Technical Specification Group Services and System Aspects **_TSGS#9(00)0446_**
Meeting #9, Hawaii, USA, 25-28 September 2000

Source: **SA WG3**

Title: **1 Corrective CR to 33.103**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CR was agreed at SA WG3 meetings #14 and #15 and are presented to TSG SA #09 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
33.102	121		R99	Clarifications on integrity and ciphering of radio bearers.	F	3.5.0	S3	S3-15	S3-000573
33.103	011		R99	Correction to BEARER definition	F	3.3.0	S3	S3-15	S3-000586

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

Document **S3-000573**
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.

33.102	**CR**	**121**	Current Version:	3.5.0

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

For submission to:	SA #9	for approval	☒	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	☒	UTRAN / Radio	☒	Core Network	□

Source:	SA WG3	**Date:**	2000-09-07
Subject:	Clarifications on integrity and ciphering of radio bearers.		
Work item:	Security		

Category:	F	Correction	☒	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	☒
					Release 00	□

Reason for change:

Alignment with TS 25.331.

- Use of "radio bearer" instead of "logical channel"
- There is only one RRC connection established between MS and Serving RNC.
- Editorial modifications.

Clauses affected: 6.4.8, 6.5.5, 6.6.2, 6.6.4.2, 6.6.5

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

6.4.8 Initialisation of synchronisation for ciphering and integrity protection

The ciphering and integrity protection algorithms are driven by counters (COUNT-C and COUNT-I) that at connection establishment need to be initialised. For that purpose the ME and the USIM have the ability to store a START value. The ME and the USIM store a START$_{CS}$ value for the CS cipher/integrity keys and a START$_{PS}$ value for the PS cipher/integrity keys. The length of START is 20 bits.

The ME only contains (valid) START values when it is powered-on and a USIM is inserted. When the ME is powered-off or the USIM is removed, the ME deletes its START values. After power-on or insertion of a USIM, the USIM sends its START values to the ME, and the ME stores them. During idle mode, the START values in the ME and in the USIM are identical and static.

At radio connection establishment for a particular serving network domain (CS or PS) the ME sends the START$_{CS}$ and the START$_{PS}$ value to the RNC in the *RRC connection setup complete* message. The ME marks the START values in the USIM as invalid by setting START$_{CS}$ and START$_{PS}$ to THRESHOLD.

The ME and the RNC initialise the 20 most significant bits of the RRC HFN (for integrity protection), the RLC HFN (for ciphering) and the MAC-d HFN (for ciphering) to the START value of the corresponding service domain; the remaining bits are initialised to 0. Also the RRC SN (for integrity protection), the RLC SN (for ciphering) and the MAC-d HFN (for ciphering) are initialised to 0.

During an ongoing radio connection, the START$_{CS}$ value in the ME is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and CS user data ~~logical channels~~radio bearers protected using CK$_{CS}$ and/or IK$_{CS,}$ incremented by 1, i.e.:

> START$_{CS}$ = MSB$_{20}$ (MAX {COUNT-C, COUNT-I | all ~~logical channels~~radio bearers (including signalling) protected with CK$_{CS}$ and IK$_{CS}$}) + 1.

Likewise, during an ongoing radio connection, the START$_{PS}$ value in the ME is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and PS user data radio bearers ~~logical channels~~ protected using CK$_{PS}$ and/or IK$_{PS}$, incremented by 1, i.e.:

> START$_{PS}$ = MSB$_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) ~~logical channels~~ protected with CK$_{PS}$ and IK$_{PS}$}) + 1.

Upon radio connection release and when a set of cipher/integrity keys is no longer used, the ME updates START$_{CS}$ and START$_{PS}$ in the USIM with the current values.

During authentication and key agreement the ME sets the START values of the corresponding service domain to 0 in the USIM and in the ME itself.

6.5.5 Integrity key selection

There may be one IK for CS connections (IK$_{CS}$), established between the CS service domain and the user and one IK for PS connections (IK$_{PS}$) established between the PS service domain and the user.

