3GPP TSG-RAN Meeting #18
New Orleans, US, 3rd-6th December 2002

Tdoc ⌘RP-020893

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **1808** ⌘ **rev** **-** ⌘ Current version: **3.c.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 [X] Radio Access Network [X] Core Network [ ]

Title:	⌘	Handling of hyper frame numbers
Source:	⌘	Ericsson, NEC, Nortel, Qualcomm
Work item code:	⌘	TEI
Date:	⌘	December 2002
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 currently unclear how hyper frame numbers (HFNs) should be incremented when a wrap around of the RLC sequence number (for ciphering) or the RRC sequence number (for integrity) is simultaneous with a re-initialisation of the HFN.

In particular it is not clear if the wrap around of the sequence number leads to that the re-initialised HFN is used or if the HFN+1 is used for a message if the re-initialisation of the HFN occurs at sequence number zero.

Summary of change: ⌘

1. It is clarified that the actions in 8.5.10.1 and 8.5.10.2 shall be applied, i,e, the HFN for integrity shall be incremented by one when a wrap around of the RRC sequence number occurs, regardless if the HFN was re-initialised by a security mode procedure at the same sequence number as the wrap round.
2. It is clarified that the HFN for ciphering re-initialised by a security mode shall be used at the activation time of the re-initialisation even if the re-initialisation is simultaneous with a wrap around of the sequence number.
3. It is clarified when the HFNs for ciphering are incremented.

Consequences if not approved: ⌘

If no clarification is made:
Different interpretations by different vendors may lead to that the HFN for ciphering and integrity gets out of sync between UE and UTRAN at CN domain switch or when new keys are taken into use. If the HFN gets out of sync, Integrity protection/ciphering will fail on the particular SRB.

	Isolated impact analysis: The CR only affects integrity protection and ciphering at CN domain switch or when new keys are taken into use. The CR therefore has isolated impact.

Clauses affected:	⌘	8.1.12.2.2, 8.5.8, 8.5.10.1, 8.5.10.2			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
		X		Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

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

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

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

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

8.1.12.2.2 Integrity protection configuration change

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

When configuring Integrity protection, UTRAN should:

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

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

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

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

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

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

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

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

2> if new keys have been received:

3> initialise the hyper frame numbers as follows:

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

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

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

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

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

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

2> if new keys have been received:

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

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

2> if new keys have not been received:

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

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

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

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

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

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

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

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

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

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

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

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

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

8.5.8 Maintenance of Hyper Frame Numbers

The MSBs of both the ciphering sequence numbers (COUNT-C) and integrity sequence numbers (COUNT-I), for the ciphering and integrity protection algorithms, respectively [40], are called the Hyper Frame Numbers (HFN).

For integrity protection, the UE shall:

1> maintain COUNT-I as specified in subclause 8.5.10.

The following hyper frame numbers types are defined:

MAC-d HFN:
24 MSB of COUNT-C for data sent over RLC TM

RLC UM HFN:
25 MSB of COUNT-C for data sent over RLC UM

RLC AM HFN:
20 MSB of COUNT-C for data sent over RLC AM

RRC HFN:
28 MSB of COUNT-I

For non-transparent mode RLC signalling radio bearers and radio bearers, the UE shall:

1> maintain one uplink and one downlink COUNT-C per signalling radio bearer and per radio bearer and one uplink and one downlink COUNT-I per signalling radio bearer.

1> increment the RLC UM HFN and RLC AM HFN in uplink and downlink by one each time the RLC sequence number wraps around in uplink and downlink respectively;

1> if the activation time for a new ciphering configuration set by an RRC procedure is equal to zero:

2> apply the configured RLC UM HFN or RLC AM HFN at this activation time, i.e. the configured HFN is not incremented.

Note: On the receiver side it may happen that the RLC PDU with sequence number equal to the activation time is lost and the first received PDU after the activation time implies a wrap around of the sequence number compared to the activation time. In this case the configured HFN is incremented by one. This action happens only when the activation time is set to a RLC PDU sequence number value other than zero.

For all transparent mode RLC signalling radio bearers and radio bearers of each CN domain, the UE shall:

1> maintain one COUNT-C, common for all signalling radio bearers and radio bearers in uplink and downlink;

1> increment the MAC-d HFN by one each time the CFN wraps around;

1> if the activation time for a new ciphering configuration set by an RRC procedure is equal to zero:

2> apply the configured MAC-d HFN at this activation time, i.e. the configured HFN is not incremented;

1> maintain one uplink and one downlink COUNT-I per signalling radio bearer.

NOTE: In this release of the specification there is only an uplink transparent mode COUNT-I, which is used for signalling radio bearer RB0.

