**TSG SA WG3 #13** **S3-000378**
**Yokohama, Japan, 24-26 May 2000**

# 3G CHANGE REQUEST

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

**TS 33.102 CR** Current Version: V3.4.0

*3G specification number ↑* *↑ CR number as allocated by 3G support team*

For submission to TSG SA#8 for approval [X] for information [ ] *(only one box should Be marked with an X)*

*list TSG meeting no. here ↑*

*Form: 3G CR cover sheet, version 1.0 The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

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

| | |
|---|---|
| **Source:** | Siemens Atea |
| **Date:** | 26-05-00 |
| **Subject:** | Clarification on terminology in user domain |
| **3G Work item:** | Security |

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

| | | |
|---|---|---|
| F | Correction | |
| A | Corresponds to a correction in a 2G specification | |
| B | Addition of feature | |
| C | Functional modification of feature | |
| D | Editorial modification | X |

**Reason for change:** 3GPP-wide the terminology ME is used to refer to the mobile equipment (instead of user equipment/UE).
8.5.1 is changed to clarify that also a USIM should be able to perform UMTS AKA.

**Clauses affected:** 3.3, 4, 6.4, 6.5, 6.6, 6.8, 7.6

**Other specs affected:**

| | | | |
|---|---|---|---|
| Other 3G core specifications | | → List of CRs: | |
| Other 2G 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:**

## 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~~ME | ~~User~~ Mobile 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 |

# 4 Overview of the security architecture

Figure 1 gives an overview of the complete 3G security architecture.

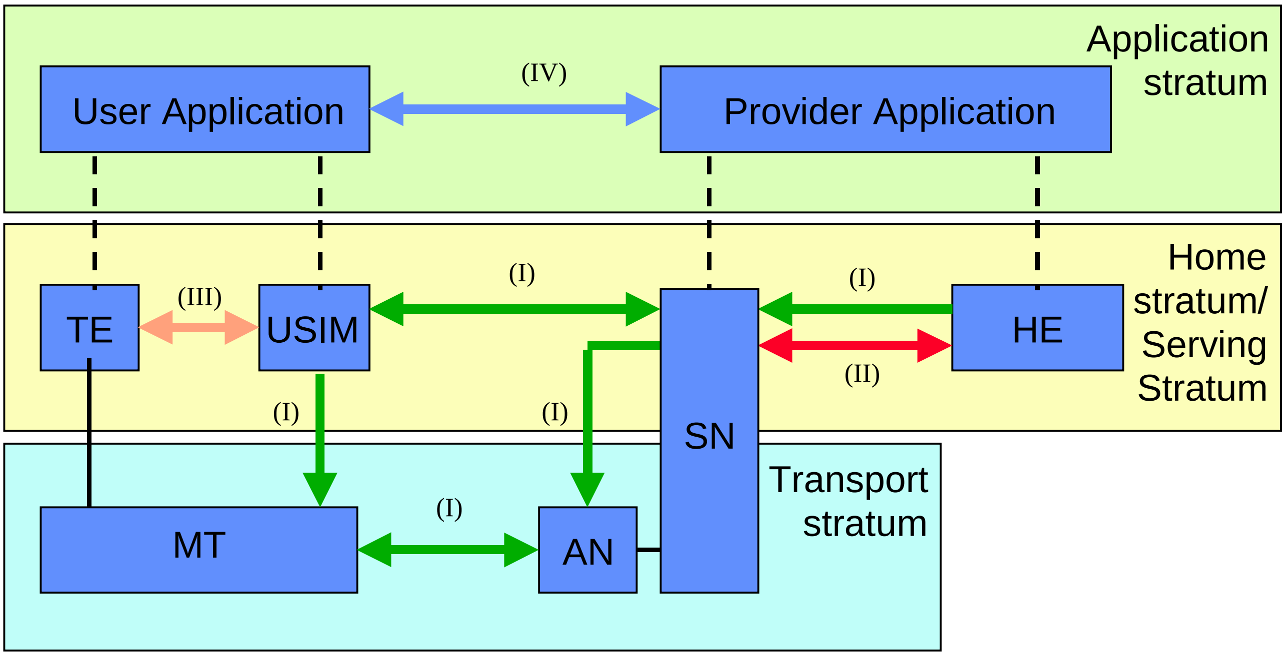



**Figure 1: Overview of the security architecture**

Five security feature groups are defined. Each of these feature groups meets certain threats, accomplishes certain security objectives:

- **Network access security (I):** the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
- **Network domain security (II):** the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;
- **User domain security (III):** the set of security features that secure access to mobile stations
- **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- **Visibility and configurability of security (V):** the set of features that enables the user to inform himself whether a security features is in operation or not and whether the use and provision of services should depend on the security feature.

Figure 2 gives an overview of the ~~UE~~ME registration and connection principles within UMTS with a CS service domain and a PS service domain. As in GSM/GPRS, user (temporary) identification, authentication and key agreement will take place independently in each service domain. User plane traffic will be ciphered using the cipher key agreed for the corresponding service domain while control plane data will be ciphered and integrity protected using the cipher and integrity keys from either one of the service domains. In clause 6 the detailed procedures are defined and when not otherwise stated they are used in both service domains.

