TSGS#8(00)272

Source **TSG-SA WG3**

Title **Corrective Release 1999 CRs to 33.102 v 3.4.0**

S3 Tdoc.	Spec.	Ver.	CR	Rev.	Cat.	Rel.	Subject
S3-000288	33.102	3.4.0	080		F	R99	Clarification on ciphering and integrity protection at intersystem handover
S3-000293	33.102	3.4.0	083		F	R99	Authentication and key agreement
S3-000294	33.102	3.4.0	084		F	R99	Conversion functions for GSM-UMTS interoperation
S3-000395	33.102	3.4.0	088	2	F	R99	Initialisation of synchronisation for ciphering and integrity protection
S3-000262	33.102	3.4.0	090		F	R99	Clarification of BEARER and DIRECTION parameters
S3-000269	33.102	3.4.0	093		F	R99	Removal of network domain security
S3-000292	33.102	3.4.0	094		F	R99	Cipher and integrity key update once every 24 hours
S3-000302	33.102	3.4.0	095		F	R99	Handling of emergency call
S3-000289	33.102	3.4.0	096		F	R99	Clarification on the HFN handling
S3-000323	33.102	3.4.0	098		F	R99	Security mode set-up procedure
S3-000323	33.102	3.4.0	100		F	R99	Replace COUNT by $START_{CS}$ and $START_{PS}$

3GPP TSG SA WG3 (Security) meeting #12
Stockholm, 11-14 April, 2000

***Document* S3-000288**
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	080	Current Version:	3.4.0

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

For submission to:	TSG SA #8	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	X	ME	X	UTRAN / Radio	X	Core Network	X

Source: SA WG3 **Date:** 2000-04-13

Subject: Clarification on ciphering and integrity protection at intersystem handover

Work item: Security

Category: *(only one category shall be marked with an X)*			**Release:**	
F	Correction	X	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:
- to clarify how the integrity protection is started at handover from GSM BSS to UTRAN
- to clarify the handling of HFN at handover from UTRAN to GSM BSS
- to update the list of unprotected messages with the Handover to UTRAN complete message
- to clarify that intersystem handover implies a change of ciphering algorithm

Clauses affected: 6.5.1, 6.8.4, 6.8.5

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.

6.5 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 ~~UE~~ MS and the RNC.

After the RRC connection establishment and execution of the security mode set-up procedure, all dedicated MS <–> 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:

- Paging Type 1
- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete
- RRC Connection Reject
- System Information (broadcasted information).
- Handover to UTRAN complete

6.8.4 Intersystem handover for CS Services – from UTRAN to GSM BSS

If ciphering has been started when an intersystem handover occurs from UTRAN to GSM BSS, the necessary information (e.g. Kc, supported/allowed GSM ciphering algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old RNC to the new GSM BSS, and to continue the communication in ciphered mode. The RNC requests the MS to send the MS Classmark, which includes information on the GSM ciphering algorithm capabilities of the MS. The intersystem handover will imply a change of ciphering algorithm from a UEA to a GSM A5. The GSM BSS includes the selected GSM ciphering mode in the handover command message sent to the MS via the RNC.

The integrity protection of signalling messages is stopped at handover to GSM BSS.

The highest hyperframe number value reached for all signaling and user data bearers during the RRC connection shall be stored in the ME/USIM at handover to GSM BSS.

6.8.5 Intersystem handover for CS Services – from GSM BSS to UTRAN

If ciphering has been started when an intersystem handover occurs from GSM BSS to UTRAN, the necessary information (e.g. CK, IK, initial HFN value information, supported/allowed UMTS algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old GSM BSS to the new RNC, and to continue the communication in ciphered mode. The GSM BSS requests the MS to send the UMTS capability information, which includes information on the initial HFN and UMTS security capabilities of the MS. The intersystem handover will imply a change of ciphering algorithm from a GSM A5 to a UEA. The target UMTS RNC includes the selected UMTS ciphering mode in the handover to UTRAN command message sent to the MS via the GSM BSS.

The integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed. The Serving RNC will do this by initiating the RRC security mode control procedure when the first RRC message (i.e. the Handover to UTRAN complete message) has been received from the MS. The UE security capability information, that has been sent from MS to RNC via the GSM radio access and the system infrastructure before the actual handover execution, will then be included in the RRC Security mode command message sent to MS and then verified by the MS (i.e. verified that it is equal to the UE security capability information stored in the MS).

3GPP TSG SA 3 Meeting #12
Stockholm, Sweden, 11-14 April 2000

***Document* S3-000293**
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	083	Current Version:	3.4.0

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

For submission to:	TSG SA #8	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	X	ME	X	UTRAN / Radio		Core Network	X

Source: SA WG3 **Date:** 13 April 2000

Subject: Authentication and key agreement

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:
Quintets should only be deleted in the VLR or SGSN when the authentication request indicated a sync failure (was incorrect implementation of CR 37r1).
MAC-S needs padding with zeros to make a full 128 bit input for f5.
The USIM does not need to store RAND for re-synchronisation
RAND-MS is no part of the authentication failure message with indication of sync failure (was incorrect implementation of CR 37r1).

Clauses affected: 6.3

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: A corresponding CR to 24.008 is required.

help.doc

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

6.3.3 Authentication and key agreement

The purpose of this procedure is to authenticate the user and establish a new pair of cipher and integrity keys between the VLR/SGSN and the USIM. During the authentication, the USIM verifies the freshness of the authentication vector that is used.

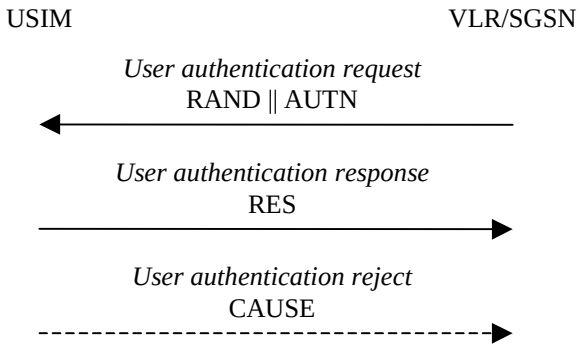


Figure 8: Authentication and key establishment

The VLR/SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR/SGSN database. The VLR/SGSN sends to the USIM the random challenge RAND and an authentication token for network authentication AUTN from the selected authentication vector.

Upon receipt the user proceeds as shown in Figure 9.

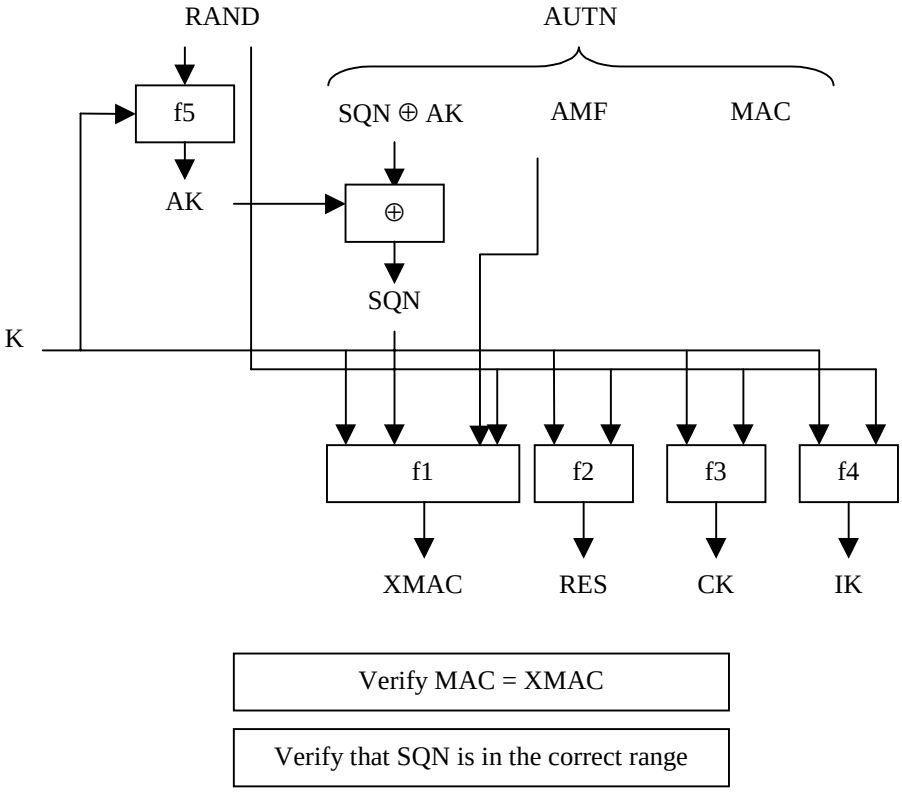


Figure 9: User authentication function in the USIM

Upon receipt of RAND and AUTN the USIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.

Next the USIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with MAC which is included in AUTN. If they are different, the user sends *user authentication reject* back to the VLR/SGSN with an indication of the cause and the user abandons the procedure. In this case, VLR/SGSN shall initiate an Authentication Failure Report procedure towards the HLR as specified in section 6.3.6. VLR/SGSN may also decide to initiate a new identification and authentication procedure towards the user.

Next the USIM verifies that the received sequence number SQN is in the correct range.

If the USIM considers the sequence number to be not in the correct range, it sends *synchronisation failure* back to the VLR/SGSN including an appropriate parameter, and abandons the procedure.

The synchronisation failure message contains the parameter AUTS. It is AUTS = Conc(SQN_{MS}) || MAC-S. Conc(SQN_{MS}) = $SQN_{MS} \oplus f5_K$(MAC-S || 0…0) is the concealed value of the counter SEQ_{MS} in the MS, and MAC-S = $f1^*_K$(SEQ_{MS} || RAND || AMF) where RAND is the random value received in the current user authentication request. f1* is a message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5 and vice versa.

The AMF used to calculate MAC-S assumes a dummy value of all zeros so that it does not need to be transmitted in the clear in the re-synch message.

The construction of the parameter AUTS in shown in the following Figure 10:

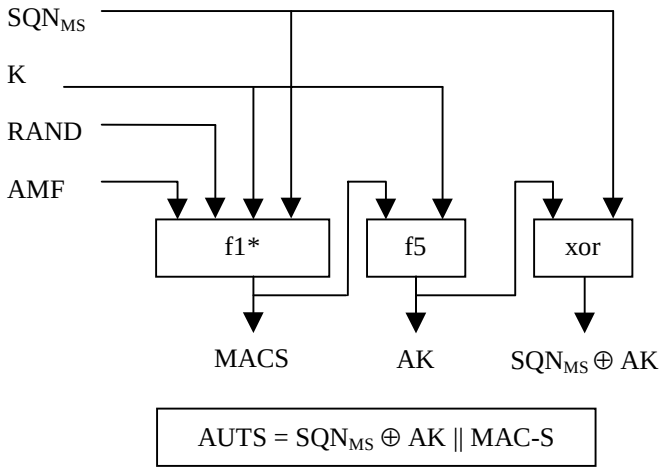


Figure 10: Construction of the parameter AUTS

If the sequence number is considered to be in the correct range however, the USIM computes RES = $f2_K$ (RAND) and includes this parameter in a *user authentication response* back to the VLR/SGSN. Finally the USIM computes the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND). Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND. If the USIM also supports GSM AKA, it shall derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK using conversion function c3. UMTS keys are sent to the MS along with the derived GSM key for UMTS-GSM interoperability purposes. USIM shall store original CK, IK until the next successful execution of AKA. ~~The USIM also stores RAND until completion of the current AKA, for re-synchronisation purposes.~~

Upon receipt of *user authentication response* the VLR/SGSN compares RES with the expected response XRES from the selected authentication vector. If XRES equals RES then the authentication of the user has passed. The VLR/SGSN also selects the appropriate cipher key CK and integrity key IK from the selected authentication vector. If XRES and RES are different, VLR/SGSN shall initiate an Authentication Failure Report procedure towards the HLR as specified in section 6.3.6. VLR/SGSN may also decide to initiate a new identification and authentication procedure towards the user.

