

21-24 May, 2001

Phoenix, USA

CR-Form-v3

**CHANGE REQUEST**

⌘ **33.105 CR CR-Num** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Deletion of the maximum size of a RRC message		
<b>Source:</b>	⌘ Nokia		
<b>Work item code:</b>	⌘ Security	<b>Date:</b>	⌘ 17/05/2001
<b>Category:</b>	⌘ A	<b>Release:</b>	⌘ REL-4
	Use <u>one</u> of the following categories: <b>F</b> (essential correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (Addition of feature), <b>C</b> (Functional modification of feature) <b>D</b> (Editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900.		Use <u>one</u> of the following releases: <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>REL-4</b> (Release 4) <b>REL-5</b> (Release 5)

<b>Reason for change:</b>	⌘ An unspecified variable X19 still exists in the specification.
<b>Summary of change:</b>	⌘ The reference to the maximum size of RRC message is deleted because such a maximum size does not exist.
<b>Consequences if not approved:</b>	⌘ Specification is incomplete

<b>Clauses affected:</b>	⌘ 5.3.7 Interface
<b>Other specs Affected:</b>	⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications
<b>Other comments:</b>	⌘

**How to create CRs using this form:**

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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://www.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 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.

## 5.3.7 Interface

### 5.3.7.1 IK

IK: the integrity key

IK[0], IK[1], ..., IK[127]

The length of IK is 128 bits.

### 5.3.7.2 COUNT-I

COUNT-I: a frame dependent input.

COUNT-I[0], COUNT-I[1], ..., COUNT-I[31]

The length of COUNT-I is 32 bits.

The input parameter COUNT-I protects against replay during a connection. It is a value incremented by one for each integrity protected message. COUNT-I consists of two parts: the HYPERFRAME NUMBER (HFN) as the most significant part and a RRC Sequence Number as the least significant part. The initial value of the hyperframe number is sent by the user to the network at connection set-up. The user stores the greatest used hyperframe number from the previous connection and increments it by one. In this way the user is assured that no COUNT-I value is re-used (by the network) with the same integrity key.

### 5.3.7.3 FRESH

FRESH: a random number generated by the RNC.

FRESH[0], FRESH[1], ..., FRESH[31]

The length of FRESH is 32 bits.

The same integrity key may be used for several consecutive connections. This FRESH value is an input to the algorithm in order to assure the network side that the user is not replaying old MAC-Is.

### 5.3.7.4 MESSAGE

MESSAGE: the signalling data.

MESSAGE[0], MESSAGE[1], ..., MESSAGE[X49-1]

The maximum length of MESSAGE is X49.

### 5.3.7.5 DIRECTION

DIRECTION: the direction of transmission of signalling messages (user to network or network to users).

DIRECTION[0]

The length of DIRECTION is 1 bit.

The same integrity key may be used for uplink and downlink channels simultaneously associated with a UE.

The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

### 5.3.7.6 MAC-I (and equivalently XMAC-I)

MAC-I: the message authentication code for data integrity authentication

MAC-I[0], MAC-I[1], ..., MAC-I[31]

The length of MAC-I is 32 bits.