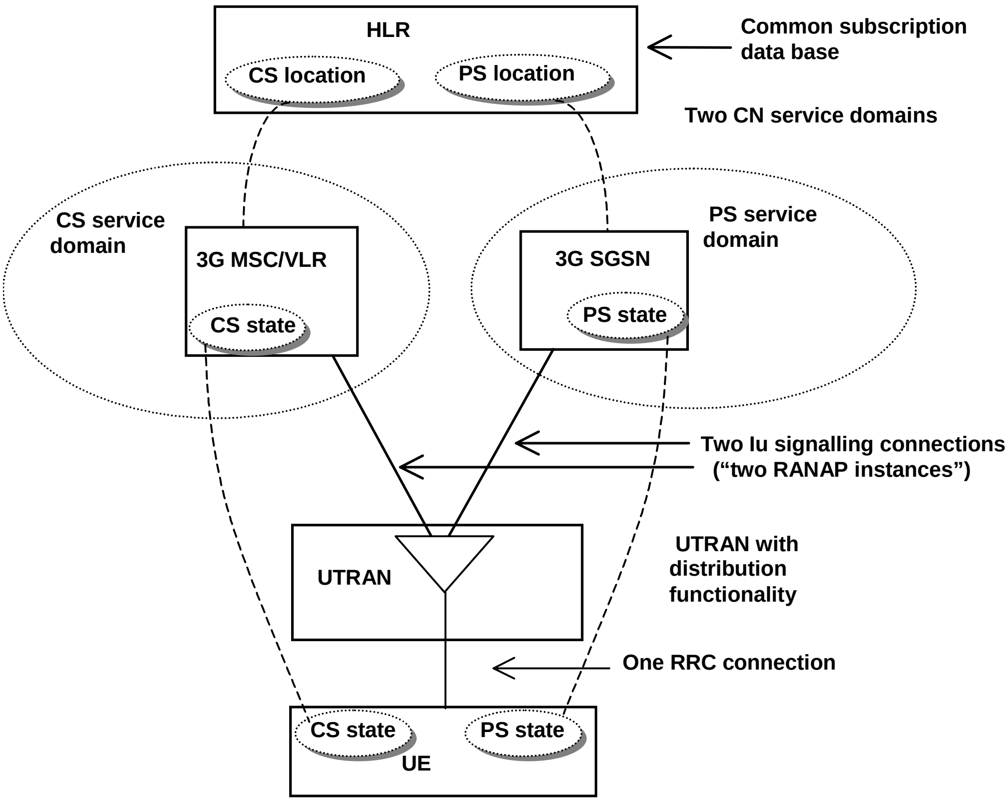



**Figure 2: Overview of the ~~UE~~ME registration and connection principles within UMTS for the separate CN architecture case when the CN consists of both a CS service domain with evolved MSC/VLR, 3G_MSC/VLR, as the main serving node and an PS service domain with evolved SGSN/GGSN, 3G_SGSN and 3G GGSN, as the main serving nodes (Extract from TS 23.121 – Figure 4-8)**

# 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~~ME as part of the security mode negotiation (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 SN have no versions of the UIA algorithm in common, then the connection shall be released.

2) If the MS and the 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 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).

## 6.4.3 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 value of the hyperframe number (the current value of COUNT) of the bearers that were protected in that RRC connection is stored in the USIM. When the next RRC connection is established that value is read from the USIM and incremented by one.

The ~~UE~~ME shall trigger the generation of a new access link key set (a cipher key and an integrity key) if the counter reaches 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.

### 6.4.4 Cipher key and integrity key identification

The key set identifier (KSI) is a number which is associated with the cipher and integrity keys derived during authentication. The key set identifier is allocated by the network and sent with the authentication request message to the mobile station where it is stored together with the calculated cipher key CK and integrity key IK. KSI in UMTS corresponds to CKSN in GSM. The USIM stores one KSI/CKSN for the PS domain key set and one KSI/CKSN for the CS domain key set.

The purpose of the key set identifier is to make it possible for the network to identify the cipher key CK and integrity key IK which are stored in the mobile station without invoking the authentication procedure. This is used to allow re-use of the cipher key CK and integrity key IK during subsequent connection set-ups.

KSI and CKSN have the same format. The key set identifier is three bits. Seven values are used to identify the key set. A value of '111' is used by the mobile station to indicate that a valid key is not available for use. At deletion of the cipher key and integrity key, the KSI is set to '111'. The value '111' in the other direction from network to mobile station is reserved.

### 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.

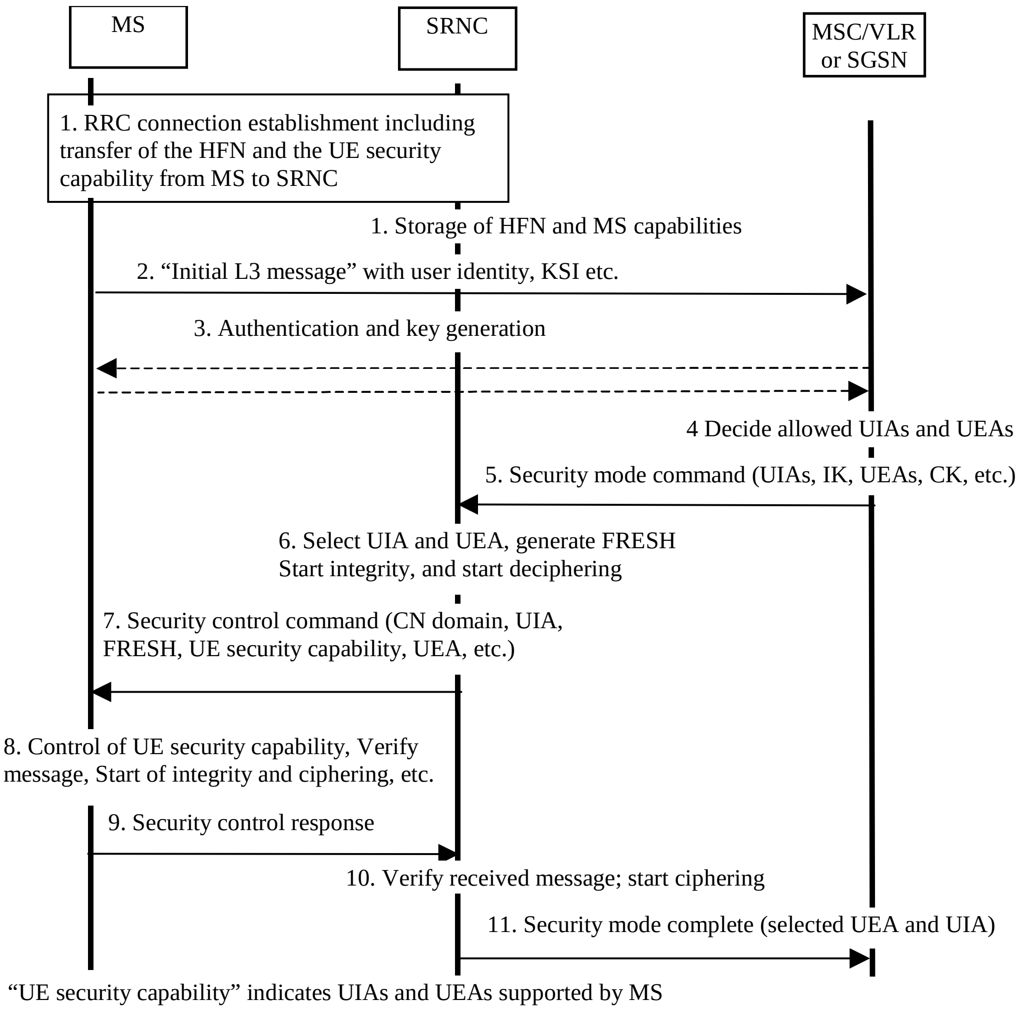



**Figure 14: Local authentication and connection set-up**

NOTE 1: The network must have the "~~UE~~ME security capability" information before the integrity protection can start, i.e. the "~~UE~~ME security capability" must be sent to the network in an unprotected message. Returning the "~~UE~~ME 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~~ME 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~~ME 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 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~~ME 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~~ME security capability received is equal to the ~~UE~~ME 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.