Conditions on the use of authentication information by the VLR/SGSN: The **VLR/SGSN** shall use a UMTS authentication vector (i.e. a quintuplet) only once and, hence, shall send out each user authentication request *RAND* || *AUTN* only once no matter whether the authentication attempt was successful or not. A consequence is that UMTS authentication vectors (quintuplets) cannot be reused.

6.3.5 Re-synchronisation procedure

A VLR/SGSN may send two types of *authentication data requests* to the HE/AuC, the (regular) one described in subsection 6.3.2 and one used in case of synchronisation failures, described in this subsection.

Upon receiving a *synchronisation failure* message from the user, the VLR/SGSN sends an *authentication data request* with a "*synchronisation failure indication*" to the HE/AuC, together with the parameters

- *RAND* sent to the MS in the preceding user authentication request and
- ~~*RAND*$_{MS}$ ||~~ *AUTS* received by the VLR/SGSN in the response to that request, as described in subsection 6.3.3.

An VLR/SGSN will not react to unsolicited "~~-~~synchronisation failure indication" messages from the MS.

The VLR/SGSN does not send new user authentication requests to the user before having received the response to its authentication data request from the HE/AuC (or before it is timed out).

When the HE/AuC receives an *authentication data request* with a "*synchronisation failure indication*" it acts as follows:

1. The HE/AuC retrieves SEQ_{MS} from Conc(SEQ_{MS}) by computing $f5_K(MAC\text{-}S \,||\, 0\ldots0)$,.
2. The HE/AuC checks if SEQ_{HE} is in the correct range, i.e. if the next sequence number generated SEQ_{HE} using would be accepted by the USIM.
3. If SEQ_{HE} is in the correct range then the HE/AuC continues with step (6), otherwise it continues with step (4).
4. The HE/AuC verifies *AUTS* (cf. subsection 6.3.3.).
5. If the verification is successful the HE/AuC resets the value of the counter SEQ_{HE} to $SEQ_{MS.}$
6. The HE/AuC sends an *authentication data response* with a new batch of authentication vectors to the VLR/SGSN. If the counter SEQ_{HE} was not reset then these authentication vectors can be taken from storage, otherwise they are newly generated after resetting SEQ_{HE}. In order to reduce the real-time computation burden on the HE/AuC, the HE/AuC may also send only a single authentication vector in the latter case.

Whenever the VLR/SGSN receives a new batch of authentication vectors from the HE/AuC in an authentication data response to an authentication data request with synchronisation failure indication it deletes the old ones for that user in the VLR/SGSN.

The user may now be authenticated based on a new authentication vector from the HE/AuC. Figure 12 shows how re-synchronisation is achieved by combining a *user authentication request* answered by a *synchronisation failure* message (as described in subclause 6.3.3) with an *authentication data request* with *synchronisation failure* indication answered by an *authentication data response* (as described in this subclause).

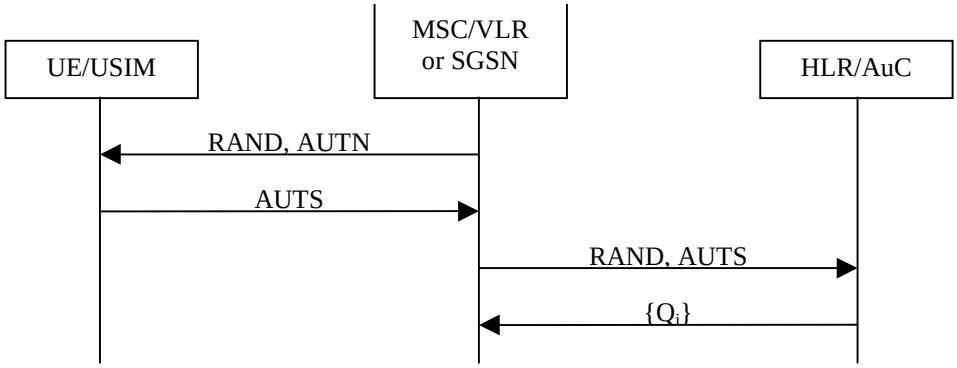


Figure 12: Resynchronisation mechanism

3GPP TSG SA 3 Meeting #12
Stockholm, Sweden, 11-14 April 2000

***Document* S3-000294**
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	084	Current Version:	3.4.0

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

For submission to:	SA#8	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 [ ] Core Network [X]

Source: TSG SA WG 3 **Date:** 13 April 2000

Subject: Conversion functions for GSM-UMTS interoperation

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 suggested modifications to the conversion functions accommodate the SAGE recommendation.

Clauses affected: 6.8.2.3

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.

6.8.2.3 VLR/SGSN

The R99+ VLR/SGSN shall perform GSM AKA using a triplet that is either:

a) retrieved from the local database,

b) provided by the HLR/AuC, or

c) provided by the previously visited VLR/SGSN.

NOTE: All triplets are originally provided by the HLR/AuC.

GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the VLR/SGSN.

When the user is attached to a UTRAN, the R99+ VLR/SGSN derives the UMTS cipher/integrity keys from the GSM cipher key using the following conversion functions:

a) c4: $CK_{[UMTS]}$ = ~~0…0~~Kc || Kc;

b) c5: $IK_{[UMTS]}$ = ~~Kc~~ Kc_1 xor Kc_2 || Kc || Kc_1 xor Kc_2;

whereby in ~~c4~~c5, Kc_i are both 32 bits long and Kc = Kc_1 || Kc_2 ~~occupies the 64 least significant bits of CK~~.

The UMTS cipher/integrity keys are then sent to the RNC where the ciphering and integrity algorithms are allocated.

When the user is attached to a GSM BSS and the user receives service from an MSC/VLR, the cipher key Kc is sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the cipher key Kc is applied in the SGSN itself.

3GPP TSG SA 3 Meeting #13
Yokohama, Japan, 24-26 May 2000

***Document* S3-000395**
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	088r2	Current Version:	3.4.0

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

For submission to:	SA#8	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 [X] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: TSG SA WG3 **Date:** 7 June 2000

Subject: Initialisation of synchronisation for ciphering and integrity protection

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 length of the START parameter used to initialise the HFN is set to 20 bits.
A description is added on how START is managed between the ME and the USIM such that a COUNT-C or COUNT-I value is never re-used.

Revision 1 (§6.4.8) modifies that both $START_{CS}$ and $START_{PS}$ are changed and at the same time. They also modify the wording, such that now the ME manages the START values on the USIM and provides the ME with a mechanism to mark START values as invalid. This changes will prevent TSG T3 from defining new USIM procedures.

Revision 2 (§6.4.8) further clarifies that two START values need to be updated.

Clauses affected: 6.4.8 (new clause), 6.5.4.1, 6.6.4.1

Other specs affected:

Other 3G core specifications	X	→ 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: Possible impact on T WG3 and RAN WG2 specifications


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 ~~corresponding~~ $START_{CS}$ and the $START_{PS}$ value to the RNC in the *RRC connection setup complete* message. The ME ~~also indicates to the USIM that a radio connection has been established, with again an indication of the serving network domain. The USIM~~ marks the ~~corresponding~~ 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 and CS user data logical channels protected using CK_{CS} and/or IK_{CS}, incremented by 1, i.e.,

$$START_{CS} = MSB_{20}\,(\,MAX\,\{COUNT\text{-}C,\ COUNT\text{-}I \mid \text{all logical channels protected with } CK_{CS} \text{ and } IK_{CS}\}) + 1.$$

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 and PS user data logical channels protected using CK_{PS} and/or IK_{PS}, incremented by 1, i.e.,

$$START_{PS} = MSB_{20}\,(\,MAX\,\{COUNT\text{-}C,\ COUNT\text{-}I \mid \text{all logical channels protected with } CK_{PS} \text{ and } IK_{PS}\}) + 1.$$

Upon radio connection release and when a set of cipher/integrity keys is no longer used, the ME updates~~informs the USIM and indicates the serving network domain and the current~~ $START_{CS}$ and $START_{PPS}$ in the USIM with the current values ~~in the USIM for that serving network domain. The USIM updates the corresponding START values and marks it them as up-to-date and marks them as valid~~.

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

6.5.4.1 COUNT-I

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

There is one COUNT-I value per logical signalling channel.

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. 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 hyperframe number RRC HFN which is incremented at each RRC SN cycle.

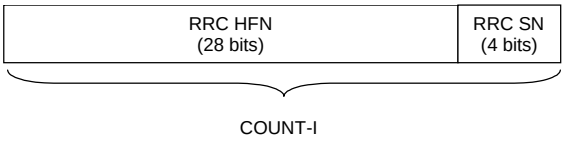


Figure 16a: The structure of COUNT-I

The hyperframe number RRC HFN is initialised by means of the parameter START, which is transmitted from ~~UE~~ME to RNC during *RRC connection establishment*. The ~~UE~~ME and the RNC then initialise the ~~X~~ 20 most significant bits of the RRC HFN to START; the remaining ~~(28-X) LSB~~ bits of the RRC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel used for signalling.

~~Editor's note: The value of X still needs to be added.~~

~~Editor's note: The description of how START is managed in the UE needs to be added.~~

6.6.4.1 COUNT-C

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

There is one COUNT-C value per logical RLC AM channel, one per logical RLC UM channel and one for all logical channels using the transparent RLC mode (and mapped onto DCH).

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

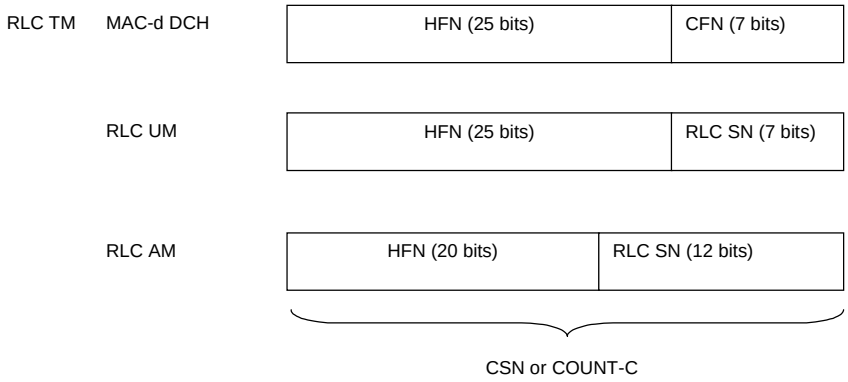


Figure 16c: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 7-bit ciphering frame number CFN of the UEFN. It is independently maintained in the ~~UE~~ME MAC entity and the SRNC MAC-d entity. The "long" sequence number is the 25-bit MAC HFN which is incremented at each CFN cycle. The ciphering sequence number CSN or COUNT-C is identical to the UEFN.

- For RLC UM mode, the "short" sequence number is the 7-bit RLC sequence number RLC SN that is available in each RLC PDU (it is not ciphered). The "long" sequence number is the 25-bit RLC 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 that is available in each RLC PDU (it is not ciphered). The "long" sequence number is the 20-bit RLC HFN which is incremented at each RLC SN cycle.

The hyperframe number HFN is initialised by means of the parameter START, which is transmitted from ~~UE~~ME to RNC in *RRC connection establishment*. The ~~UE~~ME and the RNC then initialise the ~~X~~ $_{20}$ most significant bits of the RLC HFN and MAC HFN to START; the remaining ~~LSB~~ bits of the RLC HFN and MAC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel.

