TSG-RAN Meeting #19 *RP-030104*
Birmingham, UK, 11 - 14 March 2003

Title: **CRs (Release '99 and Rel-4/Rel-5 category A) to TS 25.331 (2)**

Source: **TSG-RAN WG2**

Agenda item: **8.2.3**

Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level	Workitem
25.331	1829	-	R99	Additional Measurement reporting list	F	3.13.0	3.14.0	R2-030455	TEI
25.331	1830	-	Rel-4	Additional Measurement reporting list	A	4.8.0	4.9.0	R2-030456	TEI
25.331	1831	-	Rel-5	Additional Measurement reporting list	A	5.3.0	5.4.0	R2-030457	TEI
25.331	1832	2	R99	Correction on RRC integrity protection procedure	F	3.13.0	3.14.0	R2-030614	TEI
25.331	1833	2	Rel-4	Correction on RRC integrity protection procedure	A	4.8.0	4.9.0	R2-030615	TEI
25.331	1834	2	Rel-5	Correction on RRC integrity protection procedure	A	5.3.0	5.4.0	R2-030616	TEI
25.331	1835	-	R99	Reporting Cell Status and Event 2A	F	3.13.0	3.14.0	R2-030465	TEI
25.331	1836	-	Rel-4	Reporting Cell Status and Event 2A	A	4.8.0	4.9.0	R2-030466	TEI
25.331	1837	-	Rel-5	Reporting Cell Status and Event 2A	A	5.3.0	5.4.0	R2-030467	TEI
25.331	1838	-	R99	Correction to the handling of variable TGPS_IDENTITY and IE “Triggering condition 1/2”	F	3.13.0	3.14.0	R2-030468	TEI
25.331	1839	-	Rel-4	Correction to the handling of variable TGPS_IDENTITY and IE “Triggering condition 1/2”	A	4.8.0	4.9.0	R2-030469	TEI
25.331	1840	-	Rel-5	Correction to the handling of variable TGPS_IDENTITY and IE “Triggering condition 1/2”	A	5.3.0	5.4.0	R2-030470	TEI
25.331	1841	1	R99	Hard handover with pending ciphering activation times	F	3.13.0	3.14.0	R2-030480	TEI
25.331	1842	1	Rel-4	Hard handover with pending ciphering activation times	A	4.8.0	4.9.0	R2-030481	TEI
25.331	1843	1	Rel-5	Hard handover with pending ciphering activation times	A	5.3.0	5.4.0	R2-030482	TEI

3GPP TSG-RAN-WG2 Meeting #34 ***Tdoc ⌘R2-030455***
Sophia Antipolis, France, 17-21 February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **25.331 CR 1829** ⌘**rev** **-** ⌘ Current version: **3.13.0** ⌘

*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:	⌘	Additional Measurement reporting list		
Source:	⌘	TSG-RAN WG2		
Work item code:	⌘	TEI	***Date:*** ⌘	18/02/2003
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:	⌘	It is stated in clause 8.4.2.2 of 25.331 that the UE shall sort the additional measurements reported in MEASUREMENT REPORT message according to their "Measurement Identity" IE. It is not clearly specified how the UE should behave when not all of the additional measurements are available, but because the order of "Measurement Identity" is kept, all Additional Measurements must be sent. From the tabular notation, the IEs for reporting the measurement types described by cl 10.3.7.44-25.331 are optional (e.g. "Intra-Frequency measured results" included in "Intra-Frequency measured results list", cl 10.3.7.35 – 25.331). However, the ASN.1 defines all measurements types, in their respective results list, as mandatory. Therefore, it is not clear what the UE should send in the Additional Measurements if at the time of sending the report some results are missing.
Summary of change:	⌘	The limit of configured additional measurements is reduced to 1 per type (ie. The maximum of 4 is still kept, but they have to be of different types). It is stated that if the UE receives a configuration with more than one additional measurement of the same type, the UE behaviour is unspecified. **Impact Analysis** If only the UE implements the CR and more than one additional measurement of the same type is configured, the UE behaviour is unspecified. If only the UTRAN implements the CR the UE may send garbage on the mandatory fields or omit the additional measurements completely.
Consequences if not approved:	⌘	The UE will either send garbage on the mandatory fields or it will omit the additional measurements completely until results for all types are available. The former could mislead the UTRAN into considering measurement results that

	are not valid, whilst the latter could omit results from certain measurements that would be reported only once and are therefore lost.

Clauses affected:	⌘	8.4.2, 8.6.7.22				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

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

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

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

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

8.4.2 Measurement report

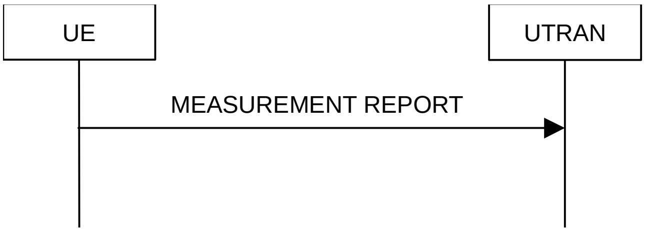

Figure 8.4.2-1: Measurement report, normal case

8.4.2.1 General

The purpose of the measurement reporting procedure is to transfer measurement results from the UE to UTRAN.

8.4.2.2 Initiation

In CELL_DCH state, the UE shall:

1> transmit a MEASUREMENT REPORT message on the uplink DCCH when the reporting criteria stored in variable MEASUREMENT_IDENTITY are met for any ongoing measurements that are being performed in the UE.

In CELL_FACH state, the UE shall:

1> transmit a MEASUREMENT REPORT message on the uplink DCCH when the reporting criteria stored in variable MEASUREMENT_IDENTITY are met for any ongoing traffic volume measurement or UE positioning measurement that is being performed in the UE;

1> include a measurement report in the IE "Measured results on RACH", as specified in the IE "Intra-frequency reporting quantity for RACH reporting" and the IE "Maximum number of reported cells on RACH" in System Information Block type 12 (or "System Information Block Type 11" if "System Information Block Type 12" is not being broadcast);

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

In TDD, if the Radio Bearer associated with the MEASUREMENT_IDENTITY fulfilling the reporting criteria for an ongoing traffic volume measurement is mapped on transport channel of type USCH, the UE shall:

1> initiate the "PUSCH CAPACITY REQUEST" procedure instead of transmitting a MEASUREMENT REPORT (TDD Only).

In CELL_PCH or URA_PCH state, the UE shall:

1> first perform the cell update procedure according to subclause 8.3.1, using the cause "uplink data transmission", in order to transit to CELL_FACH state; and then

1> transmit a MEASUREMENT REPORT message on the uplink DCCH when the reporting criteria stored in variable MEASUREMENT_IDENTITY are fulfilled for any ongoing traffic volume measurement or UE positioning measurement which is being performed in the UE.

The reporting criteria are fulfilled if either:

- the first measurement has been completed according to the requirements set in [19] or [20] for a newly initiated measurement with periodic reporting; or
- the time period indicated in the stored IE "Periodical reporting criteria" has elapsed since the last measurement report was submitted to lower layers for a given measurement; or
- an event in stored IE "Measurement reporting criteria" was triggered. Events and triggering of reports for different measurement types are described in detail in clause 14.

For the measurement, which triggered the MEASUREMENT REPORT message, the UE shall:

1> set the IE "measurement identity" to the measurement identity, which is associated with that measurement in variable MEASUREMENT_IDENTITY;

1> set the IE "measured results" to include measurements according to the IE "reporting quantity" of that measurement stored in variable MEASUREMENT_IDENTITY; and

2> if all the reporting quantities are set to "false":

3> not set the IE "measured results".

1> set the IE "Measured results" in the IE "Additional measured results" according to the IE "reporting quantity" for all measurements associated with the measurement identities included in the "Additional measurements list" stored in variable MEASUREMENT_IDENTITY of the measurement that triggered the measurement report; and

2> if more than one additional measured results are to be included:

3> include only the available additional measured results, and sort them in ascending order according to their IE "measurement identity" in the MEASUREMENT REPORT message.

1> if the MEASUREMENT REPORT message was triggered by an event (i.e. not a periodical report):

2> set the IE "Event results" according to the event that triggered the report.

The UE shall:

1> transmit the MEASUREMENT REPORT message on the uplink DCCH using either AM or UM RLC according to the stored IE "measurement reporting mode" associated with the measurement identity that triggered the report.

When the MEASUREMENT REPORT message has been submitted to lower layers for transmission:

1> the procedure ends.

8.6.7.22 Additional Measurement List

If the IE "Additional Measurement List" is received in a MEASUREMENT CONTROL message, the UE shall:

1> if the received measurement configuration in this MEASUREMENT CONTROL message, or any measurement referenced in the "Additional Measurement List" do not all have the same validity:

2> set the variable CONFIGURATION_INCOMPLETE to TRUE.

1> if any of the measurements referenced in the "Additional Measurement List" is an intra-frequency, inter-frequence or inter-RAT measurement, and this measurement is configured with event based reporting:

2> the UE behaviour is not specified.

1> if the result of this MEASUREMENT CONTROL message is such that more than one additional measurement of the same type will be referenced in the IE "Additional Measurement List" in the MEASUREMENT_IDENTITY variable:

2> the UE behaviour is not specified.

If the measurement configured with the MEASUREMENT CONTROL message triggers a measurement report, the UE shall also include the reporting quantities for the measurements referenced by the additional measurement identities. The contents of the IE "Additional Measured results" is completely determined by the measurement configuration of the referenced additional measurement.

3GPP TSG-RAN-WG2 Meeting #34 **Tdoc ⌘R2-030456**
Sophia Antipolis, France, 17-21 February 2003

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1830**	⌘**rev**	**-**	⌘	Current version:	**4.8.0** ⌘

*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:	⌘	Additional Measurement reporting list		
Source:	⌘	TSG-RAN WG2		
Work item code:	⌘	TEI	***Date:*** ⌘	18/02/2003
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: ⌘

It is stated in clause 8.4.2.2 of 25.331 that the UE shall sort the additional measurements reported in MEASUREMENT REPORT message according to their "Measurement Identity" IE.
It is not clearly specified how the UE should behave when not all of the additional measurements are available, but because the order of "Measurement Identity" is kept, all Additional Measurements must be sent.
From the tabular notation, the IEs for reporting the measurement types described by cl 10.3.7.44-25.331 are optional (e.g. "Intra-Frequency measured results" included in "Intra-Frequency measured results list", cl 10.3.7.35 – 25.331).
However, the ASN.1 defines all measurements types, in their respective results list, as mandatory.
Therefore, it is not clear what the UE should send in the Additional Measurements if at the time of sending the report some results are missing.

Summary of change: ⌘

The limit of configured additional measurements is reduced to 1 per type (ie. The maximum of 4 is still kept, but they have to be of different types). It is stated that if the UE receives a configuration with more than one additional measurement of the same type, the UE behaviour is unspecified.

Impact Analysis
If only the UE implements the CR and more than one additional measurement of the same type is configured, the UE behaviour is unspecified. If only the UTRAN implements the CR the UE may send garbage on the mandatory fields or omit the additional measurements completely.

Consequences if not approved: ⌘

The UE will either send garbage on the mandatory fields or it will omit the additional measurements completely until results for all types are available.
The former could mislead the UTRAN into considering measurement results that

	are not valid, whilst the latter could omit results from certain measurements that would be reported only once and are therefore lost.

Clauses affected:	⌘	8.4.2, 8.6.7.22				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

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

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

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

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

8.4.2 Measurement report

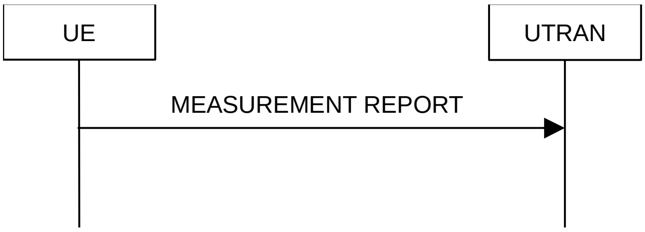

Figure 8.4.2-1: Measurement report, normal case

8.4.2.1 General

The purpose of the measurement reporting procedure is to transfer measurement results from the UE to UTRAN.

8.4.2.2 Initiation

In CELL_DCH state, the UE shall:

1> transmit a MEASUREMENT REPORT message on the uplink DCCH when the reporting criteria stored in variable MEASUREMENT_IDENTITY are met for any ongoing measurements that are being performed in the UE.

In CELL_FACH state, the UE shall:

1> transmit a MEASUREMENT REPORT message on the uplink DCCH when the reporting criteria stored in variable MEASUREMENT_IDENTITY are met for any ongoing traffic volume measurement or UE positioning measurement that is being performed in the UE;

1> include a measurement report in the IE "Measured results on RACH", as specified in the IE "Intra-frequency reporting quantity for RACH reporting" and the IE "Maximum number of reported cells on RACH" in System Information Block type 12 (or "System Information Block Type 11" if "System Information Block Type 12" is not being broadcast);

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

In TDD, if the Radio Bearer associated with the MEASUREMENT_IDENTITY fulfilling the reporting criteria for an ongoing traffic volume measurement is mapped on transport channel of type USCH, the UE shall:

1> initiate the "PUSCH CAPACITY REQUEST" procedure instead of transmitting a MEASUREMENT REPORT (TDD Only).

In CELL_PCH or URA_PCH state, the UE shall:

1> first perform the cell update procedure according to subclause 8.3.1, using the cause "uplink data transmission", in order to transit to CELL_FACH state; and then

1> transmit a MEASUREMENT REPORT message on the uplink DCCH when the reporting criteria stored in variable MEASUREMENT_IDENTITY are fulfilled for any ongoing traffic volume measurement or UE positioning measurement which is being performed in the UE.

The reporting criteria are fulfilled if either:

- the first measurement has been completed according to the requirements set in [19] or [20] for a newly initiated measurement with periodic reporting; or
- the time period indicated in the stored IE "Periodical reporting criteria" has elapsed since the last measurement report was submitted to lower layers for a given measurement; or
- an event in stored IE "Measurement reporting criteria" was triggered. Events and triggering of reports for different measurement types are described in detail in clause 14.

For the measurement, which triggered the MEASUREMENT REPORT message, the UE shall:

1> set the IE "measurement identity" to the measurement identity, which is associated with that measurement in variable MEASUREMENT_IDENTITY;

1> set the IE "measured results" to include measurements according to the IE "reporting quantity" of that measurement stored in variable MEASUREMENT_IDENTITY; and

2> if all the reporting quantities are set to "false":

3> not set the IE "measured results".

1> set the IE "Measured results" in the IE "Additional measured results" according to the IE "reporting quantity" for all measurements associated with the measurement identities included in the "Additional measurements list" stored in variable MEASUREMENT_IDENTITY of the measurement that triggered the measurement report; and

2> if more than one additional measured results are to be included:

3> include only the available additional measured results, and sort them in ascending order according to their IE "measurement identity" in the MEASUREMENT REPORT message.

1> if the MEASUREMENT REPORT message was triggered by an event (i.e. not a periodical report):

2> set the IE "Event results" according to the event that triggered the report.

The UE shall:

1> transmit the MEASUREMENT REPORT message on the uplink DCCH using either AM or UM RLC according to the stored IE "measurement reporting mode" associated with the measurement identity that triggered the report.

When the MEASUREMENT REPORT message has been submitted to lower layers for transmission:

1> the procedure ends.

8.6.7.22 Additional Measurement List

If the IE "Additional Measurement List" is received in a MEASUREMENT CONTROL message, the UE shall:

1> if the received measurement configuration in this MEASUREMENT CONTROL message, or any measurement referenced in the "Additional Measurement List" do not all have the same validity:

2> set the variable CONFIGURATION_INCOMPLETE to TRUE.

1> if any of the measurements referenced in the "Additional Measurement List" is an intra-frequency, inter-frequence or inter-RAT measurement, and this measurement is configured with event based reporting:

2> the UE behaviour is not specified.

1> if the result of this MEASUREMENT CONTROL message is such that more than one additional measurement of the same type will be referenced in the IE "Additional Measurement List" in the MEASUREMENT_IDENTITY variable:

2> the UE behaviour is not specified.

If the measurement configured with the MEASUREMENT CONTROL message triggers a measurement report, the UE shall also include the reporting quantities for the measurements referenced by the additional measurement identities. The contents of the IE "Additional Measured results" is completely determined by the measurement configuration of the referenced additional measurement.

3GPP TSG-RAN-WG2 Meeting #34
Sophia Antipolis, France, 17-21 February 2003

Tdoc ⌘R2-030457

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1831**	⌘**rev**	**-**	⌘	Current version:	**5.3.0** ⌘

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

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

Title:	⌘	Additional Measurement reporting list		
Source:	⌘	TSG-RAN WG2		
Work item code:	⌘	TEI	***Date:*** ⌘	18/02/2003
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: ⌘

It is stated in clause 8.4.2.2 of 25.331 that the UE shall sort the additional measurements reported in MEASUREMENT REPORT message according to their "Measurement Identity" IE.
It is not clearly specified how the UE should behave when not all of the additional measurements are available, but because the order of "Measurement Identity" is kept, all Additional Measurements must be sent.
From the tabular notation, the IEs for reporting the measurement types described by cl 10.3.7.44-25.331 are optional (e.g. "Intra-Frequency measured results" included in "Intra-Frequency measured results list", cl 10.3.7.35 – 25.331).
However, the ASN.1 defines all measurements types, in their respective results list, as mandatory.
Therefore, it is not clear what the UE should send in the Additional Measurements if at the time of sending the report some results are missing.

Summary of change: ⌘

The limit of configured additional measurements is reduced to 1 per type (ie. The maximum of 4 is still kept, but they have to be of different types). It is stated that if the UE receives a configuration with more than one additional measurement of the same type, the UE behaviour is unspecified.