### 6.4.6 Signalling procedures in the case of an unsuccessful integrity check

The supervision of failed integrity checks shall be performed both in the MS and the SRNC. In case of failed integrity check (i.e. faulty or missing MAC) is detected after that the integrity protection is started the concerned message shall be discarded.  This can happen on the RNC side or on the MS side.

### 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~~ME. The RNC is monitoring the COUNT 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.

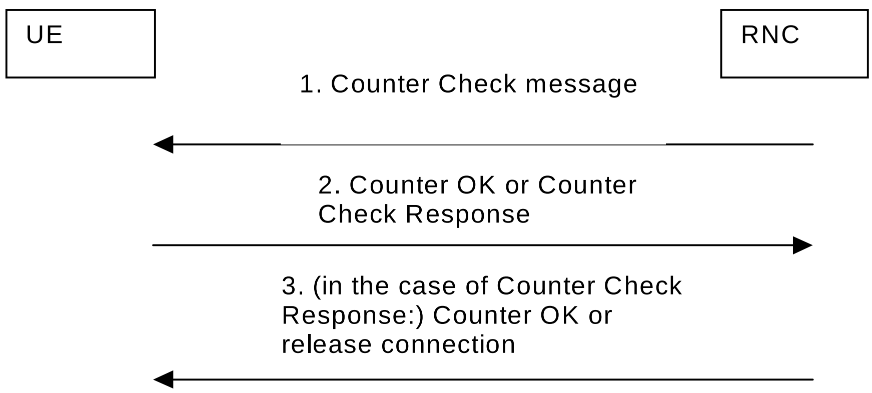



**Figure 15a: RNC periodic local authentication procedure**

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~~ME and if they agree with the current status in the ~~UE~~ME, a 'Counter OK' message is returned to the RNC. If there is a difference between the counter values in the ~~UE~~ME and the values indicated in the Counter Check message, the ~~UE~~ME 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.

# 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~~ME 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).

## 6.5.2 Layer of integrity protection

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

Integrity protection shall be apply at the RRC layer.

## 6.5.3 Data integrity protection method

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

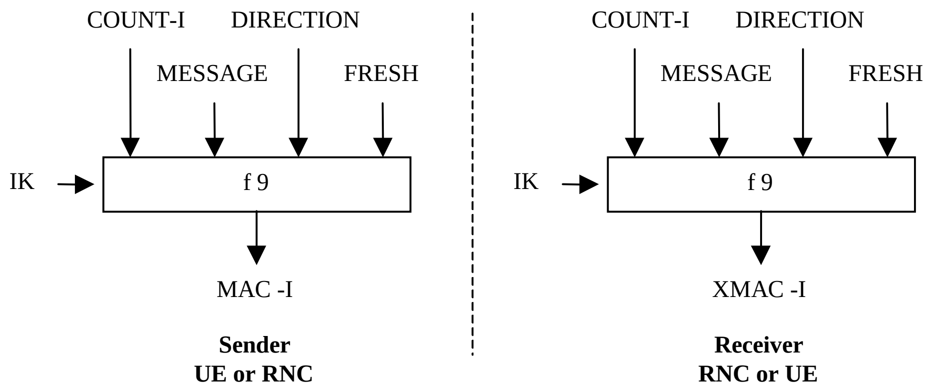



**Figure 16: Derivation of MAC-I (or XMAC-I) on a signalling message**

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

## 6.5.4 Input parameters to the integrity algorithm

### 6.5.4.1 COUNT-I

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

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.

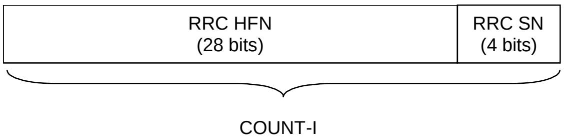



**Figure 16a: The structure of COUNT-I**

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 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~~ME 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~~ME. IK is sent from the USIM to the ~~UE~~ME upon request of the ~~UE~~ME. 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~~ME shall delete IK from memory after power-off as well as after removal of the USIM.

IK is sent from the HLR/AuC to the VLR 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.

#### 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~~ME and the RNC.

## 6.6.2 Layer of ciphering

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

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

## 6.6.3 Ciphering method

Figure 16b illustrates the use of the ciphering algorithm f8 to encrypt plaintext by applying a keystream using a bit per bit binary addition of the plaintext and the 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.

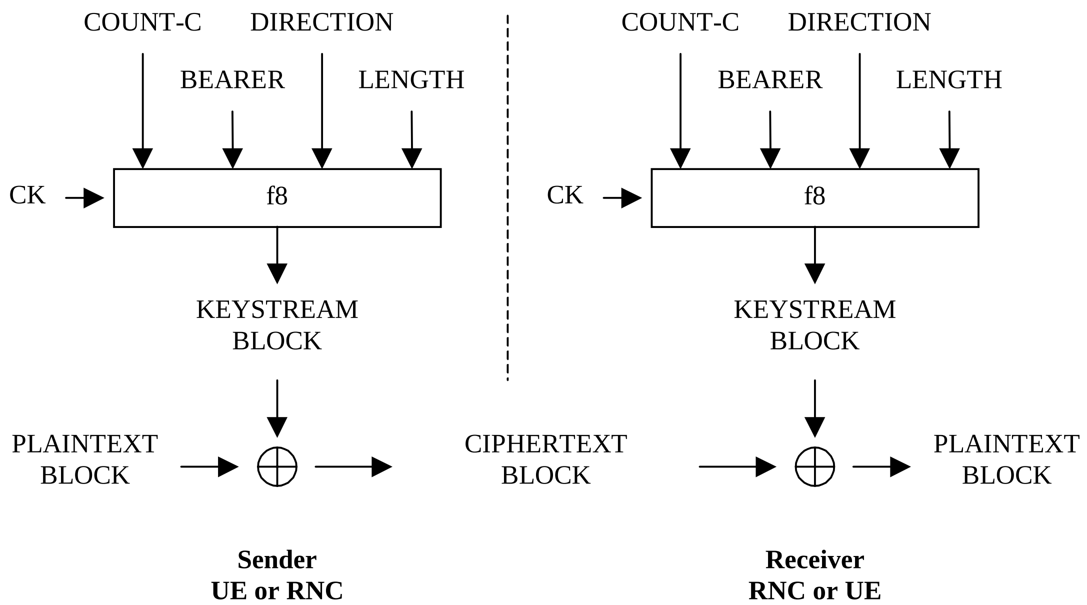



**Figure 16b: Ciphering of user and signalling data transmitted over the radio access link**

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).