~~Editor's note: The value of X still needs to be decided.~~

~~Editor's note: The description of how START is managed in the UE needs to be added.~~

3GPP TSG SA WG 3 Security #12
Stockholm, Sweden, 11-14. April 2000

***Document* S3-000262**
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	090	Current Version:	3.4.0

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

For submission to:	TSG SA # 8	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: SA WG3 **Date:** 9. April 2000

Subject: Clarification of BEARER and DIRECTION parameters

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 BEARER parameter cannot be the logical channel identity because that is not unique for one UE; instead the radio bearer identity must be used. Values for the DIRECTION bit have to be defined.

Clauses affected: 6.5.4.4, 6.6.4.3, 6.6.4.4

Other specs affected:

Other 3G core specifications	X	→ 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: Corresponding CR to 33.105 is required. Impact on RAN WG2 specification 25.301.


help.doc

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

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.

There is one COUNT-I value per logical signalling channel.

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. 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 hyperframe number RRC HFN which is incremented at each RRC SN cycle.

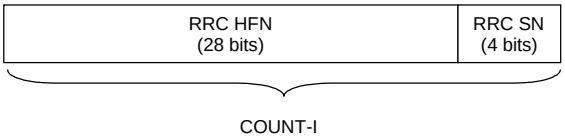


Figure 16a: The structure of COUNT-I

The hyperframe number RRC HFN is initialised by means of the parameter START, which is transmitted from UE to RNC during *RRC connection establishment*. The UE and the RNC then initialise the X most significant bits of the RRC HFN to START; the remaining (28-X) LSB of the RRC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel used for signalling.

Editor's note: The value of X still needs to be added.

Editor's note: The description of how START is managed in the UE needs to be added.

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 6.5.6.

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 UE. IK is sent from the USIM to the UE upon request of the UE. The USIM shall send IK under the condition that 1) a valid IK is available, 2) the current value of START in the USIM is up-to-date and 3) START has not reached THRESHOLD. The UE 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 or SGSN and stored in the VLR or SGSN as part of a quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) *security mode command*. The MSC/VLR or SGSN shall assure that the IK is updated at least once every 24 hours.

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 in a new *security mode command* to the user.

6.5.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that ~~for~~ 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.

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 logical channels for user data is not protected.

Signalling data for services delivered by either of both service domains is sent over common logical (signalling) channels. These 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.

6.5.6 UIA identification

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

"0001_2" : UIA1, Kasumi.

The remaining values are not defined.

6.6 Access link data confidentiality

6.6.1 General

User data and some signalling information elements are considered sensitive and must be confidentiality protected. To ensure identity confidentiality (see section 6.1), the temporary user indentity (P-)TMSI must 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 UE 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 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 logical channel is using a non-transparent RLC mode (AM or UM), ciphering is performed in the RLC sub-

layer.

- If a 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 UE and the context needed for ciphering (CK, HFN, etc.) is only known in S-RNC and the UE.

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 ciphertext. 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.

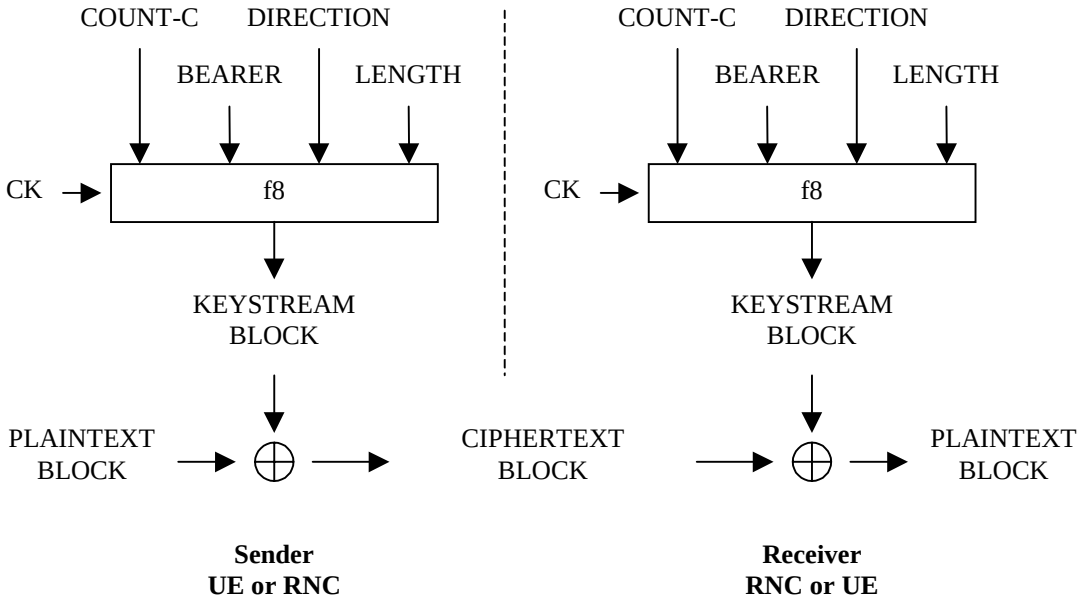


Figure 16b: Ciphering of user and signalling data transmitted over the radio access link

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 logical RLC AM channel, one per logical RLC UM channel and one for all logical channels using the transparent RLC mode (and mapped onto DCH).

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

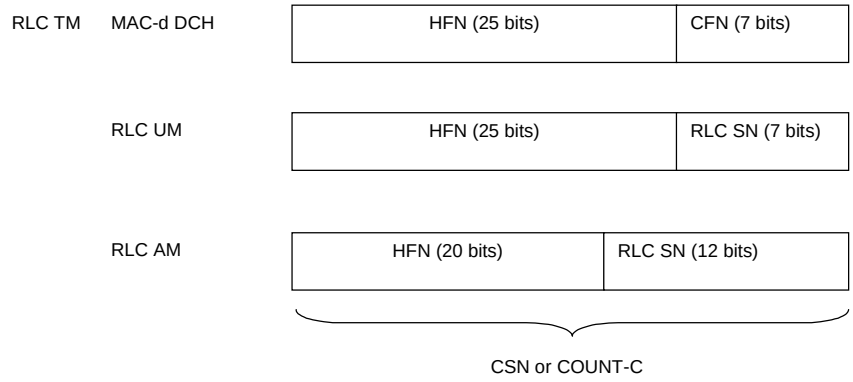


Figure 16c: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 7-bit ciphering frame number CFN of the UEFN. It is independently maintained in the UE MAC entity and the SRNC MAC-d entity. The "long" sequence number is the 25-bit MAC HFN which is incremented at each CFN cycle. The ciphering sequence number CSN or COUNT-C is identical to the UEFN.

- For RLC UM mode, the "short" sequence number is the 7-bit RLC sequence number RLC SN that is available in each RLC PDU (it is not ciphered). The "long" sequence number is the 25-bit RLC 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 that is available in each RLC PDU (it is not ciphered). The "long" sequence number is the 20-bit RLC HFN which is incremented at each RLC SN cycle.

The hyperframe number HFN is initialised by means of the parameter START, which is transmitted from UE to RNC in *RRC connection establishment*. The UE and the RNC then initialise the X most significant bits of the RLC HFN and MAC HFN to START; the remaining LSB of the RLC HFN and MAC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel.

Editor's note: The value of X still needs to be decided.

Editor's note: The description of how START is managed in the UE needs to be added.

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 cipher key to use for a particular logical channel is described in 6.6.6.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 UE. CK is sent from the USIM to the UE upon request of the UE. 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 UE 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. The VLR or SGSN shall assure that CK is updated at least once every 24 hours.

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~~logical channel~~ identifier BEARER is 5~~4~~ bits long.

There is one BEARER parameter per radio bearer~~logical channel~~ associated with the same user and multiplexed on a single 10ms physical layer frame. The radio bearer~~logical channel~~ 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.

3GPP TSG SA WG 3 Meeting #12
Stockholm, Sweden, 11-14 April 2000

***Document* S3-000269**
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	093	Current Version:	3.4.0

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

For submission to:	SA#8	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 [ ] UTRAN / Radio [ ] Core Network [X]

Source: SA WG3 **Date:** 11 April 2000

Subject: Removal of network domain security

Work item: Security

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

F	Correction	X
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	X
Release 00	

Reason for change: Decision by SA#7

Clauses affected: 3.3, 5.2, 6.3.1, 6.7.3.1, 7, Annex E

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.

3.3 Abbreviations

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
EMSI	Encrypted Mobile Subscriber Identity
EMSIN	Encrypted MSIN
~~$D_{SK(X)}$(data)~~	~~Decryption of "data" with Secret Key of X used for signing~~
~~$E_{KSXY(i)}$(data)~~	~~Encryption of "data" with Symmetric Session Key #i for sending data from X to Y~~
~~$E_{PK(X)}$(data)~~	~~Encryption of "data" with Public Key of X used for encryption~~
GI	Group Identifier
GK	Group Key
~~Hash(data)~~	~~The result of applying a collision resistant one-way hash function to "data"~~
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
~~IV~~	~~Initialisation Vector~~
~~KAC_X~~	~~Key Administration Centre of Network X~~
~~$KS_{XY}(i)$~~	~~Symmetric Session Key #i for sending data from X to Y~~
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
~~MAP~~	~~Mobile Application Part~~
MAC	Message Authentication Code
MAC-A	The message authentication code included in AUTN, computed using f1
MS	Mobile Station
MSC	Mobile Services Switching Centre
MSIN	Mobile Station Identity Number
MT	Mobile Termination
~~NE_X~~	~~Network Element of Network X~~
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
~~RND_X~~	~~Unpredictable Random Value generated by X~~
SQN	Sequence number
SQN_{UIC}	Sequence number user for enhanced user identity confidentiality
SQN_{HE}	Sequence number counter maintained in the HLR/AuC
SQN_{MS}	Sequence number counter maintained in the USIM
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TE	Terminal Equipment
TEMSI	Temporary Encrypted Mobile Subscriber Identity used for paging instead of IMSI
~~Text1~~	~~Optional Data Field~~
~~Text2~~	~~Optional Data Field~~
~~Text3~~	~~Public Key algorithm identifier and Public Key Version Number (eventually included in Public Key Certificate)~~
TMSI	Temporary Mobile Subscriber Identity
~~TTP~~	~~Trusted Third Party~~
UE	User equipment

UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
UIDN	User Identity Decryption Node
USIM	User Services Identity Module
VLR	Visitor Location Register
~~X~~	~~Network Identifier~~
XEMSI	Extended Encrypted Mobile Subscriber Identity
XRES	Expected Response
~~Y~~	~~Network Identifier~~

5.2 Network domain security

5.2.1 ~~Entity authentication~~Void

~~The following features with respect to authentication of network elements are provided:~~

- ~~**authentication mechanism agreement:** the property that two network entities can securely negotiate the mechanism for authentication that they shall use subsequently;~~
- ~~**network element authentication:** the property that a network element corroborates the identity of another network element it wants to communicate with;~~

~~This feature ensures that no malicious operational or maintenance commands can be injected into a network domain by an intruder. It provides network elements, in particular network elements belonging to different network operators, with the possibility to corroborate each other's identities before exchanging data.~~

~~This goal may be achieved either by an explicit or implicit entity authentication mechanism, to be performed each time data are exchanged between two network entities. Implicit authentication is realised by exchanging encrypted messages only, so that only an entity in possession of a certain shared key can make use of the data. The shared keys may be distributed among the network elements of a single operator in a manner outlined in Annex D.~~