Impact Analysis
If only the UE implements the CR and more than one additional measurement of the same type is configured, the UE behaviour is unspecified. If only the UTRAN implements the CR the UE may send garbage on the mandatory fields or omit the additional measurements completely.

Consequences if not approved: ⌘

The UE will either send garbage on the mandatory fields or it will omit the additional measurements completely until results for all types are available.
The former could mislead the UTRAN into considering measurement results that

are not valid, whilst the latter could omit results from certain measurements that would be reported only once and are therefore lost.

Clauses affected:	⌘	8.4.2, 8.6.7.22				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

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

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

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

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

8.4.2 Measurement report

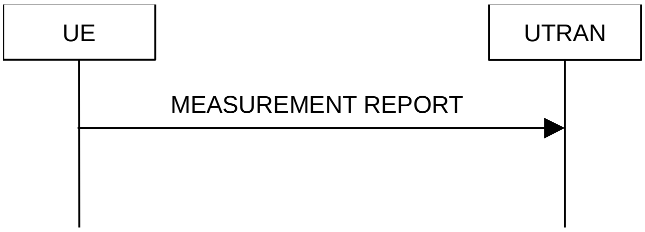

Figure 8.4.2-1: Measurement report, normal case

8.4.2.1 General

The purpose of the measurement reporting procedure is to transfer measurement results from the UE to UTRAN.

8.4.2.2 Initiation

In CELL_DCH state, the UE shall:

1> transmit a MEASUREMENT REPORT message on the uplink DCCH when the reporting criteria stored in variable MEASUREMENT_IDENTITY are met for any ongoing measurements that are being performed in the UE.

In CELL_FACH state, the UE shall:

1> transmit a MEASUREMENT REPORT message on the uplink DCCH when the reporting criteria stored in variable MEASUREMENT_IDENTITY are met for any ongoing traffic volume measurement or UE positioning measurement that is being performed in the UE;

1> include a measurement report in the IE "Measured results on RACH", as specified in the IE "Intra-frequency reporting quantity for RACH reporting" and the IE "Maximum number of reported cells on RACH" in System Information Block type 12 (or "System Information Block Type 11" if "System Information Block Type 12" is not being broadcast);

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

In TDD, if the Radio Bearer associated with the MEASUREMENT_IDENTITY fulfilling the reporting criteria for an ongoing traffic volume measurement is mapped on transport channel of type USCH, the UE shall:

1> initiate the "PUSCH CAPACITY REQUEST" procedure instead of transmitting a MEASUREMENT REPORT (TDD Only).

In CELL_PCH or URA_PCH state, the UE shall:

1> first perform the cell update procedure according to subclause 8.3.1, using the cause "uplink data transmission", in order to transit to CELL_FACH state; and then

1> transmit a MEASUREMENT REPORT message on the uplink DCCH when the reporting criteria stored in variable MEASUREMENT_IDENTITY are fulfilled for any ongoing traffic volume measurement or UE positioning measurement which is being performed in the UE.

The reporting criteria are fulfilled if either:

- the first measurement has been completed according to the requirements set in [19] or [20] for a newly initiated measurement with periodic reporting; or

- the time period indicated in the stored IE "Periodical reporting criteria" has elapsed since the last measurement report was submitted to lower layers for a given measurement; or

- an event in stored IE "Measurement reporting criteria" was triggered. Events and triggering of reports for different measurement types are described in detail in clause 14.

For the measurement, which triggered the MEASUREMENT REPORT message, the UE shall:

1> set the IE "measurement identity" to the measurement identity, which is associated with that measurement in variable MEASUREMENT_IDENTITY;

1> set the IE "measured results" to include measurements according to the IE "reporting quantity" of that measurement stored in variable MEASUREMENT_IDENTITY; and

2> if all the reporting quantities are set to "false":

3> not set the IE "measured results".

1> set the IE "Measured results" in the IE "Additional measured results" according to the IE "reporting quantity" for all measurements associated with the measurement identities included in the "Additional measurements list" stored in variable MEASUREMENT_IDENTITY of the measurement that triggered the measurement report; and

2> if more than one additional measured results are to be included:

3> include only the available additional measured results, and sort them in ascending order according to their IE "measurement identity" in the MEASUREMENT REPORT message.

1> if the MEASUREMENT REPORT message was triggered by an event (i.e. not a periodical report):

2> set the IE "Event results" according to the event that triggered the report.

The UE shall:

1> transmit the MEASUREMENT REPORT message on the uplink DCCH using either AM or UM RLC according to the stored IE "measurement reporting mode" associated with the measurement identity that triggered the report.

When the MEASUREMENT REPORT message has been submitted to lower layers for transmission:

1> the procedure ends.

8.6.7.22 Additional Measurement List

If the IE "Additional Measurement List" is received in a MEASUREMENT CONTROL message, the UE shall:

1> if the received measurement configuration in this MEASUREMENT CONTROL message, or any measurement referenced in the "Additional Measurement List" do not all have the same validity:

2> set the variable CONFIGURATION_INCOMPLETE to TRUE.

1> if any of the measurements referenced in the "Additional Measurement List" is an intra-frequency, inter-frequence or inter-RAT measurement, and this measurement is configured with event based reporting:

2> the UE behaviour is not specified.

1> if the result of this MEASUREMENT CONTROL message is such that more than one additional measurement of the same type will be referenced in the IE "Additional Measurement List" in the MEASUREMENT_IDENTITY variable:

2> the UE behaviour is not specified.

If the measurement configured with the MEASUREMENT CONTROL message triggers a measurement report, the UE shall also include the reporting quantities for the measurements referenced by the additional measurement identities. The contents of the IE "Additional Measured results" is completely determined by the measurement configuration of the referenced additional measurement.

3GPP TSG-RAN WG2 #34 **R2-030614**
Sophia Antipolis, France, 17th-21st February, 2003

CR-Form-v7

CHANGE REQUEST

⌘ **25.331 CR 1832** ⌘ **rev 2** ⌘ Current version: **3.13.0** ⌘

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 on RRC integrity protection procedure		
Source: ⌘	TSG-RAN WG2		
Work item code: ⌘	TEI	***Date:*** ⌘	February 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: ⌘ According to the current specification, when a message containing “Integrity protection mode info” arrives, UE updates its security configuration. If the message fails integrity check, UE doesn’t have any means to restore its previous security configuration. Thus, the security configuration of the UE will be different from that of UTRAN, and communication between the two will be impossible.

Summary of change: ⌘ If the integrity check of the received message fails, UE restores the previous security configuration and discard the received message.

Isolated Impact analysis:

This CR has an impact on UE implementation. If UE does not follow what is indicated in this CR, security configuration will be unsynchronized after the message containing “Integrity protection mode info” fails integrity check.

Consequences if not approved: ⌘ If a message with “Integrity protection mode info” fails integrity check, UE loses a valid security configuration, and can’t communicate with UTRAN any more.

Clauses affected: ⌘ 8.5.10, 8.5.10.1

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.

'.

8.5.10 Integrity protection

If the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" then the UE shall:

1> perform integrity protection (and integrity checking) on all RRC messages, with the following exceptions:

HANDOVER TO UTRAN COMPLETE

PAGING TYPE 1

PUSCH CAPACITY REQUEST

PHYSICAL SHARED CHANNEL ALLOCATION

RRC CONNECTION REQUEST

RRC CONNECTION SETUP

RRC CONNECTION SETUP COMPLETE

RRC CONNECTION REJECT

RRC CONNECTION RELEASE (CCCH only)

SYSTEM INFORMATION

SYSTEM INFORMATION CHANGE INDICATION

If the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Not started" then integrity protection (and integrity checking) shall not be performed on any RRC message.

For each signalling radio bearer, the UE shall use two RRC hyper frame numbers:

- "Uplink RRC HFN";
- "Downlink RRC HFN".

and two message sequence numbers:

- "Uplink RRC Message sequence number";
- "Downlink RRC Message sequence number".

The above information is stored in the variable INTEGRITY_PROTECTION_INFO per signalling radio bearer (RB0-RB4).

Upon the first activation of integrity protection for an RRC connection, UE and UTRAN initialise the "Uplink RRC Message sequence number" and "Downlink RRC Message sequence number" for all signalling radio bearers as specified in subclauses 8.6.3.5 and 8.5.10.1.

The RRC message sequence number (RRC SN) is incremented for every integrity protected RRC message.

If the IE "Integrity Protection Mode Info" is present in a received message, the UE shall:

1> perform the actions in subclause 8.6.3.5 before proceeding with the integrity check of the received message.

8.5.10.1 Integrity protection in downlink

If the UE receives an RRC message on signalling radio bearer with RB identity n, the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" and the IE 'Integrity check info' is present the UE shall:

1> check the value of the IE "RRC message sequence number" included in the IE "Integrity check info";

2> if the "Downlink RRC Message sequence number" is not present in the variable INTEGRITY_PROTECTION_INFO:

3> initialise the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with the value of the IE "RRC message sequence number" included in the IE "Integrity check info" of the received message.

2> if the "Downlink RRC Message sequence number" is present in the variable INTEGRITY_PROTECTION_INFO:

3> if the RRC message sequence number is lower than the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO:

4> increment "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with one.

NOTE: The actions above imply that also for the case the "Downlink RRC HFN" is re-initialised by a security mode control procedure, this "Downlink RRC HFN" value is incremented by one before it is applied for the integrity protection of any received message if the conditions above are fulfilled.

3> if the RRC message sequence number is equal to the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO:

4> discard the message.

1> calculate an expected message authentication code in accordance with subclause 8.5.10.3;

1> compare the expected message authentication code with the value of the received IE "message authentication code" contained in the IE "Integrity check info";

2> if the expected message authentication code and the received message authentication code are the same, the integrity check is successful:

3> update the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with the value of the IE "RRC message sequence number" included in the IE "Integrity check info" of the received RRC message.

2> if the calculated expected message authentication code and the received message authentication code differ:

3> act as if the message was not received;~~if the IE "RRC message sequence number" included in the IE "Integrity check info" is lower than the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO (in this case the "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO was incremented by one, as stated above):~~

4> ~~decrement "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO by one.~~

~~3> discard the message.~~

If the UE receives an RRC message on signalling radio bearer with identity n, the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" and the IE 'Integrity check info' is not present the UE shall:

1> discard the message.

UTRAN may transmit several copies of the same message in the downlink to increase the probability of proper reception of the message by the UE. In such a case, the RRC SN for these repeated messages should be the same.

3GPP TSG-RAN WG2 #34 ***R2-030615***
Sophia Antipolis, France, 17th-21st February, 2003

CR-Form-v7

CHANGE REQUEST

⌘ **25.331 CR 1833** ⌘ **rev 2** ⌘ Current version: **4.8.0** ⌘

*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 on RRC integrity protection procedure		
Source:	⌘	TSG-RAN WG2		
Work item code:	⌘	TEI	***Date:*** ⌘	February 2003
Category:	⌘	**A** *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.	***Release:*** ⌘	Rel-4 *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:	⌘	According to the current specification, when a message containing “Integrity protection mode info” arrives, UE updates its security configuration. If the message fails integrity check, UE doesn’t have any means to restore its previous security configuration. Thus, the security configuration of the UE will be different from that of UTRAN, and communication between the two will be impossible.
Summary of change:	⌘	If the integrity check of the received message fails, UE restores the previous security configuration and discard the received message. **Isolated Impact analysis:** This CR has an impact on UE implementation. If UE does not follow what is indicated in this CR, security configuration will be unsynchronized after the message containing “Integrity protection mode info” fails integrity check.
Consequences if not approved:	⌘	If a message with “Integrity protection mode info” fails integrity check, UE loses a valid security configuration, and can’t communicate with UTRAN any more.

Clauses affected:	⌘	8.5.10, 8.5.10.1				
		Y	**N**			
Other specs Affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		

Other comments: ⌘	

How to create CRs using this form:

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

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

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

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

'.

8.5.10 Integrity protection

If the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" then the UE shall:

1> perform integrity protection (and integrity checking) on all RRC messages, with the following exceptions:

HANDOVER TO UTRAN COMPLETE

PAGING TYPE 1

PUSCH CAPACITY REQUEST

PHYSICAL SHARED CHANNEL ALLOCATION

RRC CONNECTION REQUEST

RRC CONNECTION SETUP

RRC CONNECTION SETUP COMPLETE

RRC CONNECTION REJECT

RRC CONNECTION RELEASE (CCCH only)

SYSTEM INFORMATION

SYSTEM INFORMATION CHANGE INDICATION

If the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Not started" then integrity protection (and integrity checking) shall not be performed on any RRC message.

For each signalling radio bearer, the UE shall use two RRC hyper frame numbers:

- "Uplink RRC HFN";
- "Downlink RRC HFN".

and two message sequence numbers:

- "Uplink RRC Message sequence number";
- "Downlink RRC Message sequence number".

The above information is stored in the variable INTEGRITY_PROTECTION_INFO per signalling radio bearer (RB0-RB4).

Upon the first activation of integrity protection for an RRC connection, UE and UTRAN initialise the "Uplink RRC Message sequence number" and "Downlink RRC Message sequence number" for all signalling radio bearers as specified in subclauses 8.6.3.5 and 8.5.10.1.

The RRC message sequence number (RRC SN) is incremented for every integrity protected RRC message.

If the IE "Integrity Protection Mode Info" is present in a received message, the UE shall:

1> perform the actions in subclause 8.6.3.5 before proceeding with the integrity check of the received message.

8.5.10.1 Integrity protection in downlink

If the UE receives an RRC message on signalling radio bearer with RB identity n, the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" and the IE 'Integrity check info' is present the UE shall:

1> check the value of the IE "RRC message sequence number" included in the IE "Integrity check info";

2> if the "Downlink RRC Message sequence number" is not present in the variable INTEGRITY_PROTECTION_INFO:

3> initialise the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with the value of the IE "RRC message sequence number" included in the IE "Integrity check info" of the received message.

2> if the "Downlink RRC Message sequence number" is present in the variable INTEGRITY_PROTECTION_INFO:

3> if the RRC message sequence number is lower than the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO:

4> increment "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with one.

NOTE: The actions above imply that also for the case the "Downlink RRC HFN" is re-initialised by a security mode control procedure, this "Downlink RRC HFN" value is incremented by one before it is applied for the integrity protection of any received message if the conditions above are fulfilled.

3> if the RRC message sequence number is equal to the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO:

4> discard the message.

1> calculate an expected message authentication code in accordance with subclause 8.5.10.3;

1> compare the expected message authentication code with the value of the received IE "message authentication code" contained in the IE "Integrity check info";

2> if the expected message authentication code and the received message authentication code are the same, the integrity check is successful:

3> update the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with the value of the IE "RRC message sequence number" included in the IE "Integrity check info" of the received RRC message.

2> if the calculated expected message authentication code and the received message authentication code differ:

3> act as if the message was not received;~~if the IE "RRC message sequence number" included in the IE "Integrity check info" is lower than the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO (in this case the "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO was incremented by one, as stated above):~~

4> ~~decrement "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO by one.~~

~~3> discard the message.~~

If the UE receives an RRC message on signalling radio bearer with identity n, the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" and the IE 'Integrity check info' is not present the UE shall:

1> discard the message.

UTRAN may transmit several copies of the same message in the downlink to increase the probability of proper reception of the message by the UE. In such a case, the RRC SN for these repeated messages should be the same.

3GPP TSG-RAN WG2 #34 ***R2-030616***
Sophia Antipolis, France, 17th-21st February, 2003

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1834**	⌘ **rev**	**2**	⌘	Current version:	**5.3.0**	⌘

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

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

Title:	⌘	Correction on RRC integrity protection procedure		
Source:	⌘	TSG-RAN WG2		
Work item code:	⌘	TEI	***Date:*** ⌘	February 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: ⌘ According to the current specification, when a message containing “Integrity protection mode info” arrives, UE updates its security configuration. If the message fails integrity check, UE doesn’t have any means to restore its previous security configuration. Thus, the security configuration of the UE will be different from that of UTRAN, and communication between the two will be impossible.

Summary of change: ⌘ If the integrity check of the received message fails, UE restores the previous security configuration and discard the received message.

Isolated Impact analysis:

This CR has an impact on UE implementation. If UE does not follow what is indicated in this CR, security configuration will be unsynchronized after the message containing “Integrity protection mode info” fails integrity check.

Consequences if not approved: ⌘ If a message with “Integrity protection mode info” fails integrity check, UE loses a valid security configuration, and can’t communicate with UTRAN any more.

Clauses affected: ⌘ 8.5.10, 8.5.10.1

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

Other comments: ⌘

How to create CRs using this form:

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

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

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

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

'.

8.5.10 Integrity protection

If the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" then the UE shall:

1> perform integrity protection (and integrity checking) on all RRC messages, with the following exceptions:

HANDOVER TO UTRAN COMPLETE

PAGING TYPE 1

PUSCH CAPACITY REQUEST

PHYSICAL SHARED CHANNEL ALLOCATION

RRC CONNECTION REQUEST

RRC CONNECTION SETUP

RRC CONNECTION SETUP COMPLETE

RRC CONNECTION REJECT

RRC CONNECTION RELEASE (CCCH only)

SYSTEM INFORMATION

SYSTEM INFORMATION CHANGE INDICATION

If the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Not started" then integrity protection (and integrity checking) shall not be performed on any RRC message.

For each signalling radio bearer, the UE shall use two RRC hyper frame numbers:

- "Uplink RRC HFN";
- "Downlink RRC HFN".

and two message sequence numbers:

- "Uplink RRC Message sequence number";
- "Downlink RRC Message sequence number".

The above information is stored in the variable INTEGRITY_PROTECTION_INFO per signalling radio bearer (RB0-RB4).

