

Source: SA WG3
Title: 3 CRs to 33.102 (Rel-6)
Document for: Approval
Agenda Item: 7.3.3

The following CRs have been agreed by SA WG3 and are presented to TSG SA for approval.

TSG SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Work item
SP-040852	33.102	189	-	Rel-6	Correction of Abbreviation for USIM	D	6.2.0	S3-040904	SEC1
SP-040852	33.102	190	1	Rel-6	Correction of TMUI to TMSI in a figure	D	6.2.0	S3-041071	SEC1
SP-040852	33.102	191	3	Rel-6	Support of algorithms in UEs	C	6.2.0	S3-041073	SEC1

CR-Form-v7.1

CHANGE REQUEST

¶ 33.102 CR 189 ¶ rev - ¶ Current version: 6.2.0 ¶

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

Proposed change affects: | UICC apps ¶ ME ¶ Radio Access Network ¶ Core Network ¶

Title:	¶ Correction of Abbreviation for USIM		
Source:	¶ MCC		
Work item code:	¶ SEC1	Date:	¶ 04/11/2004
Category:	¶ D	Release:	¶ Rel-6
	Use <u>one</u> of the following categories: F (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 <u>one</u> of the following releases: Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	¶ The abbreviation for USIM is not in line with other 3GPP specifications
Summary of change:	¶ Corrected Abbreviation for USIM
Consequences if not approved:	¶ Incorrect definition of USIM may lead to confusion

Clauses affected:	¶ 3.3										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="width: 20px; text-align: center;">¶</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="width: 20px; text-align: center;">¶</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="width: 20px; text-align: center;">¶</td> <td style="width: 20px; text-align: center;">N</td> </tr> </table>	Y	N	¶	N	¶	N	¶	N	Other core specifications	¶
	Y	N									
	¶	N									
¶	N										
¶	N										
		Test specifications									
		O&M Specifications									
Other comments:	¶										

***** CHANGE *****

3.3 Abbreviations

In addition to (and partly in overlap to) the abbreviations included in TR 21.905 [3], for the purposes of the present document, the following abbreviations apply:

AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAC	The message authentication code included in AUTN, computed using f1
MAC	The message authentication code included in AUTN, computed using f1*
ME	Mobile Equipment
MS	Mobile Station
MSC	Mobile Services Switching Centre
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
SQN	Sequence number
SQN _{HE}	Individual sequence number for each user maintained in the HLR/AuC
SQN _{MS}	The highest sequence number the USIM has accepted
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TMSI	Temporary Mobile Subscriber Identity
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
USIM	User Services Universal Subscriber Identity Module
VLR	Visitor Location Register
XRES	Expected Response

CHANGE REQUEST

33.102 **CR 190** rev 1 Current version: 6.2.0

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	☞ Correction of TMUI to TMSI in a figure		
Source:	☞ SA WG3		
Work item code:	☞ SEC1	Date:	☞ 15/10/2004
Category:	☞ D	Release:	☞ Rel-6
	Use <u>one</u> of the following categories: F (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 <u>one</u> of the following releases: Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	☞ In Figure 3, iTMUI is misspelled, it should be TMSI.		
Summary of change:	☞ Correction TMUI to TMSI.		
Consequences if not approved:	☞ Spelling mistake.		

Clauses affected:	☞ 6.1.2										
Other specs affected:	<table border="1" style="border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">☞</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">☞</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">☞</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	☞	X	☞	X	☞	X	Other core specifications Test specifications O&M Specifications	☞
Y	N										
☞	X										
☞	X										
☞	X										
Other comments:	☞										

*** BEGIN SET OF CHANGES ***

6.1.2 TMSI reallocation procedure

The purpose of the mechanism described in this subsection is to allocate a new TMSI/LAI pair to a user by which he may subsequently be identified on the radio access link.

The procedure should be performed after the initiation of ciphering. The ciphering of communication over the radio path is specified in clause 6.6. The allocation of a temporary identity is illustrated in Figure 3.