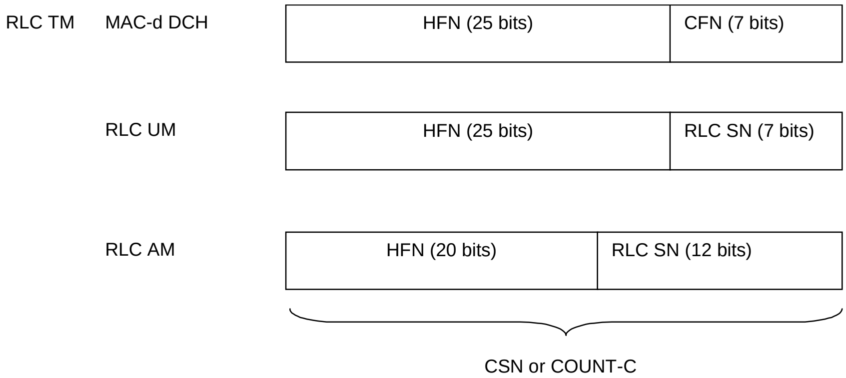



**Figure 16c: The structure of COUNT-C for all transmission modes**

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

CK is sent from the HLR/AuC to the VLR or SGSN and stored in the VLR or SGSN as part of the quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) security mode command. 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 logical channel identifier BEARER is 4 bits long.

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

#### 6.6.4.5 LENGTH

The length indicator LENGTH is 16 bits long.

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

### 6.6.5 Cipher key selection

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

The logical channels for CS user data are ciphered with $CK_{CS}$.

The logical channels for PS user data are ciphered with $CK_{PS}$.

Signalling data (for both CS an PS services) is sent over common logical channels. These logical channels are ciphered by the CK of the service domain for which the most recent security mode negotiation took place. This may require that the cipher key of an (already ciphered) ongoing signalling connection is changed, when a new RRC connection establishment occurs, or when a security mode negotiation follows a re-authentication during an ongoing connection. This change should be completed within five seconds after the security mode negotiation.

### 6.6.6 UEA identification

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

"$0000_2$" : UEA0, no encryption.

"$0001_2$" : UEA1, Kasumi.

The remaining values are not defined.

# 6.8 Interoperation and handover between UMTS and GSM

## 6.8.1 Authentication and key agreement of UMTS subscribers

### 6.8.1.1 General

For UMTS subscribers, authentication and key agreement will be performed as follows:

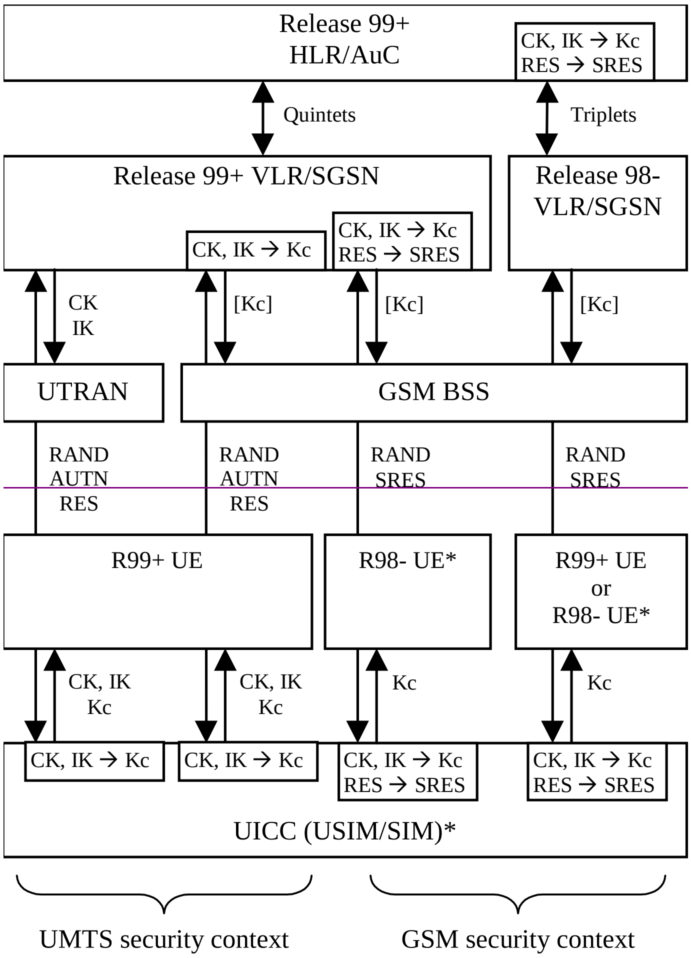
- UMTS AKA shall be applied when the user is attached to a UTRAN.
- UMTS AKA shall be applied when the user is attached to a GSM BSS, in case the user has ~~R99+ UE~~R99+ ME and also the VLR/SGSN is R99+. In this case, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and IK, by the VLR/SGSN on the network side and by the USIM on the user side.
- GSM AKA shall be applied when the user is attached to a GSM BSS, in case the user has ~~R98- UE~~R98- ME. In this case, the GSM user response SRES and the GSM cipher key Kc are derived from the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. A R98- VLR/SGSN uses the stored Kc and RES and a R99+ VLR/SGSN derives the SRES from RES and Kc from CK, IK.

NOTE: To ~~support~~ operate within a ~~R98- UE~~R98- ME the ~~UICC~~ USIM may support the SIM-ME interface as defined in GSM 11.11, and support GSM AKA ~~contain a GSM SIM application~~ which provides the corresponding GSM functionality for calculating SRES and Kc based on the 3G authentication key K and the 3G authentication algorithm implemented in the USIM. Due to the fact that the 3G authentication algorithm only computes CK/IK and RES, conversion of CK/IK to Kc shall be achieved by using the conversion function c3, and conversion of RES to SRES by c2.

- GSM AKA shall be applied when the user is attached to a GSM BSS, in case the VLR/SGSN is R98-. In this case, the USIM derives the GSM user response SRES and the GSM cipher key Kc from the UMTS user response RES and the UMTS cipher/integrity keys CK, IK.