Upon the first activation of integrity protection for an RRC connection, UE and UTRAN initialise the "Uplink RRC Message sequence number" and "Downlink RRC Message sequence number" for all signalling radio bearers as specified in subclauses 8.6.3.5 and 8.5.10.1.

The RRC message sequence number (RRC SN) is incremented for every integrity protected RRC message.

If the IE "Integrity Protection Mode Info" is present in a received message, the UE shall:

1> perform the actions in subclause 8.6.3.5 before proceeding with the integrity check of the received message.

8.5.10.1 Integrity protection in downlink

If the UE receives an RRC message on signalling radio bearer with RB identity n, the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" and the IE 'Integrity check info' is present the UE shall:

1> check the value of the IE "RRC message sequence number" included in the IE "Integrity check info";

2> if the "Downlink RRC Message sequence number" is not present in the variable INTEGRITY_PROTECTION_INFO:

3> initialise the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with the value of the IE "RRC message sequence number" included in the IE "Integrity check info" of the received message.

2> if the "Downlink RRC Message sequence number" is present in the variable INTEGRITY_PROTECTION_INFO:

3> if the RRC message sequence number is lower than the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO:

4> increment "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with one.

NOTE: The actions above imply that also for the case the "Downlink RRC HFN" is re-initialised by a security mode control procedure, this "Downlink RRC HFN" value is incremented by one before it is applied for the integrity protection of any received message if the conditions above are fulfilled.

3> if the RRC message sequence number is equal to the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO:

4> discard the message.

1> calculate an expected message authentication code in accordance with subclause 8.5.10.3;

1> compare the expected message authentication code with the value of the received IE "message authentication code" contained in the IE "Integrity check info";

2> if the expected message authentication code and the received message authentication code are the same, the integrity check is successful:

3> update the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with the value of the IE "RRC message sequence number" included in the IE "Integrity check info" of the received RRC message.

2> if the calculated expected message authentication code and the received message authentication code differ:

3> act as if the message was not received;~~if the IE "RRC message sequence number" included in the IE "Integrity check info" is lower than the "Downlink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO (in this case the "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO was incremented by one, as stated above):~~

4> ~~decrement "Downlink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO by one.~~

~~3> discard the message.~~

If the UE receives an RRC message on signalling radio bearer with identity n, the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" and the IE 'Integrity check info' is not present the UE shall:

1> discard the message.

UTRAN may transmit several copies of the same message in the downlink to increase the probability of proper reception of the message by the UE. In such a case, the RRC SN for these repeated messages should be the same.

3GPP TSG-RAN2 Meeting #34 **Tdoc ⌘R2-030465**
Sophia Antipolis, France, 17th – 21st February 2003

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1835**	⌘ **rev**	**-**	⌘	Current version:	**3.13.0**	⌘

*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:	⌘	Reporting Cell Status and Event 2A		
Source:	⌘	TSG-RAN WG2		
Work item code:	⌘	TEI	***Date:*** ⌘	01/02/2003
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 semantic description of the choice “Report cells within active set” of the IE “Reporting cell status” currently forbids the use for inter-RAT and periodic inter-frequency measurements. This could be interpreted such that this choice is valid for all event based inter-frequency measurements. This is not the case, only events 2D and 2F are allowed (and in fact required) to use this choice.

2. CR 1720 which was agreed during the last RAN meeting introduced an ambiguity into the description of measurement event 2A. Section 14.2.1.1 now specifies that the measurement report shall include “measured results for the non-used frequency that triggered the event”. This could be interpreted such that event 2A can only be triggered by non-used frequencies.
The intended behaviour is that event 2A can be triggered by the used frequency but the measured results are left out from the measurement report in this case.

Impact analysis:

A UE implementation that does not take the CR into account will not indicate to the network that the currently used frequency is the best frequency. This could trigger unwanted inter-frequency HHOs.

Summary of change: ⌘

1. The choice “Report cells within active set” is only valid for intra-frequency measurements and for the inter-frequency reporting events 2D and 2F.

2. The UE shall include the measured results only if the event was triggered by

		a non-used frequency.
Consequences if not approved:	⌘	Ambiguity remains, UEs might report measurement event 2A (change of best frequency) in different ways which could lead to problems with inter-frequency handovers.

Clauses affected:	⌘	10.3.7.61, 14.2.1.1				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

10.3.7.61 Reporting Cell Status

Indicates maximum allowed number of cells to report and whether active set cells and/or virtual active set cells and/or monitored set cells on and/or detected set cells used frequency and/or monitored set cells on non used frequency should/should not be included in the IE "Measured results".

Information Element/Group name	Need	Multi	Type and reference	Semantics description
CHOICE *reported cell*	MP			
>Report cells within active set				This choice is not valid for inter-RAT measurements. For inter-frequency measurements it is only valid for reporting events 2D and 2F (see note1).~~or periodic inter-frequency measurements~~
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report cells within monitored set cells on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report cells within active set and/or monitored set cells on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report cells within detected set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report cells within monitored set and/or detected set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report all active set cells + cells within monitored set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Enumerated (virtual/active set cells+1, virtual/active set cells+2, …., virtual/active set cells+6)	
>Report all active set cells + cells within detected set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Enumerated (virtual/active set cells+1, virtual/active set cells+2, …., virtual/active set cells+6)	
>Report all active set cells + cells within monitored set and/or detected set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Enumerated (virtual/active set cells+1, virtual/active	

Information Element/Group name	Need	Multi	Type and reference	Semantics description
			set cells+2, …., virtual/active set cells+6)	
>Report cells within virtual active set				This choice is not valid for intra-frequency or inter-RAT measurements
>>Maximum number of reported cells per reported non-used frequency	MP		Integer(1..6)	
>Report cells within monitored set on non-used frequency				This choice is not valid for intra-frequency or inter-RAT measurements
>>Maximum number of reported cells per reported non-used frequency	MP		Integer(1..6)	
>Report cells within monitored and/or virtual active set on non-used frequency				This choice is not valid for intra-frequency or inter-RAT measurements
>>Maximum number of reported cells per reported non-used frequency	MP		Integer(1..6)	
>Report all virtual active set cells + cells within monitored set on non-used frequency				This choice is not valid for intra-frequency or inter-RAT measurements
>>Maximum number of reported cells per reported non-used frequency	MP		Enumerated (virtual/active set cells+1, virtual/active set cells+2, …., virtual/active set cells+6)	
>Report cells within active set or within virtual active set or of the other RAT				If this choice is selected for inter-RAT measurements, the UE shall report only cells of the other RAT. If this choice is selected for intra-frequency measurements, the UE shall report cells within the active set. If this choice is selected for inter-frequency measurements, the UE shall report cells within the virtual active set.
>>Maximum number of reported cells	MP		Integer (1..12)	
>Report cells within active and/or monitored set on used frequency or within virtual active and/or monitored set on non-used frequency				This choice is not valid for inter-RAT measurements. If this choice is selected for intra-frequency measurements, the UE shall report cells within the active and/or monitored set. If this choice is selected for inter-frequency measurements, the UE shall report cells within the virtual active set and/or monitored set on non-used frequency.
>>Maximum number of reported cells	MP		Integer(1..12)	

NOTE 1: For Inter-frequency reporting events 2D and 2F, only CHOICE "Report cells within active set" is valid.

14.2.1.1 Event 2a: Change of best frequency.

When event 2a is configured in the UE within a measurement, the UE shall:

1> when the measurement is initiated or resumed:

2> store the used frequency in the variable BEST_FREQUENCY_2A_EVENT.

1> if equation 1 below has been fulfilled for a time period indicated by "Time to trigger" for a frequency included for that event and which is not stored in the variable BEST_FREQUENCY_2A_EVENT:

2> send a measurement report with IEs set as below:

3> set in "inter-frequency measurement event results":

4> "inter-frequency event identity" to "2a"; and

4> "Frequency info" to the frequency that triggered the event; and

4> "Non frequency related measurement event results" to the "Primary CPICH info" of the best primary CPICH for FDD cells or "Primary CCPCH info" to the "Cells parameters ID" of the best primary CCPCH for TDD cells on that frequency, not taking into account the cell individual offset.

3> if a non-used frequency triggered the measurement report:

4> include in IE "Inter-frequency measured results list" the measured results for the non-used frequency that triggered the event, not taking into account the cell individual offset;

3> if the used frequency triggered the measurement report:

4> do not include the IE "Inter-frequency measured results list" in the measurement report;

3> set the IE "additional measured results" according to subclause 8.4.2, not taking into account the cell individual offset;

2> update the variable BEST_FREQUENCY_2A_EVENT with that frequency.

Equation 1:

$$Q_{NotBest} \geq Q_{Best} + H_{2a}/2$$

The variables in the formula are defined as follows:

$\boldsymbol{Q_{Not\ Best}}$ is the quality estimate of a frequency not stored the "best frequency" in the variable BEST_FREQUENCY_2A_EVENT.

$\boldsymbol{Q_{Best}}$ is the quality estimate of the frequency stored in "best frequency" in the variable BEST_FREQUENCY_2A_EVENT.

$\boldsymbol{H_{2a}}$ is the hysteresis parameter for the event 2a in that measurement.

3GPP TSG-RAN2 Meeting #34
Sophia Antipolis, France, 17th – 21st February 2003

Tdoc ⌘R2-030466

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1836**	⌘**rev**	**-**	⌘	Current version:	**4.8.0** ⌘

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:	⌘	Reporting Cell Status and Event 2A		
Source:	⌘	TSG-RAN WG2		
Work item code:	⌘	TEI	***Date:*** ⌘	01/02/2003
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 semantic description of the choice “Report cells within active set” of the IE “Reporting cell status” currently forbids the use for inter-RAT and periodic inter-frequency measurements. This could be interpreted such that this choice is valid for all event based inter-frequency measurements. This is not the case, only events 2D and 2F are allowed (and in fact required) to use this choice.

2. CR 1720 which was agreed during the last RAN meeting introduced an ambiguity into the description of measurement event 2A. Section 14.2.1.1 now specifies that the measurement report shall include “measured results for the non-used frequency that triggered the event”. This could be interpreted such that event 2A can only be triggered by non-used frequencies.
The intended behaviour is that event 2A can be triggered by the used frequency but the measured results are left out from the measurement report in this case.

Impact analysis:

A UE implementation that does not take the CR into account will not indicate to the network that the currently used frequency is the best frequency. This could trigger unwanted inter-frequency HHOs.

Summary of change: ⌘

1. The choice “Report cells within active set” is only valid for intra-frequency measurements and for the inter-frequency reporting events 2D and 2F.

2. The UE shall include the measured results only if the event was triggered by

		a non-used frequency.
Consequences if not approved:	⌘	Ambiguity remains, UEs might report measurement event 2A (change of best frequency) in different ways which could lead to problems with inter-frequency handovers.

Clauses affected:	⌘	10.3.7.61, 14.2.1.1

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

Other comments:	⌘	

10.3.7.61 Reporting Cell Status

Indicates maximum allowed number of cells to report and whether active set cells and/or virtual active set cells and/or monitored set cells on and/or detected set cells used frequency and/or monitored set cells on non used frequency should/should not be included in the IE "Measured results".

Information Element/Group name	Need	Multi	Type and reference	Semantics description
CHOICE *reported cell*	MP			
>Report cells within active set				This choice is not valid for inter-RAT measurements. For inter-frequency measurements it is only valid for reporting events 2D and 2F (see note1).~~or periodic inter-frequency measurements~~
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report cells within monitored set cells on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report cells within active set and/or monitored set cells on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report cells within detected set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report cells within monitored set and/or detected set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report all active set cells + cells within monitored set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Enumerated (virtual/active set cells+1, virtual/active set cells+2, …., virtual/active set cells+6)	
>Report all active set cells + cells within detected set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Enumerated (virtual/active set cells+1, virtual/active set cells+2, …., virtual/active set cells+6)	
>Report all active set cells + cells within monitored set and/or detected set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Enumerated (virtual/active set cells+1, virtual/active	

Information Element/Group name	Need	Multi	Type and reference	Semantics description
			set cells+2, …., virtual/active set cells+6)	
>Report cells within virtual active set				This choice is not valid for intra-frequency or inter-RAT measurements
>>Maximum number of reported cells per reported non-used frequency	MP		Integer(1..6)	
>Report cells within monitored set on non-used frequency				This choice is not valid for intra-frequency or inter-RAT measurements
>>Maximum number of reported cells per reported non-used frequency	MP		Integer(1..6)	
>Report cells within monitored and/or virtual active set on non-used frequency				This choice is not valid for intra-frequency or inter-RAT measurements
>>Maximum number of reported cells per reported non-used frequency	MP		Integer(1..6)	
>Report all virtual active set cells + cells within monitored set on non-used frequency				This choice is not valid for intra-frequency or inter-RAT measurements
>>Maximum number of reported cells per reported non-used frequency	MP		Enumerated (virtual/active set cells+1, virtual/active set cells+2, …., virtual/active set cells+6)	
>Report cells within active set or within virtual active set or of the other RAT				If this choice is selected for inter-RAT measurements, the UE shall report only cells of the other RAT. If this choice is selected for intra-frequency measurements, the UE shall report cells within the active set. If this choice is selected for inter-frequency measurements, the UE shall report cells within the virtual active set.
>>Maximum number of reported cells	MP		Integer (1..12)	
>Report cells within active and/or monitored set on used frequency or within virtual active and/or monitored set on non-used frequency				This choice is not valid for inter-RAT measurements. If this choice is selected for intra-frequency measurements, the UE shall report cells within the active and/or monitored set. If this choice is selected for inter-frequency measurements, the UE shall report cells within the virtual active set and/or monitored set on non-used frequency.
>>Maximum number of reported cells	MP		Integer(1..12)	

NOTE 1: For Inter-frequency reporting events 2D and 2F, only CHOICE "Report cells within active set" is valid.

14.2.1.1 Event 2a: Change of best frequency.

When event 2a is configured in the UE within a measurement, the UE shall:

1> when the measurement is initiated or resumed:

2> store the used frequency in the variable BEST_FREQUENCY_2A_EVENT.

1> if equation 1 below has been fulfilled for a time period indicated by "Time to trigger" for a frequency included for that event and which is not stored in the variable BEST_FREQUENCY_2A_EVENT:

2> send a measurement report with IEs set as below:

3> set in "inter-frequency measurement event results":

4> "inter-frequency event identity" to "2a"; and

4> "Frequency info" to the frequency that triggered the event; and

4> "Non frequency related measurement event results" to the "Primary CPICH info" of the best primary CPICH for FDD cells or "Primary CCPCH info" to the "Cells parameters ID" of the best primary CCPCH for TDD cells on that frequency, not taking into account the cell individual offset.

3> if a non-used frequency triggered the measurement report:

4> include in IE "Inter-frequency measured results list" the measured results for the non-used frequency that triggered the event, not taking into account the cell individual offset;

3> if the used frequency triggered the measurement report:

4> do not include the IE "Inter-frequency measured results list" in the measurement report;

3> set the IE "additional measured results" according to subclause 8.4.2, not taking into account the cell individual offset;

2> update the variable BEST_FREQUENCY_2A_EVENT with that frequency.

Equation 1:

$$Q_{NotBest} \geq Q_{Best} + H_{2a}/2$$

The variables in the formula are defined as follows:

$\boldsymbol{Q_{Not\ Best}}$ is the quality estimate of a frequency not stored the "best frequency" in the variable BEST_FREQUENCY_2A_EVENT.

$\boldsymbol{Q_{Best}}$ is the quality estimate of the frequency stored in "best frequency" in the variable BEST_FREQUENCY_2A_EVENT.

$\boldsymbol{H_{2a}}$ is the hysteresis parameter for the event 2a in that measurement.

3GPP TSG-RAN2 Meeting #34 **_Tdoc ⌘R2-030467_**
Sophia Antipolis, France, 17th – 21st February 2003

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1837**	⌘**rev**	**-**	⌘	Current version:	**5.3.0** ⌘

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

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

Title:	⌘	Reporting Cell Status and Event 2A		
Source:	⌘	TSG-RAN WG2		
Work item code:	⌘	TEI	***Date:*** ⌘	01/02/2003
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: ⌘

1. The semantic description of the choice “Report cells within active set” of the IE “Reporting cell status” currently forbids the use for inter-RAT and periodic inter-frequency measurements. This could be interpreted such that this choice is valid for all event based inter-frequency measurements. This is not the case, only events 2D and 2F are allowed (and in fact required) to use this choice.

2. CR 1720 which was agreed during the last RAN meeting introduced an ambiguity into the description of measurement event 2A. Section 14.2.1.1 now specifies that the measurement report shall include “measured results for the non-used frequency that triggered the event”. This could be interpreted such that event 2A can only be triggered by non-used frequencies.
   The intended behaviour is that event 2A can be triggered by the used frequency but the measured results are left out from the measurement report in this case.

Impact analysis:

A UE implementation that does not take the CR into account will not indicate to the network that the currently used frequency is the best frequency. This could trigger unwanted inter-frequency HHOs.

Summary of change: ⌘

1. The choice “Report cells within active set” is only valid for intra-frequency measurements and for the inter-frequency reporting events 2D and 2F.

2. The UE shall include the measured results only if the event was triggered by

		a non-used frequency.
Consequences if not approved:	⌘	Ambiguity remains, UEs might report measurement event 2A (change of best frequency) in different ways which could lead to problems with inter-frequency handovers.

Clauses affected:	⌘	10.3.7.61, 14.2.1.1				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

10.3.7.61 Reporting Cell Status

Indicates maximum allowed number of cells to report and whether active set cells and/or virtual active set cells and/or monitored set cells on and/or detected set cells used frequency and/or monitored set cells on non used frequency should/should not be included in the IE "Measured results".

