3GPP TSG SA WG 3 (Security) meeting #15
Washington (USA), 12—14 September, 2000

Document **S3-000586**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.103	**CR**	**xxx**	Current Version:	3.3.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	SA #9	for approval	X	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [X] Core Network [ ]

Source: Nokia **Date:** 2000-09-08

Subject: Correction to BEARER definition

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	[X]	**Release:**	Phase 2	[ ]
A	Corresponds to a correction in an earlier release	[ ]		Release 96	[ ]
B	Addition of feature	[ ]		Release 97	[ ]
C	Functional modification of feature	[ ]		Release 98	[ ]
D	Editorial modification	[ ]		Release 99	[X]
				Release 00	[ ]

Reason for change:

The definition and length of the data element BEARER has been corrected. BEARER is a 5-bit radio bearer identifier (as already specified in TS 33.102).

Ciphering and integrity protection is performed per radio bearer, not per logical channel.

Clauses affected: 4.3.2, 4.3.3, 4.4.1, 4.4.2

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR

4.3.2 Data confidentiality (DC_{UE})

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

The UE shall store the following data elements:

a) UEA-MS: the ciphering capabilities of the UE;

b) CK: the cipher key;

c) UEA: the selected ciphering function;

In addition, when in dedicated mode:

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) BEARER: a ~~logical channel~~radio bearer identifier;

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

Table 6 provides an overview of the data elements stored on the UE to support the mechanism for data confidentiality:

Table 6: UE – Data Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UEA-MS	Ciphering capabilities of the UE	1 per UE	Permanent	16 bits	Mandatory
CK	Cipher key	1 per mode	Updated at execution of AKA protocol	128 bits	Mandatory
UEA	Selected ciphering capability	1 per UE	Updated at connection establishment	4 bits	Mandatory
COUNT-C_{UP}	Time varying parameter for synchronisation of ciphering	1 per ~~logical channel~~radio bearer	Lifetime of a ~~logical channel~~radio bearer	32 bits	Mandatory
COUNT-C_{DOWN}	Time varying parameter for synchronisation of ciphering	1 per ~~logical channel~~radio bearer	Lifetime of a ~~logical channel~~radio bearer	32 bits	Mandatory
BEARER	~~Logical channel~~Radio bearer identifier	1 per ~~logical channel~~radio bearer	Lifetime of a ~~logical channel~~radio bearer	~~8~~5 bits	Mandatory
DIRECTION	An indication of the direction of transmission uplink or downlink	1 per ~~logical channel~~radio bearer	Lifetime of a ~~logical channel~~radio bearer	1 bit	Mandatory

The following cryptographic functions shall be implemented on the UE:

- f8: access link encryption function (note 1).
- c4: Conversion function for interoperation with GSM from Kc (GSM) to CK (UMTS).

NOTE 1: The security architecture TS 33.102 refers to UEA , f8 is a specific implementation of UEA as defined in Cryptographic algorithm requirements TS 33.105.

Table 7 provides an overview of the cryptographic functions implemented on the UE to support the mechanism for data

confidentiality.

Table 7: UE – Data Confidentiality – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f8	Access link encryption function	1-16	Permanent	Standardised	One at least is mandatory
c4	Conversion function for interoperation with GSM	1	Permanent	Standardised	Optional

4.3.3 Data integrity (DI_{UE})

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

The UE shall store the following data elements:

a) UIA-MS: the integrity capabilities of the UE.

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: a network challenge;

Table 8 provides an overview of the data elements stored on the UE to support the mechanism for data confidentiality:

Table 8: UE – Data Integrity – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UIA-MS	Ciphering capabilities of the UE	1 per UE	Permanent	16 bits	Mandatory
UIA	Selected ciphering capability	1 per UE	Updated at connection establishment	4 bits	Mandatory
IK	Integrity key	1 per mode	Updated by the execution of the AKA protocol	128 bits	Mandatory
DIRECTION	An indication of the direction of transmission uplink or downlink	1 per ~~logical channel~~radio bearer	Lifetime of a ~~logical channel~~radio bearer	1 bit	Mandatory
COUNT-I_{UP}	Synchronisation value	1	Lifetime of a connection	32 bits	Mandatory
COUNT-I_{DOWN}	Synchronisation value	1	Lifetime of a connection	32 bits	Mandatory
FRESH	Network challenge	1	Lifetime of a connection	32 bits	Mandatory
MAC-I XMAC-I	Message authentication code	1	Updated by the execution of the AKA protocol	32 bits	Mandatory

The following cryptographic functions shall be implemented on the UE:

- f9: access link integrity function (note 1).
- c5: Conversion function for interoperation with GSM Kc (GSM) > IK (UMTS)

NOTE 1: The security architecture TS 33.102 refers to UIA, f9 is a specific implementation of UIA as defined in Cryptographic algorithm requirements TS 33.105.

Table 9 provides an overview of the cryptographic functions implemented in the UE:

Table 9: UE – 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
c5	Conversion function for interoperation with GSM	1	Permanent	Standardised	Optional

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 ~~logical channel~~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	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 ~~logical channel~~radio bearer	Lifetime of a ~~logical channel~~radio bearer	32 bits	Mandatory
COUNT-C_{DOWN}	Time varying parameter for synchronisation of ciphering	1 per ~~logical channel~~radio bearer	Lifetime of a ~~logical channel~~radio bearer	32 bits	Mandatory
BEARER	~~Logical channel~~Radio bearer identifier	1 per ~~logical channel~~radio bearer	Lifetime of a ~~logical channel~~radio bearer	~~8~~5 bits	Mandatory
DIRECTION	An indication of the direction of transmission uplink or downlink	1 per ~~logical channel~~radio bearer	Lifetime of a ~~logical channel~~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:

Table11: 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

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 to support the mechanism for data confidentiality:

Table12: UE – 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 ~~logical channel~~radio bearer	Lifetime of a ~~logical channel~~radio bearer	1 bit	Mandatory
COUNT-I_{UP}	Synchronisation value	1	Lifetime of a connection	32 bits	Mandatory
COUNT-I_{DOWN}	Synchronisation value	1	Lifetime of a connection	32 bits	Mandatory
FRESH	MS challenge	1	Lifetime of a connection	32 bits	Mandatory
MAC-I XMAC-I	Message authentication code	1	Updated by the execution of the AKA protocol	32 bits	Mandatory

The following cryptographic functions shall be implemented on the UE:

- f9: access link integrity function.

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

Table 13: UE – 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