The execution of the UMTS (resp. GSM) AKA results in the establishment of a UMTS (resp. GSM) security context between the user and the serving network domain to which the VLR/SGSN belongs. The user needs to separately establish a security context with each serving network domain.

Figure 18 shows the different scenarios that can occur with UMTS subscribers using either R98- or ~~R99+ UE~~R99+ ME in a mixed network architecture.


Release 99+
HLR/AuC
CK, IK → Kc
RES → SRES
Quintets
Triplets
Release 99+ VLR/SGSN
CK, IK → Kc
CK, IK → Kc
RES → SRES
Release 98-
VLR/SGSN
CK
IK
[Kc]
[Kc]
[Kc]
UTRAN
GSM BSS
RAND
AUTN
RES
RAND
AUTN
RES
RAND
SRES
RAND
SRES
R99+ UE
R98- UE*
R99+ UE
or
R98- UE*
CK, IK
Kc
CK, IK
Kc
Kc
Kc
CK, IK → Kc
CK, IK → Kc
CK, IK → Kc
RES → SRES
CK, IK → Kc
RES → SRES
UICC (USIM/SIM)*
UMTS security context
GSM security context

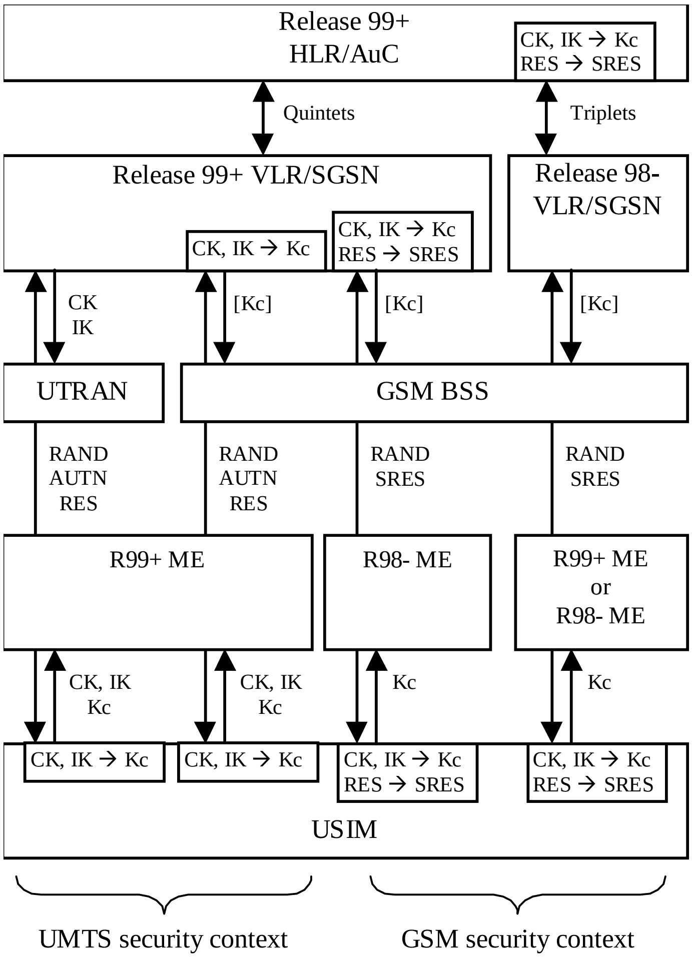



**Figure 18: Authentication and key agreement of UMTS subscribers**

Note that the UMTS parameters RAND, AUTN and RES are sent transparently through the UTRAN or GSM BSS and that the GSM parameters RAND and SRES are sent transparently through the GSM BSS.

In case of a GSM BSS, ciphering is applied in the GSM BSS for services delivered via the MSC/VLR, and by the SGSN for services delivered via the SGSN. In the latter case the GSM cipher key Kc is not sent to the GSM BSS.

In case of a UTRAN, ciphering and integrity are always applied in the RNC, and the UMTS cipher/integrity keys CK an IK are always sent to the RNC.

## 6.8.1.2 R99+ HLR/AuC

Upon receipt of an *authentication data request* from a R99+ VLR/SGSN for a UMTS subscriber, a R99+ HLR/AuC shall send quintuplets, generated as specified in 6.3.

Upon receipt of an *authentication data request* from a R98- VLR/SGSN for a UMTS subscriber, a R99+ HLR/AuC shall send triplets, derived from quintuplets using the following conversion functions:

a) c1: $RAND_{[GSM]} = RAND$

b) c2: $SRES_{[GSM]} = XRES_1$ [xor $XRES_2$ [xor $XRES_3$ [xor $XRES_4$]]]

c) c3: $Kc_{[GSM]} = CK_1 \text{ xor } CK_2 \text{ xor } IK_1 \text{ xor } IK_2$

whereby $XRES_i$ are all 32 bit long and XRES = $XRES_1$ [|| $XRES_2$ [|| $XRES_3$ [|| $XRES_4$]]] dependent on the length of XRES, and $CK_i$ and $IK_i$ are both 64 bits long and $CK = CK_1 \| CK_2$ and $IK = IK_1 \| IK_2$.

### 6.8.1.3 R99+ VLR/SGSN

The AKA procedure will depend on the terminal capabilities, as follows:

- **UMTS subscriber with ~~R99+ UE~~R99+ ME**

  When the user has ~~R99+ UE~~R99+ ME, UMTS AKA shall be performed using a quintuplet that is either:

  a) retrieved from the local database,

  b) provided by the HLR/AuC, or

  c) provided by the previously visited R99+ VLR/SGSN.

Note: Originally all quintuplets are provided by the HLR/AuC.

UMTS AKA results in the establishment of a UMTS security context; the UMTS cipher/integrity keys CK and IK and the key set identifier KSI are stored in theVLR/SGSN.

When the user is attached to a UTRAN, the UMTS cipher/integrity keys are sent to the RNC, where the cipher/integrity algorithms are allocated.

When the user is attached to a GSM BSS, UMTS AKA is followed by the derivation of the GSM cipher key from the UMTS cipher/integrity keys. When the user receives service from an MSC/VLR, the derived cipher key Kc is then sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the derived cipher key Kc is applied in the SGSN itself.

UMTS authentication and key freshness is always provided to UMTS subscribers with ~~R99+ UE~~R99+ ME independently of the radio access network.