Information Element/Group name	Need	Multi	Type and reference	Semantics description
CHOICE *reported cell*	MP			
>Report cells within active set				This choice is not valid for inter-RAT measurements. For inter-frequency measurements it is only valid for reporting events 2D and 2F (see note1).~~or periodic inter-frequency measurements~~
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report cells within monitored set cells on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report cells within active set and/or monitored set cells on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report cells within detected set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report cells within monitored set and/or detected set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Integer(1..6)	
>Report all active set cells + cells within monitored set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Enumerated (virtual/active set cells+1, virtual/active set cells+2, …., virtual/active set cells+6)	
>Report all active set cells + cells within detected set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Enumerated (virtual/active set cells+1, virtual/active set cells+2, …., virtual/active set cells+6)	
>Report all active set cells + cells within monitored set and/or detected set on used frequency				This choice is not valid for inter-RAT or inter-frequency measurements
>>Maximum number of reported cells	MP		Enumerated (virtual/active set cells+1, virtual/active	

Information Element/Group name	Need	Multi	Type and reference	Semantics description
			set cells+2, …., virtual/active set cells+6)	
>Report cells within virtual active set				This choice is not valid for intra-frequency or inter-RAT measurements
>>Maximum number of reported cells per reported non-used frequency	MP		Integer(1..6)	
>Report cells within monitored set on non-used frequency				This choice is not valid for intra-frequency or inter-RAT measurements
>>Maximum number of reported cells per reported non-used frequency	MP		Integer(1..6)	
>Report cells within monitored and/or virtual active set on non-used frequency				This choice is not valid for intra-frequency or inter-RAT measurements
>>Maximum number of reported cells per reported non-used frequency	MP		Integer(1..6)	
>Report all virtual active set cells + cells within monitored set on non-used frequency				This choice is not valid for intra-frequency or inter-RAT measurements
>>Maximum number of reported cells per reported non-used frequency	MP		Enumerated (virtual/active set cells+1, virtual/active set cells+2, …., virtual/active set cells+6)	
>Report cells within active set or within virtual active set or of the other RAT				If this choice is selected for inter-RAT measurements, the UE shall report only cells of the other RAT. If this choice is selected for intra-frequency measurements, the UE shall report cells within the active set. If this choice is selected for inter-frequency measurements, the UE shall report cells within the virtual active set.
>>Maximum number of reported cells	MP		Integer (1..12)	
>Report cells within active and/or monitored set on used frequency or within virtual active and/or monitored set on non-used frequency				This choice is not valid for inter-RAT measurements. If this choice is selected for intra-frequency measurements, the UE shall report cells within the active and/or monitored set. If this choice is selected for inter-frequency measurements, the UE shall report cells within the virtual active set and/or monitored set on non-used frequency.
>>Maximum number of reported cells	MP		Integer(1..12)	

NOTE 1: For Inter-frequency reporting events 2D and 2F, only CHOICE "Report cells within active set" is valid.

14.2.1.1 Event 2a: Change of best frequency.

When event 2a is configured in the UE within a measurement, the UE shall:

1> when the measurement is initiated or resumed:

2> store the used frequency in the variable BEST_FREQUENCY_2A_EVENT.

1> if equation 1 below has been fulfilled for a time period indicated by "Time to trigger" for a frequency included for that event and which is not stored in the variable BEST_FREQUENCY_2A_EVENT:

2> send a measurement report with IEs set as below:

3> set in "inter-frequency measurement event results":

4> "inter-frequency event identity" to "2a"; and

4> "Frequency info" to the frequency that triggered the event; and

4> "Non frequency related measurement event results" to the "Primary CPICH info" of the best primary CPICH for FDD cells or "Primary CCPCH info" to the "Cells parameters ID" of the best primary CCPCH for TDD cells on that frequency, not taking into account the cell individual offset.

3> if a non-used frequency triggered the measurement report:

4> include in IE "Inter-frequency measured results list" the measured results for the non-used frequency that triggered the event, not taking into account the cell individual offset;

3> if the used frequency triggered the measurement report:

4> do not include the IE "Inter-frequency measured results list" in the measurement report;

3> set the IE "additional measured results" according to subclause 8.4.2, not taking into account the cell individual offset;

2> update the variable BEST_FREQUENCY_2A_EVENT with that frequency.

Equation 1:

$$Q_{NotBest} \geq Q_{Best} + H_{2a}/2$$

The variables in the formula are defined as follows:

$\boldsymbol{Q_{Not\ Best}}$ is the quality estimate of a frequency not stored the "best frequency" in the variable BEST_FREQUENCY_2A_EVENT.

$\boldsymbol{Q_{Best}}$ is the quality estimate of the frequency stored in "best frequency" in the variable BEST_FREQUENCY_2A_EVENT.

$\boldsymbol{H_{2a}}$ is the hysteresis parameter for the event 2a in that measurement.

3GPP TSG- RAN WG2 Meeting #34
Sophia-Antipolis, France, 17-21 February 2003

Tdoc ⌘R2-030468

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1838**	⌘ **rev**	**-**	⌘	Current version:	**3.13.0** ⌘

*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 the handling of variable TGPS_IDENTITY and IE “Triggering condition 1/2”		
Source:	⌘	TSG-RAN WG2		
Work item code:	⌘	TEI	***Date:*** ⌘	11/02/2003
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. To align the behaviour specified in other places, the "Current TGPS Status Flag" for the pattern sequence in the variable TGPS_IDENTITY shall be set to "inactive" after deactivating the corresponding compressed mode pattern sequence.

2. The UE shall activate the stored pattern sequence based on the "TGPS status flag" in the variable TGPS_IDENTITY, instead of "Current TGPS status flag".

3. It is impossible to indicate detected set cells in the IE "Triggering condition 1". And the IE "Triggering condition 2" is mandatory for event 1a or 1e, not 1a or 1c.

4. According to CellSelectReselectInfoSIB-11-12-RSCP in ASN.1, the Qoffset$2_{s,n}$ shall be absent if the IE "Cell_selection_and_reselection_quality_measure" has the value RSCP.

Summary of change: ⌘

1. In section 8.6.6.15, add action to set the "Current TGPS Status Flag" for the pattern sequence in the variable TGPS_IDENTITY to "inactive".

2. In section 8.6.6.15, change the "Current TGPS Status Flag" to "TGPS Status Flag".

3. In section 8.6.7.16, remove the case of 1b or 1f and change “1a or 1c” to “1a or 1e”.

4. In section 10.3.2.4, change the word “optional” to “absent”.

		Impact analysis: Impacted functionality: the procedures to handle the variable TGPS_IDENTITY and IE “Triggering condition 1/2” Correction type: Clarification of a function where the specification is incomplete, ambiguous and/or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise Interoperability: • Isolated impact: the impact is isolated; only the corrected functionality is affected. • UE impact only. If a UE does not implement this CR, it may cause the wrong UE behaviour while receiving next IE “DPCH Compressed mode info” and may make the compressed mode fail to be activated or deactivated.
Consequences if not approved:	⌘	If the UE does not set "Current TGPS Status Flag" in the variable TGPS_IDENTITY correctly, it may cause the wrong UE behaviour while receiving next IE “DPCH Compressed mode info” and may make the compressed mode fail to be activated or deactivated.

Clauses affected:	⌘	8.6.6.15, 8.6.7.16, 10.3.2.4				
		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.

8.6.6.15 DPCH Compressed mode info

If the IE "DPCH compressed mode info" is included, and if the IE group "transmission gap pattern sequence configuration parameters" is included, the UE shall for each transmission gap pattern sequence perform the following consistency checks:

1> if the UE, according to its measurement capabilities, and for all supported bands of the UTRA mode or RAT associated with the measurement purpose indicated by IE "TGMP", requires UL compressed mode, and CHOICE 'UL/DL mode' indicates 'DL only':

2> set the variable INVALID_CONFIGURATION to TRUE.

1> if the UE, according to its measurement capabilities, and for all supported bands of the UTRA mode or RAT associated with the measurement purpose indicated by IE "TGMP", requires DL compressed mode, and CHOICE 'UL/DL mode' indicates 'UL only':

2> set the variable INVALID_CONFIGURATION to TRUE.

1> if the UE, according to its measurement capabilities, does not require UL compressed mode for any of supported band of the UTRA mode or RAT associated with the measurement purpose indicated by the IE "TGMP", and CHOICE 'UL/DL mode' indicates 'UL only' or 'UL and DL':

2> set the variable INVALID_CONFIGURATION to TRUE.

1> if the UE, according to its measurement capabilities, does not require DL compressed mode for any supported band of the UTRA mode or RAT associated with the measurement purpose indicated by the IE "TGMP", and CHOICE 'UL/DL mode' indicates 'DL only' or 'UL and DL':

2> set the variable INVALID_CONFIGURATION to TRUE.

1> if UE already has an active transmission gap pattern sequence that, according to IE "TGMP", has the same measurement purpose, and both patterns will be active after the new configuration has been taken into use:

2> set the variable INVALID_CONFIGURATION to TRUE.

If variable INVALID_CONFIGURATION has value FALSE after UE has performed the checks above, the UE shall:

1> if pattern sequence corresponding to IE "TGPSI" is already active (according to "Current TGPS Status Flag") in the variable TGPS_IDENTITY):

2> if the "TGPS Status Flag" in this message is set to "deactivate" for the corresponding pattern sequence:

3> deactivate this pattern sequence at the beginning of the frame, indicated by IE "Activation time"(see subclause 8.6.3.1) received in this message, when the new configuration received in this message is taken into use.

3> set the "Current TGPS Status Flag" for this pattern sequence in the variable TGPS_IDENTITY to "inactive".

2> if the "TGPS Status Flag" in this message is set to "activate" for the corresponding pattern sequence:

3> deactivate this pattern sequence at the beginning of the frame, indicated by IE "Activation time"(see subclause 8.6.3.1) received in this message, when the new configuration received in this message is taken into use.

NOTE: The temporary deactivation of pattern sequences for which the status flag is set to "activate" can be used by the network to align the timing of already active patterns with newly activated patterns.

1> update each pattern sequence to the variable TGPS_IDENTITY according to the IE "TGPSI";

1> update into the variable TGPS_IDENTITY the configuration information defined by IE group" transmission gap pattern sequence configuration parameters ";

1> after the new configuration has been taken into use:

2> activate the stored pattern sequence corresponding to each IE "TGPSI" for which the "~~Current~~ TGPS status flag" in the variable TGPS_IDENTITY is set to "activate" at the time indicated by IE "TGCFN"; and

2> begin the inter-frequency and/or inter-RAT measurements corresponding to the pattern sequence measurement purpose of each activated pattern sequence;

2> if the new configuration is taken into use at the same CFN as indicated by IE "TGCFN":

3> start the concerned pattern sequence immediately at that CFN.

1> monitor if the parallel transmission gap pattern sequences create an illegal overlap, and in case of overlap, take actions as specified in subclause 8.2.11.2.

If the IE "DPCH compressed mode info" is included, and if the IE group "transmission gap pattern sequence configuration parameters" is not included, the UE shall:

1> if pattern sequence corresponding to IE "TGPSI" is already active (according to "Current TGPS Status Flag" in the variable TGPS_IDENTITY):

2> if the "TGPS Status Flag" in this message is set to "deactivate" for the corresponding pattern sequence:

3> deactivate this pattern sequence at the beginning of the frame, indicated by IE "Activation time"(see subclause 8.6.3.1) received in this message, when the new configuration received in this message is taken into use;

3> set the "Current TGPS Status Flag" for this pattern sequence in the variable TGPS_IDENTITY to "inactive".

2> if the "TGPS Status Flag" in this message is set to "activate" for the corresponding pattern sequence:

3> deactivate this pattern sequence at the beginning of the frame, indicated by IE "Activation time"(see subclause 8.6.3.1) received in this message, when the new configuration received in this message is taken into use.

NOTE: The temporary deactivation of pattern sequences for which the status flag is set to "activate" can be used by the network to align the timing of already active patterns with newly activated patterns.

1> after the new configuration has been taken into use:

2> at the time indicated by IE "TGCFN":

3> activate the stored pattern sequence corresponding to each IE "TGPSI" for which the "TGPS status flag" is set to "activate"; and

3> set the "Current TGPS Status Flag" for this pattern sequence in the variable TGPS_IDENTITY to "active".

2> begin the inter-frequency and/or inter-RAT measurements corresponding to the pattern sequence measurement purpose of each activated pattern sequence;

2> if the new configuration is taken into use at the same CFN as indicated by IE "TGCFN":

3> start the concerned pattern sequence immediately at that CFN.

For transmission gap pattern sequences stored in variable TGPS_IDENTITY, but not identified in IE "TGPSI" (either due to the absence of the IE "DPCH compressed mode info" in the received message or due to not receiving the corresponding TGPSI value in the IE "DPCH compressed mode info"), the UE shall:

1> if the received message implies a timing re-initialised hard handover (see subclause 8.3.5.1):

2> deactivate such transmission gap pattern sequences at the beginning of the frame, indicated by IE "Activation time" (see subclause 8.6.3.1) received in this message; and

2> set IE "Current TGPS Status Flag" in corresponding UE variable TGPS_IDENTITY to 'inactive'.

1> if the received message not implies a timing re-initialised hard handover (see subclause 8.3.5.1):

2> continue such transmission gap pattern sequence according to IE "Current TGPS Status Flag" in the corresponding UE variable TGPS_IDENTITY.

Uplink and downlink compressed mode methods are described in [27]. For UL "higher layer scheduling" compressed mode method and transport format combination selection, see [15].

8.6.7.16 Intra-frequency measurement

If IE "Intra-frequency measurement" is received by the UE in a MEASUREMENT CONTROL message, where IE "measurement command" has the value "setup", but IE "Intra-frequency measurement quantity", IE "Intra-frequency reporting quantity", "CHOICE Report criteria" or "parameters required for each event" (given "CHOICE report criteria" is set to "intra-frequency measurement reporting criteria") is not received, the UE shall:

1> clear all stored measurement control information related associated to this measurement identity in variable MEASUREMENT_IDENTITY;

1> set the variable CONFIGURATION_INCOMPLETE to TRUE.

In case of 1a or 1e~~c (resp. 1b or 1f)~~ event-triggered reporting:

1> if the IE "Intra-frequency measurement quantity~~criteria~~" is set to "pathloss", the UE shall:

2> if detected set cells are indicated as possibly triggering the event within the IEs "Triggering condition 2" ~~(resp. "Triggering condition 1")~~:

3> set the variable CONFIGURATION_INCOMPLETE to TRUE.

10.3.2.4 Cell selection and re-selection info for SIB11/12

Information Element/Group name	Need	Multi	Type and reference	Semantics description
$\text{Qoffset1}_{s,n}$	MD		Integer(-50..50)	Default value is 0. [dB]
$\text{Qoffset2}_{s,n}$	CV-*FDD-Quality-Measure*		Integer(-50..50)	Default value is 0. [dB]
Maximum allowed UL TX power	MD		Maximum allowed UL TX power 10.3.6.39	According to UE_TXPWR_MAX_RACH in [4], [dBm]. If applied to FDD or TDD cells, the default is the Maximum allowed UL TX power for the serving cell. If applied to a GSM cell, the default is the UE maximum output power applicable for this GSM cell, according to the UE's radio access capability.
HCS neighbouring cell information	OP		HCS Neighbouring cell information 10.3.7.11	
CHOICE *mode*	MP			
>FDD				
>>Qqualmin	CV-*FDD-Serving-Cell*		Integer (-24..0)	Ec/N0, [dB] Default value is Qqualmin for the serving cell
>>Qrxlevmin	MD		Integer (-115..-25 by step of 2)	RSCP, [dBm] Default value is Qrxlevmin for the serving cell
>TDD				
>>Qrxlevmin	MD		Integer (-115..-25 by step of 2)	RSCP, [dBm] Default value is Qrxlevmin for the serving cell
>GSM				
>>Qrxlevmin	MD		Integer (-115..-25 by step of 2)	GSM RSSI, [dBm] Default value is Qrxlevmin for the serving cell

Condition	Explanation
FDD-Quality-Measure	This IE is mandatory and has a default value for Intra/Inter Frequency Cells if the IE "Cell selection and reselection quality measure" has the value CPICH Ec/No. Otherwise the IE is ~~optional~~absent.
FDD-Serving-Cell	This IE is mandatory and has a default value if the serving cell is an FDD cell. Otherwise the IE is mandatory present.

3GPP TSG- RAN WG2 Meeting #34
Sophia-Antipolis, France, 17-21 February 2003

Tdoc ⌘R2-030469

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1839**	⌘**rev**	**-**	⌘	Current version:	**4.8.0**	⌘

*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 the handling of variable TGPS_IDENTITY and IE "Triggering condition 1/2"		
Source:	⌘	TSG-RAN WG2		
Work item code:	⌘	TEI	***Date:*** ⌘	11/02/2003
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. To align the behaviour specified in other places, the "Current TGPS Status Flag" for the pattern sequence in the variable TGPS_IDENTITY shall be set to "inactive" after deactivating the corresponding compressed mode pattern sequence. 2. The UE shall activate the stored pattern sequence based on the "TGPS status flag" in the variable TGPS_IDENTITY, instead of "Current TGPS status flag". 3. It is impossible to indicate detected set cells in the IE "Triggering condition 1". And the IE "Triggering condition 2" is mandatory for event 1a or 1e, not 1a or 1c. 4. According to CellSelectReselectInfoSIB-11-12-RSCP in ASN.1, the Qoffset2$_{s,n}$ shall be absent if the IE "Cell_selection_and_reselection_quality_measure" has the value RSCP.
Summary of change:	⌘	1. In section 8.6.6.15, add action to set the "Current TGPS Status Flag" for the pattern sequence in the variable TGPS_IDENTITY to "inactive". 2. In section 8.6.6.15, change the "Current TGPS Status Flag" to "TGPS Status Flag". 3. In section 8.6.7.16, remove the case of 1b or 1f and change "1a or 1c" to "1a or 1e". 4. In section 10.3.2.4, change the word "optional" to "absent".