COUNT-C and COUNT-I are defined in [40], with the following supplement for COUNT-C: for transparent mode RLC radio bearers with a transmission time interval of x radio frames (x = 2, 4, 8), the MAC PDU is carried by L1 in x consecutive radio frames due to radio frame segmentation. In this case, the CFN of the first radio frame in the TTI shall be used as the CFN component of COUNT-C for ciphering of all data in the TTI [15].

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> 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.

8.5.10.2 Integrity protection in uplink

Prior to sending an RRC message using the signalling radio bearer with radio bearer identity n, and the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" the UE shall:

1> increment "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with 1, even if the message is a retransmission of a previously transmitted message.

1> if the~~When~~ "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO equals zero:

2> ~~becomes 0, the UE shall~~ increment "Uplink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO by one~~with 1~~;

Note: the actions above imply that also for the case the "Uplink RRC HFN" is re-initialised by a security mode control procedure, this "Uplink RRC HFN" is incremented before it is applied in the integrity protection of any transmitted message if the conditions above are fulfilled.

Note: For SRB0, this is also valid in case the MSN has been increased by N302 +1 resulting in a wrap around. Then the uplink RRC HFN is incremented by 1.

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

1> replace the "Message authentication code" in the IE "Integrity check info" in the message with the calculated message authentication code;

1> replace the "RRC Message sequence number" in the IE "Integrity check info" in the message with contents set to the new value of the "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO.

In the response message for the procedure ordering the security reconfiguration, the UE indicates the activation time, for each signalling radio bearer except for the signalling radio bearer that was used for this security reconfiguration procedure. When the new integrity configuration is to be applied in uplink, UTRAN should start to apply the new integrity protection configuration according to the activation time for each signalling radio bearer (except for the

signalling radio bearer which is used to send the message that is reconfiguring the security configuration) where the new configuration is to be applied starting from and including reception of the response message).

8.5.10.3 Calculation of message authentication code

The UE shall calculate the message authentication code in accordance with [40]. The input parameter MESSAGE [40] for the integrity algorithm shall be constructed by:

1> setting the "Message authentication code" in the IE "Integrity check info" in the message to the value of the IE "RB identity" for the signalling radio bearer;

1> setting the "RRC Message sequence number" in the IE "Integrity check info" in the message to zero;

1> encoding the message;

1> appending RRC padding (if any) as a bit string to the encoded bit string as the least significant bits.

For usage on an RRC message transmitted or received on the radio bearer with identity n, the UE shall:

1> construct the input parameter COUNT-I [40] by appending the following IEs from the IE "Signalling radio bearer specific integrity protection information" for radio bearer n in the variable INTEGRITY_PROTECTION_INFO:

2> for uplink:

3> "Uplink RRC HFN", as the MSB, and "Uplink RRC Message sequence number", as LSB.

2> for downlink:

3> "Downlink RRC HFN", as the MSB, and the IE "RRC message sequence number" included in the IE "Integrity check info", as LSB.

3GPP TSG-RAN Meeting #18
New Orleans, US, 3rd-6th December 2002

Tdoc ⌘RP-020893

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **1809** ⌘ **rev** **-** ⌘ Current version: **4.7.0** ⌘

*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 [X] Radio Access Network [X] Core Network [ ]

Title: ⌘	Handling of hyper frame numbers	
Source: ⌘	Ericsson, NEC, Nortel, Qualcomm	
Work item code: ⌘	TEI	***Date:*** ⌘ December 2002
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 currently unclear how hyper frame numbers (HFNs) should be incremented when a wrap around of the RLC sequence number (for ciphering) or the RRC sequence number (for integrity) is simultaneous with a re-initialisation of the HFN.

In particular it is not clear if the wrap around of the sequence number leads to that the re-initialised HFN is used or if the HFN+1 is used for a message if the re-initialisation of the HFN occurs at sequence number zero.

Summary of change: ⌘

1. It is clarified that the actions in 8.5.10.1 and 8.5.10.2 shall be applied, i,e, the HFN for integrity shall be incremented by one when a wrap around of the RRC sequence number occurs, regardless if the HFN was re-initialised by a security mode procedure at the same sequence number as the wrap round.
2. It is clarified that the HFN for ciphering re-initialised by a security mode shall be used at the activation time of the re-initialisation even if the re-initialisation is simultaneous with a wrap around of the sequence number.
3. It is clarified when the HFNs for ciphering are incremented.

Consequences if not approved: ⌘

If no clarification is made:
Different interpretations by different vendors may lead to that the HFN for ciphering and integrity gets out of sync between UE and UTRAN at CN domain switch or when new keys are taken into use. If the HFN gets out of sync, Integrity protection/ciphering will fail on the particular SRB.