~~Explicit authentication mechanisms can be achieved by asymmetrically based protocols (e.g. by using digital signatures) or by symmetric (e.g. challenge-response) protocols. Again, for explicit symmetric authentication, the necessary keys may be distributed as proposed in Annex E.~~

5.2.2 ~~Data confidentiality~~Void

~~The following security features are provided with respect to confidentiality of data exchanged between network elements:~~

- ~~**cipher algorithm agreement:** the property that two network elements can securely negotiate the algorithm that they shall use subsequently;~~
- ~~**cipher key agreement:** the property that two network elements agree on a cipher key that they may use subsequently;~~
- ~~**confidentiality of exchanged data:** the property that data exchanged between two network elements cannot be eavesdropped;~~

~~In case authentication data can be eavesdropped in the network domain, serious fraud problems will arise. Therefore, these features are needed to ensure the confidentiality of sensitive data, e.g. authentication or other subscriber data inside the network domain. The first two features may be realised in course of an authentication mechanism performed by the network elements; the agreed cipher key is then used for securing signalling and user data by means of the agreed cipher algorithm.~~

5.2.3 ~~Data integrity~~Void

~~The following security features are provided with respect to integrity of data exchanged between two network elements:~~

- ~~**integrity algorithm agreement:** the property that two network elements can securely negotiate the integrity algorithm that they shall use subsequently;~~
- ~~**integrity key agreement:** the property that two network elements agree on an integrity key that they may use subsequently;~~
- ~~**data integrity and data origin authentication of signalling data:** the property that the receiving network element is able to verify that signalling data has not been modified in an unauthorised way since it was sent by the sending element and that the data origin of the signalling data received is indeed the one claimed;~~

~~The feature data integrity of signalling data ensures that operation and maintenance commands or user data exchanged between two network elements cannot be modified by an intruder without being detected, while the third feature ensures that no malicious operational or maintenance commands can be injected into a network domain by an intruder~~

~~The first two features may be realised in course of an authentication mechanism performed by the network entities involved; the agreed integrity key is then used for securing integrity of the exchanged data by means of the agreed integrity algorithm.~~

5.2.4 Fraud information gathering system

NOTE: Some feature will be provided which will allow fraud information to be exchanged between 3GMS providers according to time constraints that yet have to be defined.

6.3.1 General

The mechanism described here achieves mutual authentication by the user and the network showing knowledge of a secret key K which is shared between and available only to the USIM and the AuC in the user's HE. In addition the USIM and the HE keep track of counters SEQ_{MS} and SEQ_{HE} respectively to support network authentication.

The method was chosen in such a way as to achieve maximum compatibility with the current GSM security architecture and facilitate migration from GSM to UMTS. The method is composed of a challenge/response protocol identical to the GSM subscriber authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication derived from the ISO standard ISO/IEC 9798-4 (section 5.1.1).

An overview of the mechanism is shown in Figure 5.

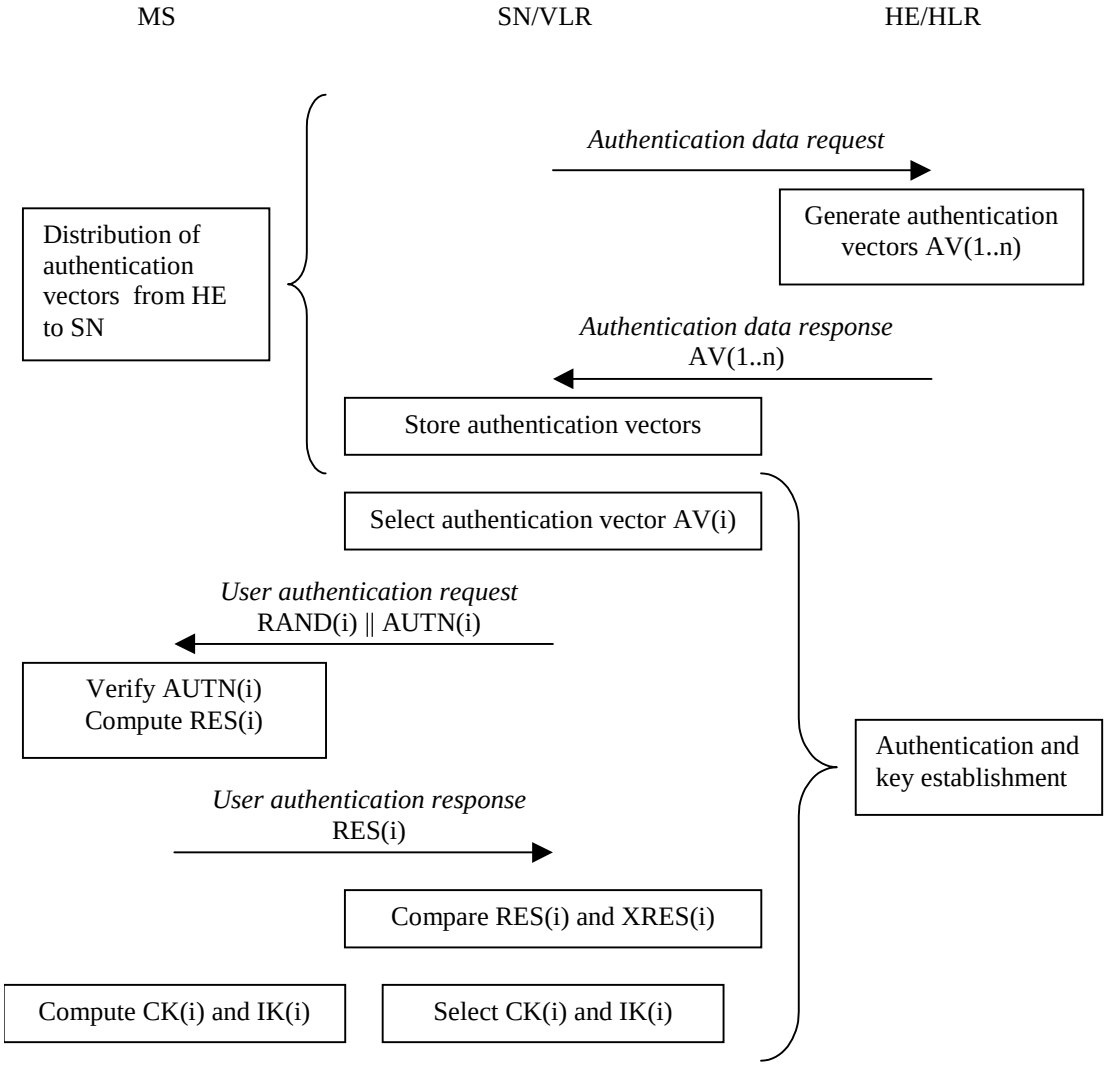


Figure 5: Authentication and key agreement

Upon receipt of a request from the VLR/SGSN, the HE/AuC sends an ordered array of *n* authentication vectors (the equivalent of a GSM "triplet") to the VLR/SGSN. Each authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the VLR/SGSN and the USIM.

When the VLR/SGSN initiates an authentication and key agreement, it selects the next authentication vector from the array and sends the parameters RAND and AUTN to the user. The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the VLR/SGSN. The USIM also computes CK and IK. The VLR/SGSN compares the received RES with XRES. If they match the VLR/SGSN considers the authentication and key agreement exchange to be successfully completed. The established keys CK and IK will then be transferred by the

USIM and the VLR/SGSN to the entities which perform ciphering and integrity functions.

VLR/SGSNs can offer secure service even when HE/AuC links are unavailable by allowing them to use previously derived cipher and integrity keys for a user so that a secure connection can still be set up without the need for an authentication and key agreement. Authentication is in that case based on a shared integrity key, by means of data integrity protection of signalling messages (see 6.4).

The authenticating parties shall be the AuC of the user's HE (HE/AuC) and the USIM in the user's mobile station. The mechanism consists of the following procedures:

A procedure to distribute authentication information from the HE/AuC to the VLR/SGSN. This procedure is described in 6.3.2. The VLR/SGSN is assumed to be trusted by the user's HE to handle authentication information securely. It is also assumed that the intra-system links between the VLR/SGSN to the HE/AuC are adequately secure. ~~Mechanisms to secure these links are described in clause 7.~~ It is further assumed that the user trusts the HE.

A procedure to mutually authenticate and establish new cipher and integrity keys between the VLR/SGSN and the MS. This procedure is described in 6.3.3.

A procedure to distribute authentication data from a previously visited VLR to the newly visited VLR. This procedure is described in 6.3.4. It is also assumed that the links between VLR/SGSNs are adequately secure. ~~Mechanisms to secure these links are described in clause 7.~~

6.7.3.1 General case

We assume that signalling links within the network are confidentially protected on a link-by-link basis. In particular, we assume that the UE to RNC signalling links are protected using access link security domain keys (see clause 6). ~~We also assume that VLR to RNC signalling links and core network signalling links are protected using network security domain keys (see clause 7)~~. Note that if network-wide encryption can be provided across serving network boundaries (e.g. because inter-network TFO is available) then the signalling links requiring protection will cross network boundaries. In this situation it is important to note that the two serving networks may not be roaming partners yet they still must be able to confidentially protect inter-network signalling by establishing appropriate keys.

The key management scheme for network-wide encryption involves establishing an end-to-end session key between the end points of the traffic channel. It should not be possible to obtain this key by eavesdropping on any transmission links within the network. However, it may be possible to obtain the end-to-end key by compromising certain nodes within the network (e.g. nodes where link encryption terminates).

To satisfy lawful interception requirements it must be possible to decrypt end-to-end encrypted traffic within the core network to provide access to plaintext user traffic. Thus, the end-to-end encryption key (and decryption facilities) must be available in the core network for lawful interception reasons.

Issues for further study:

- Specification of key management scheme for the general case;
- The ability to terminate network-wide encryption key management at network gateways for inter-network user traffic channels.

7 ~~Network domain security mechanisms~~Void

~~This subclause describes mechanisms for establishing secure signalling links between network nodes, in particular between SN/VLRs and HE/AuCs. Such procedures may be incorporated into the roaming agreement establishment process.~~

~~7.1 Overview of Mechanism~~

~~The proposed mechanism consists of three layers.~~

~~7.1.1 Layer I~~

~~Layer I is a secret key transport mechanism based on an asymmetric crypto-system and is aimed at agreeing on a symmetric session key for each direction of communication between two networks X and Y.~~

~~NOTE 1: For secure transmission of sensitive data between elements of one and the same network operator only Layer II and Layer III will be involved. In this case Layer I can be dropped. There will also be only one symmetric key in this case, to be used for communication between network elements of one network operator in both directions.~~

~~The party wishing to send sensitive data initiates the mechanism and chooses the symmetric session key it wishes to use for sending the data to the other party. The other party shall choose a symmetric session key of its own, used for sending data in the other direction. This second key shall be transported immediately after the first key has been successfully transported. The session symmetric keys are protected by asymmetric techniques. They are exchanged between certain elements called the *Key Administration Centres* (KACs) of the network operators X and Y. The format of the Layer I transmissions is based on ISO/IEC 11770-3: *Key Management — Mechanisms using Asymmetric Techniques* [10]. Public Keys may be exchanged between a pair of network operators when setting up their roaming agreement (manual roaming) or they may be distributed by a TTP e.g. in case of automatic roaming.~~

~~NOTE 2: In the case of manual roaming no general PKI is required.~~

~~NOTE 3: For the transmission of the messages, no special assumptions regarding the transport protocol are made, a possible example would be IP.~~