Consequences if not approved:	⌘	If the UE does not set "Current TGPS Status Flag" in the variable TGPS_IDENTITY correctly, it may cause the wrong UE behaviour while receiving next IE “DPCH Compressed mode info” and may make the compressed mode fail to be activated or deactivated.

Clauses affected:	⌘	8.6.6.15, 8.6.7.16, 10.3.2.4				
		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.

8.6.6.15 DPCH Compressed mode info

If the IE "DPCH compressed mode info" is included, and if the IE group "transmission gap pattern sequence configuration parameters" is included, the UE shall for each transmission gap pattern sequence perform the following consistency checks:

1> if the UE, according to its measurement capabilities, and for all supported bands of the UTRA mode or RAT associated with the measurement purpose indicated by IE "TGMP", requires UL compressed mode, and CHOICE 'UL/DL mode' indicates 'DL only':

2> set the variable INVALID_CONFIGURATION to TRUE.

1> if the UE, according to its measurement capabilities, and for all supported bands of the UTRA mode or RAT associated with the measurement purpose indicated by IE "TGMP", requires DL compressed mode, and CHOICE 'UL/DL mode' indicates 'UL only':

2> set the variable INVALID_CONFIGURATION to TRUE.

1> if the UE, according to its measurement capabilities, does not require UL compressed mode for any of supported band of the UTRA mode or RAT associated with the measurement purpose indicated by the IE "TGMP", and CHOICE 'UL/DL mode' indicates 'UL only' or 'UL and DL':

2> set the variable INVALID_CONFIGURATION to TRUE.

1> if the UE, according to its measurement capabilities, does not require DL compressed mode for any supported band of the UTRA mode or RAT associated with the measurement purpose indicated by the IE "TGMP", and CHOICE 'UL/DL mode' indicates 'DL only' or 'UL and DL':

2> set the variable INVALID_CONFIGURATION to TRUE.

1> if UE already has an active transmission gap pattern sequence that, according to IE "TGMP", has the same measurement purpose, and both patterns will be active after the new configuration has been taken into use:

2> set the variable INVALID_CONFIGURATION to TRUE.

If variable INVALID_CONFIGURATION has value FALSE after UE has performed the checks above, the UE shall:

1> if pattern sequence corresponding to IE "TGPSI" is already active (according to "Current TGPS Status Flag") in the variable TGPS_IDENTITY):

2> if the "TGPS Status Flag" in this message is set to "deactivate" for the corresponding pattern sequence:

3> deactivate this pattern sequence at the beginning of the frame, indicated by IE "Activation time"(see subclause 8.6.3.1) received in this message, when the new configuration received in this message is taken into use.

3> set the "Current TGPS Status Flag" for this pattern sequence in the variable TGPS_IDENTITY to "inactive".

2> if the "TGPS Status Flag" in this message is set to "activate" for the corresponding pattern sequence:

3> deactivate this pattern sequence at the beginning of the frame, indicated by IE "Activation time"(see subclause 8.6.3.1) received in this message, when the new configuration received in this message is taken into use.

NOTE: The temporary deactivation of pattern sequences for which the status flag is set to "activate" can be used by the network to align the timing of already active patterns with newly activated patterns.

1> update each pattern sequence to the variable TGPS_IDENTITY according to the IE "TGPSI";

1> update into the variable TGPS_IDENTITY the configuration information defined by IE group" transmission gap pattern sequence configuration parameters ";

1> after the new configuration has been taken into use:

2> activate the stored pattern sequence corresponding to each IE "TGPSI" for which the "~~Current ~~TGPS status flag" in the variable TGPS_IDENTITY is set to "activate" at the time indicated by IE "TGCFN"; and

2> begin the inter-frequency and/or inter-RAT measurements corresponding to the pattern sequence measurement purpose of each activated pattern sequence;

2> if the new configuration is taken into use at the same CFN as indicated by IE "TGCFN":

3> start the concerned pattern sequence immediately at that CFN.

1> monitor if the parallel transmission gap pattern sequences create an illegal overlap, and in case of overlap, take actions as specified in subclause 8.2.11.2.

If the IE "DPCH compressed mode info" is included, and if the IE group "transmission gap pattern sequence configuration parameters" is not included, the UE shall:

1> if pattern sequence corresponding to IE "TGPSI" is already active (according to "Current TGPS Status Flag" in the variable TGPS_IDENTITY):

2> if the "TGPS Status Flag" in this message is set to "deactivate" for the corresponding pattern sequence:

3> deactivate this pattern sequence at the beginning of the frame, indicated by IE "Activation time"(see subclause 8.6.3.1) received in this message, when the new configuration received in this message is taken into use;

3> set the "Current TGPS Status Flag" for this pattern sequence in the variable TGPS_IDENTITY to "inactive".

2> if the "TGPS Status Flag" in this message is set to "activate" for the corresponding pattern sequence:

3> deactivate this pattern sequence at the beginning of the frame, indicated by IE "Activation time"(see subclause 8.6.3.1) received in this message, when the new configuration received in this message is taken into use.

NOTE: The temporary deactivation of pattern sequences for which the status flag is set to "activate" can be used by the network to align the timing of already active patterns with newly activated patterns.

1> after the new configuration has been taken into use:

2> at the time indicated by IE "TGCFN":

3> activate the stored pattern sequence corresponding to each IE "TGPSI" for which the "TGPS status flag" is set to "activate"; and

3> set the "Current TGPS Status Flag" for this pattern sequence in the variable TGPS_IDENTITY to "active".

2> begin the inter-frequency and/or inter-RAT measurements corresponding to the pattern sequence measurement purpose of each activated pattern sequence;

2> if the new configuration is taken into use at the same CFN as indicated by IE "TGCFN":

3> start the concerned pattern sequence immediately at that CFN.

For transmission gap pattern sequences stored in variable TGPS_IDENTITY, but not identified in IE "TGPSI" (either due to the absence of the IE "DPCH compressed mode info" in the received message or due to not receiving the corresponding TGPSI value in the IE "DPCH compressed mode info"), the UE shall:

1> if the received message implies a timing re-initialised hard handover (see subclause 8.3.5.1):

2> deactivate such transmission gap pattern sequences at the beginning of the frame, indicated by IE "Activation time" (see subclause 8.6.3.1) received in this message; and

2> set IE "Current TGPS Status Flag" in corresponding UE variable TGPS_IDENTITY to 'inactive'.

1> if the received message not implies a timing re-initialised hard handover (see subclause 8.3.5.1):

2> continue such transmission gap pattern sequence according to IE "Current TGPS Status Flag" in the corresponding UE variable TGPS_IDENTITY.

Uplink and downlink compressed mode methods are described in [27]. For UL "higher layer scheduling" compressed mode method and transport format combination selection, see [15].

8.6.7.16 Intra-frequency measurement

If IE "Intra-frequency measurement" is received by the UE in a MEASUREMENT CONTROL message, where IE "measurement command" has the value "setup", but IE "Intra-frequency measurement quantity", IE "Intra-frequency reporting quantity", "CHOICE Report criteria" or "parameters required for each event" (given "CHOICE report criteria" is set to "intra-frequency measurement reporting criteria") is not received, the UE shall:

1> clear all stored measurement control information related associated to this measurement identity in variable MEASUREMENT_IDENTITY;

1> set the variable CONFIGURATION_INCOMPLETE to TRUE.

In case of 1a or 1e~~c (resp. 1b or 1f)~~ event-triggered reporting:

1> if the IE "Intra-frequency measurement quantity~~criteria~~" is set to "pathloss", the UE shall:

2> if detected set cells are indicated as possibly triggering the event within the IEs "Triggering condition 2" ~~(resp. "Triggering condition 1")~~:

3> set the variable CONFIGURATION_INCOMPLETE to TRUE.

10.3.2.4 Cell selection and re-selection info for SIB11/12

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Qoffset1$_{s,n}$	MD		Integer(-50..50)	Default value is 0. [dB]
Qoffset2$_{s,n}$	CV-*FDD-Quality-Measure*		Integer(-50..50)	Default value is 0. [dB]
Maximum allowed UL TX power	MD		Maximum allowed UL TX power 10.3.6.39	According to UE_TXPWR_MAX_RACH in [4], [dBm]. If applied to FDD or TDD cells, the default is the Maximum allowed UL TX power for the serving cell. If applied to a GSM cell, the default is the UE maximum output power applicable for this GSM cell, according to the UE's radio access capability.
HCS neighbouring cell information	OP		HCS Neighbouring cell information 10.3.7.11	
CHOICE *mode*	MP			
>FDD				
>>Qqualmin	CV-*FDD-Serving-Cell*		Integer (-24..0)	Ec/N0, [dB] Default value is Qqualmin for the serving cell
>>Qrxlevmin	MD		Integer (-115..-25 by step of 2)	RSCP, [dBm] Default value is Qrxlevmin for the serving cell
>TDD				
>>Qrxlevmin	MD		Integer (-115..-25 by step of 2)	RSCP, [dBm] Default value is Qrxlevmin for the serving cell
>GSM				
>>Qrxlevmin	MD		Integer (-115..-25 by step of 2)	GSM RSSI, [dBm] Default value is Qrxlevmin for the serving cell

Condition	Explanation
FDD-Quality-Measure	This IE is mandatory and has a default value for Intra/Inter Frequency Cells if the IE "Cell selection and reselection quality measure" has the value CPICH Ec/No. Otherwise the IE is ~~optional~~absent.
FDD-Serving-Cell	This IE is mandatory and has a default value if the serving cell is an FDD cell. Otherwise the IE is mandatory present.

3GPP TSG- RAN WG2 Meeting #34
Sophia-Antipolis, France, 17-21 February 2003

Tdoc ⌘R2-030470

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1840**	⌘ **rev**	**-**	⌘	Current version:	**5.3.0** ⌘

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

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

Title:	⌘	Correction to the handling of variable TGPS_IDENTITY and IE “Triggering condition 1/2”		
Source:	⌘	TSG-RAN WG2		
Work item code:	⌘	TEI	***Date:*** ⌘	11/02/2003
Category:	⌘	**A** *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.	***Release:*** ⌘	Rel-5 *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. To align the behaviour specified in other places, the "Current TGPS Status Flag" for the pattern sequence in the variable TGPS_IDENTITY shall be set to "inactive" after deactivating the corresponding compressed mode pattern sequence. 2. The UE shall activate the stored pattern sequence based on the "TGPS status flag" in the variable TGPS_IDENTITY, instead of "Current TGPS status flag". 3. It is impossible to indicate detected set cells in the IE "Triggering condition 1". And the IE "Triggering condition 2" is mandatory for event 1a or 1e, not 1a or 1c. 4. According to CellSelectReselectInfoSIB-11-12-RSCP in ASN.1, the Qoffset2$_{s,n}$ shall be absent if the IE "Cell_selection_and_reselection_quality_measure" has the value RSCP.
Summary of change: ⌘	1. In section 8.6.6.15, add action to set the "Current TGPS Status Flag" for the pattern sequence in the variable TGPS_IDENTITY to "inactive". 2. In section 8.6.6.15, change the "Current TGPS Status Flag" to "TGPS Status Flag". 3. In section 8.6.7.16, remove the case of 1b or 1f and change “1a or 1c” to “1a or 1e”. 4. In section 10.3.2.4, change the word “optional” to “absent”.

Consequences if not approved:	⌘	If the UE does not set "Current TGPS Status Flag" in the variable TGPS_IDENTITY correctly, it may cause the wrong UE behaviour while receiving next IE “DPCH Compressed mode info” and may make the compressed mode fail to be activated or deactivated.

Clauses affected:	⌘	8.6.6.15, 8.6.7.16, 10.3.2.4				
		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.

8.6.6.15 DPCH Compressed mode info

If the IE "DPCH compressed mode info" is included, and if the IE group "transmission gap pattern sequence configuration parameters" is included, the UE shall for each transmission gap pattern sequence perform the following consistency checks:

1> if the UE, according to its measurement capabilities, and for all supported bands of the UTRA mode or RAT associated with the measurement purpose indicated by IE "TGMP", requires UL compressed mode, and CHOICE 'UL/DL mode' indicates 'DL only':

2> set the variable INVALID_CONFIGURATION to TRUE.

1> if the UE, according to its measurement capabilities, and for all supported bands of the UTRA mode or RAT associated with the measurement purpose indicated by IE "TGMP", requires DL compressed mode, and CHOICE 'UL/DL mode' indicates 'UL only':

2> set the variable INVALID_CONFIGURATION to TRUE.

1> if the UE, according to its measurement capabilities, does not require UL compressed mode for any of supported band of the UTRA mode or RAT associated with the measurement purpose indicated by the IE "TGMP", and CHOICE 'UL/DL mode' indicates 'UL only' or 'UL and DL':

2> set the variable INVALID_CONFIGURATION to TRUE.

1> if the UE, according to its measurement capabilities, does not require DL compressed mode for any supported band of the UTRA mode or RAT associated with the measurement purpose indicated by the IE "TGMP", and CHOICE 'UL/DL mode' indicates 'DL only' or 'UL and DL':

2> set the variable INVALID_CONFIGURATION to TRUE.

1> if UE already has an active transmission gap pattern sequence that, according to IE "TGMP", has the same measurement purpose, and both patterns will be active after the new configuration has been taken into use:

2> set the variable INVALID_CONFIGURATION to TRUE.

If variable INVALID_CONFIGURATION has value FALSE after UE has performed the checks above, the UE shall:

1> if pattern sequence corresponding to IE "TGPSI" is already active (according to "Current TGPS Status Flag") in the variable TGPS_IDENTITY):

2> if the "TGPS Status Flag" in this message is set to "deactivate" for the corresponding pattern sequence:

3> deactivate this pattern sequence at the beginning of the frame, indicated by IE "Activation time"(see subclause 8.6.3.1) received in this message, when the new configuration received in this message is taken into use.

3> set the "Current TGPS Status Flag" for this pattern sequence in the variable TGPS_IDENTITY to "inactive".

2> if the "TGPS Status Flag" in this message is set to "activate" for the corresponding pattern sequence:

3> deactivate this pattern sequence at the beginning of the frame, indicated by IE "Activation time"(see subclause 8.6.3.1) received in this message, when the new configuration received in this message is taken into use.

NOTE: The temporary deactivation of pattern sequences for which the status flag is set to "activate" can be used by the network to align the timing of already active patterns with newly activated patterns.

1> update each pattern sequence to the variable TGPS_IDENTITY according to the IE "TGPSI";

1> update into the variable TGPS_IDENTITY the configuration information defined by IE group" transmission gap pattern sequence configuration parameters ";

1> after the new configuration has been taken into use:

2> activate the stored pattern sequence corresponding to each IE "TGPSI" for which the "~~Current~~ TGPS status flag" in the variable TGPS_IDENTITY is set to "activate" at the time indicated by IE "TGCFN"; and

2> begin the inter-frequency and/or inter-RAT measurements corresponding to the pattern sequence measurement purpose of each activated pattern sequence;

2> if the new configuration is taken into use at the same CFN as indicated by IE "TGCFN":

3> start the concerned pattern sequence immediately at that CFN.

1> monitor if the parallel transmission gap pattern sequences create an illegal overlap, and in case of overlap, take actions as specified in subclause 8.2.11.2.

If the IE "DPCH compressed mode info" is included, and if the IE group "transmission gap pattern sequence configuration parameters" is not included, the UE shall:

1> if pattern sequence corresponding to IE "TGPSI" is already active (according to "Current TGPS Status Flag" in the variable TGPS_IDENTITY):

2> if the "TGPS Status Flag" in this message is set to "deactivate" for the corresponding pattern sequence:

3> deactivate this pattern sequence at the beginning of the frame, indicated by IE "Activation time"(see subclause 8.6.3.1) received in this message, when the new configuration received in this message is taken into use;

3> set the "Current TGPS Status Flag" for this pattern sequence in the variable TGPS_IDENTITY to "inactive".

2> if the "TGPS Status Flag" in this message is set to "activate" for the corresponding pattern sequence:

3> deactivate this pattern sequence at the beginning of the frame, indicated by IE "Activation time"(see subclause 8.6.3.1) received in this message, when the new configuration received in this message is taken into use.

NOTE: The temporary deactivation of pattern sequences for which the status flag is set to "activate" can be used by the network to align the timing of already active patterns with newly activated patterns.

1> after the new configuration has been taken into use:

2> at the time indicated by IE "TGCFN":

3> activate the stored pattern sequence corresponding to each IE "TGPSI" for which the "TGPS status flag" is set to "activate"; and

3> set the "Current TGPS Status Flag" for this pattern sequence in the variable TGPS_IDENTITY to "active".

2> begin the inter-frequency and/or inter-RAT measurements corresponding to the pattern sequence measurement purpose of each activated pattern sequence;

2> if the new configuration is taken into use at the same CFN as indicated by IE "TGCFN":

3> start the concerned pattern sequence immediately at that CFN.

For transmission gap pattern sequences stored in variable TGPS_IDENTITY, but not identified in IE "TGPSI" (either due to the absence of the IE "DPCH compressed mode info" in the received message or due to not receiving the corresponding TGPSI value in the IE "DPCH compressed mode info"), the UE shall:

1> if the received message implies a timing re-initialised hard handover (see subclause 8.3.5.1):

2> deactivate such transmission gap pattern sequences at the beginning of the frame, indicated by IE "Activation time" (see subclause 8.6.3.1) received in this message; and

2> set IE "Current TGPS Status Flag" in corresponding UE variable TGPS_IDENTITY to 'inactive'.