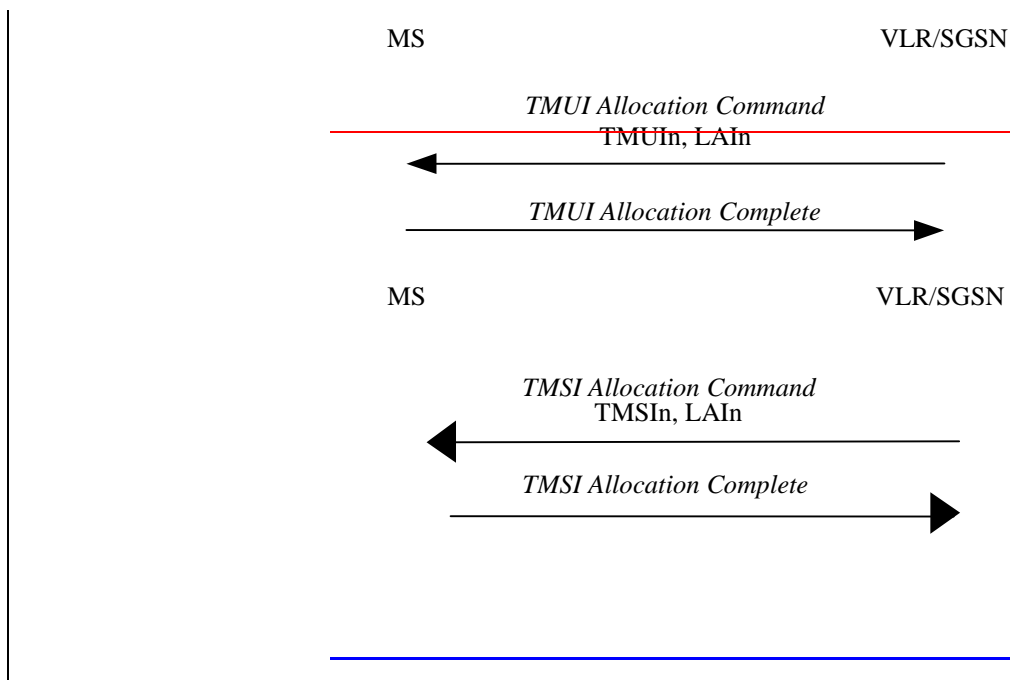


Figure 3: TMSI allocation

The allocation of a temporary identity is initiated by the VLR.

The VLR generates a new temporary identity (TMSIn) and stores the association of TMSIn and the permanent identity IMSI in its database. The TMSI should be unpredictable. The VLR then sends the TMSIn and (if necessary) the new location area identity LAIn to the user.

Upon receipt the user stores TMSIn and automatically removes the association with any previously allocated TMSI. The user sends an acknowledgement back to the VLR.

Upon receipt of the acknowledgement the VLR removes the association with the old temporary identity TMSIo and the IMSI (if there was any) from its database.

***END SET OF CHANGES ***

CHANGE REQUEST

⌘ 33.102 CR 191 ⌘ rev 3 ⌘ Current version: 6.2.0 ⌘

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

Proposed change affects: | UICC apps ME Radio Access Network Core Network

Title:	⌘ Support of algorithms in UEs and RNCs		
Source:	⌘ SA WG3		
Work item code:	⌘ SEC1	Date:	⌘ 18/11/2004
Category:	⌘ C	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories: F (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 <u>one</u> of the following releases: Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	⌘ There is a need to specify clearly in the specification which algorithms are mandatory to support in UTRAN.
Summary of change:	⌘ Specify which algorithms are mandatory to be supported in UTRAN
Consequences if not approved:	⌘ Reduced interoperability.

Clauses affected:	⌘ 6.5, 6.6										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	⌘	X	⌘	X	⌘	X	Other core specifications Test specifications O&M Specifications	⌘
Y	N										
⌘	X										
⌘	X										
⌘	X										
Other comments:	⌘										

***** START OF CHANGE *****

6.5 Access link data integrity

6.5.1 General

Most control signalling information elements that are sent between the MS and the network are considered sensitive and must be integrity protected. A message authentication function shall be applied on these signalling information elements transmitted between the ME and the RNC.