- **UMTS subscriber with ~~R98- UE~~R98- ME**

When the user has ~~R98- UE~~R98- ME, the R99+ VLR/SGSN shall perform GSM AKA using a triplet that is either

a) derived by means of the conversion functions c2 and c3 in the R99+ VLR/SGSN from a quintuplet that is:

   i) retrieved from the local database,

   ii) provided by the HLR/AuC, or

   iii) provided by the previously visited R99+ VLR/SGSN, or

b) provided as a triplet by the previously visited MSC/VLR or SGSN.

NOTE: R99+ VLR/SGSN will always provide quintuplets for UMTS subscribers.

NOTE: For a UMTS subscriber, all triplets are derived from quintuplets, be it in the HLR/AuC or in an VLR/SGSN.

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.

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

UMTS authentication and key freshness cannot be provided to UMTS subscriber with ~~R98- UE~~R98- ME.

### 6.8.1.4 ~~R99+ UE~~R99+ ME

~~R99+ UE~~R99+ ME with a USIM inserted and attached to a UTRAN shall only participate in UMTS AKA and shall not participate in GSM AKA.

~~R99+ UE~~R99+ ME with a USIM inserted and attached to a GSM BSS shall participate in UMTS AKA and may participate in GSM AKA. Participation in GSM AKA is required to allow registration in a R98- VLR/SGSN.

The execution of UMTS AKA results in the establishment of a UMTS security context; the UMTS cipher/integrity keys CK and IK and the key set identifier KSI are passed to the ~~UE~~ME. If the USIM supports GSM AKA, the ~~The UE~~ME shall also receive a GSM cipher key Kc derived at the USIM.

The execution of 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 ~~UE~~ME.

### 6.8.1.5 ~~UICC (~~USIM~~/SIM)~~

The ~~UICC~~ USIM

- shall support UMTS AKA ~~(UICC shall contain USIM application)~~ and
- may support backwards compatibility with the GSM system, which consists of
  - GSM cipher key derivation (conversion function c3) and GSM AKA ~~(UICC may contain a SIM application)~~ to access the GSM BSS;
  - SIM-ME interface [GSM 11.11] to operate within R98- ME.
  - ~~. Support of GSM AKA is required to allow access to GSM BSS with a R98- VLR/SGSN and/or with a R98- UE.~~

When the ~~UE~~ME provides the ~~UICC~~ USIM with RAND and AUTN, UMTS AKA shall be executed. If the verification of AUTN is successful, the ~~UICC~~ USIM shall respond with the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The ~~UICC~~ USIM shall store CK and IK as current security context data. If the USIM supports access to GSM BSS, ~~The~~ the ~~UICC~~ USIM shall also derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK using conversion function c3 and send the derived Kc to the ~~R99+ UE~~R99+ ME. In case the verification of AUTN is not successful, the ~~UICC~~ USIM shall respond with an appropriate error indication to the ~~R99+ UE~~R99+ ME.

When the ~~UE~~ME provides the ~~UICC~~ USIM with only RAND, GSM AKA shall be executed, if supported. The ~~UICC~~ USIM first computes the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The ~~UICC~~ USIM then derives the GSM user response SRES and the GSM cipher key Kc using the conversion functions c2 and c3. The ~~UICC~~ USIM then stores the GSM cipher key Kc and sends the GSM user response SRES and the GSM cipher key Kc to the ~~UE~~ME.

In case the ~~UICC~~ USIM does not support GSM AKA (conversion function c3 is not available to derive Kc and pass it to the ~~R99+ UE~~R99+ ME), the ~~R99+ UE~~R99+ ME shall be informed. A ~~UICC~~ USIM that does not support GSM AKA cannot operate under a R98- VLR/SGSN or in a ~~R98- UE~~R98- ME.

## 6.8.2 Authentication and key agreement for GSM subscribers

### 6.8.2.1 General

For GSM subscribers, GSM AKA shall always be used.

The execution of the GSM AKA results in the establishment of a GSM security context between the user and the serving network domain to which the VLR/SGSN belongs. The user needs to separately establish a security context with each serving network domain.

When in a UTRAN, the UMTS cipher/integrity keys CK and IK are derived from the GSM cipher key Kc by the ~~UE~~ME and the VLR/SGSN, both R99+ entities.

Figure 19 shows the different scenarios that can occur with GSM subscribers using either R98- or ~~R99+ UE~~R99+ ME in a mixed network architecture.

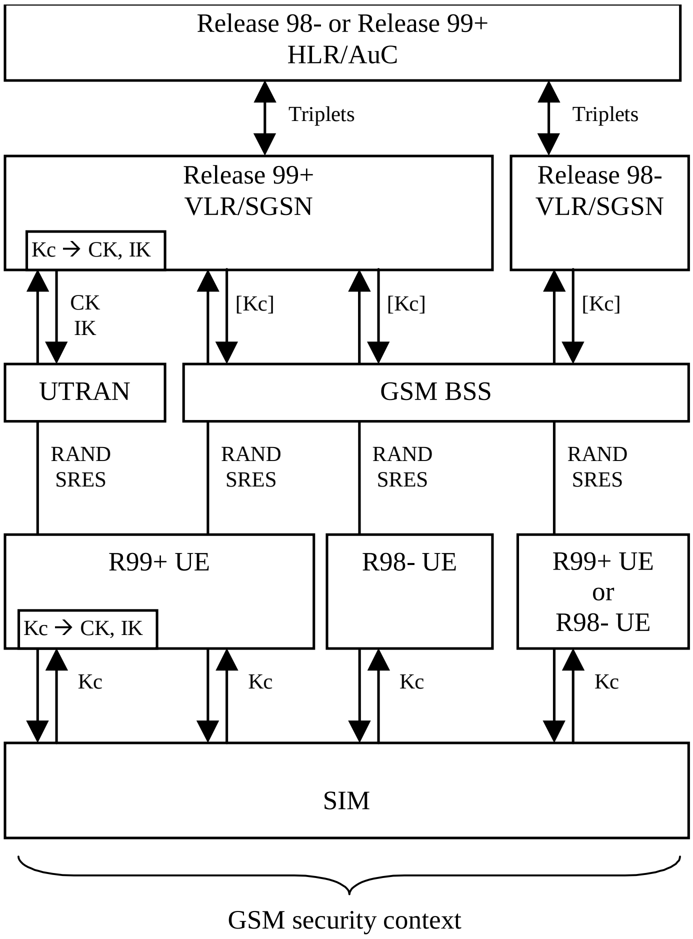



**Figure 19: Authentication and key agreement for GSM subscribers**

Note that the GSM parameters RAND and RES are sent transparently through the UTRAN or GSM BSS.

In case of a GSM BSS, ciphering is applied in the GSM BSS for services delivered via the MSC/VLR, and by the SGSN for services delivered via the SGSN. In the latter case the GSM cipher key Kc is not sent to the GSM BSS.