1> if the received message not implies a timing re-initialised hard handover (see subclause 8.3.5.1):

2> continue such transmission gap pattern sequence according to IE "Current TGPS Status Flag" in the corresponding UE variable TGPS_IDENTITY.

Uplink and downlink compressed mode methods are described in [27]. For UL "higher layer scheduling" compressed mode method and transport format combination selection, see [15].

8.6.7.16 Intra-frequency measurement

If IE "Intra-frequency measurement" is received by the UE in a MEASUREMENT CONTROL message, where IE "measurement command" has the value "setup", but IE "Intra-frequency measurement quantity", IE "Intra-frequency reporting quantity", "CHOICE Report criteria" or "parameters required for each event" (given "CHOICE report criteria" is set to "intra-frequency measurement reporting criteria") is not received, the UE shall:

1> clear all stored measurement control information related associated to this measurement identity in variable MEASUREMENT_IDENTITY;

1> set the variable CONFIGURATION_INCOMPLETE to TRUE.

In case of 1a or 1e~~c (resp. 1b or 1f)~~ event-triggered reporting:

1> if the IE "Intra-frequency measurement quantity~~criteria~~" is set to "pathloss", the UE shall:

2> if detected set cells are indicated as possibly triggering the event within the IEs "Triggering condition 2" ~~(resp. "Triggering condition 1")~~:

3> set the variable CONFIGURATION_INCOMPLETE to TRUE.

10.3.2.4 Cell selection and re-selection info for SIB11/12

Information Element/Group name	Need	Multi	Type and reference	Semantics description	Version
Qoffset1$_{s,n}$	MD		Integer(-50..50)	Default value is 0. [dB]	
Qoffset2$_{s,n}$	CV-*FDD-Quality-Measure*		Integer(-50..50)	Default value is 0. [dB]	
Maximum allowed UL TX power	MD		Maximum allowed UL TX power 10.3.6.39	According to UE_TXPWR_MAX_RACH in [4], [dBm]. If applied to FDD or TDD cells, the default is the Maximum allowed UL TX power for the serving cell. If applied to a GSM cell, the default is the UE maximum output power applicable for this GSM cell, according to the UE's radio access capability.	
HCS neighbouring cell information	OP		HCS Neighbouring cell information 10.3.7.11		
CHOICE *mode*	MP				
>FDD					
>>Qqualmin	CV-*FDD-Serving-Cell*		Integer (-24..0)	Ec/N0, [dB] Default value is Qqualmin for the serving cell	
>>Qrxlevmin	MD		Integer (-115..-25 by step of 2)	RSCP, [dBm] Default value is Qrxlevmin for the serving cell	
>>Delta$_{Qrxlevmin}$	CV-*Delta*		Integer(-4..-2 by step of 2)	If present, the actual value of Qrxlevmin = Qrxlevmin + Delta$_{Qrxlevmin}$	REL-5
>TDD					
>>Qrxlevmin	MD		Integer (-115..-25 by step of 2)	RSCP, [dBm] Default value is Qrxlevmin for the serving cell	
>> Delta$_{Qrxlevmin}$	CV-*Delta*		Integer(-4..-2 by step of 2)	If present, the actual value of Qrxlevmin = Qrxlevmin + Delta$_{Qrxlevmin}$	REL-5
>GSM					
>>Qrxlevmin	MD		Integer (-115..-25 by step of 2)	GSM RSSI, [dBm] Default value is Qrxlevmin for the serving cell	

Condition	Explanation
FDD-Quality-Measure	This IE is mandatory and has a default value for Intra/Inter Frequency Cells if the IE "Cell selection and reselection quality measure" has the value CPICH Ec/No. Otherwise the IE is ~~optional~~absent.
FDD-Serving-Cell	This IE is mandatory and has a default value if the serving cell is an FDD cell. Otherwise the IE is mandatory present.
Delta	This IE is optional if Qrxlevmin is present and the value of Qrxlevmin is below –115dBm. It is not needed otherwise.

3GPP TSG-RAN WG2 Meeting #34 **_Tdoc ⌘R2-030480_**
Sophia Antipolis, France, 17th- 21st February 2003

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**	**1841**	⌘ **rev**	**1**	⌘	Current version:	**3.13.0**	⌘

*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:	⌘	Hard handover with pending ciphering activation times		
Source:	⌘	TSG-RAN WG2		
Work item code:	⌘	TEI	***Date:*** ⌘	12/02/2003
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. In the current specification it is unclear how the UE will react if a hard handover is performed while there is a pending ciphering activation time from a previous procedure for a TM radio bearer. If a hard handover is performed in this situation, the activation time set by the previous procedure has no longer a meaning since the CFN changes (in the case of timing re-initialised HHO). The ciphering activation time for TM may be pending after any procedure where ciphering related activation times are set (Security mode command, RB setup, Inter-RAT handover from GSM)The delay of a hard handover until the activation time have elapsed (up to 2.5s) may cause the call to be dropped and it is therefore proposed that the actions for this scenario are clarified.
2. It is incorrectly stated that the UE shall apply the new Integrity Protection configuration exactly at the RRC sequence number indicated by the activation time. In the case where some RRC messages are lost, it is required that the UE apply the new Integrity Protection on the first message with RRC sequence number higher than that indicated in the activation time.
3. In December 2002, RAN2 agreed on CR1808 where it was clarified in 8.5.8, that in case of the activation time for a new ciperhing configuration is zero, and there is a wrap-around of the HFN (roll-over) the HFN shall not be incremented by one. In the case of Timing re-initialized Hard Handover and Handover to UTRAN we specify today the UE shall on activating the dedicated physical channels, at the CFN value indicated in the response message IE “COUNT-C activation time”, increment the HFN by one. This requirement could be seen as contradicting the requirement in 8.5.8.
4. In CR 1532 the actions when new keys are pending during SRNS relocation were stated. However, the CR should have explicitly stated that the

requirements were for AM and UM bearers only.

Summary of change: ⌘

1. It is proposed to clarify that if a timing re-initialised hard handover is performed while there is a pending ciphering activation time for a TM radio bearer from a previous procedure, the pending ciphering configuration shall be applied immediately.
2. The UE shall apply the new IP configuration as soon as it receives the first message with RRC sequence number higher than that indicated in the activation time to cover the case where messages are lost in the downlink or if the SRB is not configured for in-sequence delivery.
3. It is clarified that the UE shall increment the HJFN by 1 even in the case where COUNT-C activationtime is set to zero, for Handover to UTRAN and Hard Handover.
4. It is clarified that the change in CR1532, related to the pending activation times are related to UM and AM modes only.

Consequences if not approved: ⌘

1. If the CR is not implemented, timing re-initilised hard handover following another procedure (during a pending ciphering activation time) may fail and the call would be dropped.
2. There is no UTRAN implementation impact; however, the COUNT-I will get unsynchronized in the case where messages are lost or delayed(no in-sequence delivery).
3. If UE does not implement per this CR then HFN would be misaligned between the UE and UTRAN causing ciphering failure.
4. This is UTRAN affecting only and is merely to clarify and avoid potential incorrect UTRAN implementations.

Impact analysis: Change #1

Impacted functionality: timing re-initialised hard handover following a procedure where activation times related to ciphering are set (Security mode command, RB setup, Inter-RAT handover)

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- CR implemented only by UTRAN: The CR has no UTRAN impact
- CR implemented only by the UE: If the CR is not implemented, timing re-initilised hard handover following another procedure (during a pending ciphering activation time) may fail and the call would be dropped.

Change#2:

Impacted Functionality: Integrity Protection

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- CR implemented only by UTRAN: The CR has no UTRAN impact
- CR implemented only by the UE: The COUNT-I will get unsynchronized in the case where messages are lost or delayed(no in-sequence delivery) causing Integrity Protection failure.

Change #3:

Impacted Functionality: Ciphering

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- CR implemented only by UTRAN: The CR has no UTRAN impact
- CR implemented only by the UE: The HFN will get unsynchronized causing Security failure.

Change #4:

Impacted Functionality: SRNS relocation

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- CR implemented only by UTRAN: The CR has only UTRAN impact. There is no functionality in R99 to support SRNS relocation in case of pending TM bearer ciphering activation times
- CR implemented only by the UE: No impact to UE.

Clauses affected:	⌘	8.6.6.28; 8.6.3.5.3; 8.6.3.4, 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.

8.6.6.28 Downlink DPCH info common for all radio links

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

1> if the IE "Downlink DPCH info common for all RL" is included in a message used to perform a hard handover:

2> perform actions for the IE "Timing indication" as specified in subclause 8.5.15.2, and subclause 8.3.5.1 or 8.3.5.2.

1> ignore the value received in IE "CFN-targetSFN frame offset";

1> if the IE "Downlink DPCH power control information" is included:

2> perform actions for the IE "DPC Mode" according to [29].

1> if the IE choice "mode" is set to 'FDD':

2> if the IE "Downlink rate matching restriction information" is included:

3> set the variable INVALID_CONFIGURATION to TRUE.

2> perform actions for the IE "spreading factor";

2> perform actions for the IE "Fixed or Flexible position";

2> perform actions for the IE "TFCI existence";

2> if the IE choice "SF" is set to 256:

3> store the value of the IE "Number of bits for pilot bits".

2> if the IE choice "SF" set to 128:

3> store the value of the IE "Number of bits for pilot bits".

1> if the IE choice "mode" is set to 'TDD':

2> perform actions for the IE "Common timeslot info".

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

1> if any ciphering configuration for a radio bearer using RLC-TM ~~is pending~~ ~~from a previous procedure~~ has not been applied, due to that the activation time ~~for the radio bearer~~ from a previous procedure has not elapsed:

2> apply the ~~pending~~ ciphering configuration immediately and consider the activation time from the previous procedure to be elapsed;

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

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

1> start to perform ciphering on the radio bearer in lower layers while not incrementing the HFN;

1> 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 lies at least 200 frames ahead of the CFN in which the response message is first transmitted;

1> calculate the START value according to subclause 8.5.9;

1> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the response message;

1> at the CFN value as indicated in the response message in the IE "COUNT-C activation time":

2> 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

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

2> increment the HFN component of the COUNT-C variable by one even if the ‘COUNT-C activation time’ is set to zero;

2> 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;

2> step the COUNT-C variable, as normal, at each CFN value, i.e. the HFN component is no longer fixed in value but incremented at each CFN cycle.

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;

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" and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND.

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 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.

8.6.3.4 Ciphering mode info

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

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

1> ignore this second attempt to change the ciphering configuration; and

1> set the variable INCOMPATIBLE_SECURITY_RECONFIGURATION to TRUE.

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

1> if none of the IE "Status" in the variable CIPHERING STATUS has the value "Started", and this IE "Ciphering mode info" was included in a message that is not the message SECURITY MODE COMMAND; or

1> if the IE "Ciphering Mode Info" was received in the message SECURITY MODE COMMAND and there does not exist exactly one ciphering activation time in the IE "Radio bearer downlink ciphering activation time info" for each established RLC-AM and RLC-UM radio bearers included in the IE "RB information" in the IE "ESTABLISHED_RABS" for the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN; or

1> if the IE "Ciphering Mode Info" was received in the message SECURITY MODE COMMAND and the IE "Ciphering activation time for DPCH" is not included in the message, and there exist radio bearers using RLC-TM according to the IE "RB information" in the IE "ESTABLISHED_RABS" for the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN; or

1> if the IE "Ciphering Mode Info" was received in the message SECURITY MODE COMMAND and there does not exist exactly one ciphering activation time in the IE "Radio bearer downlink ciphering activation time info" for each established signalling radio bearer included in the IE "Signalling radio bearer information" in the IE "ESTABLISHED_RABS":

2> ignore this attempt to change the ciphering configuration;

2> set the variable INVALID_CONFIGURATION to TRUE;

2> perform the actions as specified in subclause 8.1.12.4c.

1> set the IE "Reconfiguration" in the variable CIPHERING_STATUS to TRUE;

1> set the IE "Status" in the variable CIPHERING_STATUS of the CN domains for which the IE "Status" of the variable SECURITY_MODIFICATION is set to "Affected" to "Started";

1> apply the new ciphering configuration in the lower layers for all RBs that belong to a CN domain for which the IE "Status" of the variable SECURITY_MODIFICATION is set to "Affected" and all signalling radio bearers:

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

2> for each radio bearer that belongs to a CN domain for which the IE "Status" of the variable SECURITY_MODIFICATION is set to "Affected" and all signalling radio bearers:

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

1> apply the new ciphering configuration as follows:

2> if the ciphering configuration for a AM or UM radio bearer or signalling radio bearer from a previously received SECURITY MODE COMMAND has not yet been applied because of the corresponding activation times not having elapsed and the current received message includes the IE "DL Counter Synch Info" or the current received message is a RADIO BEARER RECONFIGURATION message and includes the IE "New U-RNTI":

3> if the previous SECURITY MODE COMMAND was received due to new keys being received:

4> consider the new ciphering configuration to include the received new keys; and

4> initialise the HFN values of the COUNT-C for the corresponding radio bearers or signalling radio bearers according to subclause 8.1.12.

3> else:

4> consider the new ciphering configuration to include the keys associated with the LATEST_CONFIGURED_CN_DOMAIN; and

4> initialise the HFN values of the COUNT-C for the corresponding radio bearers or signalling radio bearers according to subclause 8.1.12 using the START value associated with the LATEST_CONFIGURED_CN_DOMAIN to be transmitted in the response to the current message (and not the START value in the most recently transmitted IE "START list" or IE "START" at the reception of the SECURITY MODE COMMAND).

3> apply the new ciphering configuration in uplink and downlink immediately following RLC re-establishment.

2> if the IE "Ciphering activation time for DPCH" is present in the IE "Ciphering mode info" and the UE was in CELL_DCH state prior to this procedure:

3> for radio bearers using RLC-TM:

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

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

2> if the IE "Radio bearer downlink ciphering activation time info" is present:

3> apply the following procedure for each radio bearer and signalling radio bearers using RLC-AM or RLC-UM indicated by the IE "RB identity":

4> suspend uplink transmission on the radio bearer or the signalling radio bearer (except for the SRB where the response message is transmitted) according to the following:

5> do not transmit RLC PDUs with sequence number greater than or equal to the uplink activation time, where the uplink activation time is selected according to the rules below.

4> select an "RLC sequence number" at which (activation) time the new ciphering configuration shall be applied in uplink for that radio bearer according to the following:

5> consider a ciphering activation time in uplink to be pending until the RLC sequence number of the next RLC PDU to be transmitted for the first time is equal to or larger than the selected activation time;

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

6> set a suitable value that would ensure a minimised delay in the change to the latest ciphering configuration.

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

6> for radio bearers and signalling radio bearers except SRB2:

7> set the same value as the pending ciphering activation time.

6> for signalling radio bearer SRB2:

7> set a suitable value that would ensure a minimised delay in the change to the latest ciphering configuration.

4> store the selected "RLC sequence number" for that radio bearer in the entry for the radio bearer in the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO;

4> switch to the new ciphering configuration according to the following:

5> use the old ciphering configuration for the transmitted and received RLC PDUs with RLC sequence numbers smaller than the corresponding RLC sequence numbers indicated in the IE "Radio bearer uplink ciphering activation time info" sent to UTRAN and in the received IE "Radio bearer downlink ciphering activation time info" received from UTRAN, respectively;

5> use the new ciphering configuration for the transmitted and received RLC PDUs with RLC sequence numbers greater than or equal to the corresponding RLC sequence numbers indicated in the IE "Radio bearer uplink ciphering activation time info" sent to UTRAN and in the received IE "Radio bearer downlink ciphering activation time info" received from UTRAN, respectively;

5> for a radio bearer using RLC-AM, when the RLC sequence number indicated in the IE "Radio bearer downlink ciphering activation time info" falls below the RLC receiving window and the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" falls below the RLC transmission window, the UE may release the old ciphering configuration for that radio bearer;

5> if an RLC reset or re-establishment occurs before the activation time for the new ciphering configuration has been reached, ignore the activation time and apply the new ciphering configuration both in uplink and downlink immediately after the RLC reset or RLC re-establishment.

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

1> not change the ciphering configuration.

8.6.3.5.3 Integrity Protection modification in case of new keys or initialisation of signalling connection

The UE shall:

1> if the IE "Integrity protection mode command" has the value "modify" and the IE "Status" in the variable INTEGRITY_PROTECTION_INFO has the value "Started" and this IE was included in SECURITY MODE COMMAND:

2> store the (oldest currently used) integrity protection configuration until activation times have elapsed for the new integrity protection configuration to be applied on all signalling radio bearers;

2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer n, at the first received message with RRC Sequence number, greater than or at the RRC sequence number, ~~for each signalling radio bearer n,~~ indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info";

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

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

2> set the content of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO according to the following:

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

4> select a value of the RRC sequence number at which (activation) time the new integrity protection configuration shall be applied in uplink for that signalling radio bearer according to the following:

5> for each signalling radio bearer that has no pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:

6> set a suitable value that would ensure a minimised delay in the change to the latest integrity protection configuration.

5> for signalling radio bearer that has a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:

6> set the same value as the pending activation time for integrity protection;

5> consider an integrity protection activation time in uplink to be pending until the selected activation time (as above) is equal to the next RRC sequence number to be used, which means that the last RRC message using the old integrity protection configuration has been submitted to lower layers.

4> for signalling radio bearer RB0:

5> set the value of the included RRC sequence number to greater than or equal to the current value of the RRC sequence number for signalling radio bearer RB0 in the variable INTEGRITY_PROTECTION_INFO, plus the value of the constant N302 plus one.

4> prohibit the transmission of RRC messages on all signalling radio bearers, except for RB2, with RRC SN greater than or equal to the value in the "RRC message sequence number list" for the signalling radio bearer in the IE "Uplink integrity protection activation info" of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.