	Isolated impact analysis: The CR only affects integrity protection and ciphering at CN domain switch or when new keys are taken into use. The CR therefore has isolated impact.

Clauses affected:	⌘	8.1.12.2.2, 8.5.8, 8.5.10.1, 8.5.10.2			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
		X		Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

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

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

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

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

8.1.12.2.2 Integrity protection configuration change

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

When configuring Integrity protection, UTRAN should:

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

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

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

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

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

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

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

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

2> if new keys have been received:

3> initialise the hyper frame numbers as follows:

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

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

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

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

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

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

2> if new keys have been received:

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

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

2> if new keys have not been received:

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

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

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

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

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

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

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

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

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

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

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

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

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

8.5.8 Maintenance of Hyper Frame Numbers

The MSBs of both the ciphering sequence numbers (COUNT-C) and integrity sequence numbers (COUNT-I), for the ciphering and integrity protection algorithms, respectively [40], are called the Hyper Frame Numbers (HFN).

For integrity protection, the UE shall:

1> maintain COUNT-I as specified in subclause 8.5.10.

The following hyper frame numbers types are defined:

MAC-d HFN:
24 MSB of COUNT-C for data sent over RLC TM

RLC UM HFN:
25 MSB of COUNT-C for data sent over RLC UM

RLC AM HFN:
20 MSB of COUNT-C for data sent over RLC AM

RRC HFN:
28 MSB of COUNT-I

For non-transparent mode RLC signalling radio bearers and radio bearers, the UE shall:

1> maintain one uplink and one downlink COUNT-C per signalling radio bearer and per radio bearer and one uplink and one downlink COUNT-I per signalling radio bearer.

1> increment the RLC UM HFN and RLC AM HFN in uplink and downlink by one each time the RLC sequence number wraps around in uplink and downlink respectively;

1> if the activation time for a new ciphering configuration set by an RRC procedure is equal to zero:

2> apply the configured RLC UM HFN or RLC AM HFN at this activation time, i.e. the configured HFN is not incremented.

Note: On the receiver side it may happen that the RLC PDU with sequence number equal to the activation time is lost and the first received PDU after the activation time implies a wrap around of the sequence number compared to the activation time. In this case the configured HFN is incremented by one. This action happens only when the activation time is set to a RLC PDU sequence number value other than zero.

For all transparent mode RLC signalling radio bearers and radio bearers of each CN domain, the UE shall:

1> maintain one COUNT-C, common for all signalling radio bearers and radio bearers in uplink and downlink;

1> increment the MAC-d HFN by one each time the CFN wraps around;

1> if the activation time for a new ciphering configuration set by an RRC procedure is equal to zero:

2> apply the configured MAC-d HFN at this activation time, i.e. the configured HFN is not incremented;

1> maintain one uplink and one downlink COUNT-I per signalling radio bearer.

NOTE: In this release of the specification there is only an uplink transparent mode COUNT-I, which is used for signalling radio bearer RB0.

COUNT-C and COUNT-I are defined in [40], with the following supplement for COUNT-C: for transparent mode RLC radio bearers with a transmission time interval of x radio frames (x = 2, 4, 8), the MAC PDU is carried by L1 in x consecutive radio frames due to radio frame segmentation. In this case, the CFN of the first radio frame in the TTI shall be used as the CFN component of COUNT-C for ciphering of all data in the TTI [15].

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> 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.

8.5.10.2 Integrity protection in uplink

Prior to sending an RRC message using the signalling radio bearer with radio bearer identity n, and the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" the UE shall:

1> increment "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with 1, even if the message is a retransmission of a previously transmitted message.

1> if the~~When~~ "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO equals zero:

2> ~~becomes 0, the UE shall~~ increment "Uplink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO by one~~with 1~~;

Note: the actions above imply that also for the case the "Uplink RRC HFN" is re-initialised by a security mode control procedure, this "Uplink RRC HFN" is incremented before it is applied in the integrity protection of any transmitted message if the conditions above are fulfilled.

Note: For SRB0, this is also valid in case the MSN has been increased by N302 +1 resulting in a wrap around. Then the uplink RRC HFN is incremented by 1.

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

1> replace the "Message authentication code" in the IE "Integrity check info" in the message with the calculated message authentication code;

1> replace the "RRC Message sequence number" in the IE "Integrity check info" in the message with contents set to the new value of the "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO.

