that the START value will be the same in RRC CONNECTION SETUP COMPLETE and INITIAL DIRECT TRANSFER which is the intended behaviour.

2 Currently, it is not clear if UE, when storing START values on USIM (or in ME in case of SIM) calculates a 'new' START value, hereby avoiding that HFN values are not reused for the next RRC connection.

Summary of change: ⌘

1 Sections 8.5.9: It is clarified when COUNT-I and/or COUNT-C has not been initialised, the START value calculation in 8.5.9 is not performed and instead the UE **shall** use the START value stored on the USIM (or in ME in case of SIM). **The Rel-5 implementation is different than the R'99/Rel-4.**

2 Sections 8.5.2 and 8.5.22: It is added that UE should peform a START value calculation prior to storing the START value on USIM (or in ME in case of SIM).

3 In revision 2 of the CR, the wording in 8.5.9 is changed since the first IDT of a signalling connection should contain the same START value as the RRC CONNECTION SETUP COMPLETE and not the value "THRESHOLD" (which at

this stage is stored in the START field in USIM)
Also, other procedures could require a calculation of the START value before the security mode command procedure is successfully completed (e.g. CELL UPDATE, SRNS relocation). In all these cases, the START value in any transmitted UL message **shall** have the same value as the RRC CONNECTIONSETUP COMPLETE.

Consequences if not approved: ⌘

1 If the CR is not implemented the START value calculation in 8.5.9 can not be performed as specified in cases where the COUNT-I/ COUNT-C has not been initialised. If this undefined COUNT calculation results in a value, and the message IDT and RRC Connection setup complete are received in the wrong order, there might be ciphering and/or integrity protection failures.

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

Impact analysis:

Impacted functionality: Handling of START value

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

Interoperability:

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

Clauses affected: ⌘ 8.5.2, 8.5.9, 8.5.22

Other specs affected: ⌘

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

Other comments: ⌘

How to create CRs using this form:

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

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

8.5.2 Actions when entering idle mode from connected mode

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

1> clear or set variables upon leaving UTRA RRC connected mode as specified in subclause 13.4;

1> attempt to select a suitable cell to camp on.

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

1> perform cell selection.

While camping on a cell, the UE shall:

1> acquire system information according to the system information procedure in subclause 8.1;

1> perform measurements according to the measurement control procedure specified in subclause 8.4; and

1> if the UE is registered:

2> be prepared to receive paging messages according to the paging procedure in subclause 8.2.

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

1> delete any NAS system information received in connected mode;

1> acquire the NAS system information in system information block type 1; and

1> proceed according to subclause 8.6.1.2.

When entering idle mode, the UE shall:

1> if the USIM is present, for each CN domain:

2> if a new security key set was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:

3> set the START value for this domain to zero; and

3> store this START value for this domain in the USIM.

2> else:

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

4> delete the ciphering and integrity keys that are stored in the USIM for that CN domain;

4> inform the deletion of these keys to upper layers.

3> else:

4> store the current "START" value for this CN domain on the USIM.

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

1> else:

2> if the SIM is present, for each CN domain:

3> if a new security key set was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:

4> set the START value for this domain to zero; and

4> store this START value for this domain in the UE

3> else:

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

5> delete the Kc key for this CN domain;

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

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

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

4> else:

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

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

8.5.9 START value calculation

In connected mode, ~~if COUNT-C and/or COUNT-I has been initialised for a CN domain 'X'~~if a security mode command procedure has been successfully completed for a CN domain during the current RRC connection, the START value for that CN domain ~~'X'~~ is calculated as:

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

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

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

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

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

If a security mode command procedure has not been successfully completed for a CN domain during the current RRC connection, the UE shall use the latest transmitted START value for this CN domain.

8.5.22 Actions when entering another RAT from connected mode

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

1> if the USIM is present, for each CN domain:

2> if a new security key set was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:

3> set the START value for this domain to zero and;

3> store this START value for this domain in the USIM;

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

2> else:

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

1> if the SIM is present, for each CN domain:

2> if a new security key was received for this CN domain but was not used either for integrity protection or ciphering during this RRC connection:

3> set the START value for this domain to zero and;

3> store this START value for this domain in the USIM.

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

2> else:

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