SECURITY MODE COMPLETE (Step 7)

Information Element	Value/remark
RRC transaction identifier	0
Integrity check info	
- Message Authentication code	This IE is checked to see if it is present. The value is compared against the XMAC-I value computed by SS. The first/ leftmost bit of the bit string contains the most significant bit of the MAC-I.
- RRC Message sequence number	This IE is checked to see if it is present. The value is used by SS to compute the XMAC-I value.
Uplink integrity protection activation info	
- RRC message sequence number list	
-RRC message sequence number	Check to see if the RRC SN for RB 0 is present
-RRC message sequence number	Check to see if the RRC SN for RB 1 is present
-RRC message sequence number	Check to see if the RRC SN for RB 2 is present
-RRC message sequence number	Check to see if the RRC SN for RB 3 is present
-RRC message sequence number	Check to see if the RRC SN for RB 4 is present
Radio bearer uplink ciphering activation time info	
- Radio bearer activation time	
- RB Identity	1
- RLC sequence number	Check to see if the RLC SN for RB1is present
- RB Identity	2
- RLC sequence number	SS records this value. See step 8 in 'expected sequence'
- RB Identity	3
- RLC sequence number	Check to see if the RLC SN for RB3 is present
- RB Identity	4
- RLC sequence number	Check to see if the RLC SN for RB4 is present
- RB Identity	20
- RLC sequence number	Check to see if the RLC SN for RB20 is present

8.1.7.1b.5 Test requirement

After step 2 the UE shall transmit a SECURITY MODE FAILURE message to report the protocol error detected in the first SECURITY MODE COMMAND message.

After step 4 the UE shall transmit a SECURITY MODE FAILURE message to report on the invalid configuration detected in the second SECURITY MODE COMMAND message.

At step 7 SS checks that the SECURITY MODE COMPLETE message is received ciphered using the old configuration and that the calculated "integrity check info" IE is correct according to the new integrity protection configuration (new key and HFN set to zero).

After step 7 SS verifies that all uplink signalling messages on RB2 are integrity protected with the new integrity protection configuration.

After uplink ciphering activation time has elapsed, SS verifies that the UE CAPABILITY INFORMATION message received is ciphered with the new ciphering configuration as indicated in the SECURITY MODE COMMAND (Step 6) message.

After downlink ciphering activation time has elapsed, SS shall apply ciphering to all downlink messages using the new ciphering configuration. At least one more cycle between step 8 and step 10 shall be repeated correctly after activation time on both directions has elapsed and the messages on both directions shall be ciphered and integrity protected.

8.1.7.1c Security mode control in CELL_DCH state (CN Domain switch and new keys at RRC message sequence number wrap around)

8.1.7.1c.1 Definition

8.1.7.1c.2 Conformance requirement

Upon reception of the SECURITY MODE COMMAND message, the UE shall:

…

2> set the variable LATEST_CONFIGURED_CN_DOMAIN equal to the IE "CN domain identity";

2> set the IE "Status" in the variable SECURITY_MODIFICATION for the CN domain indicated in the IE "CN domain identity" in the received SECURITY MODE COMMAND to the value "Affected";

…

If a new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN, the UE shall:

1> set the START value for the CN domain indicated in the variable LATEST_CONFIGURED_CN_DOMAIN to zero;

1> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":

2> for integrity protection in the downlink on each signalling radio bearer except RB2:

3> if IE "Integrity protection mode command" has the value "start":

…

3> else:

4> for the first message for which the RRC sequence number in a received RRC message for this signalling radio bearer is equal to or greater than the activation time as indicated in IE "Downlink integrity protection activation info" as included in the IE "Integrity protection mode info":

5> start using the new integrity key;

5> for this signalling radio bearer:

6> set the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero.

2> for integrity protection in the uplink on each signalling radio bearer except RB2:

3> for the first message for which the RRC sequence number in a to be transmitted RRC message for this signalling radio bearer is equal to the activation time as indicated in IE "Uplink integrity protection activation info" included in the transmitted SECURITY MODE COMPLETE message:

4> start using the new integrity key;

4> for this signalling radio bearer:

5> set the IE "Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the uplink COUNT-I to zero.

2> for integrity protection in the downlink on signalling radio bearer RB2:

3> at the received SECURITY MODECOMMAND:

4> start using the new integrity key;

4> set the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero.

2> for integrity protection in the uplink on signalling radio bearer RB2 :

3> at the transmitted SECURITY MODE COMPLETE:

4> start using the new integrity key;

4> set the IE "Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the uplink COUNT-I to zero.

1> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":

2> for each signalling radio bearer and for each radio bearer for the CN domain indicated in the variable LATEST_CONFIGURED_CN_DOMAIN:

3> if the IE "Status" in the variable CIPHERING_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers using RLC-TM:

4> at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info":

5> start using the new key in uplink and downlink;

5> set the HFN component of the COUNT-C to zero.