~~7.1.2 Layer II~~

~~In Layer II the agreed symmetric keys for sending and receiving data are distributed by the KACs in each network to the relevant network elements. For example, an AuC will normally send sensitive authentication data to VLRs belonging to other networks and will therefore get a session key from its KAC. Layer II is carried out entirely inside one operator's network. It is clear that the distribution of the symmetric keys to the network elements must be carried out in a secure way, as not to compromise the whole system. Therefore, in Annex E a mechanism for distributing the keys, which very similar to that of Layer I, is proposed for Layer II.~~

~~7.1.3 Layer III~~

~~Layer III uses the distributed symmetric keys for securely exchanging sensitive data between the network elements of one operator (internal use) or different operators (external use) by means of a symmetric encryption algorithm. A block cipher (e.g. BEANO, which has been developed by ETSI SAGE [11]) shall be used for this purpose, as defined in 3G TS 33.105. The encrypted (resp. authenticity/integrity protected) messages will be transported via the MAP protocol.~~

~~7.1.4 General Overview~~

~~Figure 16 provides an overview of the whole mechanism. Note that the messages are not fully specified in this figure. Rather, only the "essential" parts of the messages are given. More details on the format of the messages in the single layers will be provided in subsequent chapters.~~

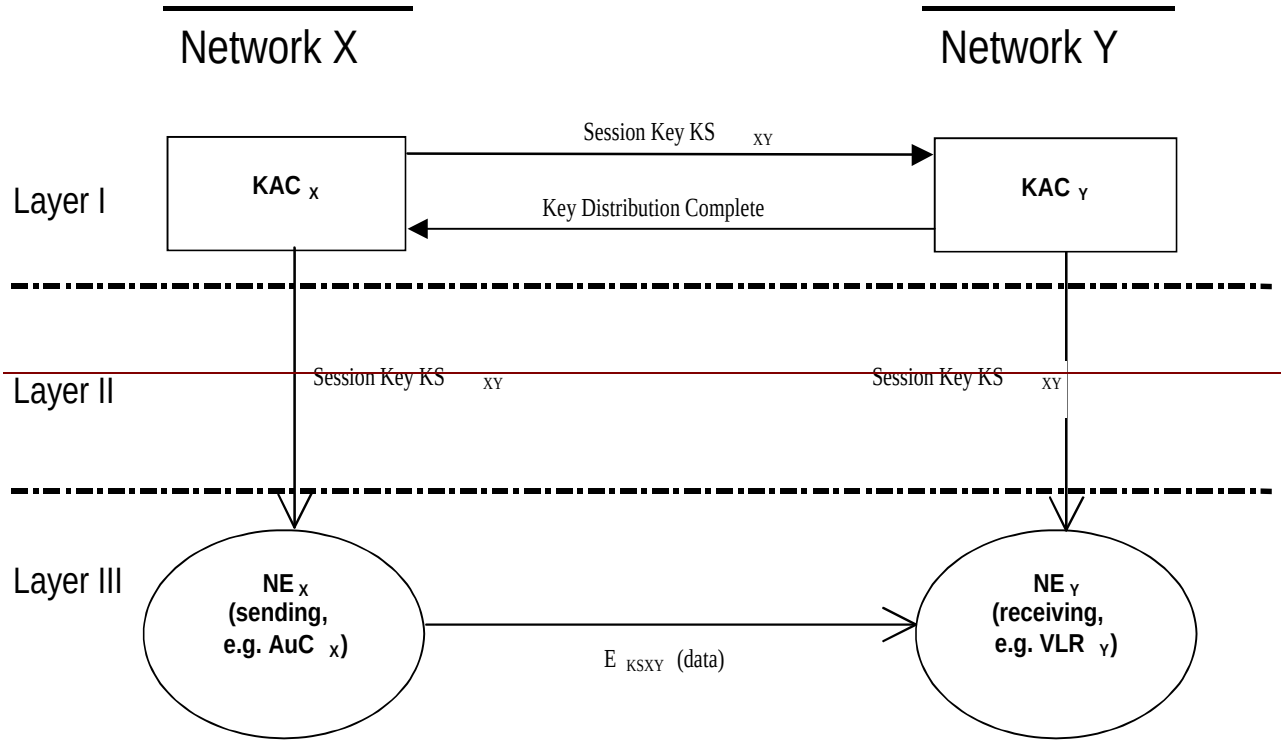


Figure 20: Overview of Proposed Mechanism

E_{KSXY}(data) denotes encryption of data by a symmetric algorithm using the session key from network X to network Y. (If the data are sent inside one operator's network, X = Y).

7.2 Layer I Message Format

Layer I describes the communication between two newly defined network entities of different networks, the so-called Key Administration Centres (KACs).

NOTE: We do not make any assumptions about the protocols to be used for this communications, although IP might be the most likely candidate.

7.2.1 Properties and Tasks of Key Administration Centres

There is only one KAC per network operator. KACs perform the following tasks:

- Generation and storage of its own asymmetric key pairs (different key pairs used for signing/verifying and encrypting/decrypting, cf. 7.2.2)
- Storage of public keys of KACs of other network operators
- Generation and storage of symmetric session keys for sending sensitive information to network entities of other networks
- Reception and storage of symmetric session keys for receiving sensitive information from network entities of other networks
- Secure distribution of symmetric session keys to network entities in the same network

Due to these sensitive tasks, a KAC has to be physically secured.

7.2.2 Transport of Session Keys

The transport of session keys in Layer I is based on asymmetric cryptographic techniques (cf. [10]).

[Note: Public key certificates shall be included in Text3 if required.]

In order to establish a symmetric session key with version no. i to be used for sending data from X to Y, the KAC_X sends a message containing the following data to the KAC_Y:

$E_{PK(Y)}\{X||Y||i||KS_{XY}(i)||RND_X||Text1||D_{SK(X)}(Hash(X||Y||i||KS_{XY}(i)||RND_X||Text1))||Text2\}||Text3$

The reasons for this message format are as follows:

- Encrypting the message with the public key used for encrypting of the receiving network Y provides message confidentiality, while decrypting the message body with the private key used for signing of the sending network X provides message integrity and authenticity.
- X includes RND_X to make sure that the message contents contains some random data before signing.

NOTE: The hash function used shall be collision resistant and have the one-way property.

The symmetric session keys $KS_{XY}(i)$ should be periodically updated by this process, thereby moving on to $KS_{XY}(i+1)$. For each new session key KS_{XY} i is incremented by one.

After having successfully decrypted the key transport message and having verified the digital signature of the sending network, including the hash value, and having checked the received i the receiving network starts Layer II activities.

If anything goes wrong, e.g. computing the hash value of $X||Y||i||KS_{XY}(i)||RND_X||Text1$ does not yield the expected result, a RESEND message should be sent by Y to X in the form

RESEND||Y||X

Y shall reject messages with i smaller or equal than the currently used i.

After having successfully distributed the symmetric session key received by network X to its own network entities, network Y sends to X a Key Distribution Complete Message. This is an indication to KAC_X to start with the distribution of the key to its own entities, which can then start to use the key immediately. The message takes the form

$KEY\_DIST\_COMPLETE||Y||X||i||RND_Y||D_{SK(Y)}(Hash(KEY\_DIST\_COMPLETE||Y||X||i||RND_Y)$

where i indicates the distributed key and RND_Y is a random number generated by Y. The digital signature is appended for integrity and authenticity purposes. Y includes RND_Y to make sure that the message contents determined by X will be modified before signing.

Since most of the signalling messages to be secured are bidirectional in character, immediately after successful completion the procedure described here shall be repeated, now with Y choosing a key $KS_{YX}(i)$ to be used in the reverse direction, and X being the receiving party. Thereby keys for both directions are established.

7.3 Layer II Message Format

It shall be stressed here once again that the distribution of the symmetric session keys, which has to be performed in Layer II, must be done securely. For a detailed proposal which is based on the asymmetric key transport mechanism of Layer I, see Annex E.

In order to ensure that no network element starts enciphering with a key that not all potentially corresponding network elements have received yet, the following approach is suggested:

The distribution of the session keys KS_{XY} in network X having initiated the Layer I message exchange should not begin before the Key Distribution Complete Message from the receiving network Y has been received by KAC_X in Layer I. As soon as a network element of X has received a session key KS_{XY}, it may start enciphering with this key.

A similar statement holds if the transported session keys are used internally only: In this case, all network elements of X should get the symmetric session keys KS_{XX} for internal use as decryption keys (marked with flag RECEIVED) first; if all network elements of X have acknowledged that they have recovered these keys, the KAC_X sends the same key KS_{XX} again as encryption keys (marked with flag SEND). Again, as soon as a network element of X has received an encryption key (marked with flag SEND), it may start enciphering with this key.

7.4 Layer III Message Format

7.4.1 General Structure of Layer III Messages

Layer III messages are transported via the MAP protocol, that means, they form the payload of a MAP message after the original MAP message header. For Layer III Messages, three levels of protection (or protection modes) are defined providing the following security features:

Protection Mode 0: No Protection

Protection Mode 1: Integrity, Authenticity

Protection Mode 2: Confidentiality, Integrity, Authenticity

NOTE: GTP based transmission data will also contain sensitive data. This data will require an equal level of security (e.g. authentication parameters, subscriber profile information, etc.). The specifications will extended to address GTP based transmissions using industry standard techniques (such as IPSEC) where appropriate. The possibility of extending these mechanisms to secure CAP/INAP signalling is also being investigated.

Layer III messages consists of a Security Header and the Layer III Message Body that is protected by the symmetric encryption algorithm, using the symmetric session keys that were distributed in layer II. Layer III Messages have the following structure:

Security Header	Layer III Message Body

In all three protection modes, the security header is transmitted in cleartext. It shall comprise the following information:

- protection mode;
- other security parameters (if required, e.g. IV, Version No. of Key Used, Encryption Algorithm Identifier, Mode of Operation of Encryption Algorithm, cf. section 7.4.3).

Both parts of the Layer III messages, security header and message body, will become part of the "new" MAP message body. Therefore, the complete "new" MAP messages take the following form in this proposal:

MAP Message Header	MAP Message Body

	Layer III Message

MAP Message Header	Security Header	Layer III Message Body

Like the security header, the MAP message header is transmitted in cleartext. In protection mode 2 providing confidentiality, the Layer III Message Body is essentially the encrypted "old" MAP message body. For integrity and authenticity, an encrypted hash calculated on the MAP message header, security header and the "old" MAP message body in cleartext is included in the Layer III Message Body in protection modes 1 and 2. In protection mode 0 no protection is offered, therefore the Layer III Message Body is identical to the "old" MAP message body in cleartext in this case.

Summing up, the Protected MAP Message (i.e. the Layer III Message) is a sequence of data elements consisting of the MAP Message Header, the Security Header and the Layer III Message Body. In the following subchapters, the contents

of the Layer III Message Body for the different protection modes and the security header will be specified in greater detail.

7.4.2 Format of Layer III Message Body

7.4.2.1 Protection Mode 0

Protection Mode 0 offers no protection at all. Therefore, the Layer III message body in protection mode 0 is identical to the original MAP message body in cleartext.

7.4.2.2 Protection Mode 1

The message body of Layer III messages in protection mode 1 takes the following form:

$$Cleartext||TVP||E_{KSXY(i)}(Hash(\text{MAP Header}||\text{Security Header}||Cleartext||TVP))$$

where "Cleartext" is the message body of the original MAP message in cleartext. Therefore, in Protection Mode 1 the Layer III Message Body is a sequence of the following data elements and data types:

- Cleartext (OCTET STRING)
- Time Variant Parameter (UTCTime)
- Integrity Check (OCTET STRING)

Authentication of origin is achieved by encrypting the hash value of the cleartext, since only a network element knowing $KS_{XY}(i)$ can encrypt in this way. Message integrity and validation is achieved by hashing and encrypting the cleartext.