The data integrity of radio bearers ~~logical channels~~ for user data is not protected.

The signalling radio bearers are used for transfer of s~~S~~ignalling data for services delivered by ~~either of~~ both CS and PS service domains ~~is sent over common logical (signalling) channels~~. These signalling radio bearers ~~logical channels~~ are data integrity protected by the IK of the service domain for which the most recent security mode negotiation took place. This may require that the integrity key of an (already integrity protected) ongoing signalling connection has to be changed, when a new ~~RRC~~ connection is established ~~(~~with another service domain~~)~~, or when a security mode negotiation follow a re-authentication during an ongoing connection. This change should be completed within five seconds after the security mode negotiation.

6.6.2 Layer of ciphering

The ciphering function is performed either in the RLC sub-layer or in the MAC sub-layer, according to the following rules:

- ~~If a logical channel is expected to be supported on a common transport channel and has to be ciphered, it shall~~

~~use UM RLC mode and ciphering is performed at the RLC sub-layer.~~

- If a radio bearer ~~logical channel~~ is using a non-transparent RLC mode (AM or UM), ciphering is performed in the RLC sub-layer.

- If a radio bearer ~~logical channel~~ is using the transparent RLC mode, ciphering is performed in the MAC sub-layer (MAC-d entity).

Ciphering when applied is performed in the S-RNC and the ME and the context needed for ciphering (CK, HFN, etc.) is only known in S-RNC and the ME.

6.6.4.2 CK

The cipher key CK is 128 bits long.

There may be one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user. ~~Which~~ The CK~~cipher key~~ to use for a particular radio bearer ~~logical channel~~ is described in 6.6.~~6~~5. For UMTS subscribers, CK is established during UMTS AKA, as the output of the cipher key derivation function f3, available in the USIM and in HLR/AuC. For GSM subscribers that access the UTRAN, CK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 8.2.

CK is stored in the USIM and a copy is stored in the ME. CK is sent from the USIM to the ME upon request of the ME. The USIM shall send CK under the condition that 1) a valid CK is available, 2) the current value of START in the USIM is up-to-date and 3) START has not reached THRESHOLD. The ME shall delete CK from memory after power-off as well as after removal of the USIM.

CK is sent from the HLR/AuC to the VLR or SGSN and stored in the VLR or SGSN as part of the quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) security mode command.

At handover, the CK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed. The cipher CK remains unchanged at handover.

6.6.5 Cipher key selection

There is one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user.

The radio bearers ~~logical channels~~ for CS user data are ciphered with CK_{CS}.

The radio bearers ~~logical channels~~ for PS user data are ciphered with CK_{PS}.

The signalling radio bearers are used for transfer of s~~S~~ignalling data ~~(~~for services delivered by both CS and PS service~~s)~~ domains ~~is sent over common logical channels~~. These signalling radio bearers ~~logical channels~~ are ciphered by the CK of the service domain for which the most recent security mode negotiation took place. This may require that the cipher key of an (already ciphered) ongoing signalling connection ~~is~~ has to be changed, when a new ~~RRC~~ connection is ~~establishment~~ established with another service domain~~occurs~~, or when a security mode negotiation follows a re-authentication during an ongoing connection. This change should be completed within five seconds after the security mode negotiation.

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** **011** 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
list expected approval meeting # here ↑

for approval ☒
for information □

strategic □
non-strategic □
(for SMG use only)

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: (U)SIM □ ME ☒ UTRAN / Radio ☒ Core Network □
(at least one should be marked with an X)

Source: SA WG3 **Date:** 2000-09-08

Subject: Correction to BEARER definition

Work item: Security

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

F Correction ☒
A Corresponds to a correction in an earlier release □
B Addition of feature □
C Functional modification of feature □
D Editorial modification □

Release:

Phase 2 □
Release 96 □
Release 97 □
Release 98 □
Release 99 ☒
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 ($\mathrm{DI}_{\mathrm{UE}}$)

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