After the RRC connection establishment and execution of the security mode set-up procedure, all dedicated MS <ñ> network control signalling messages (e.g. RRC, MM, CC, GMM, and SM messages) shall be integrity protected. The Mobility Management layer in the MS supervises that the integrity protection is started (see section 6.4.5).

All signalling messages except the following ones shall then be integrity protected:

- HANDOVER TO UTRAN COMPLETE
- PAGING TYPE 1
- PUSCH CAPACITY REQUEST
- PHYSICAL SHARED CHANNEL ALLOCATION
- RRC CONNECTION REQUEST
- RRC CONNECTION SETUP
- RRC CONNECTION SETUP COMPLETE
- RRC CONNECTION REJECT
- RRC CONNECTION RELEASE (CCCH only)
- SYSTEM INFORMATION (BROADCAST INFORMATION)
- SYSTEM INFORMATION CHANGE INDICATION
- TRANSPORT FORMAT COMBINATION CONTROL (TM DCCH only)

6.5.2 Layer of integrity protection

~~The UIA shall be implemented in the ME and in the RNC.~~

Integrity protection shall be applied at the RRC layer.

6.5.3 Data integrity protection method

Figure 16 illustrates the use of the integrity algorithm f9 to authenticate the data integrity of a signalling message.

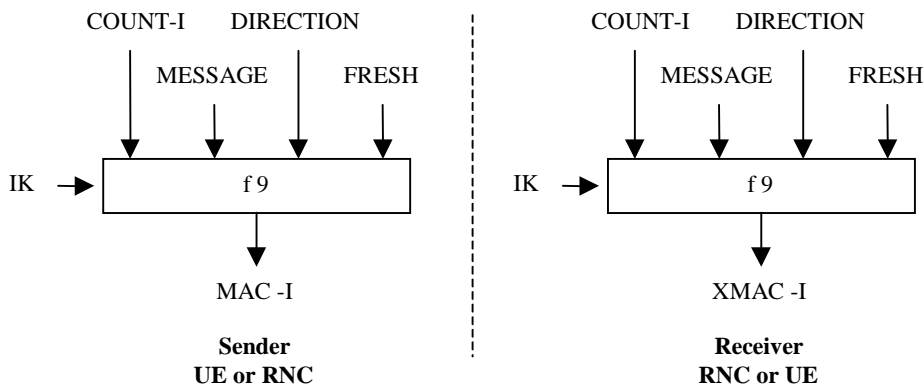


Figure 16: Derivation of MAC-I (or XMAC-I) on a signalling message

The input parameters to the algorithm are the Integrity Key (IK), the integrity sequence number (COUNT-I), a random value generated by the network side (FRESH), the direction bit DIRECTION and the signalling data MESSAGE. Based on these input parameters the user computes message authentication code for data integrity MAC-I using the integrity algorithm f9. The MAC-I is then appended to the message when sent over the radio access link. The receiver computes XMAC-I on the message received in the same way as the sender computed MAC-I on the message sent and verifies the data integrity of the message by comparing it to the received MAC-I.

6.5.4 Input parameters to the integrity algorithm

6.5.4.1 COUNT-I

The integrity sequence number COUNT-I is 32 bits long.

For signalling radio bearers (RB 0-4) there is one COUNT-I value per up-link signalling radio bearer and one COUNT-I value per down-link signalling radio bearer.

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number forms the least significant bits of COUNT-I while the "long" sequence number forms the most significant bits of COUNT-I. The "short" sequence number is the 4-bit RRC sequence number (RRC SN) that is available in each RRC PDU. The "long" sequence number is the 28-bit RRC hyper frame number (RRC HFN) which is incremented at each RRC SN cycle.

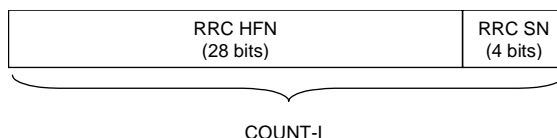


Figure 16a: The structure of COUNT-I

The RRC HFN is initialised by means of the parameter START, which is described in section 6.4.8. The ME and the RNC then initialise the 20 most significant bits of the RRC HFN to START; the remaining bits of the RRC HFN are initialised to 0.