[Note: The case X=Y, i.e. only one key for sending and receiving, corresponds to internal use inside network X.]

Note that protection mode 1 is compatible to the present MAP protocol, since everything appended to the cleartext may be ignored by a receiver incapable of decrypting.

7.4.2.3 Protection Mode 2

The Layer III Message Body in protection mode 2 takes the following form:

$$E_{KSXY(i)}(Cleartext||TVP||Hash(\text{MAP Header}||\text{Security Header}||Cleartext||TVP))$$

where "Cleartext" is the original MAP message in cleartext. Therefore, in protection mode 2 the Layer III message body is just an OCTET STRING which can only be interpreted after having decrypted it. After decryption, the data structure is similar to that in Protection Mode 1.

Message confidentiality is achieved by encrypting with the session key. This also provides for authentication of origin, since only a network element knowing KSXY(i) can encrypt in this way. Message integrity and validation is achieved by hashing the cleartext. TVP is a random number that avoids traceability.

[Note1: There is need for replay protection of Layer III messages; this is for further study.
By making use of a TVP as timestamp (perhaps derived from an overall present master time) this could be achieved.]

[Note2: In protection mode 2, the original MAP message body will be encrypted in order to achieve confidentiality. For integrity and authenticity, an encrypted hash calculated on the MAP message header and body in cleartext (i.e. the original MAP message) is appended to the messages in protection mode 1 and 2. All protection modes need a security header to be added.
When implementing these changes, care has to be taken that the maximum length of a MAP message (approx. 250 byte) is not exceeded by the protected MAP messages of Layer III, otherwise substantial changes to the underlying SS7 protocol levels (TCAP and SCCP) would have to be made.]

7.4.3 Structure of Security Header

The security header is a sequence of the following data elements and data types:

- Protection Mode (INTEGER)
- Key Identifier (INTEGER)
- Algorithm Identifier (AlgorithmIdentifier)
- Mode of Operation (INTEGER)
- Initialisation Vector (OCTET STRING OPTIONAL)

NOTE: Whether the Initialisation Vector is needed depends on the mode of operation of the encryption algorithm.

7.5 Mapping of MAP Messages and Modes of Protection

The network operator should be able to assign the mode of protection to each MAP message in order to adapt the level of protection according to its own security policy. Guidance may be obtained from the SS7 Signalling Protocols Threat Analysis [12].

7.6 Distribution of security parameters to UTRAN

Confidentiality and integrity between the user and the network is handled by the UE/USIM and the RNC.

The security parameters for the confidentiality and integrity algorithms must be distributed from the core network to the RNC over the Iu interface in a secure manner. The actual mechanism for securing these parameters has not yet been identified.

Annex E ~~(informative)~~: Void
~~A Proposal for Layer II Message Format~~

~~E.1 Introduction~~

~~In Layer II symmetric session keys (to encrypt/decrypt data before sending/after receiving) are distributed by the KACs in each network to the relevant network elements. For example, an AuC_X will normally send sensitive authentication data to VLR_Y and will therefore get a session KS_{XY} key from its KAC_X. Layer II is carried out entirely inside one operator's network.~~

~~However, in order to achieve a more consistent overall scheme, in this annex it is suggested to use for Layer II the same mechanism for distributing the keys as in Layer I. This requires the KACs of the different networks to generate and distribute asymmetric key pairs for the network elements of that network. These key pairs will then be used to transfer the symmetric session keys in the same way as in Layer I.~~

~~The public and private key pairs needed for the network entities should be distributed to the entities in a secure way, which is in principle an operation & maintenance task. One way to do this is to distribute the key pairs, along with the necessary crypto-software, to the network entities in the form of chipcards, which can also carry out the necessary computations. Therefore, all that has to be added to the present network entities are chipcard readers with a standardised interface. Thus, on adoption of this proposal, in addition to their present tasks, the network entities would have to:~~

- ~~Store the symmetric session keys to encrypt/decrypt data before sending/after receiving to/from network entities of other networks (external) and of their own network (internal);~~
- ~~Encrypt/decrypt MAP messages according to their Mode of protection (cf. 7.4). The necessary computations may be carried out by a chipcard.~~

~~In addition to their tasks listed in 7.2.1 of the main document, the KACs would have to:~~

- ~~Generate and store asymmetric key pairs for network entities in the same network;~~
- ~~Distribute asymmetric key pairs to network entities in the same network.~~

~~E.2 Proposed Layer II Message Format~~

~~The Layer II messages themselves take the same form as in 7.2 of the main document, where the 'receiving network Y' has to be replaced by 'receiving network entity NE_X' (or X by NE_Y). Further, the Key Distribution Complete message is not needed in Layer II. However, the distribution of the session keys KS_{XY} in network X having initiated the Layer I message exchange should not begin before the Key Distribution Complete Message from the receiving network Y has been received by the KAC_X in Layer I. As soon as a network element of X has received a session key KS_{XY}, it may start enciphering with this key. A similar statement holds if the transported keys are used internally only: In this case, all network elements of X should get the symmetric session key KS_{XX} to be used internal for encryption (marked as decryption key with flag RECEIVE) first; if all network elements have acknowledged that they have recovered these keys, the KAC_X sends the same key again (marked as encryption key with flag SEND). Again, as soon as a network element has received the session key KS_{XX} (with flag SEND), it may start enciphering with this key.~~

~~[Note: As for layer I, no assumptions about the transport protocol are made, although IP might be a good candidate.]~~

~~E.2.1 Sending a session key for decryption~~

~~In order to transport a symmetric session key (marked with flag RECEIVE) with version no. i to be used to decrypt received data from network elements of network X in NE_Y, the KAC of Y sends a message containing the following data to NE_Y:~~

$E_{PK(NEY)}$
$\{X||NE_Y||RECEIVE||i||KS_{XY}(i)||RND_Y||Text1||D_{SK(Y)}(Hash(X||NE_Y||RECEIVE||i||KS_{XY}(i)||RND_Y||Text1))||Text2\}||Text3$

After having successfully decrypted the key transport message and having verified the digital signature of the sending network including the hash value, the receiving network entity sends an key installed message to its Key Administration Centre KAC_Y. The message takes the form

$KEY\_INSTALLED||X||NE_Y||RND_Y||i$

This message can only be sent by the receiving network entity, because only this entity can know about RND_Y. If anything goes wrong, e.g. computing the Hash of $X||NE_Y||RECEIVE||i||KS_{XY}(i)||RND_Y||Text1$ does not yield the expected result, a RESEND message should be sent by NE_Y to KAC_Y in the form

$RESEND||NE_Y$

E.2.2 Sending a session key for encryption

In order to transport a symmetric SEND key with version no. i to be used for sending data from NE_X to network elements of network Y, KAC_X sends a message containing the following data to NE_X:

$E_{PK(NEX)}\{NE_X||Y||SEND||i||KS_{XY}(i)||RND_X||Text1||D_{SK(X)}(Hash(NE_X||Y||SEND||i||KS_{XY}(i)||RND_X||Text1))||Text2\}||Text3$

3GPP TSG SA WG 3 (Security) meeting #12
Stockholm, 11—14 April, 2000

Document **S3-000292**
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	094	Current Version:	3.4.0

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

For submission to:	SA #8	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 [ ] UTRAN / Radio [ ] Core Network [X]

Source: SA WG3 **Date:** 2000-04-14

Subject: Cipher and integrity key update once every 24 hours

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 indication that “the VLR/SGSN shall assure that IK and CK are updated at least once every 24 hours” is removed.

Clauses affected: 6.5.4.2, 6.6.4.2

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: This does not exclude that for R00 a procedure to better control the lifetime of the keys is fully specified.


help.doc

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

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 6.5.6.

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 UE. IK is sent from the USIM to the UE upon request of the UE. The USIM shall send IK under the condition that 1) a valid IK is available, 2) the current value of START in the USIM is up-to-date and 3) START has not reached THRESHOLD. The UE 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 or SGSN and stored in the VLR or SGSN as part of a quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) *security mode command*. ~~The MSC/VLR or SGSN shall assure that the IK is updated at least once every 24 hours.~~

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.

6.6.4.2 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 cipher key to use for a particular logical channel is described in 6.6.6.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 UE. CK is sent from the USIM to the UE upon request of the UE. 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 UE 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. ~~The VLR or SGSN shall assure that CK is updated at least once every 24 hours.~~

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.

3GPP TSG SA WG3 (Security) meeting #11
Stockholm, Sweden, 11-14 April 2000

***Document* S3-000302**
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	095	Current Version:	3.4.0

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

For submission to:	TSG SA #8	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	X

Source: SA WG3 **Date:** 2000-04-13

Subject: Handling of emergency call

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 handling of emergency call from a security poit of view is not specified.

Clauses affected: 6.3.3.2 (New clause)

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.

6.3.3.2 Emergency calls

Emergency call is a service in the CS domain ,

6.3.3.2.1 Valid USIM present

When a valid USIM is present an emergency call will use the normal security mode setup procedure. This means that it is integrity and confidentiality protected in the same way as a normal call.

6.3.3.2.2 No valid USIM present

Emergency calls may as a serving network option be performed even

1. without any (U)SIM present in the UE

2. when user authentication fails (USIM present)

3. when authentication is impossible to perform (USIM present but network failure or invalid USIM)

In these cases no security mode setup procedure is performed. This means that the call will be conducted without integrity and confidentiality protection.

3GPP TSG SA WG3 (Security) meeting #12
Stockholm, 11-14 April, 2000

***Document* S3-000289**
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**	**096**	Current Version:	3.4.0

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

For submission to: TSG SA #8 *list expected approval meeting # here ↑*

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

Source: SA WG3 **Date:** 2000-04-13

Subject: Clarification on the HFN handling

Work item: Security

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

F	Correction	[X]
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	[X]
Release 00	[ ]

Reason for change:
- to clarify that the initial HFN information contains one HFN per CN domain
- to clarify that the start usage of new generated IK and CK implies a reset of the initial HFN, i.e. a reset of the COUNT-C and COUNT-I parameters
- editorial modifications

Clauses affected: 6.4.1, 6.4.2, 6.4.5

Other specs affected:

Other 3G core specifications	[X]	→ 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: Impact on T WG3 specification 31.102


help.doc

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

6.4 Local authentication and connection establishment

Local authentication is obtained by integrity protection functionality.

6.4.1 Cipher key and integrity key setting

Authentication and key setting are triggered by the authentication procedure and described in 6.3. Authentication and key setting may be initiated by the network as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber (i.e. P-TMSI, TMSI or IMSI) is known by the VLR/SGSN. The CK and IK are stored in the VLR/SGSN and transferred to the RNC when needed. The CK and IK for the CS domain are stored on the USIM and updated at the next authentication from this domain. The CK and IK for the PS domain are stored on the USIM and updated at the next authentication from this domain.

If an authentication procedure is performed during a connection (PS or CS mode), the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the UE as part of the security mode ~~negotiation~~ set-up procedure (see 6.4.5) that follows the authentication procedure.

6.4.2 Ciphering and integrity mode negotiation

When an MS wishes to establish a connection with the network, the MS shall indicate to the network in the MS/USIM Classmark which cipher and integrity algorithms the MS supports. This information itself must be integrity protected. As it is the case that the RNC does not have the integrity key IK when receiving the MS/USIM Classmark this information must be stored in the RNC. The data integrity of the classmark is performed, during the security mode set-up procedure by use of the most recently generated IK (see section 6.4.5).

The network shall compare its integrity protection capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the network ~~SN~~ have no versions of the UIA algorithm in common, then the connection shall be released.

2) If the MS and the network ~~SN~~ have at least one version of the UIA algorithm in common, then the network shall select one of the mutually acceptable versions of the UIA algorithm for use on that connection.