2> start applying the new integrity protection configuration in the uplink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Uplink integrity protection activation info", included in the variable INTEGRITY_PROTECTION_ACTIVATION_INFO;

2> start applying the new integrity protection configuration in the uplink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration;

2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info";

NOTE: For signalling radio bearers that have a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration, UTRAN should set this value in IE "Downlink integrity protection activation info".

2> start applying the new integrity protection configuration in the downlink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration.

3GPP TSG-RAN WG2 Meeting #34 **Tdoc ⌘R2-030481**
Sophia Antipolis, France, 17th- 21st February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **25.331 CR 1842** ⌘**rev** **1** ⌘ Current version: **4.8.0** ⌘

*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: ⌘	Hard handover with pending ciphering activation times		
Source: ⌘	TSG-RAN WG2		
Work item code: ⌘	TEI	***Date:*** ⌘	12/02/2003
Category: ⌘	A	***Release:*** ⌘	Rel-4

b

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. In the current specification it is unclear how the UE will react if a hard handover is performed while there is a pending ciphering activation time from a previous procedure for a TM radio bearer. If a hard handover is performed in this situation, the activation time set by the previous procedure has no longer a meaning since the CFN changes (in the case of timing re-initialised HHO). The ciphering activation time for TM may be pending after any procedure where ciphering related activation times are set (Security mode command, RB setup, Inter-RAT handover from GSM). The delay of a hard handover until the activation time have elapsed (up to 2.5s) may cause the call to be dropped and it is therefore proposed that the actions for this scenario are clarified.

2. It is incorrectly stated that the UE shall apply the new Integrity Protection configuration exactly at the RRC sequence number indicated by the activation time. In the case where some RRC messages are lost, it is required that the UE apply the new Integrity Protection on the first message with RRC sequence number higher than that indicated in the activation time.

3. In December 2002, RAN2 agreed on CR1808 where it was clarified in 8.5.8, that in case of the activation time for a new ciperhing configuration is zero, and there is a wrap-around of the HFN (roll-over) the HFN shall not be incremented by one. In the case of Timing re-initialized Hard Handover and Handover to UTRAN we specify today the UE shall on activating the dedicated physical channels, at the CFN value indicated in the response message IE “COUNT-C activation time”, increment the HFN by one. This requirement could be seen as contradicting the requirement in 8.5.8.

4. In CR 1532 the actions when new keys are pending during SRNS relocation

	were stated. However, the CR should have explicitly stated that the requirements were for AM and UM bearers only.
Summary of change: ⌘	1. It is proposed to clarify that if a timing re-initialised hard handover is performed while there is a pending ciphering activation time for a TM radio bearer from a previous procedure, the pending ciphering configuration shall be applied immediately. 2. The UE shall apply the new IP configuration as soon as it receives the first message with RRC sequence number higher than that indicated in the activation time to cover the case where messages are lost in the downlink or if the SRB is not configured for in-sequence delivery. 3. It is clarified that the UE shall increment the HJFN by 1 even in the case where COUNT-C activationtime is set to zero, for Handover to UTRAN and Hard Handover. 4. It is clarified that the change in CR1532, related to the pending activation times are related to UM and AM modes only.
Consequences if not approved: ⌘	1. If the CR is not implemented, timing re-initilised hard handover following another procedure (during a pending ciphering activation time) may fail and the call would be dropped. 2. There is no UTRAN implementation impact; however, the COUNT-I will get unsynchronized in the case where messages are lost or delayed(no in-sequence delivery). 3. If UE does not implement per this CR then HFN would be misaligned between the UE and UTRAN causing ciphering failure. 4. This is UTRAN affecting only and is merely to clarify and avoid potential incorrect UTRAN implementations. **Impact analysis:** <u>Impacted functionality</u>: timing re-initialised hard handover following a procedure where activation times related to ciphering are set (Security mode command, RB setup, Inter-RAT handover) <u>Correction type</u>: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise <u>Interoperability:</u> • Isolated impact: the impact is isolated; only the corrected functionality is affected • CR implemented only by UTRAN: The CR has no UTRAN impact • CR implemented only by the UE: If the CR is not implemented, timing re-initilised hard handover following another procedure (during a pending ciphering activation time) may fail and the call would be dropped. Change#2: Impacted Functionality: Integrity Protection <u>Correction type</u>: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise. <u>Interoperability:</u>

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- CR implemented only by UTRAN: The CR has no UTRAN impact
- CR implemented only by the UE: The COUNT-I will get unsynchronized in the case where messages are lost or delayed(no in-sequence delivery) causing Integrity Protection failure.

Change #3:

Impacted Functionality: Ciphering

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- CR implemented only by UTRAN: The CR has no UTRAN impact
- CR implemented only by the UE: The HFN will get unsynchronized causing Security failure.

Change #4:

Impacted Functionality: SRNS relocation

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- CR implemented only by UTRAN: The CR has only UTRAN impact. There is no functionality in R99 to support SRNS relocation in case of pending TM bearer ciphering activation times
- CR implemented only by the UE: No impact to UE.

Clauses affected:	⌘	8.6.6.28				
		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.

8.6.6.28 Downlink DPCH info common for all radio links

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

1> if the IE "Downlink DPCH info common for all RL" is included in a message used to perform a hard handover:

2> perform actions for the IE "Timing indication" as specified in subclause 8.5.15.2, and subclause 8.3.5.1 or 8.3.5.2.

1> ignore the value received in IE "CFN-targetSFN frame offset";

1> if the IE "Downlink DPCH power control information" is included:

2> perform actions for the IE "DPC Mode" according to [29].

1> if the IE choice "mode" is set to 'FDD':

2> if the IE "Downlink rate matching restriction information" is included:

3> set the variable INVALID_CONFIGURATION to TRUE.

2> perform actions for the IE "spreading factor";

2> perform actions for the IE "Fixed or Flexible position";

2> perform actions for the IE "TFCI existence";

2> if the IE choice "SF" is set to 256:

3> store the value of the IE "Number of bits for pilot bits".

2> if the IE choice "SF" set to 128:

3> store the value of the IE "Number of bits for pilot bits".

1> if the IE choice "mode" is set to 'TDD':

2> perform actions for the IE "Common timeslot info".

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

1> if any ciphering configuration for a radio bearer using RLC-TM has not been applied, due to that the activation time from a previous procedure has not elapsed:

2> apply the ciphering configuration immediately and consider the activation time from the previous procedure to be elapsed;

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

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

1> start to perform ciphering on the radio bearer in lower layers while not incrementing the HFN;

1> 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 lies at least 200 frames ahead of the CFN in which the response message is first transmitted;

1> calculate the START value according to subclause 8.5.9;

1> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the response message;

1> at the CFN value as indicated in the response message in the IE "COUNT-C activation time":

2> 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

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

2> increment the HFN component of the COUNT-C variable by one even if the “COUNT-C activation time” is equal to zero;

2> 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;

2> step the COUNT-C variable, as normal, at each CFN value, i.e. the HFN component is no longer fixed in value but incremented at each CFN cycle.

8.6.3.5.3 Integrity Protection modification in case of new keys or initialisation of signalling connection

The UE shall:

1> if the IE "Integrity protection mode command" has the value "modify" and the IE "Status" in the variable INTEGRITY_PROTECTION_INFO has the value "Started" and this IE was included in SECURITY MODE COMMAND:

2> store the (oldest currently used) integrity protection configuration until activation times have elapsed for the new integrity protection configuration to be applied on all signalling radio bearers;

2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer n, at the first received message with RRC Sequence number, greater than or at the RRC sequence number, ~~for each signalling radio bearer n,~~ indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info";

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

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

2> set the content of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO according to the following:

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

4> select a value of the RRC sequence number at which (activation) time the new integrity protection configuration shall be applied in uplink for that signalling radio bearer according to the following:

5> for each signalling radio bearer that has no pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:

6> set a suitable value that would ensure a minimised delay in the change to the latest integrity protection configuration.

5> for signalling radio bearer that has a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:

6> set the same value as the pending activation time for integrity protection;

5> consider an integrity protection activation time in uplink to be pending until the selected activation time (as above) is equal to the next RRC sequence number to be used, which means that the last RRC message using the old integrity protection configuration has been submitted to lower layers.

4> for signalling radio bearer RB0:

5> set the value of the included RRC sequence number to greater than or equal to the current value of the RRC sequence number for signalling radio bearer RB0 in the variable INTEGRITY_PROTECTION_INFO, plus the value of the constant N302 plus one.

4> prohibit the transmission of RRC messages on all signalling radio bearers, except for RB2, with RRC SN greater than or equal to the value in the "RRC message sequence number list" for the signalling radio bearer in the IE "Uplink integrity protection activation info" of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.

2> start applying the new integrity protection configuration in the uplink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Uplink integrity protection activation info", included in the variable INTEGRITY_PROTECTION_ACTIVATION_INFO;

2> start applying the new integrity protection configuration in the uplink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration;

2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info";

NOTE: For signalling radio bearers that have a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration, UTRAN should set this value in IE "Downlink integrity protection activation info".

2> start applying the new integrity protection configuration in the downlink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration.

8.3.6.3 Reception of HANDOVER TO UTRAN COMMAND message by the UE

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

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

The UE may:

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

The UE shall:

1> store a U-RNTI value (32 bits), which is derived by the IEs "SRNC identity" (12 bits) and "S-RNTI 2" (10 bits) included in IE "U-RNTI-short". In order to produce a full size U-RNTI value, a full size "S-RNTI" (20 bits) shall be derived by padding the IE "S-RNTI 2" with 10 zero bits in the most significant positions; and

1> initialise the variable ESTABLISHED_SIGNALLING_CONNECTIONS with the signalling connections that remains after the handover according to the specifications of the source RAT;

1> initialise the variable UE_CAPABILITIES_TRANSFERRED with the UE capabilities that have been transferred to the network up to the point prior to the handover, if any;

1> initialise the variable TIMERS_AND_CONSTANTS to the default values and start to use those timer and constants values;

1> if IE "Specification mode" is set to "Preconfiguration" and IE "Preconfiguration mode" is set to "Predefined configuration":

2> initiate the radio bearer and transport channel configuration in accordance with the predefined parameters identified by the IE "Predefined configuration identity";

2> initiate the physical channels in accordance with the predefined parameters identified by the IE "Predefined radio configuration identity" and the received physical channel information elements;

2> store information about the established radio access bearers and radio bearers according to the IE "Predefined configuration identity"; and

2> set the IE "RAB Info Post" in the variable ESTABLISHED_RABS and the IE "Re-establishment timer" in the IE "RAB Info" in the variable ESTABLISHED_RABS to "useT314".

1> if IE "Specification mode" is set to "Preconfiguration" and IE "Preconfiguration mode" is set to "Default configuration":

2> initiate the radio bearer and transport channel configuration in accordance with the default parameters identified by the IE "Default configuration mode" and IE "Default configuration identity";

2> initiate the physical channels in accordance with the default parameters identified by the IE "Default configuration mode" and IE "Default configuration identity" and the received physical channel information elements;

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

2> set the IE "RAB Info Post" in the variable ESTABLISHED_RABS and the IE "Re-establishment timer" in the IE "RAB Info" in the variable ESTABLISHED_RABS to "useT314".

1> if IE "Specification mode" is set to "Preconfiguration":

2> use the following values for parameters that are neither signalled within the HANDOVER TO UTRAN COMMAND message nor included within pre-defined or default configuration:

3> 0 dB for the power offset $P_{\text{Pilot-DPDCH}}$ bearer in FDD;

3> calculate the Default DPCH Offset Value using the following formula:

3> in FDD:

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

3> in TDD:

Default DPCH Offset Value = (SRNTI 2 mod 7)

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

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

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

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

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

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" and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND.

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 for this IE other than the default, "Now", that 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.

8.6.3.4 Ciphering mode info

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

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

1> ignore this second attempt to change the ciphering configuration; and

1> set the variable INCOMPATIBLE_SECURITY_RECONFIGURATION to TRUE.

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

1> if none of the IE "Status" in the variable CIPHERING STATUS has the value "Started", and this IE "Ciphering mode info" was included in a message that is not the message SECURITY MODE COMMAND; or

1> if the IE "Ciphering Mode Info" was received in the message SECURITY MODE COMMAND and there does not exist exactly one ciphering activation time in the IE "Radio bearer downlink ciphering activation time info" for each established RLC-AM and RLC-UM radio bearers included in the IE "RB information" in the IE "ESTABLISHED_RABS" for the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN; or

1> if the IE "Ciphering Mode Info" was received in the message SECURITY MODE COMMAND and the IE "Ciphering activation time for DPCH" is not included in the message, and there exist radio bearers using RLC-TM according to the IE "RB information" in the IE "ESTABLISHED_RABS" for the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN; or

1> if the IE "Ciphering Mode Info" was received in the message SECURITY MODE COMMAND and there does not exist exactly one ciphering activation time in the IE "Radio bearer downlink ciphering activation time info" for each established signalling radio bearer included in the IE "Signalling radio bearer information" in the IE "ESTABLISHED_RABS":

2> ignore this attempt to change the ciphering configuration;

2> set the variable INVALID_CONFIGURATION to TRUE;

2> perform the actions as specified in subclause 8.1.12.4c.

1> set the IE "Reconfiguration" in the variable CIPHERING_STATUS to TRUE;

1> set the IE "Status" in the variable CIPHERING_STATUS of the CN domains for which the IE "Status" of the variable SECURITY_MODIFICATION is set to "Affected" to "Started";

1> apply the new ciphering configuration in the lower layers for all RBs that belong to a CN domain for which the IE "Status" of the variable SECURITY_MODIFICATION is set to "Affected" and all signalling radio bearers:

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

2> for each radio bearer that belongs to a CN domain for which the IE "Status" of the variable SECURITY_MODIFICATION is set to "Affected" and all signalling radio bearers:

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

1> apply the new ciphering configuration as follows:

2> if the ciphering configuration for a AM or UM radio bearer or signalling radio bearer from a previously received SECURITY MODE COMMAND has not yet been applied because of the corresponding activation times not having elapsed and the current received message includes the IE "DL Counter Synch Info" or the current received message is a RADIO BEARER RECONFIGURATION message and includes the IE "New U-RNTI":

3> if the previous SECURITY MODE COMMAND was received due to new keys being received:

4> consider the new ciphering configuration to include the received new keys; and

4> initialise the HFN values of the COUNT-C for the corresponding radio bearers or signalling radio bearers according to subclause 8.1.12.

3> else:

4> consider the new ciphering configuration to include the keys associated with the LATEST_CONFIGURED_CN_DOMAIN; and

4> initialise the HFN values of the COUNT-C for the corresponding radio bearers or signalling radio bearers according to subclause 8.1.12 using the START value associated with the LATEST_CONFIGURED_CN_DOMAIN to be transmitted in the response to the current message (and not the START value in the most recently transmitted IE "START list" or IE "START" at the reception of the SECURITY MODE COMMAND).

3> apply the new ciphering configuration in uplink and downlink immediately following RLC re-establishment.

2> if the IE "Ciphering activation time for DPCH" is present in the IE "Ciphering mode info" and the UE was in CELL_DCH state prior to this procedure:

3> for radio bearers using RLC-TM:

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

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

2> if the IE "Radio bearer downlink ciphering activation time info" is present:

3> apply the following procedure for each radio bearer and signalling radio bearers using RLC-AM or RLC-UM indicated by the IE "RB identity":

4> suspend uplink transmission on the radio bearer or the signalling radio bearer (except for the SRB where the response message is transmitted) according to the following:

5> do not transmit RLC PDUs with sequence number greater than or equal to the uplink activation time, where the uplink activation time is selected according to the rules below.

4> select an "RLC sequence number" at which (activation) time the new ciphering configuration shall be applied in uplink for that radio bearer according to the following:

5> consider a ciphering activation time in uplink to be pending until the RLC sequence number of the next RLC PDU to be transmitted for the first time is equal to or larger than the selected activation time;

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

6> set a suitable value that would ensure a minimised delay in the change to the latest ciphering configuration.

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

6> for radio bearers and signalling radio bearers except SRB2:

7> set the same value as the pending ciphering activation time.

6> for signalling radio bearer SRB2:

7> set a suitable value that would ensure a minimised delay in the change to the latest ciphering configuration.

4> store the selected "RLC sequence number" for that radio bearer in the entry for the radio bearer in the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO;

4> switch to the new ciphering configuration according to the following:

5> use the old ciphering configuration for the transmitted and received RLC PDUs with RLC sequence numbers smaller than the corresponding RLC sequence numbers indicated in the IE "Radio bearer uplink ciphering activation time info" sent to UTRAN and in the received IE "Radio bearer downlink ciphering activation time info" received from UTRAN, respectively;

5> use the new ciphering configuration for the transmitted and received RLC PDUs with RLC sequence numbers greater than or equal to the corresponding RLC sequence numbers indicated in the IE "Radio bearer uplink ciphering activation time info" sent to UTRAN and in the received IE "Radio bearer downlink ciphering activation time info" received from UTRAN, respectively;

5> for a radio bearer using RLC-AM, when the RLC sequence number indicated in the IE "Radio bearer downlink ciphering activation time info" falls below the RLC receiving window and the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" falls below the RLC transmission window, the UE may release the old ciphering configuration for that radio bearer;

5> if an RLC reset or re-establishment occurs before the activation time for the new ciphering configuration has been reached, ignore the activation time and apply the new ciphering configuration both in uplink and downlink immediately after the RLC reset or RLC re-establishment.

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

1> not change the ciphering configuration.