6.5.4.2 IK

The integrity key IK is 128 bits long.

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. Which integrity key to use for a particular connection is described in 6.5.5.

For UMTS subscribers IK is established during UMTS AKA as the output of the integrity key derivation function f4, that is available in the USIM and in the HLR/AuC. For GSM subscribers, that access the UTRAN, IK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 6.8.2.

IK is stored in the USIM and a copy is stored in the ME. IK is sent from the USIM to the ME upon request of the ME. The USIM shall send IK under the condition that a valid IK is available. The ME shall trigger a new authentication procedure if the current value of $START_{CS}$ or $START_{PS}$ in the USIM are not up-to-date or $START_{CS}$ or $START_{PS}$ have reached THRESHOLD. The ME shall delete IK from memory after power-off as well as after removal of the USIM.

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

At handover, the IK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed, and the synchronisation procedure is resumed. The IK remains unchanged at handover.

6.5.4.3 FRESH

The network-side nonce FRESH is 32 bits long.

There is one FRESH parameter value per user. The input parameter FRESH protects the network against replay of signalling messages by the user. At connection set-up the RNC generates a random value FRESH and sends it to the user in the (RRC) *security mode command*. The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection. This mechanism assures the network that the user is not replaying any old MAC-Is.

At handover with relocation of the S-RNC, the new S-RNC generates its own value for the FRESH parameter and sends it to the ME in the RRC message that indicates a new UTRAN Radio Network Temporary Identity due to a SRNC relocation (see TS 25.331 [17]).

6.5.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that the integrity algorithm used to compute the message authentication codes would use an identical set of input parameter values for the up-link and for the down-link messages. The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

6.5.4.5 MESSAGE

The signalling message itself with the radio bearer identity. The latter is appended in front of the message. Note that the radio bearer identity is not transmitted with the message but it is needed to avoid that for different instances of message authentication codes the same set of input parameters is used.

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 for user data is not protected.

The signalling radio bearers are used for transfer of signalling data for services delivered by both CS and PS service domains. These signalling radio bearers 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 connection is established with another service domain, or when a security mode negotiation follows a re-authentication during an ongoing connection. This change should be completed by the RNC within five seconds after receiving the security mode command from the VLR/SGSN.

NOTE: For the behaviour of the terminal regarding key changes see section 6.4.5.

6.5.6 UIA identification

Each UMTS Integrity Algorithm (UIA) will be assigned a 4-bit identifier. Currently, the following values have been defined:

"0001₂" : UIA1, Kasumi.

The remaining values are not defined.

[It shall be mandatory for UEs and RNCs to implement UJA1.](#)

The use of Kasumi for the integrity protection function f9 is specified in TS 35.201 [11] and TS 35.202 [12]. Implementers' test data and design conformance data is provided in TS 35.203 [13] and TS 35.202 [14].

6.6 Access link data confidentiality

6.6.1 General

User data and some signalling information elements are considered sensitive and should be confidentiality protected. To ensure identity confidentiality (see section 6.1), the temporary user identity (P-)TMSI should be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it.

These needs for a protected mode of transmission are fulfilled by a confidentiality function which is applied on dedicated channels between the ME and the RNC.

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

6.6.3 Ciphering method

Figure 16b illustrates the use of the ciphering algorithm f8 to encrypt plaintext by applying a keystream using a bit per bit binary addition of the plaintext and the keystream. The plaintext may be recovered by generating the same keystream using the same input parameters and applying a bit per bit binary addition with the ciphertext.

