3GPP TSG-SA WG 3 - S3#18
Phoenix, USA, May 21th – 24th, 2001

Tdoc S3-010185

CR-Form-v3

CHANGE REQUEST

⌘ **TS 33.103 CR ???** ⌘ rev **-** ⌘ Current version: **3.5.0** ⌘

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

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

Title:	⌘	The multiplicity of Data integrity symbols
Source:	⌘	Nokia Networks
Work item code:	⌘	***Date:*** ⌘ May 10, 2001
Category:	⌘ **D**	***Release:*** ⌘ R99

Use one of the following categories:
F *(essential 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)*

Reason for change:	⌘	Some inconsistencies with TS 33.102
Summary of change:	⌘	Change UE to RNC and change multiplicity values in table12. (New values based on TS 33.102 chapters 6.5.4.1 and 6.5.4.3)
Consequences if not approved:	⌘	

Clauses affected:	⌘	4.4		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ 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/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.

4.4 Radio network controller

4.4.1 Data confidentiality (DC_{rnc})

The RNC shall support the UMTS mechanism for data confidentiality of user and signalling data described in 6.6 of 3G TS 33.102.

The RNC shall store the following data elements:

a) UEA-RNC: the ciphering capabilities of the RNC;

In addition, when in dedicated mode:

b) UEA: the selected ciphering function;

c) CK: the cipher key;

d) COUNT-C_{UP}: a time varying parameter for synchronisation of ciphering for the uplink;

e) COUNT-C_{DOWN}: a time varying parameter for synchronisation of ciphering for the downlink;

f) DIRECTION: An indication of the direction of transmission uplink or downlink to ensure a different cipher is applied

g) BEARER: a radio bearer identifier.

Table 10 provides an overview of the data elements stored in the RNC to support the mechanism for data confidentiality:

Table 10: RNC – Data Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UEA-RNC	Ciphering capabilities of the ~~UE~~RNC	1	Permanent	16 bits	Mandatory
UEA	Selected ciphering capability	1 per user and per mode	Updated at connection establishment	4 bits	Mandatory
CK	Cipher key	1 per user and per mode	Updated at connection establishment	128 bits	Mandatory
COUNT-C_{UP}	Time varying parameter for synchronisation of ciphering	1 per radio bearer	Lifetime of a radio bearer	32 bits	Mandatory
COUNT-C_{DOWN}	Time varying parameter for synchronisation of ciphering	1 per radio bearer	Lifetime of a radio bearer	32 bits	Mandatory
BEARER	Radio bearer identifier	1 per radio bearer	Lifetime of a radio bearer	5 bits	Mandatory
DIRECTION	An indication of the direction of transmission uplink or downlink	1 per radio bearer	Lifetime of a radio bearer	1 bit	Mandatory

The following cryptographic functions shall be implemented in the RNC:

- f8: access link encryption function.

Table 11 provides an overview of the cryptographic functions ~~that shall be~~ implemented in the RNC to support the mechanism for data confidentiality:

Table11: RNC – Data ~~integrity~~ confidentiality – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
~~f9~~f8	Access link ~~data integrity~~encryption function	1-16	Permanent	Standardised	One at least is mandatory

4.4.2 Data integrity (DI_{rnc})

The RNC shall support the UMTS mechanism for data integrity of signalling data described in 6.4 of 3G TS 33.102.

The RNC shall store the following data elements:

a) UIA-RNC: the integrity capabilities of the RNC;

In addition, when in dedicated mode:

b) UIA: the selected UMTS integrity algorithm;

c) IK: an integrity key;

d) COUNT-I_{UP}: a time varying parameter for synchronisation of data integrity in the uplink direction;

e) COUNT-I_{DOWN}: a time varying parameter for synchronisation of data integrity in the downlink direction;

f) DIRECTION An indication of the direction of transmission uplink or downlink to ensure a different cipher is applied;

g) FRESH: an MS challenge.

Table 12 provides an overview of the data elements stored on the ~~UE~~ RNC to support the mechanism for data confidentiality:

Table12: ~~UE~~ RNC – Data Integrity – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UIA-RNC	Data integrity capabilities of the RNC	1	Permanent	16 bits	Mandatory
UIA	Selected data integrity capability	1 per user	Lifetime of a connection	4 bits	Mandatory
IK	Integrity key	1 per user	Lifetime of a connection	128 bits	Mandatory
DIRECTION	An indication of the direction of transmission uplink or downlink	1 per radio bearer	Lifetime of a radio bearer	1 bit	Mandatory
COUNT-I_{UP}	Synchronisation value	1 per radio bearer	Lifetime of a connection	32 bits	Mandatory
COUNT-I_{DOWN}	Synchronisation value	1 per radio bearer	Lifetime of a connection	32 bits	Mandatory
FRESH	MS challenge	1 per user	Lifetime of a connection	32 bits	Mandatory
MAC-I XMAC-I	Message authentication code	1 per user	Updated by the execution of the f9 function~~AKA protocol~~	32 bits	Mandatory

The following cryptographic functions shall be implemented on the ~~UE~~RNC:

- f9: access link integrity function.

Table 13 provides an overview of the cryptographic functions implemented in the ~~UE~~RNC:

Table 13: ~~UE~~ RNC – Data Integrity – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f9	Access link data integrity function	1-16	Permanent	Standardised	One at least is mandatory