In the response message for the procedure ordering the security reconfiguration, the UE indicates the activation time, for each signalling radio bearer except for the signalling radio bearer that was used for this security reconfiguration procedure. When the new integrity configuration is to be applied in uplink, UTRAN should start to apply the new integrity protection configuration according to the activation time for each signalling radio bearer (except for the signalling radio bearer which is used to send the message that is reconfiguring the security configuration) where the new configuration is to be applied starting from and including reception of the response message).

8.5.10.3 Calculation of message authentication code

The UE shall calculate the message authentication code in accordance with [40]. The input parameter MESSAGE [40] for the integrity algorithm shall be constructed by:

1> setting the "Message authentication code" in the IE "Integrity check info" in the message to the value of the IE "RB identity" for the signalling radio bearer;

1> setting the "RRC Message sequence number" in the IE "Integrity check info" in the message to zero;

1> encoding the message;

1> appending RRC padding (if any) as a bit string to the encoded bit string as the least significant bits.

For usage on an RRC message transmitted or received on the radio bearer with identity n, the UE shall:

1> construct the input parameter COUNT-I [40] by appending the following IEs from the IE "Signalling radio bearer specific integrity protection information" for radio bearer n in the variable INTEGRITY_PROTECTION_INFO:

2> for uplink:

3> "Uplink RRC HFN", as the MSB, and "Uplink RRC Message sequence number", as LSB.

2> for downlink:

3> "Downlink RRC HFN", as the MSB, and the IE "RRC message sequence number" included in the IE "Integrity check info", as LSB.

3GPP TSG-RAN Meeting #18
New Orleans, US, 3rd-6th December 2002

Tdoc ⌘RP-020893

CR-Form-v7

CHANGE REQUEST

⌘ **25.331** **CR** **1810** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*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 [X] Radio Access Network [X] Core Network [ ]

Title: ⌘	Handling of hyper frame numbers	
Source: ⌘	Ericsson, NEC, Nortel, Qualcomm	
Work item code: ⌘	TEI	***Date:*** ⌘ December 2002
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 currently unclear how hyper frame numbers (HFNs) should be incremented when a wrap around of the RLC sequence number (for ciphering) or the RRC sequence number (for integrity) is simultaneous with a re-initialisation of the HFN.

In particular it is not clear if the wrap around of the sequence number leads to that the re-initialised HFN is used or if the HFN+1 is used for a message if the re-initialisation of the HFN occurs at sequence number zero.

Summary of change: ⌘

1. It is clarified that the actions in 8.5.10.1 and 8.5.10.2 shall be applied, i,e, the HFN for integrity shall be incremented by one when a wrap around of the RRC sequence number occurs, regardless if the HFN was re-initialised by a security mode procedure at the same sequence number as the wrap round.
2. It is clarified that the HFN for ciphering re-initialised by a security mode shall be used at the activation time of the re-initialisation even if the re-initialisation is simultaneous with a wrap around of the sequence number.
3. It is clarified when the HFNs for ciphering are incremented.

Consequences if not approved: ⌘

If no clarification is made:
Different interpretations by different vendors may lead to that the HFN for ciphering and integrity gets out of sync between UE and UTRAN at CN domain switch or when new keys are taken into use. If the HFN gets out of sync, Integrity protection/ciphering will fail on the particular SRB.

	Isolated impact analysis: The CR only affects integrity protection and ciphering at CN domain switch or when new keys are taken into use. The CR therefore has isolated impact.

Clauses affected:	⌘	8.1.12.2.2, 8.5.8, 8.5.10.1, 8.5.10.2			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
		X		Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

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

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

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

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

8.1.12.2.2 Integrity protection configuration change

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

When configuring Integrity protection, UTRAN should:

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

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

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

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

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

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

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

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

2> if new keys have been received:

3> initialise the hyper frame numbers as follows:

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

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

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

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

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

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

2> if new keys have been received:

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

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

2> if new keys have not been received:

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

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

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

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

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

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

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

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

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

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

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

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

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

8.5.8 Maintenance of Hyper Frame Numbers

The MSBs of both the ciphering sequence numbers (COUNT-C) and integrity sequence numbers (COUNT-I), for the ciphering and integrity protection algorithms, respectively [40], are called the Hyper Frame Numbers (HFN).

For integrity protection, the UE shall:

1> maintain COUNT-I as specified in subclause 8.5.10.

The following hyper frame numbers types are defined:

MAC-d HFN:
24 MSB of COUNT-C for data sent over RLC TM

RLC UM HFN:
25 MSB of COUNT-C for data sent over RLC UM

RLC AM HFN:
20 MSB of COUNT-C for data sent over RLC AM

RRC HFN:
28 MSB of COUNT-I

For non-transparent mode RLC signalling radio bearers and radio bearers, the UE shall:

1> maintain one uplink and one downlink COUNT-C per signalling radio bearer and per radio bearer and one uplink and one downlink COUNT-I per signalling radio bearer.