The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the network have no versions of the UEA algorithm in common and the network is not prepared to use an unciphered connection, then the connection shall be released.

2) If the MS and the network have no versions of the UEA algorithm in common and the user (respectively the user's HE) and the network are willing to use an unciphered connection, then an unciphered connection shall be used.

~~2~~3) If the MS and the network have at least one version of the UEA algorithm in common, then the network shall select one of the mutually acceptable versions of the UEA algorithm for use on that connection.

~~3) If the MS and the network have no versions of the UEA algorithm in common and the user (respectively the user's HE) and the SN are willing to use an unciphered connection, then an unciphered connection shall be used.~~

Because of the separate mobility management for CS and PS services, one CN domain may, independent of the other CN, establish a connection to one and the same MS. Change of ciphering and integrity mode (algorithms) at establishment of a second MS to CN connection shall not be permitted. The preferences and special requirements for the ciphering and integrity mode setting shall be common for both domains. (e.g. the order of preference of the algorithms).

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and MSC/VLR respective SGSN. The three exceptions when it is not mandatory to start integrity protection are:

- If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.

- If there is no MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), i.e. in the case of deactivation indication sent from the MS followed by connection release.

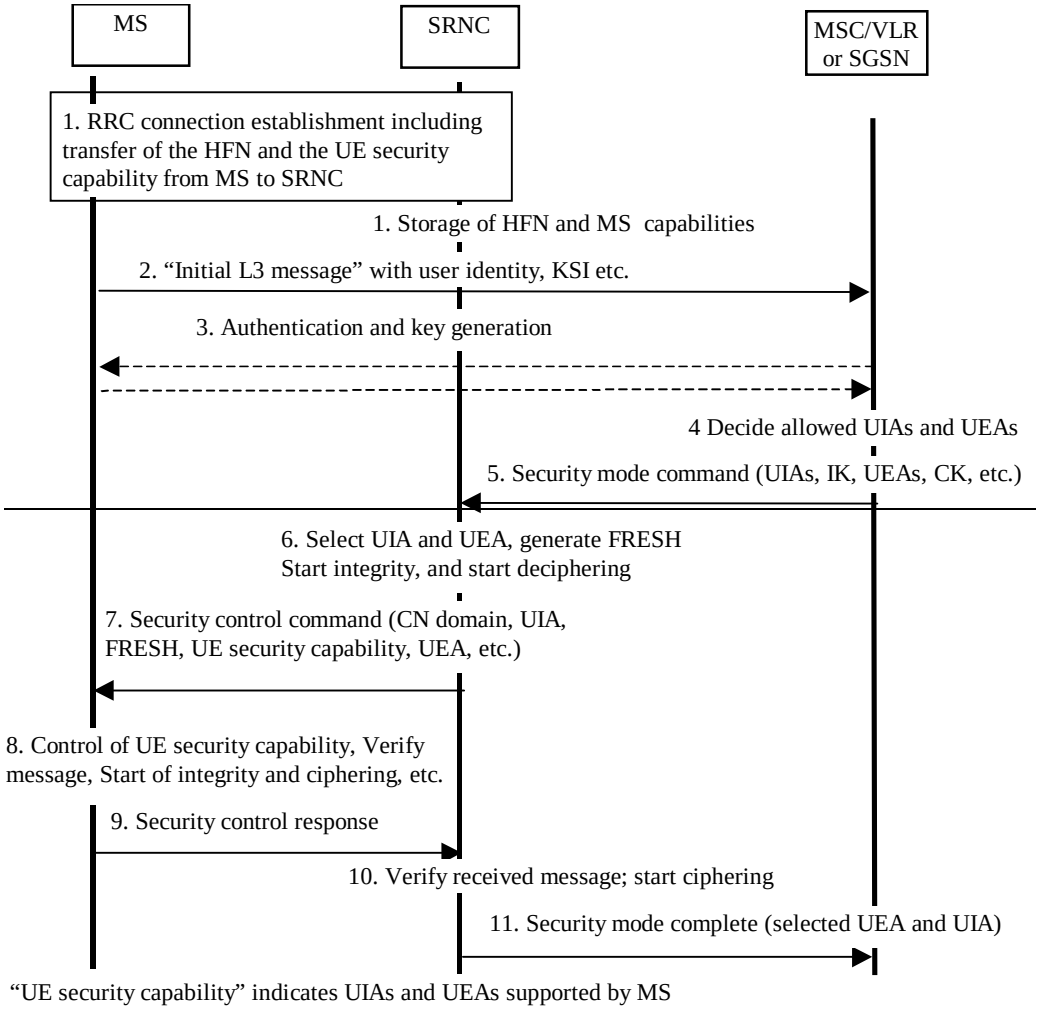
- If the only MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.

When the integrity protection shall be started, the only procedures between MS and MSC/VLR respective SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to MSC/VLR or SGSN) and before the security mode set-up procedure are the following:

- Identification by a permanent identity (i.e. request for IMSI), and

- Authentication and key agreement

The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.



"UE security capability" indicates UIAs and UEAs supported by MS

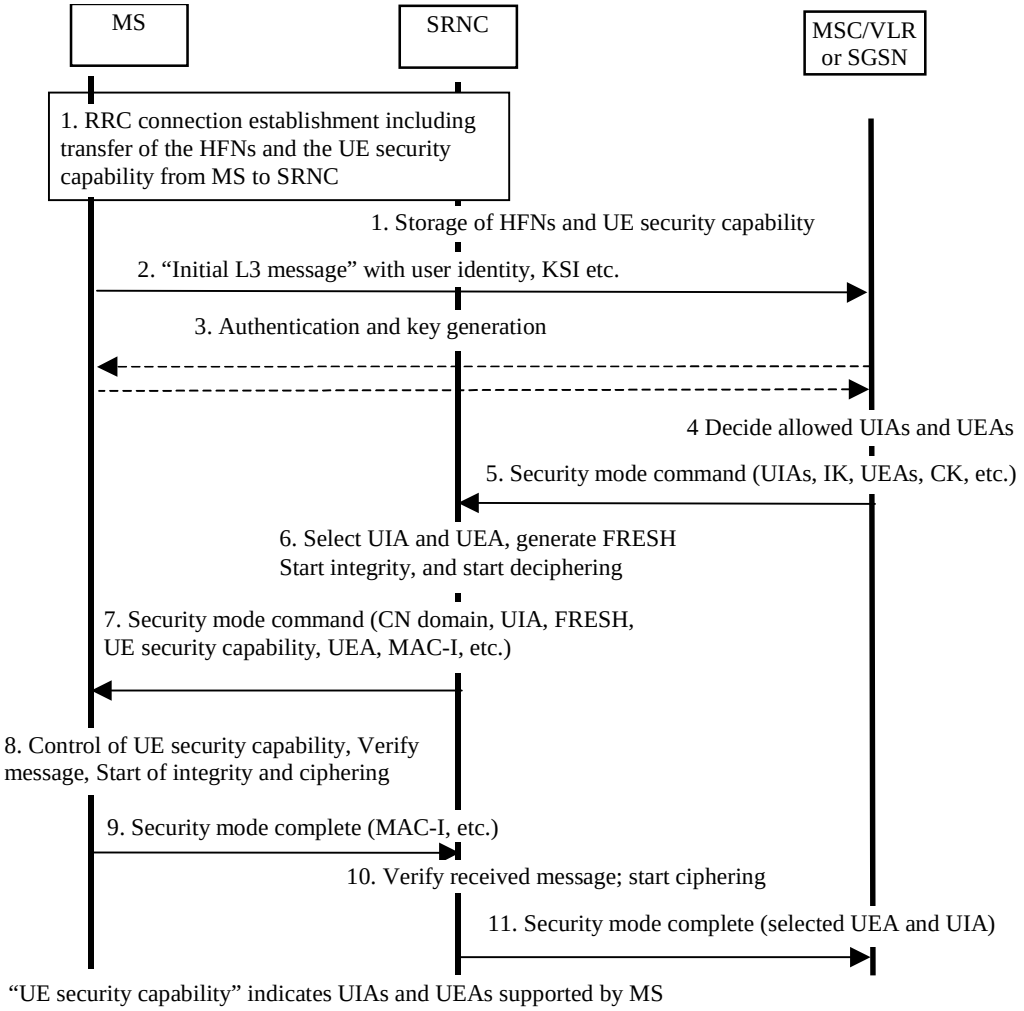


Figure 14: Local authentication and connection set-up

NOTE 1: The network must have the "UE security capability" information before the integrity protection can start, i.e. the "UE security capability" must be sent to the network in an unprotected message. Returning the "UE security capability" later on to the ~~UE~~ ME in a protected message will give ~~UE~~ ME the possibility to verify that it was the correct "UE security capability" that reached the network.
~~This latter point, as well as the RRC interwork described below, is yet to be agreed in RAN WG2.~~

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the UE security ~~capabiltiy~~capability and the initial hyperframe numbers (HFN) for the CS service domain respective the PS service domain. The UE security capability information includes the ciphering capabilities (UEAs) and the integrity capabilities (UIAs) of the MS. The initial HFN is used to initialise the HFN to be used as part of ~~one of~~ the input parameters COUNT-I, for the integrity algorithm, and COUNT-C, for the ciphering algorithm. The ~~COUNT-I parameter (together with COUNT which is used for ciphering) is~~initial HFNs and the UE security capability information are stored in the SRNC.

2. The MS sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the ~~relevant CN domain~~MSC/VLR or SGSN. This message contains ~~relevant MM information~~ e.g. the user identity and the KSI. The included KSI (Key Set Identifier) is the ~~number~~ KSI allocated by the ~~CN~~ CS service domain or PS service domain at the last authentication for this CN domain.

3. User identity request may be performed (see 6.2). Authentication of the user and generation of new security keys (IK and CK) may be performed (see 6.3.3). A new KSI will then also be allocated.

4. The ~~CN node~~ MSC/VLR or SGSN determines which UIAs and UEAs that are allowed to be used.

5. The ~~CN~~ MSC/VLR or SGSN initiates integrity ~~(~~and ~~possible also~~ ciphering~~)~~ by sending the RANAP message Security Mode Command to SRNC. This message contains a list of allowed UIAs and the IK to be used. If ciphering shall be started, it ~~It may also~~ contains the allowed UEAs and the CK to be used. If a new authentication and security key generation has been performed (see 3 above), this shall be indicated in the message sent to the SRNC. The indication of new generated keys implies that the initial HFN to be used shall be reset (i.e. set to zero) at start use of the new keys. Otherwise, it is the HFN already available in the SRNC that shall be used (see 1. above).

6. The SRNC decides which algorithms to use by selecting from the list of allowed algorithms, ~~the first UEA and the first UIA it~~ and the list of algorithms supported by the MS~~supports~~ (see 6.4.2). The SRNC generates a random value FRESH and initiates the downlink integrity protection. If the requirements received in the Security mode command can not be fulfilled, the SRNC ~~supports no UIA algorithms in the list, it~~ sends a SECURITY MODE REJECT message to ~~Cn~~the requesting MSC/VLR or SGSN. The further actions are described in 6.4.2.

7. The SRNC generates the RRC message Security ~~control~~ mode command. The message includes the UE security capability, the UIA and FRESH to be used and ~~possibly~~ if ciphering shall be started also the UEA to be used. Additional information (start of ciphering) may also be included. Because of that the MS can have two ciphering and integrity key sets~~Since we have two CNs with an IK each~~, the network must indicate which ~~IK~~ key set to use. This is obtained by including a CN type indicator information in the "Security ~~control~~ mode command" message. Before sending this message to the MS, the SRNC generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.