In case of a UTRAN, ciphering is always applied in the RNC, and the UMTS cipher/integrity keys CK an IK are always sent to the RNC.

### 6.8.2.2 R99+ HLR/AuC

Upon receipt of an *authentication data request* for a GSM subscriber, a R99+ HLR/AuC shall send triplets generated as specified in GSM 03.20.

### 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;

b) c5: $IK_{[UMTS]}$ = Kc || Kc;

whereby in c4, Kc 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.

#### 6.8.2.4 ~~R99+ UE~~R99+ ME

~~R99+ UE~~R99+ ME with a SIM inserted, shall participate only in GSM AKA.

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 ~~UE~~ME.

When the user is attached to a UTRAN, ~~R99+ UE~~R99+ ME shall derive the UMTS cipher/integrity keys CK and IK from the GSM cipher key Kc using the conversion functions c4 and c5.

### 6.8.3 Distribution and use of authentication data between VLRs/SGSNs

The distribution of authentication data (unused authentication vectors and/or current security context data) between R99+ VLRs/SGSNs of the same service network domain is performed according to chapter 6.3.4. The following four cases are distinguished related to the distribution of authentication data between VLRs/SGSNs (of the same or different releases). Conditions for the distribution of such data and for its use when received at VLRn/SGSNn are indicated for each case:

a) R99+ VLR/SGSN to R99+ VLR/SGSN

UMTS and GSM authentication vectors can be distributed between R99+ VLRs/SGSNs. Note that originally all authentication vectors (quintuplets for UMTS subscribers and triplets for GSM subscribers) are provided by the HLR/AuC.

Current security context data can be distributed between R99+ VLRs/SGSNs. VLRn/SGSNn shall not use current security context data received from VLRo/SGSNo to authenticate the subscriber using local authentication in the following cases:

i) Security context to be established at VLRn/SGSNn requires a different set of keys than the one currently in use at VLRo/SGSNo. This change of security context is caused by a change of ~~UE~~ME release (R'99 ~~UE~~ME ←→ R'98 ~~UE~~ME) when the user registers at VLRn/SGSNn.

ii) Authentication data from VLRo includes Kc+CKSN but no unused AVs and the subscriber has a R'99 ~~UE~~ME (under GSM BSS or UTRAN). In this situation, VLRn have no indication of whether the subscriber is GSM or UMTS and it is not able to decide whether Kc received can be used (in case the subscriber were a GSM subscriber).

In these two cases, received current security context data shall be discarded and a new AKA procedure shall be performed.

b) R98- VLR/SGSN to R98- VLR/SGSN

Only triplets can be distributed between R98- VLRs/SGSNs. Note that originally for GSM subscribers, triplets are generated by HLR/AuC and for UMTS subscribers, they are derived from UMTS authentication vectors by R99+ HLR/AuC. UMTS AKA is not supported and only GSM security context can be established by a R98- VLR/SGSN.

R98- VLRs are not prepared to distribute current security context data.

Since only GSM security context can be established under R98- SGSNs, security context data can be distributed and used between R98- SGSNs.

c) R99+ VLR/SGSN to R98- VLR/SGSN

R99+ VLR/SGSN can distribute to a new R98- VLR/SGSN triplets originally provided by HLR/AuC for GSM subscribers or can derive triplets from stored quintuplets originally provided by R99+ HLR/AuC for UMTS subscribers. Note that R98- VLR/SGSN can only establish GSM security context.

R99+ VLRs shall not distribute current security context data to R98- VLRs.

Since R98- SGSNs are only prepared to handle GSM security context data, R99+ SGSNs shall only distribute GSM security context data (Kc, CKSN) to R98- SGSNs.

d) R98- VLR/SGSN to R99+ VLR/SGSN.

In order to not establish a GSM security context for a UMTS subscriber, triplets provided by a R98- VLR/SGSN can only be used by a R99+ VLR/SGSN to establish a GSM security context under GSM-BSS with a ~~R98- UE~~R98- ME.

In all other cases, R99+ VLR/SGSN shall request fresh AVs (either triplets or quintuplets) to HE. In the event, the R99+ VLR/SGSN receives quintuplets, it shall discard the triplets provided by the R98- VLR/SGSN.

R98- VLRs are not prepared to distribute current security context data.

R98- SGSNs can distribute GSM security context data only. The use of this information at R99+ SGSNn shall be performed according to the conditions stated in a).

## 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.

### 6.8.4.1 UMTS security context

A UMTS security context in UTRAN is only established for a UMTS subscriber with a ~~R99+ UE~~R99+ ME. At the network side, three cases are distinguished:

a) In case of a handover to a GSM BSS controlled by the same MSC/VLR, the MSC/VLR derives the GSM cipher key Kc from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and sends Kc to the target BSC (which forwards it to the BTS).

b) In case of a handover to a GSM BSS controlled by other R98- MSC/VLR, the initial MSC/VLR derives the GSM cipher key from the stored UMTS cipher/integrity keys (using the conversion function c3) and sends it to the target BSC via the new MSC/VLR controlling the BSC. The initial MSC/VLR remains the anchor point throughout the service.

c) In case of a handover to a GSM BSS controlled by another R99+ MSC/VLR, the initial MSC/VLR sends the stored UMTS cipher/integrity keys CK and IK to the new MSC/VLR. The initial MSC/VLR also derives Kc and sends it to the new MSC/VLR. The new MSC/VLR store the keys and sends the received GSM cipher key Kc to the target BSC (which forwards it to the BTS). The initial MSC/VLR remains the anchor point throughout the service.

At the user side, in either case, the ~~UE~~ME applies the derived GSM cipher key Kc received from the USIM during the last UMTS AKA procedure.

### 6.8.4.2 GSM security context

A GSM security context in UTRAN is only established for a GSM subscribers with a ~~R99+ UE~~R99+ ME. At the network side, two cases are distinguished:

a) In case of a handover to a GSM BSS controlled by the same MSC/VLR, the MSC/VLR sends the stored GSM cipher key Kc to the target BSC (which forwards it to the BTS).

b) In case of a handover to a GSM BSS controlled by another MSC/VLR (R99+ or R98-), the initial MSC/VLR sends the stored GSM cipher key Kc to the BSC via the new MSC/VLR controlling the target BSC. The initial MSC/VLR remains the anchor point throughout the service.