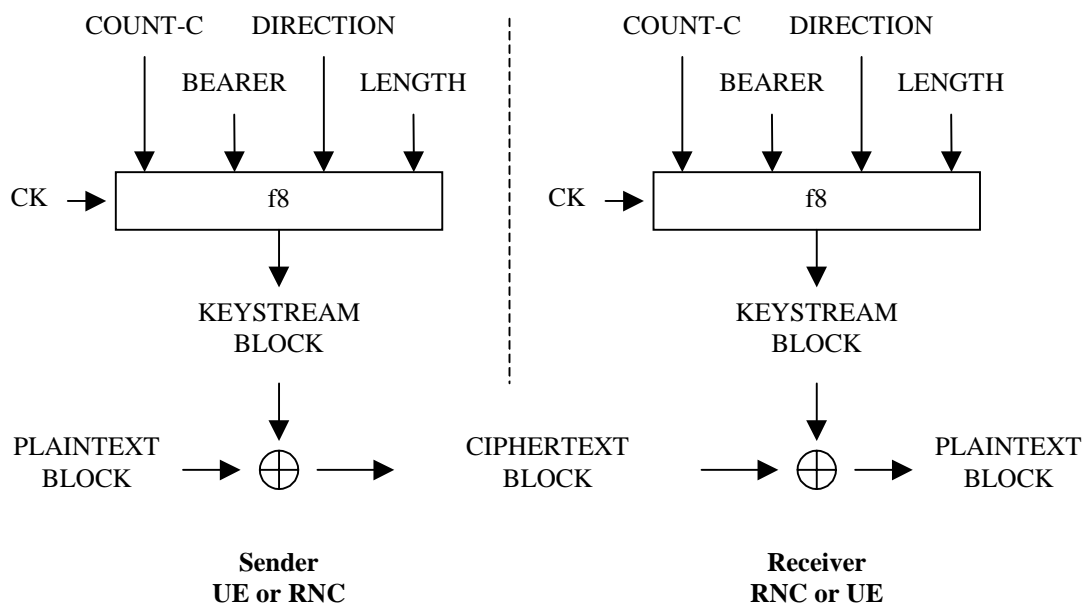


Figure 16b: Ciphering of user and signalling data transmitted over the radio access link

The input parameters to the algorithm are the cipher key CK, a time dependent input COUNT-C, the bearer identity BEARER, the direction of transmission DIRECTION and the length of the keystream required LENGTH. Based on these input parameters the algorithm generates the output keystream block KEYSTREAM which is used to encrypt the input plaintext block PLAINTEXT to produce the output ciphertext block CIPHERTEXT.

The input parameter LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

6.6.4 Input parameters to the cipher algorithm

6.6.4.1 COUNT-C

The ciphering sequence number COUNT-C is 32 bits long.

There is one COUNT-C value per up-link radio bearer and one COUNT-C value per down-link radio bearer using RLC AM or RLC UM. For all transparent mode RLC radio bearers of the same CN domain COUNT-C is the same, and COUNT-C is also the same for uplink and downlink.

COUNT-C is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number forms the least significant bits of COUNT-C while the "long" sequence number forms the most significant bits of COUNT-C. The update of COUNT-C depends on the transmission mode as described below (see figure 16c).