3GPP TSG-RAN WG2 Meeting #34
Sophia Antipolis, France, 17th- 21st February 2003

Tdoc ⌘R2-0302482

CR-Form-v7

CHANGE REQUEST

⌘ **25.331 CR 1843** ⌘**rev** **1** ⌘ Current version: **5.3.0** ⌘

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

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

Title: ⌘	Hard handover with pending ciphering activation times		
Source: ⌘	TSG-RAN WG2		
Work item code: ⌘	TEI	***Date:*** ⌘	19/02/2003
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: ⌘

1. In the current specification it is unclear how the UE will react if a hard handover is performed while there is a pending ciphering activation time from a previous procedure for a TM radio bearer. If a hard handover is performed in this situation, the activation time set by the previous procedure has no longer a meaning since the CFN changes (in the case of timing re-initialised HHO). The ciphering activation time for TM may be pending after any procedure where ciphering related activation times are set (Security mode command, RB setup, Inter-RAT handover from GSM). The delay of a hard handover until the activation time have elapsed (up to 2.5s) may cause the call to be dropped and it is therefore proposed that the actions for this scenario are clarified.
2. It is incorrectly stated that the UE shall apply the new Integrity Protection configuration exactly at the RRC sequence number indicated by the activation time. In the case where some RRC messages are lost, it is required that the UE apply the new Integrity Protection on the first message with RRC sequence number higher than that indicated in the activation time.

3. In December 2002, RAN2 agreed on CR1808 where it was clarified in 8.5.8, that in case of the activation time for a new ciperhing configuration is zero, and there is a wrap-around of the HFN (roll-over) the HFN shall not be incremented by one. In the case of Timing re-initialized Hard Handover and Handover to UTRAN we specify today the UE shall on activating the dedicated physical channels, at the CFN value indicated in the response message IE “COUNT-C activation time”, increment the HFN by one. This requirement could be seen as contradicting the requirement in 8.5.8.

4. In CR 1532 the actions when new keys are pending during SRNS

relocation were stated. However, the CR should have explicitly stated that the requirements were for AM and UM bearers only.

Summary of change: ⌘

1. It is proposed to clarify that if a timing re-initialised hard handover is performed while there is a pending ciphering activation time for a TM radio bearer from a previous procedure, the pending ciphering configuration shall be applied immediately.
2. The UE shall apply the new IP configuration as soon as it receives the first message with RRC sequence number higher than that indicated in the activation time to cover the case where messages are lost in the downlink or if the SRB is not configured for in-sequence delivery.
3. It is clarified that the UE shall increment the HJFN by 1 even in the case where COUNT-C activationtime is set to zero, for Handover to UTRAN and Hard Handover.
4. It is clarified that the change in CR1532, related to the pending activation times are related to UM and AM modes only.

Consequences if not approved: ⌘

1. If the CR is not implemented, timing re-initilised hard handover following another procedure (during a pending ciphering activation time) may fail and the call would be dropped.
2. There is no UTRAN implementation impact; however, the COUNT-I will get unsynchronized in the case where messages are lost or delayed(no in-sequence delivery).
3. If UE does not implement per this CR then HFN would be misaligned between the UE and UTRAN causing ciphering failure.
4. This is UTRAN affecting only and is merely to clarify and avoid potential incorrect UTRAN implementations.

Impact analysis:

Impacted functionality: timing re-initialised hard handover following a procedure where activation times related to ciphering are set (Security mode command, RB setup, Inter-RAT handover)

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- CR implemented only by UTRAN: The CR has no UTRAN impact
- CR implemented only by the UE: If the CR is not implemented, timing re-initilised hard handover following another procedure (during a pending ciphering activation time) may fail and the call would be dropped.

Change#2:

Impacted Functionality: Integrity Protection

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- CR implemented only by UTRAN: The CR has no UTRAN impact
- CR implemented only by the UE: The COUNT-I will get unsynchronized in the case where messages are lost or delayed(no in-sequence delivery) causing Integrity Protection failure.

Change #3:

Impacted Functionality: Ciphering

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- CR implemented only by UTRAN: The CR has no UTRAN impact
  - CR implemented only by the UE: The HFN will get unsynchronized causing Security failure.

Change #4:

Impacted Functionality: SRNS relocation

Correction type: Clarification of a function where the specification is incomplete, ambiguous and/ or inconsistent. Does not affect implementations behaving like indicated in the CR, would affect implementations supporting the corrected functionality otherwise.

Interoperability:

- Isolated impact: the impact is isolated; only the corrected functionality is affected
- CR implemented only by UTRAN: The CR has only UTRAN impact. There is no functionality in R99 to support SRNS relocation in case of pending TM bearer ciphering activation times
  - CR implemented only by the UE: No impact to UE.

Clauses affected:	⌘	8.6.6.28				
		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.

8.6.6.28 Downlink DPCH info common for all radio links

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

1> if the IE "Downlink DPCH info common for all RL" is included in a message used to perform a hard handover:

2> perform actions for the IE "Timing indication" as specified in subclause 8.5.15.2, and subclause 8.3.5.1 or 8.3.5.2.

1> ignore the value received in IE "CFN-targetSFN frame offset";

1> if the IE "Downlink DPCH power control information" is included:

2> perform actions for the IE "DPC Mode" according to [29].

1> if the IE choice "mode" is set to 'FDD':

2> if the IE "Downlink rate matching restriction information" is included:

3> set the variable INVALID_CONFIGURATION to TRUE.

2> perform actions for the IE "spreading factor";

2> perform actions for the IE "Fixed or Flexible position";

2> perform actions for the IE "TFCI existence";

2> if the IE choice "SF" is set to 256:

3> store the value of the IE "Number of bits for pilot bits".

2> if the IE choice "SF" set to 128:

3> store the value of the IE "Number of bits for pilot bits".

1> if the IE choice "mode" is set to 'TDD':

2> perform actions for the IE "Common timeslot info".

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

1> if any ciphering configuration for a radio bearer using RLC-TM has not been applied, due to that the activation time from a previous procedure has not elapsed:

2> apply the ciphering configuration immediately and consider the activation time from the previous procedure to be elapsed;

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

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

1> start to perform ciphering on the radio bearer in lower layers while not incrementing the HFN;

1> 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 lies at least 200 frames ahead of the CFN in which the response message is first transmitted;

1> calculate the START value according to subclause 8.5.9;

1> include the calculated START values for each CN domain in the IE "START list" in the IE "Uplink counter synchronisation info" in the response message;

1> at the CFN value as indicated in the response message in the IE "COUNT-C activation time":

2> 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

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

2> increment the HFN component of the COUNT-C variable by one even if the “COUNT-C activation time” is equal to zero;

2> 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;

2> step the COUNT-C variable, as normal, at each CFN value, i.e. the HFN component is no longer fixed in value but incremented at each CFN cycle.

8.6.3.5.3 Integrity Protection modification in case of new keys or initialisation of signalling connection

The UE shall:

1> if the IE "Integrity protection mode command" has the value "modify" and the IE "Status" in the variable INTEGRITY_PROTECTION_INFO has the value "Started" and this IE was included in SECURITY MODE COMMAND:

2> store the (oldest currently used) integrity protection configuration until activation times have elapsed for the new integrity protection configuration to be applied on all signalling radio bearers;

2> start applying the new integrity protection configuration in the downlink for each signalling radio bearer n, at the first received message with RRC Sequence number greater than or at the RRC sequence number, ~~for each signalling radio bearer n,~~ indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info", included in the IE "Integrity protection mode info";

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

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

2> set the content of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO according to the following:

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

4> select a value of the RRC sequence number at which (activation) time the new integrity protection configuration shall be applied in uplink for that signalling radio bearer according to the following:

5> for each signalling radio bearer that has no pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:

6> set a suitable value that would ensure a minimised delay in the change to the latest integrity protection configuration.

5> for signalling radio bearer that has a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration:

6> set the same value as the pending activation time for integrity protection;

5> consider an integrity protection activation time in uplink to be pending until the selected activation time (as above) is equal to the next RRC sequence number to be used, which means that the last RRC message using the old integrity protection configuration has been submitted to lower layers.

4> for signalling radio bearer RB0:

5> set the value of the included RRC sequence number to greater than or equal to the current value of the RRC sequence number for signalling radio bearer RB0 in the variable INTEGRITY_PROTECTION_INFO, plus the value of the constant N302 plus one.

4> prohibit the transmission of RRC messages on all signalling radio bearers, except for RB2, with RRC SN greater than or equal to the value in the "RRC message sequence number list" for the signalling radio bearer in the IE "Uplink integrity protection activation info" of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO.

2> start applying the new integrity protection configuration in the uplink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Uplink integrity protection activation info", included in the variable INTEGRITY_PROTECTION_ACTIVATION_INFO;

2> start applying the new integrity protection configuration in the uplink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration;

2> start applying the new integrity protection configuration in the downlink at the RRC sequence number, for each RBn, except for signalling radio bearer RB2, indicated by the entry for signalling radio bearer n in the "RRC message sequence number list" in the IE "Downlink integrity protection activation info";

NOTE: For signalling radio bearers that have a pending activation time as set for integrity protection by a previous procedure changing the integrity protection configuration, UTRAN should set this value in IE "Downlink integrity protection activation info".

2> start applying the new integrity protection configuration in the downlink at the RRC sequence number for signalling radio bearer RB2, as specified for the procedure initiating the integrity protection reconfiguration.

8.3.6.3 Reception of HANDOVER TO UTRAN COMMAND message by the UE

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

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

The UE may:

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

The UE shall:

1> store a U-RNTI value (32 bits), which is derived by the IEs "SRNC identity" (12 bits) and "S-RNTI 2" (10 bits) included in IE "U-RNTI-short". In order to produce a full size U-RNTI value, a full size "S-RNTI" (20 bits) shall be derived by padding the IE "S-RNTI 2" with 10 zero bits in the most significant positions; and

1> initialise the variable ESTABLISHED_SIGNALLING_CONNECTIONS with the signalling connections that remains after the handover according to the specifications of the source RAT;

1> initialise the variable UE_CAPABILITIES_TRANSFERRED with the UE capabilities that have been transferred to the network up to the point prior to the handover, if any;

1> initialise the variable TIMERS_AND_CONSTANTS to the default values and start to use those timer and constants values;

1> if IE "Specification mode" is set to "Preconfiguration" and IE "Preconfiguration mode" is set to "Predefined configuration":

2> initiate the radio bearer and transport channel configuration in accordance with the predefined parameters identified by the IE "Predefined configuration identity";

2> initiate the physical channels in accordance with the predefined parameters identified by the IE "Predefined radio configuration identity" and the received physical channel information elements;

2> store information about the established radio access bearers and radio bearers according to the IE "Predefined configuration identity"; and

2> set the IE "RAB Info Post" in the variable ESTABLISHED_RABS and the IE "Re-establishment timer" in the IE "RAB Info" in the variable ESTABLISHED_RABS to "useT314".

1> if IE "Specification mode" is set to "Preconfiguration" and IE "Preconfiguration mode" is set to "Default configuration":

2> initiate the radio bearer and transport channel configuration in accordance with the default parameters identified by the IE "Default configuration mode" and IE "Default configuration identity";

2> initiate the physical channels in accordance with the default parameters identified by the IE "Default configuration mode" and IE "Default configuration identity" and the received physical channel information elements;

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

2> set the IE "RAB Info Post" in the variable ESTABLISHED_RABS and the IE "Re-establishment timer" in the IE "RAB Info" in the variable ESTABLISHED_RABS to "useT314".

1> if IE "Specification mode" is set to "Preconfiguration":

2> use the following values for parameters that are neither signalled within the HANDOVER TO UTRAN COMMAND message nor included within pre-defined or default configuration:

3> 0 dB for the power offset $P_{\text{Pilot-DPDCH}}$ bearer in FDD;

3> calculate the Default DPCH Offset Value using the following formula:

3> in FDD:

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

3> in TDD:

Default DPCH Offset Value = (SRNTI 2 mod 7)

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

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

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

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

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

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" and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND.

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 for this IE other than the default, "Now", that 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.

8.6.3.4 Ciphering mode info

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

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

1> ignore this second attempt to change the ciphering configuration; and

1> set the variable INCOMPATIBLE_SECURITY_RECONFIGURATION to TRUE.

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

1> if none of the IE "Status" in the variable CIPHERING STATUS has the value "Started", and this IE "Ciphering mode info" was included in a message that is not the message SECURITY MODE COMMAND; or

1> if the IE "Ciphering Mode Info" was received in the message SECURITY MODE COMMAND and there does not exist exactly one ciphering activation time in the IE "Radio bearer downlink ciphering activation time info" for each established RLC-AM and RLC-UM radio bearers included in the IE "RB information" in the IE "ESTABLISHED_RABS" for the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN; or

1> if the IE "Ciphering Mode Info" was received in the message SECURITY MODE COMMAND and the IE "Ciphering activation time for DPCH" is not included in the message, and there exist radio bearers using RLC-TM according to the IE "RB information" in the IE "ESTABLISHED_RABS" for the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN; or

1> if the IE "Ciphering Mode Info" was received in the message SECURITY MODE COMMAND and there does not exist exactly one ciphering activation time in the IE "Radio bearer downlink ciphering activation time info" for each established signalling radio bearer included in the IE "Signalling radio bearer information" in the IE "ESTABLISHED_RABS":

2> ignore this attempt to change the ciphering configuration;

2> set the variable INVALID_CONFIGURATION to TRUE;

2> perform the actions as specified in subclause 8.1.12.4c.

1> set the IE "Reconfiguration" in the variable CIPHERING_STATUS to TRUE;

1> set the IE "Status" in the variable CIPHERING_STATUS of the CN domains for which the IE "Status" of the variable SECURITY_MODIFICATION is set to "Affected" to "Started";

1> apply the new ciphering configuration in the lower layers for all RBs that belong to a CN domain for which the IE "Status" of the variable SECURITY_MODIFICATION is set to "Affected" and all signalling radio bearers:

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

2> for each radio bearer that belongs to a CN domain for which the IE "Status" of the variable SECURITY_MODIFICATION is set to "Affected" and all signalling radio bearers:

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

1> apply the new ciphering configuration as follows:

2> if the ciphering configuration for a AM or UM radio bearer or signalling radio bearer from a previously received SECURITY MODE COMMAND has not yet been applied because of the corresponding activation times not having elapsed and the current received message includes the IE "DL Counter Synch Info" or the current received message is a RADIO BEARER RECONFIGURATION message and includes the IE "New U-RNTI":

3> if the previous SECURITY MODE COMMAND was received due to new keys being received:

4> consider the new ciphering configuration to include the received new keys; and

4> initialise the HFN values of the COUNT-C for the corresponding radio bearers or signalling radio bearers according to subclause 8.1.12.

3> else:

4> consider the new ciphering configuration to include the keys associated with the LATEST_CONFIGURED_CN_DOMAIN; and

4> initialise the HFN values of the COUNT-C for the corresponding radio bearers or signalling radio bearers according to subclause 8.1.12 using the START value associated with the LATEST_CONFIGURED_CN_DOMAIN to be transmitted in the response to the current message (and not the START value in the most recently transmitted IE "START list" or IE "START" at the reception of the SECURITY MODE COMMAND).

3> apply the new ciphering configuration in uplink and downlink immediately following RLC re-establishment.

2> if the IE "Ciphering activation time for DPCH" is present in the IE "Ciphering mode info" and the UE was in CELL_DCH state prior to this procedure:

3> for radio bearers using RLC-TM:

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

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

2> if the IE "Radio bearer downlink ciphering activation time info" is present:

3> apply the following procedure for each radio bearer and signalling radio bearers using RLC-AM or RLC-UM indicated by the IE "RB identity":

4> suspend uplink transmission on the radio bearer or the signalling radio bearer (except for the SRB where the response message is transmitted) according to the following:

5> do not transmit RLC PDUs with sequence number greater than or equal to the uplink activation time, where the uplink activation time is selected according to the rules below.

4> select an "RLC sequence number" at which (activation) time the new ciphering configuration shall be applied in uplink for that radio bearer according to the following:

5> consider a ciphering activation time in uplink to be pending until the RLC sequence number of the next RLC PDU to be transmitted for the first time is equal to or larger than the selected activation time;

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

6> set a suitable value that would ensure a minimised delay in the change to the latest ciphering configuration.

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

6> for radio bearers and signalling radio bearers except SRB2:

7> set the same value as the pending ciphering activation time.

6> for signalling radio bearer SRB2:

7> set a suitable value that would ensure a minimised delay in the change to the latest ciphering configuration.

4> store the selected "RLC sequence number" for that radio bearer in the entry for the radio bearer in the variable RB_UPLINK_CIPHERING_ACTIVATION_TIME_INFO;

4> switch to the new ciphering configuration according to the following:

5> use the old ciphering configuration for the transmitted and received RLC PDUs with RLC sequence numbers smaller than the corresponding RLC sequence numbers indicated in the IE "Radio bearer uplink ciphering activation time info" sent to UTRAN and in the received IE "Radio bearer downlink ciphering activation time info" received from UTRAN, respectively;

5> use the new ciphering configuration for the transmitted and received RLC PDUs with RLC sequence numbers greater than or equal to the corresponding RLC sequence numbers indicated in the IE "Radio bearer uplink ciphering activation time info" sent to UTRAN and in the received IE "Radio bearer downlink ciphering activation time info" received from UTRAN, respectively;

5> for a radio bearer using RLC-AM, when the RLC sequence number indicated in the IE "Radio bearer downlink ciphering activation time info" falls below the RLC receiving window and the RLC sequence number indicated in the IE "Radio bearer uplink ciphering activation time info" falls below the RLC transmission window, the UE may release the old ciphering configuration for that radio bearer;

5> if an RLC reset or re-establishment occurs before the activation time for the new ciphering configuration has been reached, ignore the activation time and apply the new ciphering configuration both in uplink and downlink immediately after the RLC reset or RLC re-establishment.

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

1> not change the ciphering configuration.