If the non-anchor MSC/VLR is R99+, then the anchor MSC/VLR also derives and sends to the non-anchor MSC/VLR the UMTS cipher/integrity keys CK and IK. The non-anchor MSC/VLR stores all keys. This is done to allow subsequent handovers in a non-anchor R99+ MSC/VLR.

At the user side, in either case, the ~~UE~~ME applies the stored GSM cipher key Kc.

## 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 integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed.

### 6.8.5.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with ~~R99+ UE~~R99+ ME under GSM BSS controlled by a R99+ VLR/SGSN. At the network side, two cases are distinguished:

a) In case of a handover to a UTRAN controlled by the same MSC/VLR, the stored UMTS cipher/integrity keys CK and IK are sent to the target RNC.

b) In case of a handover to a UTRAN controlled by another MSC/VLR, the initial MSC/VLR sends the stored UMTS cipher/integrity keys CK and IK to the new RNC via the new MSC/VLR that controls the target RNC. The initial MSC/VLR remains the anchor point for throughout the service.

   The anchor MSC/VLR also derives and sends to the non-anchor MSC/VLR the GSM cipher key Kc. The non-anchor MSC/VLR stores all keys. This is done to allow subsequent handovers in a non-anchor R99+ MSC/VLR.

At the user side, in either case, the ~~UE~~ME applies the stored UMTS cipher/integrity keys CK and IK.

### 6.8.5.2 GSM security context

Handover from GSM BSS to UTRAN with a GSM security context is only possible for a GSM subscriber with a ~~R99+ UE~~R99+ ME. At the network side, two cases are distinguished:

a) In case of a handover to a UTRAN controlled by the same MSC/VLR, UMTS cipher/integrity keys CK and IK are derived from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and sent to the target RNC.

b) In case of a handover to a UTRAN controlled by another MSC/VLR, the initial MSC/VLR (R99+ or R98-) sends the stored GSM cipher key Kc to the new MSC/VLR controlling the target RNC. That MSC/VLR derives UMTS cipher/integrity keys CK and IK which are then forwarded to the target RNC. The initial MSC/VLR remains the anchor point for throughout the service.

At the user side, in either case, the ~~UE~~ME derives the UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and applies them.

## 6.8.6 Intersystem change for PS Services – from UTRAN to GSM BSS

### 6.8.6.1 UMTS security context

A UMTS security context in UTRAN is only established for UMTS subscribers. At the network side, three cases are distinguished:

a) In case of an intersystem change to a GSM BSS controlled by the same SGSN, the SGSN derives the GSM cipher key Kc from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and applies it.

b) In case of an intersystem change to a GSM BSS controlled by another R99+ SGSN, the initial SGSN sends the stored UMTS cipher/integrity keys CK and IK to the new SGSN. The new SGSN stores the keys, derives the GSM cipher key Kc and applies the latter. The new SGSN becomes the new anchor point for the service.

c) In case of an intersystem change to a GSM BSS controlled by a R98- SGSN, the initial SGSN derives the GSM cipher key Kc and sends the GSM cipher key Kc to the new SGSN. The new SGSN stores the GSM cipher key Kc and applies it. The new SGSN becomes the new anchor point for the service.

At the user side, in all cases, the ~~UE~~ME applies the derived GSM cipher key Kc received from the USIM during the last UMTS AKA procedure.

#### 6.8.6.2 GSM security context

A GSM security context in UTRAN is only established for GSM subscribers. At the network side, two cases are distinguished:

a) In case of an intersystem change to a GSM BSS controlled by the same SGSN, the SGSN starts to apply the stored GSM cipher key Kc.

b) In case of an intersystem change to a GSM BSS controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the BSC. The new SGSN stores the key and applies it. The new SGSN becomes the new anchor point for the service.

At the user side, in both cases, the ~~UE~~ME applies the GSM cipher key Kc that is stored.

### 6.8.7 Intersystem change for PS services – from GSM BSS to UTRAN

#### 6.8.7.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with ~~R99+ UE~~R99+ ME connected to a R99+ VLR/SGSN. At the network side, two cases are distinguished:

a) In case of an intersystem change to a UTRAN controlled by the same SGSN, the stored UMTS cipher/integrity keys CK and IK are sent to the target RNC.

b) In case of an intersystem change to a UTRAN controlled by another SGSN, the initial SGSN sends the stored UMTS cipher/integrity keys CK and IK to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. The new SGSN then stores the UMTS cipher/integrity keys CK and IK and sends them to the target RNC.

At the user side, in both cases, the ~~UE~~ME applies the stored UMTS cipher/integrity keys CK and IK.

#### 6.8.7.2 GSM security context

A GSM security context in GSM BSS can be either:

- **Established for a UMTS subscriber**

  A GSM security context for a UMTS subscriber is established in case the user has a ~~R98- UE~~R98- ME, where intersystem change to UTRAN is not possible, or in case the user has a R99+~~UE~~ME but the SGSN is R98-, where intersystem change to UTRAN implies a change to a R99+ SGSN.

  As result, in case of intersystem change to a UTRAN controlled by another R99+ SGSN, the initial R98- SGSN sends the stored GSM cipher key Kc to the new SGSN controlling the target RNC.

  Since the new R99+ SGSN has no indication of whether the subscriber is GSM or UMTS, a R99+ SGSN shall perform a new UMTS AKA when receiving Kc from a R98- SGSN. A UMTS security context using fresh quintuplets is then established between the R99+ SGSN and the USIM. The new SGSN becomes the new anchor point for the service.

  At the user side, new keys shall be agreed during the new UMTS AKA initiated by the R99+ SGSN.

- **Established for a GSM subscriber**

Handover from GSM BSS to UTRAN for GSM subscriber is only possible with R99+ UER99+ ME. At the network side, three cases are distinguished:

a) In case of an intersystem change to a UTRAN controlled by the same SGSN, the SGSN derives UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and sends them to the target RNC.

b) In case of an intersystem change from a R99+ SGSN to a UTRAN controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. The new SGSN stores the GSM cipher key Kc and derives the UMTS cipher/integrity keys CK and IK which are then forwarded to the target RNC.

c) In case of an intersystem change from an R98-SGSN to a UTRAN controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. To ensure use of UMTS keys for a possible UMTS subscriber (superfluous in this case), a R99+ SGSN will perform a new AKA when a R99+UEME is coming from a R98-SGSN.

At the user side, in all cases, the UEME derives the UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and applies them. In case c) these keys will be over-written with a new CK, IK pair due to the new AKA.

## 7.6 Distribution of security parameters to UTRAN

Confidentiality and integrity between the user and the network is handled by the ~~UE~~ME/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.