8. At reception of the Security ~~control~~ mode command message, the MS controls that the UE security capability received is equal to the UE security capability sent in the initial message. The MS computes XMAC-I on the message received by using the indicated UIA, the stored COUNT-I and the received FRESH parameter. The MS verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.

9. If all controls are successful, the MS compiles the RRC message Security ~~control command response~~mode complete and generates the MAC-I for this message. If any control is not successful, the procedure ends in the MS~~a SECURITY CONTROL REJECT message is sent from the MS~~.

10. At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

11. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC to the ~~CN node~~ MSC/VLR or SGSN ends the procedure.

The Security mode command to MS starts the downlink integrity protection, i.e. also all following downlink messages sent to the MS are integrity protected and possibly ciphered. The Security mode ~~command response~~complete from MS starts the uplink integrity protection and possible ciphering, i.e. also all following messages sent from the MS are integrity protected and possibly ciphered.

3GPP TSG SA 3 Meeting #13
Yokohama, Japan, 24-26 Mai 2000

Document S3-000323b
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	098	Current Version:	3.4.0

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

For submission to:	SA#8	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	X	ME	X	UTRAN / Radio		Core Network	

Source: TSG SA WG3 **Date:** 18 Mai 2000

Subject: Security mode set-up procedure

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	X

Reason for change: Change COUNT to COUNT-C

Clauses affected: 6.4.5

Other specs affected:

Other 3G core specifications	X	→ 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.

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and MSC/VLR respective SGSN. The three exceptions when it is not mandatory to start integrity protection are:

- If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.
- If there is no MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), i.e. in the case of deactivation indication sent from the MS followed by connection release.
- If the only MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.

When the integrity protection shall be started, the only procedures between MS and MSC/VLR respective SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to MSC/VLR or SGSN) and before the security mode set-up procedure are the following:

- Identification by a permanent identity (i.e. request for IMSI), and
- Authentication and key agreement

The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.

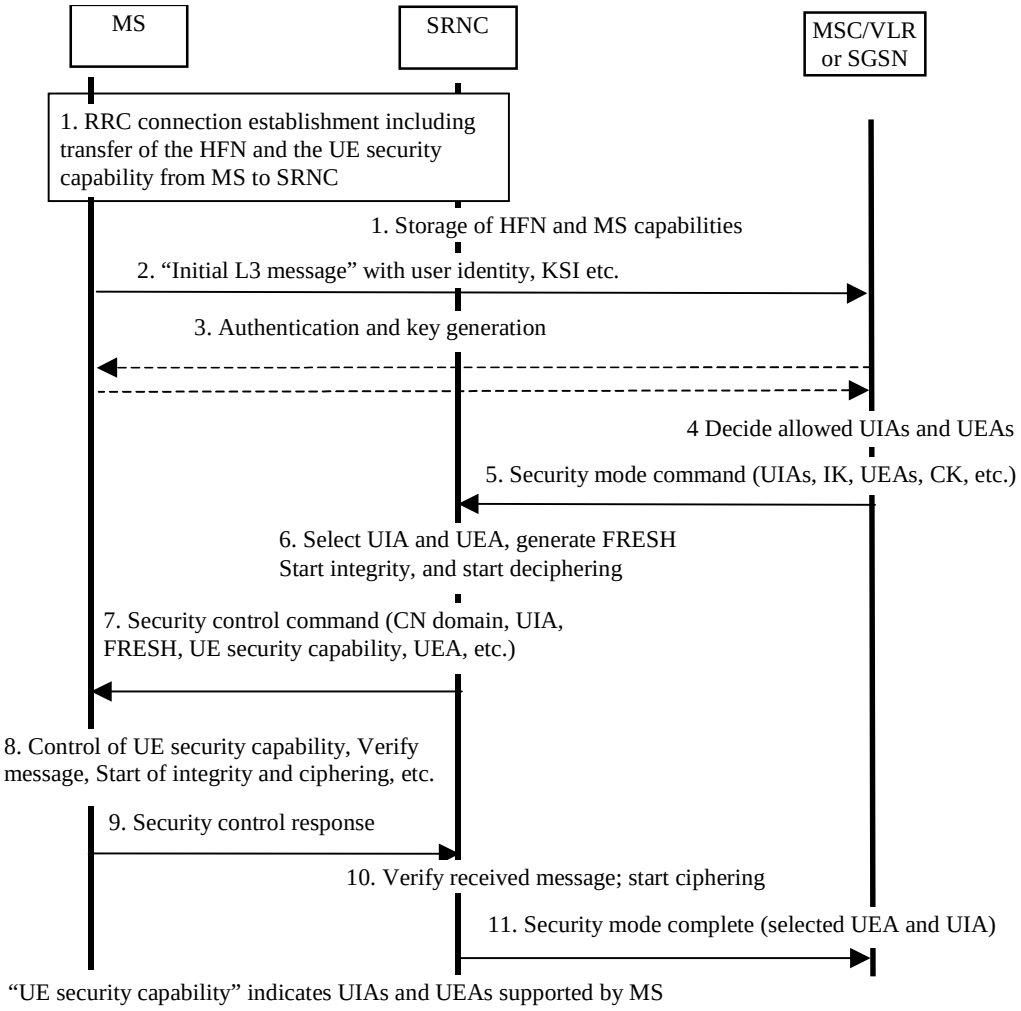


Figure 14: Local authentication and connection set-up

NOTE 1: The network must have the "UE security capability" information before the integrity protection can start, i.e. the "UE security capability" must be sent to the network in an unprotected message. Returning the "UE security capability" later on to the UE in a protected message will give UE the possibility to verify that it was the correct "UE security capability" that reached the network.
This latter point, as well as the RRC interwork described below, is yet to be agreed in RAN WG2.

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the UE security capabiltiy and the hyperframe number to be used as part of one of the input parameters for the integrity algorithm and for the ciphering algorithm. The COUNT-I parameter (together with COUNT-C which is used for ciphering) is stored in the SRNC.

2. The MS sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the relevant CN domain. This message contains relevant MM information e.g. KSI. The KSI (Key Set Identifier) is the number allocated by the CN at the last authentication for this CN domain.

3. Authentication of the user and generation of new security keys (IK and CK) may be performed. A new KSI will then also be allocated.

4. The CN node determines which UIAs and UEAs that are allowed to be used.

5. The CN initiates integrity (and possible also ciphering) by sending the RANAP message Security Mode Command to SRNC. This message contains a list of allowed UIAs and the IK to be used. It may also contain the allowed UEAs and the CK to be used.

6. The SRNC decides which algorithms to use by selecting from the list of allowed algorithms, the first UEA and the first UIA it supports. The SRNC generates a random value FRESH and initiates the downlink integrity protection. If SRNC supports no UIA algorithms in the list, it sends a SECURITY MODE REJECT message to CN.

7. The SRNC generates the RRC message Security control command. The message includes the UE security capability, the UIA and FRESH to be used and possibly also the UEA to be used. Additional information (start of ciphering) may also be included. Since we have two CNs with an IK each, the network must indicate which IK to use. This is obtained by including a CN type indicator information in "Security control command". Before sending this message to the MS, the SRNC generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.

8. At reception of the Security control command message, the MS controls that the UE security capability received is equal to the UE security capability sent in the initial message. The MS computes XMAC-I on the message received by using the indicated UIA, the stored COUNT-I and the received FRESH parameter. The MS verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.

9. If all controls are successful, the MS compiles the RRC message Security control command response and generates the MAC-I for this message. If any control is not successful, a SECURITY CONTROL REJECT message is sent from the MS.

10. At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

11. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC to the CN node ends the procedure.

The Security mode command to MS starts the downlink integrity protection, i.e. also all following downlink messages sent to the MS are integrity protected and possibly ciphered. The Security mode command response from MS starts the uplink integrity protection and possible ciphering, i.e. also all following messages sent from the MS are integrity protected and possibly ciphered.

3GPP TSG SA 3 Meeting #13
Yokohama, Japan, 24-26 May 2000

Document S3-000323d
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	100	Current Version:	3.4.0

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

For submission to:	SA#8	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	X	ME	X	UTRAN / Radio		Core Network	

Source: TSG SA WG3 **Date:** 18 Mai 2000

Subject: Replace COUNT by $START_{CS}$ and $START_{PS}$

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	X

Reason for change: Alignment with CR88

Clauses affected: 6.4.3, 6.4.7

Other specs affected:

Other 3G core specifications	X	→ 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: Possible impact on T WG3 specifications

help.doc

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

6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement which generates cipher/integrity keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time an RRC connection is released the ~~highest~~ values ~~of the hyperframe number (the current value of COUNT~~START$_{CS}$ and START$_{PS}$~~)~~ of the bearers that were protected in that RRC connection ~~is~~ are stored in the USIM. When the next RRC connection is established that values ~~is~~ are read from the USIM ~~and incremented by one~~.

The UE shall trigger the generation of a new access link key set (a cipher key and an integrity key) if START$_{CS}$ or START$_{PS}$ ~~the counter~~ reache~~s~~ a maximum value set by the operator and stored in the USIM at the next RRC connection request message sent out or during an RRC connection. When this maximum value is reached the cipher key and integrity key stored on USIM shall be deleted.

This mechanism will ensure that a cipher/integrity key set cannot be reused beyond the limit set by the operator.

6.4.7 Signalling procedure for periodic local authentication

The following procedure is used by the RNC to periodically perform a local authentication. At the same time, the amount of data sent during the RRC connection is periodically checked by the RNC and the UE. The RNC is monitoring the COUNT-C and COUNT-I value associated to each radio bearer. The procedure is triggered whenever any of these values reaches a critical checking value. The granularity of these checking values and the values themselves are defined by the visited network. All messages in the procedure are integrity protected.

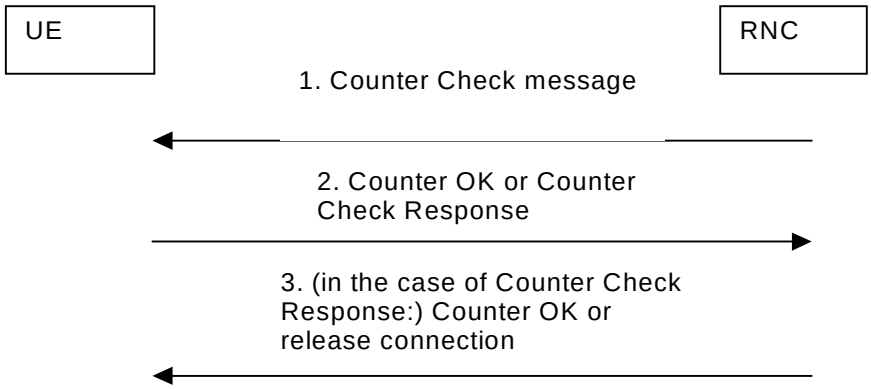


Figure 15a: RNC periodic local authentication procedure

1. When a checking value is reached (e.g. the value in some fixed bit position in the hyperframe number is changed), a Counter Check message is sent by the RNC. The Counter Check message contains the most significant parts of the counter values (which reflect amount of data sent and received) from each active radio bearer.

2. The counter values in the Counter Check message are checked by UE and if they agree with the current status in the UE, a 'Counter OK' message is returned to the RNC. If there is a difference between the counter values in the UE and the values indicated in the Counter Check message, the UE sends a Counter Check response to the RNC. The form of this message is similar to the Counter Check message.

3. In case the RNC receives the 'Counter OK' message the procedure is completed. In case the RNC receives the Counter Check response it compares the counter values indicated in it to counter values in the RNC. If there is no difference or if the difference is acceptable then the RNC completes the procedure by sending the 'Counter OK' message. Otherwise, the connection is released.