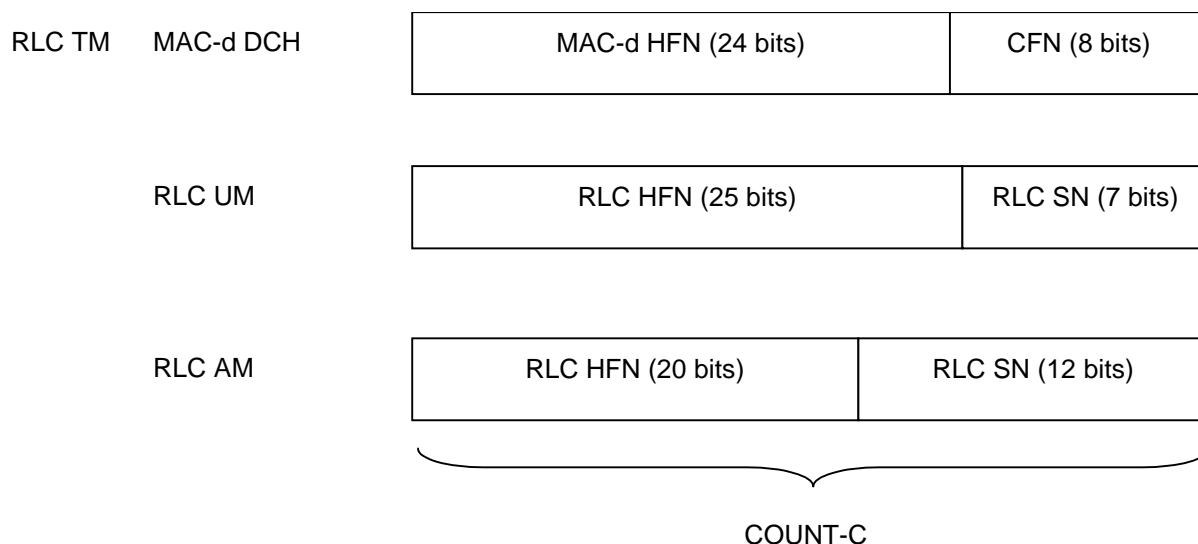


Figure 16c: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 8-bit connection frame number CFN of COUNT-C. It is independently maintained in the ME MAC-d entity and the SRNC MAC-d entity. The "long" sequence number is the 24-bit MAC-d HFN, which is incremented at each CFN cycle.
- For RLC UM mode, the "short" sequence number is the 7-bit RLC sequence number (RLC SN) and this is part of the RLC UM PDU header. The "long" sequence number is the 25-bit RLC UM HFN which is incremented at each RLC SN cycle.
- For RLC AM mode, the "short" sequence number is the 12-bit RLC sequence number (RLC SN) and this is part of the RLC AM PDU header. The "long" sequence number is the 20-bit RLC AM HFN which is incremented at each RLC SN cycle.

The hyperframe number HFN is initialised by means of the parameter START, which is described in section 6.4.8. The ME and the RNC then initialise the 20 most significant bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN to START. The remaining bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN are initialised to zero.

When a new radio bearer is created during a RRC connection in ciphered mode, the HFN is initialised by the current START value (see section 6.4.8).

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. The CK to use for a particular radio bearer is described in 6.6.5. For UMTS subscribers, CK is established during UMTS AKA, as the output of the cipher key derivation function f_3 , 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 K_c , 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 a valid CK is available. The ME shall trigger a new authentication procedure if the current value of $START_{CS}$ or $START_{PS}$ in the USIM have 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/SGSN and stored in the VLR/SGSN as part of the quintet. It is sent from the VLR/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.

6.6.4.3 BEARER

The radio bearer identifier BEARER is 5 bits long.

There is one BEARER parameter per radio bearer associated with the same user and multiplexed on a single 10ms physical layer frame. The radio bearer identifier is input to avoid that for different keystream an identical set of input parameter values is used.

6.6.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the keystreams for the up-link and for the down-link would use the an identical set of input parameter values. The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

6.6.4.5 LENGTH

The length indicator LENGTH is 16 bits long.

The length indicator determines the length of the required keystream block. LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

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 for CS user data are ciphered with CK_{CS} .

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

The signalling radio bearers are used for transfer of signalling data for services delivered by both CS and PS service domains. These signalling radio bearers 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 has to be changed, when a new connection is established with another service domain, or when a security mode negotiation follows a re-authentication during an ongoing connection. This change should be completed by the RNC within five seconds after receiving the security mode command from the VLR/SGSN.

NOTE: For the behaviour of the terminal regarding key changes see section 6.4.5.

6.6.6 UEA identification

Each UEA will be assigned a 4-bit identifier. Currently the following values have been defined:

"0000₂" : UEA0, no encryption.

"0001₂" : UEA1, Kasumi.

The remaining values are not defined.

[It shall be mandatory for UEs to implement UEA0 and UEA1.](#)

The use of Kasumi for the ciphering function f8 is specified in TS 35.201 [11] and TS 35.202 [12]. Implementers' test data and design conformance data is provided in TS 35.203 [13] and TS 35.202 [14].

***** END OF CHANGE *****