1> increment the RLC UM HFN and RLC AM HFN in uplink and downlink by one each time the RLC sequence number wraps around in uplink and downlink respectively;

1> if the activation time for a new ciphering configuration set by an RRC procedure is equal to zero:

2> apply the configured RLC UM HFN or RLC AM HFN at this activation time, i.e. the configured HFN is not incremented.

Note: On the receiver side it may happen that the RLC PDU with sequence number equal to the activation time is lost and the first received PDU after the activation time implies a wrap around of the sequence number compared to the activation time. In this case the configured HFN is incremented by one. This action happens only when the activation time is set to a RLC PDU sequence number value other than zero.

For all transparent mode RLC signalling radio bearers and radio bearers of each CN domain, the UE shall:

1> maintain one COUNT-C, common for all signalling radio bearers and radio bearers in uplink and downlink;

1> increment the MAC-d HFN by one each time the CFN wraps around;

1> if the activation time for a new ciphering configuration set by an RRC procedure is equal to zero:

2> apply the configured MAC-d HFN at this activation time, i.e. the configured HFN is not incremented;

1> maintain one uplink and one downlink COUNT-I per signalling radio bearer.

NOTE: In this release of the specification there is only an uplink transparent mode COUNT-I, which is used for signalling radio bearer RB0.

COUNT-C and COUNT-I are defined in [40], with the following supplement for COUNT-C: for transparent mode RLC radio bearers with a transmission time interval of x radio frames (x = 2, 4, 8), the MAC PDU is carried by L1 in x consecutive radio frames due to radio frame segmentation. In this case, the CFN of the first radio frame in the TTI shall be used as the CFN component of COUNT-C for ciphering of all data in the TTI [15].

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> 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.

8.5.10.2 Integrity protection in uplink

Prior to sending an RRC message using the signalling radio bearer with radio bearer identity n, and the "Status" in the variable INTEGRITY_ PROTECTION_INFO has the value "Started" the UE shall:

1> increment "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO with 1, even if the message is a retransmission of a previously transmitted message.

1> if the ~~When~~ "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO equals~~becomes~~ zero~~0~~:

2> ~~, the UE shall~~ increment "Uplink RRC HFN" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO by one~~with 1~~;

Note: the actions above imply that also for the case the "Uplink RRC HFN" is re-initialised by a security mode control procedure, this "Uplink RRC HFN" is incremented before it is applied in the integrity protection of any transmitted message if the conditions above are fulfilled.

Note: For SRB0, this is also valid in case the MSN has been increased by N302 +1 resulting in a wrap around. Then the uplink RRC HFN is incremented by 1.

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

1> replace the "Message authentication code" in the IE "Integrity check info" in the message with the calculated message authentication code;

1> replace the "RRC Message sequence number" in the IE "Integrity check info" in the message with contents set to the new value of the "Uplink RRC Message sequence number" for signalling radio bearer RBn in the variable INTEGRITY_PROTECTION_INFO.

In the response message for the procedure ordering the security reconfiguration, the UE indicates the activation time, for each signalling radio bearer except for the signalling radio bearer that was used for this security reconfiguration procedure. When the new integrity configuration is to be applied in uplink, UTRAN should start to apply the new integrity protection configuration according to the activation time for each signalling radio bearer (except for the signalling radio bearer which is used to send the message that is reconfiguring the security configuration) where the new configuration is to be applied starting from and including reception of the response message).

8.5.10.3 Calculation of message authentication code

The UE shall calculate the message authentication code in accordance with [40]. The input parameter MESSAGE [40] for the integrity algorithm shall be constructed by:

1> setting the "Message authentication code" in the IE "Integrity check info" in the message to the value of the IE "RB identity" for the signalling radio bearer;

1> setting the "RRC Message sequence number" in the IE "Integrity check info" in the message to zero;

1> encoding the message;

1> appending RRC padding (if any) as a bit string to the encoded bit string as the least significant bits.

For usage on an RRC message transmitted or received on the radio bearer with identity n, the UE shall:

1> construct the input parameter COUNT-I [40] by appending the following IEs from the IE "Signalling radio bearer specific integrity protection information" for radio bearer n in the variable INTEGRITY_PROTECTION_INFO:

2> for uplink:

3> "Uplink RRC HFN", as the MSB, and "Uplink RRC Message sequence number", as LSB.

2> for downlink:

3> "Downlink RRC HFN", as the MSB, and the IE "RRC message sequence number" included in the IE "Integrity check info", as LSB.