3> if the IE "Status" in the variable CIPHERING_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers and signalling radio bearers using RLC-AM and RLC-UM:

4> in the downlink, at the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info":

5> start using the new key;

5> set the HFN component of the downlink COUNT-C to zero.

4> in the uplink, at the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info":

5> start using the new key;

5> set the HFN component of the uplink COUNT-C to zero.

1> consider the value of the latest transmitted START value to be zero.

…

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> 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.

…

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

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

1> if 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> start applying the new integrity protection configuration in the downlink 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> set the content of the variable INTEGRITY_PROTECTION_ACTIVATION_INFO according to the following:

…

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";

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.

Reference

3GPP TS 25.331 clauses 8.1.12.3, 8.6.3.4, 8.6.3.5.

8.1.7.1c.3 Test purpose

To verify that the UE correctly modifies the integrity protection and ciphering configuration with a newly generated PS domain keyset for when previously using the CS domain keyset.

To verify that the UE can handle change of integrity protection key when the RRC message sequence number wraps around when the SECURITY MODE COMMAND is received.

8.1.7.1c.4 Method of test

Initial Condition

System Simulator: 1 cell.

UE: has entered PS+CS-DCCH+DTCH_DCH (state 6-14) using procedure P24 as specified in clause 7.4 of TS 34.108.

Test Procedure

The UE is in CELL_DCH state.

The SS transmits UE CAPABILITY ENQUIRY message repeatedly on the downlink DCCH using RLC-UM mode on SRB1. The UE shall respond to each downlink message with a UE CAPABILITY INFORMATION message on the uplink DCCH using RLC-AM. SS then sends UE CAPABILITY INFORMATION CONFIRM message to the UE using RLC-AM. This procedure is repeated until the RRC message sequence number for SRB 2 in downlink equals 15.

The SS initiates an Authentication procedure, which will result in the generation of a new security keyset (CK/IK). The SS transmits a valid SECURITY MODE COMMAND message which includes the correct downlink activation times and "Integrity check info" IE.

Then the UE shall check the integrity check info and shall start to configure ciphering in downlink according to the first valid SECURITY MODE COMMAND message. The UE shall transmit a SECURITY MODE COMPLETE message which contains the correct uplink activation times and also "Integrity check info" IE using the new integrity protection configuration.

The SS records the uplink ciphering activation time for RB 2.

Next, the SS transmits UE CAPABILITY ENQUIRY message repeatedly on the downlink DCCH using RLC-AM mode. The UE shall respond to each downlink message with a UE CAPABILITY INFORMATION message on the uplink DCCH using RLC-AM. SS then send UE CAPABILITY INFORMATION CONFIRM message to the UE. This cycle repeats itself until both the uplink and downlink ciphering activation time for RB 2 has elapsed. SS checks all uplink UE CAPABILITY INFORMATION messages are integrity-protected by UIA algorithm, and that the messages

contain the correct values for "Integrity check info" IE. This can be verified in the SS through the reception of a correctly ciphered and integrity-protected UE CAPABILITY INFORMATION message.

The SS transmits UE CAPABILITY ENQUIRY message on the downlink DCCH using RLC-UM mode on SRB1. The UE shall respond to this message with a UE CAPABILITY INFORMATION message on the uplink DCCH using RLC-AM. SS then send UE CAPABILITY INFORMATION CONFIRM message to the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				The UE is in CELL_DCH state.
2	←		UE CAPABILITY ENQUIRY	The SS repeats step 2, 3 and 4 until its internal downlink RRC message sequence number for RB 2 has the value 15.
3	→		UE CAPABILITY INFORMATION	The UE shall send this message on the uplink DCCH using RLC-AM. SS verifies that the last UE CAPABILITY INFORMATION message is both integrity-protected and ciphered correctly.
4	←		UE CAPABILITY INFORMATION CONFIRM	
5	←		AUTHENTICATION and CIPHERING REQUEST	GMM message which will result in the generation of a new security keyset
6	→		AUTHENTICATION AND CIPHERING RESPONSE	GMM
7	←		SECURITY MODE COMMAND	See specific message contents.
8	→		SECURITY MODE COMPLETE	The SS verifies that this message is sent using the old ciphering configuration. SS records the uplink ciphering activation time for RB 2.
9	←		UE CAPABILITY ENQUIRY	The SS repeats step 9, 10 and 11 until its internal uplink and downlink RLC SN have both surpassed the uplink and downlink ciphering activation time specified for RB2. This message is sent on the downlink DCCH using RLC-AM.
10	→		UE CAPABILITY INFORMATION	The UE shall send this message on the uplink DCCH using RLC-AM. SS verifies that the last UE CAPABILITY INFORMATION message is both integrity-protected and ciphered correctly.
11	←		UE CAPABILITY INFORMATION CONFIRM	
12	←		UE CAPABILITY ENQUIRY	The SS sends this message with the downlink RRC message sequence number for SRB 1 with the value 0.
13	→		UE CAPABILITY INFORMATION	The UE shall send this message on the uplink DCCH using RLC-AM. SS verifies that the last UE CAPABILITY INFORMATION message is both integrity-protected and ciphered correctly.
14	←		UE CAPABILITY INFORMATION CONFIRM	

Specific Message Contents

SECURITY MODE COMMAND (Step 7)

Use the same message content as found in clause 9 of TS 34.108, with the following exceptions:

Information Element	Value/remark
RRC transaction identifier	0
Integrity check info	
Message authentication code	Calculated result in SS. The first/ leftmost bit of the bit string contains the most significant bit of the MAC-I.
RRC Message sequence number	Next RRC SN
Security Capability	Same as originally sent by UE (and stored in SS)
Ciphering mode info	
Ciphering mode command	Start/restart
Ciphering algorithm	UEA1
Radio bearer downlink ciphering activation time info	
RB Identity	1
RLC sequence number	Current RLC SN
RB Identity	2
RLC sequence number	Current RLC SN + 2
RB Identity	3
RLC sequence number	Current RLC SN
RB Identity	4
RLC sequence number	Current RLC SN
RB Identity	20
RLC sequence number	Current RLC SN
Integrity protection mode info	
Integrity protection mode command	Modify
Downlink integrity protection activation info	
	Current RRC SN for SRB0
	Current RRC SN for SRB1
	0
	Current RRC SN for SRB3
	Current RRC SN for SRB4
Integrity protection algorithm	UIA1
CN domain identity	PS Domain

NOTE: "Current RLC SN" is defined as the value of VT(S) in the SS at the time when the SECURITY MODE COMMAND is submitted to RLC for transmission, that is, the RLC send sequence number of the next transmitted RLC PDU on the particular radio bearer. "Current RRC SN" is defined as the RRC message sequence number of the next transmitted RRC message on the particular radio bearer.

SECURITY MODE COMPLETE (Step 8)

Use the same message content as found in clause 9 of TS 34.108, with the following exceptions:

Information Element	Value/remark
RRC transaction identifier	0
Integrity check info	
- Message Authentication code	This IE is checked to see if it is present. The value is compared against the XMAC-I value computed by SS. The first/ leftmost bit of the bit string contains the most significant bit of the MAC-I.
- RRC Message sequence number	This IE is checked to see if it is present. The value is compared against the XMAC-I value computed by SS.
Uplink integrity protection activation info	
- RRC message sequence number list	Check to see if the RRC SN for RB 0 to RB 4 are present
-RRC message sequence number	Check to see if the RRC SN for RB 0 is present
-RRC message sequence number	Check to see if the RRC SN for RB 1 is present
-RRC message sequence number	Check to see if the RRC SN for RB 2 is present
-RRC message sequence number	Check to see if the RRC SN for RB 3 is present
-RRC message sequence number	Check to see if the RRC SN for RB 4 is present
Radio bearer uplink ciphering activation time info	
- Radio bearer activation time	
- RB Identity	1
- RLC sequence number	Check to see if the RLC SN for RB1 is present
- RB Identity	2
- RLC sequence number	SS records this value. See step 10 in 'expected sequence'
- RB Identity	3
- RLC sequence number	Check to see if the RLC SN for RB3 is present
- RB Identity	4
- RLC sequence number	Check to see if the RLC SN for RB4 is present
- RB Identity	20
- RLC sequence number	Check to see if the RLC SN for RB20 is present

8.1.7.1c.5 Test requirement

After step 7 the SS checks that the SECURITY MODE COMPLETE message is received ciphered using the old configuration and that the calculated "integrity check info" IE is correct.

After step 8 SS verifies that all uplink signalling messages on RB2 are integrity protected with UIA1 algorithm.

After uplink ciphering activation time has lapsed, SS verifies that the UE CAPABILITY INFORMATION message received is integrity protected with UIA algorithm and ciphered with the new ciphering configuration and algorithm indicated in the SECURITY MODE COMMAND (Step 7) message.

After downlink ciphering activation time has lapsed, SS shall apply ciphering to all downlink messages using the new configuration. At least one more cycle between step 9 and step 11 shall be repeated correctly after activation time on both directions has lapsed and the messages on both directions shall be ciphered and integrity protected..

8.1.7.1d Security mode control in CELL_DCH state interrupted by a cell update

8.1.7.1d.1 Definition

8.1.7.1d.2 Conformance requirement

If:

- a cell update procedure according to subclause 8.3.1 is initiated; and
- the received SECURITY MODE COMMAND message causes either,
  - the IE "Reconfiguration" in the variable CIPHERING_STATUS to be set to TRUE; and/or
  - the IE "Reconfiguration" in the variable INTEGRITY_PROTECTION_INFO to be set to TRUE: