Leliwa Technical Bulletin

UMTS Security

Date: 20.11.2009

Revision: 008/UMS/009

Author: Jakub Bluszcz

LELIWA

Table of contents

Introduction

This document describes 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.

UMTS offers the following security features (see Fig. 1):

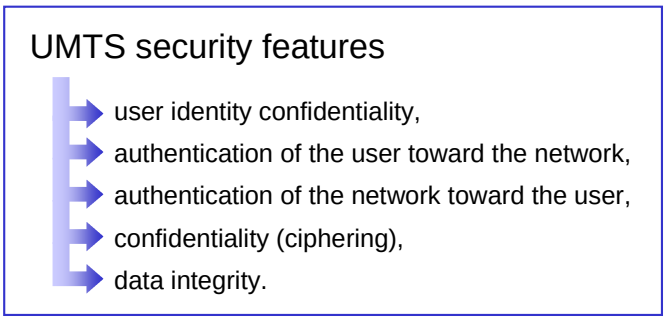

Figure 1 UMTS security features

As in GSM/GPRS, user (temporary) identification, authentication and key agreement takes place independently in each service domain. User plane traffic is ciphered using the cipher key agreed for the corresponding service domain while control plane data is ciphered and integrity protected using the cipher and integrity keys from either one of the service domains.

User identity confidentiality

The permanent user identity (IMSI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link. To achieve this, the user is normally identified by a temporary identity by which he is known by the visited serving network.

This mechanism allows the identification of a user on the radio access link by means of a Temporary / Packet-Temporary Mobile Subscriber Identity (TMSI/P-TMSI). A TMSI / P-TMSI has local significance only in the Location Area (LA) or Routing Area (RA) in which the user is registered. Outside that area it is accompanied by an appropriate Location Area Identification (LAI) or Routing Area Identification (RAI) in order to avoid ambiguities. The association between the permanent and temporary user identities is kept by the VLR/SGSN in which the user is registered.

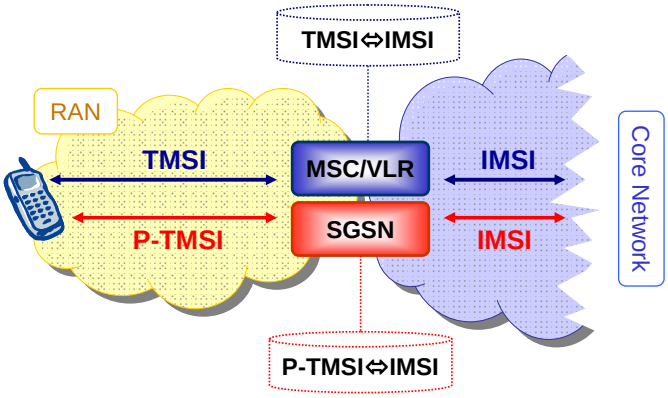

Figure 2 User identity confidentiality

The TMSI / P-TMSI, when available, is normally used to identify the user on the radio access path, for instance in paging requests, location update requests, attach requests, service requests, connection re-establishment requests and detach requests.

To avoid user traceability, which may lead to the compromise of user identity confidentiality, the user is not identified for a long period by means of the same temporary identity. In addition any signalling or user data that might reveal the user's identity is ciphered on the radio access link.

If a TMSI provided by an MS is unknown in the network e.g. due to a data base failure, the network requires the MS to provide its IMSI. In this case the identification procedure is used before the TMSI reallocation procedure is initiated.

The reallocation of a TMSI can be performed either by a unique procedure described in the next section or implicitly by a location updating procedure.

TMSI reallocation procedure

The purpose of the TMSI reallocation procedure is to allocate a new TMSI/LAI pair to a user by which he may subsequently be identified on the radio access link. The procedure is performed after the initiation of ciphering. The allocation of a temporary identity is illustrated in Fig. 3.

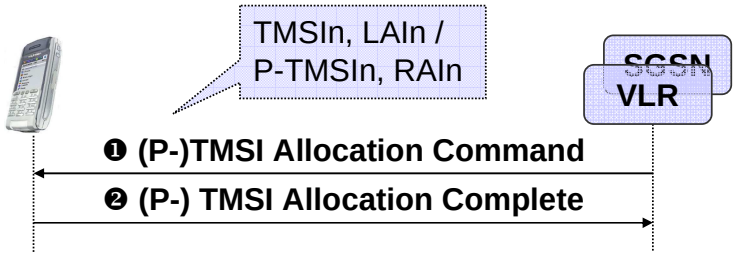

Figure 3 TMSI allocation

❶ The VLR generates a new temporary identity (TMSIn) and stores the association of TMSIn and the permanent identity IMSI in its database. The VLR then sends the TMSIn and optionally the new location area identity LAIn to the user. Upon receipt the user stores TMSIn and automatically removes the association with any previously allocated TMSI.

❷ The user sends an acknowledgement back to the VLR. Upon receipt of the acknowledgement the VLR removes the association with the old temporary identity TMSIo and the IMSI (if there was any) from its database.

Distribution of IMSI and authentication data

In case a user identifies itself using a TMSIo/LAIo pair that was not assigned by the visited VLRn and the visited VLRn and the previously visited VLRo exchange authentication data, the visited VLRn request the previously visited VLRo to send the permanent user identity and optionally temporary authentication data.

If the previously visited VLRo cannot be contacted or cannot retrieve the user identity, the visited VLRn requests the user to identify itself by means of its permanent user identity.

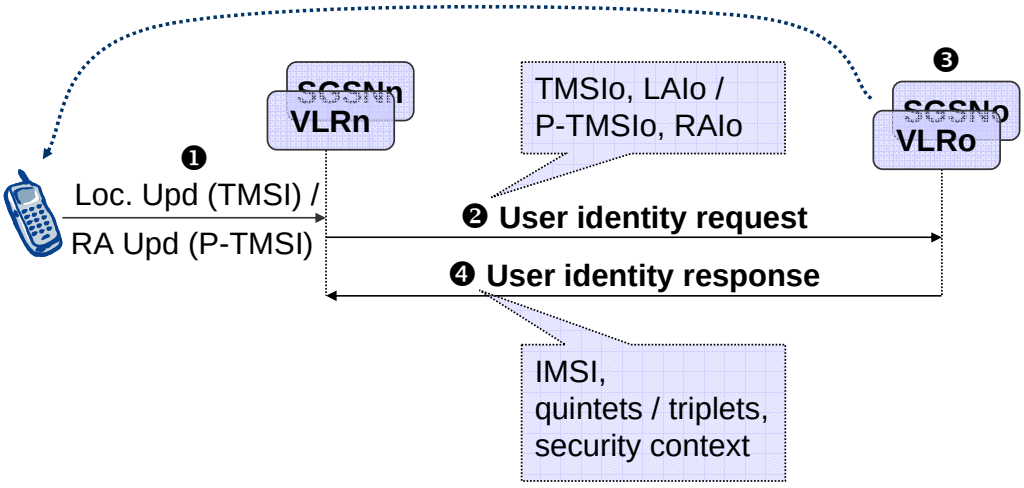

Figure 4 Distribution of IMSI between VLRs / SGSNs

❶ The procedure is invoked by the newly visited VLRn/SGSNn after the receipt of a *Location update request* / *Routing area update* request from the user wherein the user is identified by means of a temporary user identity TMSIo/P-TMSIo and the location area identity LAIo / routing area identity RAIo under the jurisdiction of a previously visited VLRo/SGSNo that belongs to the same serving network domain as the newly visited VLRn/SGSNn.

❷ The VLRn/SGSNn sends a *User identity request* to the VLRo/SGSNo, this message contains TMSIo and LAIo / P-TMSIo and RAIo.

❸ The VLRo/SGSNo searches the user data in the database. If the user is found, the VLRo/SGSNo sends a *user identity response* back that:

- includes the IMSI
- may include a number of unused authentication vectors (quintets or triplets),
- may include the current security context data: CK, IK and KSI (UMTS) or Kc and CKSN (GSM).

If the user cannot be identified the VLRo/SGSNo sends a *User identity response* indicating that the user identity cannot be retrieved.

❹ If the VLRn/SGSNn receives a *User identity response* with an IMSI, it creates an entry and stores any authentication vectors and any data on the current security context.

If the VLRn/SGSNn receives a *User identity response* indicating that the user could not be identified, it initiates the user identification procedure described in the next section.

Identification by a permanent identity

The mechanism is invoked whenever the user cannot be identified by means of a temporary identity. In particular, it is used when the user registers for the first time in a serving network, or when the serving network cannot retrieve the IMSI from the TMSI / P-TMSI by which the user identifies itself on the radio path.

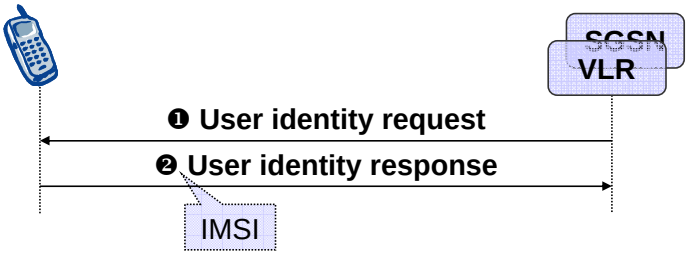

Figure 5 Identification by the permanent identity

❶ The mechanism is initiated by the visited VLR/SGSN that requests the user to send its permanent identity.

❷ The user's response contains the IMSI in clear text. This represents a breach in the provision of user identity confidentiality.

Entity authentication

Two security features related to entity authentication are provided:

- **user authentication:** the property that the serving network corroborates the user identity of the user,
- **network authentication:** the property that the user corroborates that he is connected to a serving network that is authorised by the user's HE to provide him services; this includes the guarantee that this authorisation is recent.

The entity authentication occurs at each connection set-up between the user and the network. Two mechanisms have been included: an authentication mechanism using an authentication vector delivered by the user's HE to the serving network, and a local authentication mechanism using the integrity key established between the user and serving network during the previous execution of the authentication and key establishment procedure.

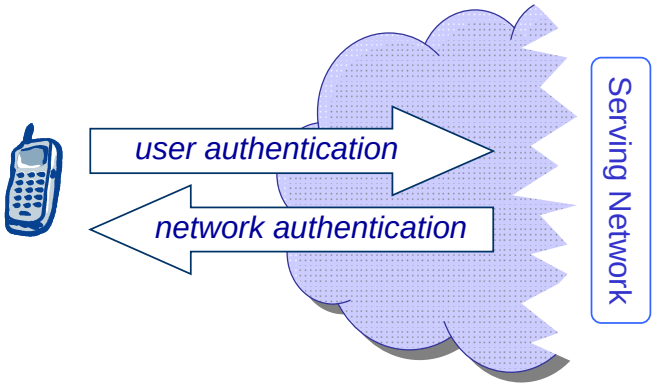

Figure 6 Entity authentication

Authentication and key agreement

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 SQN_{MS} and SQN_{HE} respectively to support network authentication. The sequence number SQN_{HE} is an individual counter for each user and the sequence number SQN_{MS} denotes the highest sequence number the USIM has accepted.

The method was chosen in such a way as to achieve maximum compatibility with the 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.

An overview of the mechanism is shown in Fig. 7.

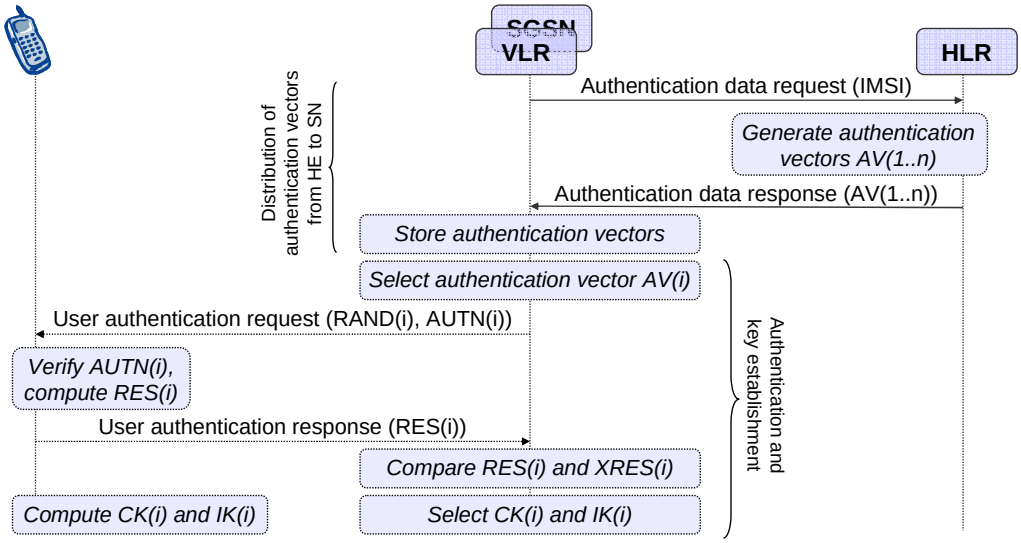

Figure 7 Authentication and key agreement

The *Authentication data request* includes the IMSI and the requesting node type (PS or CS). Upon receipt of a request from the VLR/SGSN, the HE/AuC sends an ordered array of *n* authentication vectors AV(1..n), (the equivalent of a GSM 'triplet') to the VLR/SGSN. The authentication vectors are ordered based on sequence number. 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 ordered array and sends the parameters RAND and AUTN to the user. Authentication vectors in a particular node are used on an FIFO basis. 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.

Generation of authentication vectors

Fig. 8 shows the generation of an authentication vector AV by the HE/AuC.

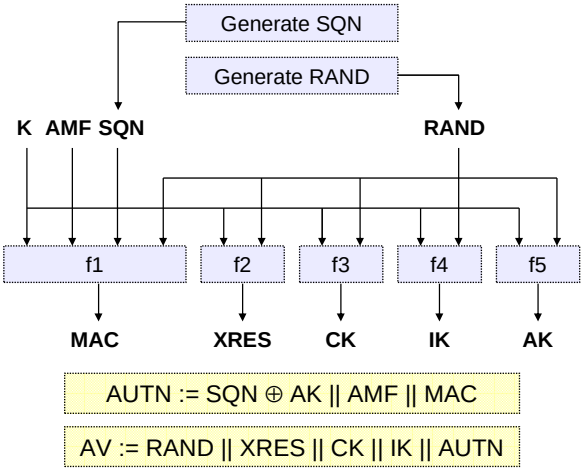

Figure 8 Generation of authentication vectors

The HE/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND. For each user the HE/AuC keeps track of a counter SQN_{HE}.

Subsequently the following values are computed:

- a **Message Authentication Code MAC** = $f1_K$(SQN || RAND || AMF) where f1 is a message authentication function;
- an **eXpected RESponse XRES** = $f2_K$ (RAND) where f2 is a message authentication function;
- a **Cipher Key CK** = $f3_K$ (RAND) where f3 is a key generating function;
- an **Integrity Key IK** = $f4_K$ (RAND) where f4 is a key generating function;
- an **Anonymity Key AK** = $f5_K$ (RAND) where f5 is a key generating function or f5 ≡ 0.

Finally the authentication token AUTN = SQN ⊕ AK || AMF || MAC is constructed.

AK is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user. The concealment of the sequence number is to protect against passive attacks only.

An authentication and key management field AMF is included in the authentication token of each authentication vector. Example uses of AMF includes:

- support multiple authentication algorithms and keys (This mechanism is useful for disaster recovery purposes. AMF may be used to indicate the algorithm and key used to generate a particular authentication vector.)
- changing sequence number verification parameters (This mechanism is used to change dynamically the limit on the difference between the highest SEQ accepted so far and a received sequence number SEQ.)
- setting threshold values to restrict the lifetime of cipher and integrity keys (The USIM contains a mechanism to limit the amount of data that is protected by an access link key set. The AMF field may be used by the operator to set or adjust this limit in the USIM).

Fig. 9 shows the summary of all authentication parameters.

	Parameter name	**Length**
K	authentication Key	128 bits
RAND	RANDom challenge	128 bits
SQN	SeQuence Numbers	48 bits
AK	Anonymity Key	48 bits
AMF	Authentication Management Field	16 bits
MAC	Message Authentication Code	64 bits
MAC-S	Message Authentication Code	64 bits
CK	Cipher Key	128 bits
IK	Integrity Key	128 bits
RES	authentication RESponse	var. 4-16 octets

Figure 9 Authentication parameters

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.

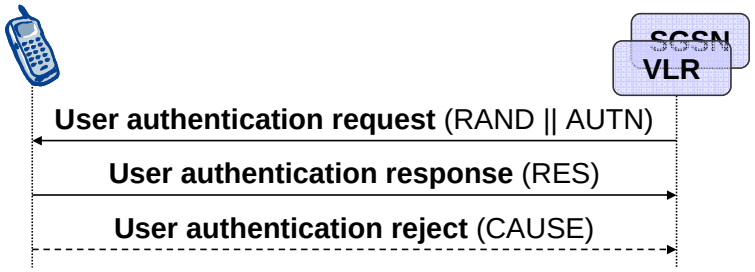

Figure 10 Authentication and key establishment

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

Upon receipt the user proceeds as shown in Fig. 11.

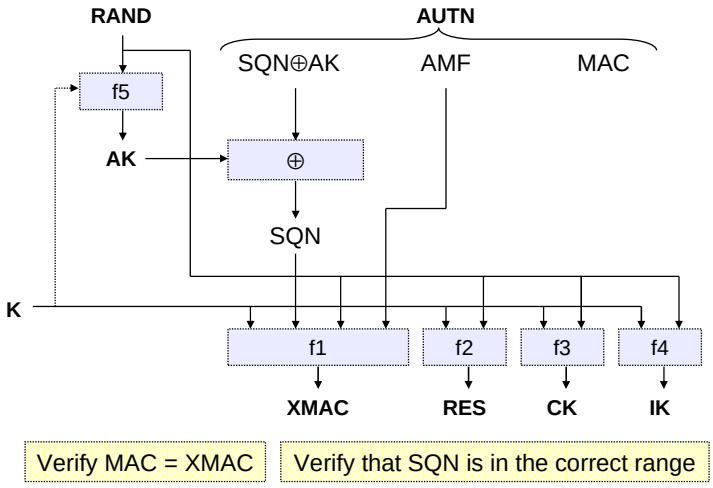

Figure 11 User authentication function in the USIM

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 initiates an *Authentication failure report* procedure towards the HLR. 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 correct, 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).

If the USIM also supports conversion function c3, it derives the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK.

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 initiates an *Authentication failure report* procedure towards the HLR and may also decide to initiate a new identification and authentication procedure towards the user.

Sequence numbers

The verification of the SQN by the USIM will cause the MS to reject an attempt by the VLR/SGSN to re-use a quintet to establish a particular UMTS security context more than once. In general therefore the VLR/SGSN can use a quintet only once.

The mechanisms for verifying the freshness of sequence numbers in the USIM to some extent allows the out-of-order use of sequence numbers. This is to ensure that the authentication failure rate due to synchronisation failures is sufficiently low. This requires the capability of the USIM to store information on past successful authentication events (e.g. sequence numbers). The mechanism ensures that a sequence number can still be accepted if it is among the last x = 32 sequence numbers generated. The same minimum number x needs to be used across the systems to guarantee that the synchronisation failure rate is sufficiently low under various usage scenarios, in particular simultaneous registration in the CS- and the PS-service domains and user movement between VLRs/SGSNs which do not exchange authentication information.

If the USIM considers the sequence number to be not in the correct range, it sends *Synchronisation failure* back to the VLR/SGSN and abandons the procedure, see Fig. 12.

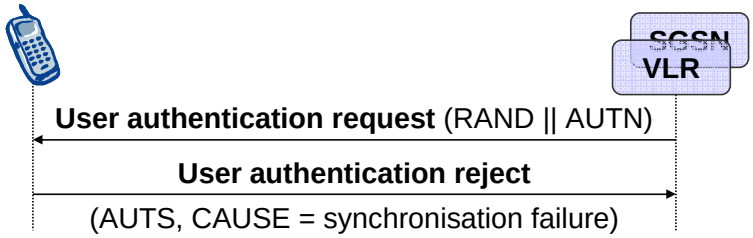

Figure 12 Synchronisation failure

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

The construction of the parameter AUTS in shown in the Fig. 13.

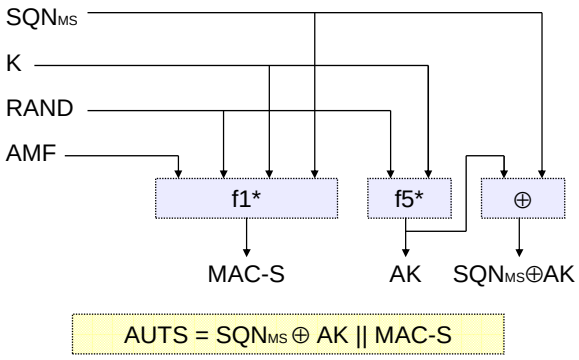

Figure 13 Construction of the parameter AUTS

Re-synchronisation procedure

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

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
- *AUTS* received by the VLR/SGSN in the response to that request,

When the HE/AuC receives an *authentication data request* with a '*synchronisation failure indication*" it retrieves SQN_{MS} from Conc(SQN_{MS}) by computing Conc(SQN_{MS}) ⊕ $f5^*_K(RAND)$ and checks if SQN_{HE} is in the correct range, i.e. if the next sequence number generated SQN_{HE} using would be accepted by the USIM.

If SQN_{HE} is in the correct range then the HE/AuC sends an *authentication data response* with a new batch of authentication vectors to the VLR/SGSN.

Otherwise it verifies *AUTS* and if the verification is successful the HE/AuC resets the value of the counter SQN_{HE} to SQN_{MS}.

Whenever the VLR/SGSN receives a new batch of authentication vectors it deletes the old ones for that user in the VLR/SGSN and the user may now be authenticated based on a new authentication vector.

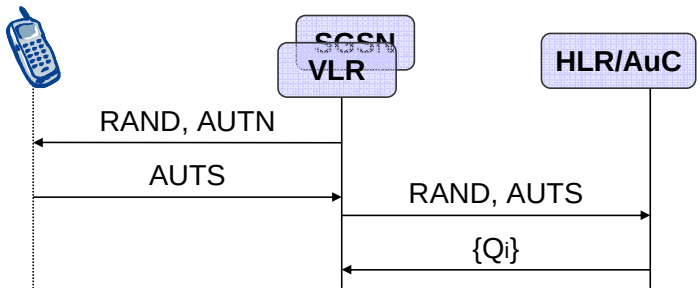

Figure 14 Re-synchronisation mechanism

Reporting authentication failures

The purpose of this procedure is to provide a mechanism for reporting authentication failures from the serving environment back to the home environment, see Fig. 15.

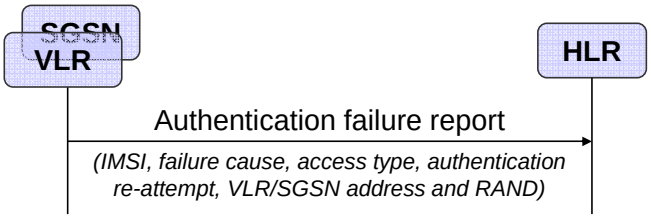

Figure 15 Reporting authentication failure from VLR/SGSN to HLR

The procedure is invoked by the serving network VLR/SGSN when the authentication procedure fails. The *Authentication failure report* contains among other parameters: subscriber identity, failure cause code (wrong network signature / wrong user response), VLR/SGSN address and RAND.

The HE may cancel the location of the user after receiving an *authentication failure report* and stores the received data so that further processing to detect possible fraud situations could be performed.

Confidentiality

Four security features related to confidentiality are provided:

- **cipher algorithm agreement** (MS and the SN securely negotiate the algorithm that they use subsequently),
- **cipher key agreement** (MS and the SN agree on a cipher key that they use subsequently),
- **confidentiality of user data** (user data cannot be overheard on the radio access interface),
- **confidentiality of signalling data** (signalling data cannot be overheard on the radio access interface).

Cipher key and integrity key setting

Authentication and key setting are triggered by the authentication procedure described earlier in this chapter. 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 and separately for PS domain are stored on the USIM and updated at the next authentication from each domain.

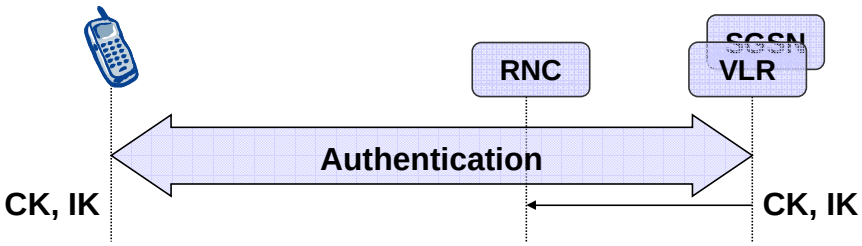

Figure 16 Cipher key and integrity key setting

Ciphering and integrity mode negotiation

When an MS wishes to establish a connection with the network, the MS indicates to the network in the MS/USIM Classmark which cipher and integrity algorithms the MS supports. This information itself is 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.

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 MS 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 MS 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 and a value of '111' is used by the MS to indicate that a valid key is not available for use).

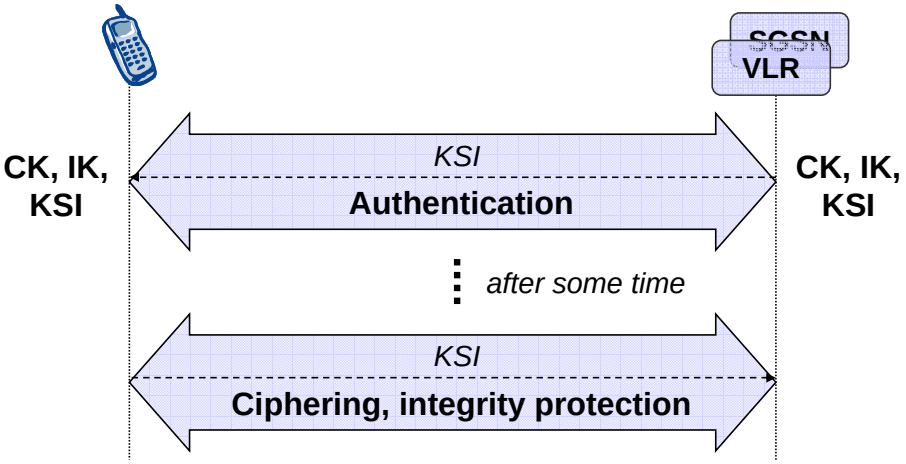

Figure 17 Cipher key and integrity key identification

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. The USIM therefore contains a mechanism to limit the amount of data that is protected by an access link key set.

The lifetime of cipher and integrity keys is limited by *THRESHOLD* values that can be set or adjust by the operator and send to the USIM inside AMF field of the authentication vector.

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.

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

The ciphering sequence number COUNT-C and integrity sequence number COUNT-I are both 32 bits long. The ME and the RNC initialise the 20 most significant bits of the COUNT-C and OUNT-I to the current value of START and the remaining bits to zero at the start of ciphering. Than the COUNT-C and COUNT-I is incremented at each RLC cycle.

During authentication and key agreement the START value associated with the new key set of the corresponding service domain is set to 0 in the USIM and in the ME.

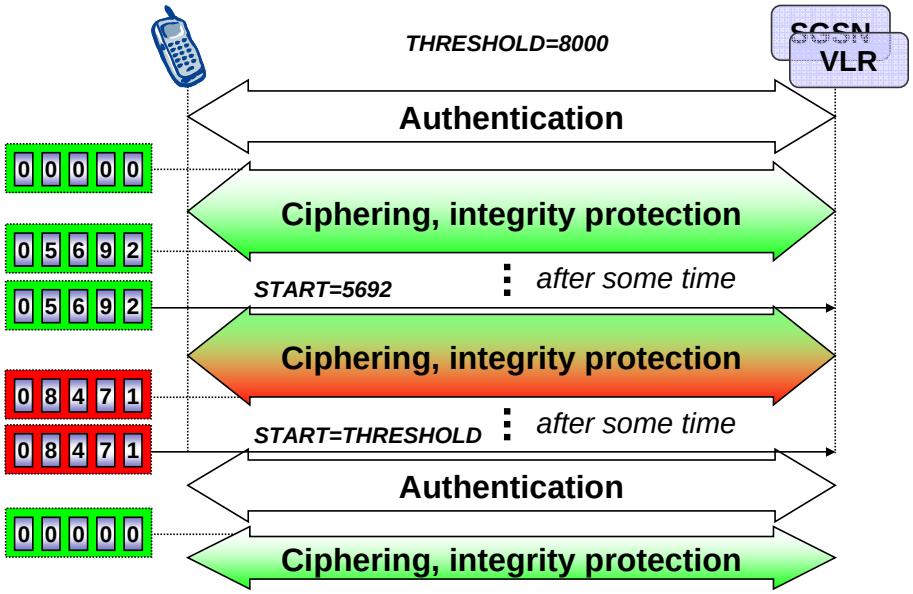

Figure 18 Cipher key and integrity key lifetime

Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up.

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

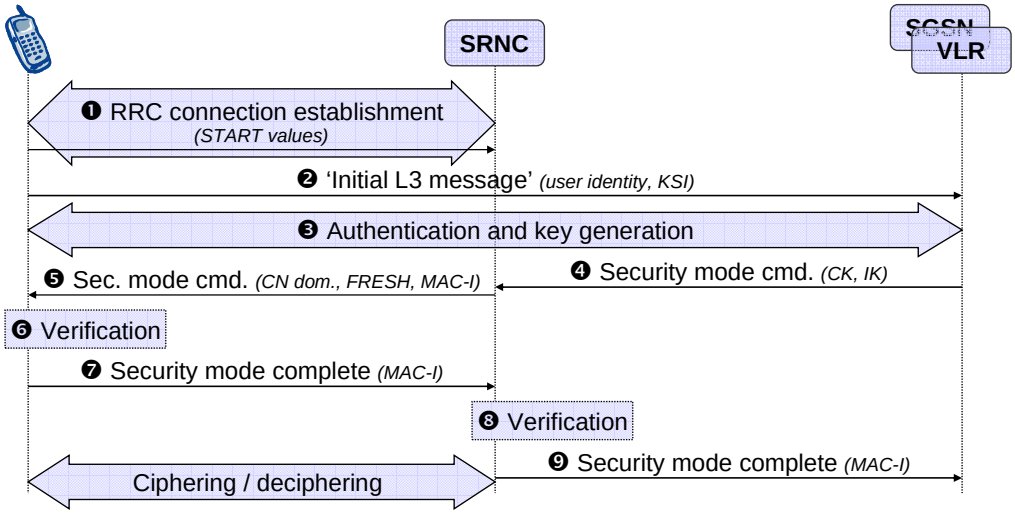

Figure 19 Local authentication and connection set-up

❶ RRC connection establishment includes the transfer from MS to RNC of the ciphering capabilities (UEAs) and the integrity capabilities (UIAs) of the MS. Optionally the GSM Classmarks 2 and 3 and the START values for the CS/PS service domain are included. The START values and the UE security capability information are stored in the SRNC.

❷ The MS sends the Initial L3 message (*Location update request, CM service request, Routing area update request, Attach request, Paging response etc.*) to the VLR/SGSN. This message contains the user identity and the KSI.

❸ User identity request, authentication of the user and generation of new security keys (IK and CK) may be performed. A new KSI will then also be allocated.

❹ The VLR/SGSN initiates integrity and ciphering by sending the RANAP message *Security Mode Command* to SRNC that contains the IK and CK to be used. If a new authentication and security key generation has been performed, this is indicated in the message sent to the SRNC. The indication of new generated keys implies that the START value is to be reset at start use of the new keys. Otherwise, it is the START value already available in the SRNC that is used.

❺ The SRNC generates the RRC message *Security mode command*. The message includes the random value FRESH to be used for integrity protection. Because of that the MS can have two ciphering and integrity key sets, the network must indicate which key set to use. This is obtained by including a CN type indicator information in the *Security 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.

❻ The MS computes XMAC-I on the message received by using the 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.

❼ The MS compiles the RRC message *Security mode complete* and generates the MAC-I for this message. If verification is not successful, the procedure ends in the MS.

❽ 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.

❾ The transfer of the RANAP message *Security mode complete* from SRNC to the VLR/SGSN ends the procedure.

The Security mode command to MS starts the downlink integrity protection, i.e. this and all following downlink messages sent to the MS are integrity protected using the new integrity configuration. The Security mode complete from MS starts the uplink integrity protection, i.e. this and all following messages sent from the MS are integrity protected using the new integrity configuration. When ciphering shall be started, the Ciphering Activation time information that is exchanged between SRNC and MS during the Security mode set-up procedure sets the RLC Sequence Number/Connection Frame Number when to start ciphering in Downlink respective Uplink using the new ciphering configuration.

Ciphering method

Fig. 20 illustrates the use of the ciphering algorithm f8 to encrypt plaintext by applying a keystream using a bit per bit binary addition of the plaintext and the keystream. The plaintext may be recovered by generating the same keystream using the same input parameters and applying a bit per bit binary addition with the ciphertext.

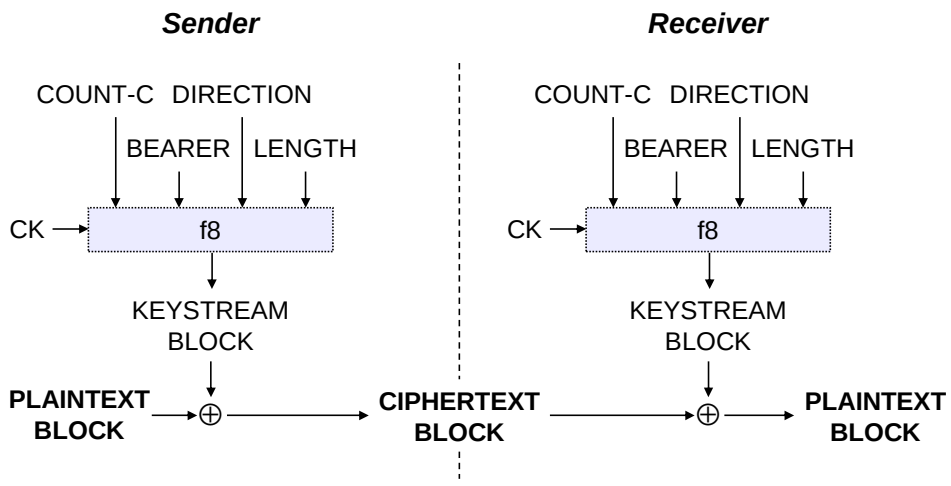

Figure 20 Ciphering of user and signalling data

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.

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

The DIRECTION identifier is input to avoid that for the keystreams for the up-link and for the down-link would use the identical set of input parameter values.

The LENGTH indicator determines the length of the required keystream block.

There is one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user. The radio bearers for CS user data are ciphered with CK_{CS}. The radio bearers for PS user data are ciphered with CK_{PS}. The signalling radio bearers are used for transfer of signalling data for services delivered by both CS and PS service domains. These signalling radio bearers are ciphered by the CK of the service domain for which the most recent security mode negotiation took place.

Data integrity

Three security features related to data integrity are provided:

- **integrity algorithm agreement** (the MS and the SN securely negotiate the integrity algorithm that they use subsequently),
- **integrity key agreement** (the MS and the SN agree on an integrity key that they use subsequently),
- **data integrity and origin authentication of signalling data** (the property that the receiving entity (MS or SN) is able to verify that signalling data has not been modified in an unauthorised way since it was sent by the sending entity (SN or MS) and that the data origin of the signalling data received is indeed the one claimed).

Integrity key agreement and integrity algorithm agreement is realised by means of a mechanism that are described earlier in this chapter.

Data integrity protection method

Fig. 21 illustrates the use of the integrity algorithm f9 to authenticate the data integrity of a signalling message.

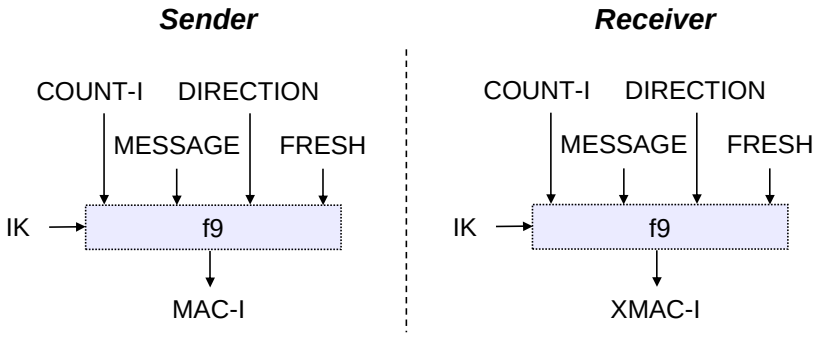

Figure 21 Derivation of MAC-I (or XMAC-I) on a signalling message

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.

The network-side nonce **FRESH** is 32 bits long. 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.

There may be one **IK** for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user. The data integrity of radio bearers for user data is not protected. The signalling radio bearers are used for transfer of signalling data for services delivered by both CS and PS service domains. These signalling radio bearers are data integrity protected by the IK of the service domain for which the most recent security mode negotiation took place.

The rest of the input parameters have exactly the same meaning as for algorithm for ciphering described in the previous section.

Unsuccessful integrity check

The supervision of failed integrity checks is 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 is discarded.

UMTS – GSM interoperation

UMTS subscriber connected to GSM BSS

UMTS AKA is applied when the user is attached to a GSM BSS, in case the user has a ME capable of UMTS AKA 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.

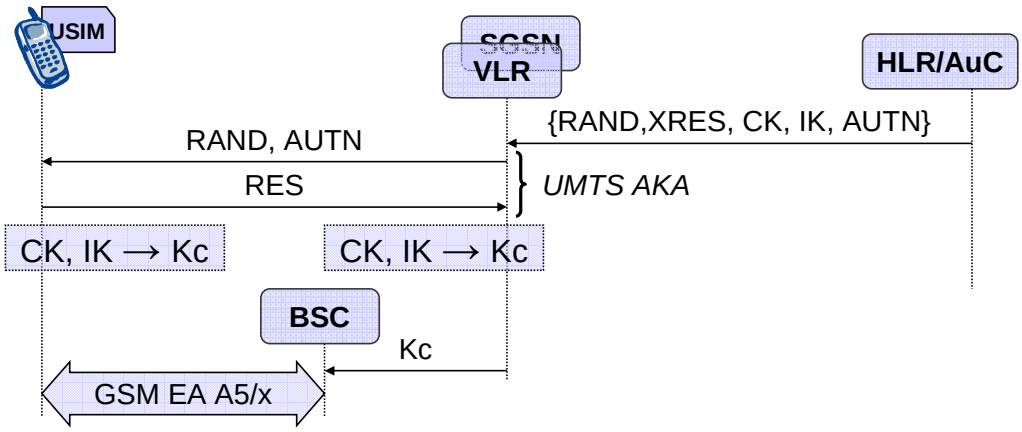

Figure 22 User attached to GSM BSS with UMTS AKA capable ME (VLR/SGSN R99+)

GSM AKA is applied when the user is attached to a GSM BSS, in case the user has a ME not capable of UMTS AKA. 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.

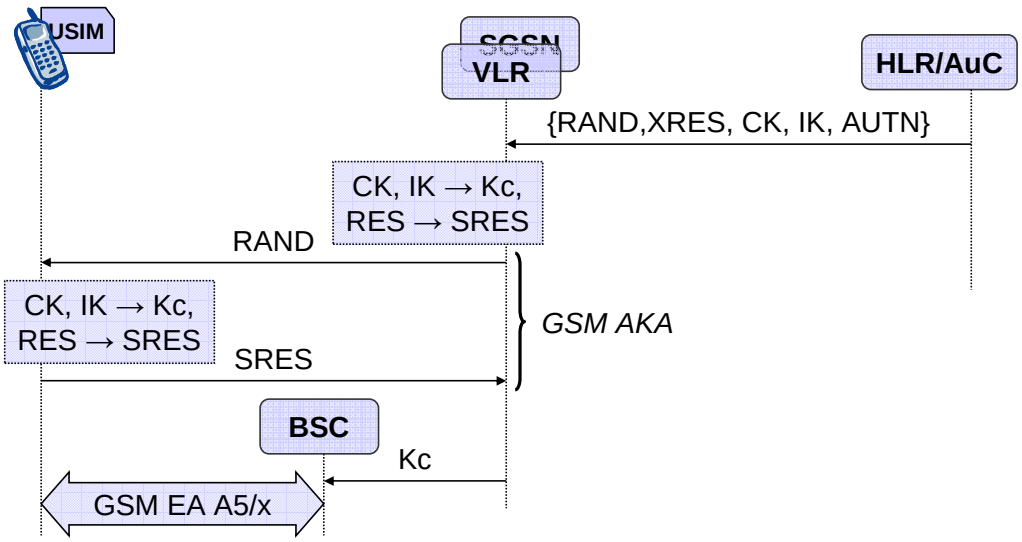

Figure 23 User attached to GSM BSS with UMTS AKA non-capable ME (VLR/SGSN R99+)

GSM AKA is 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.

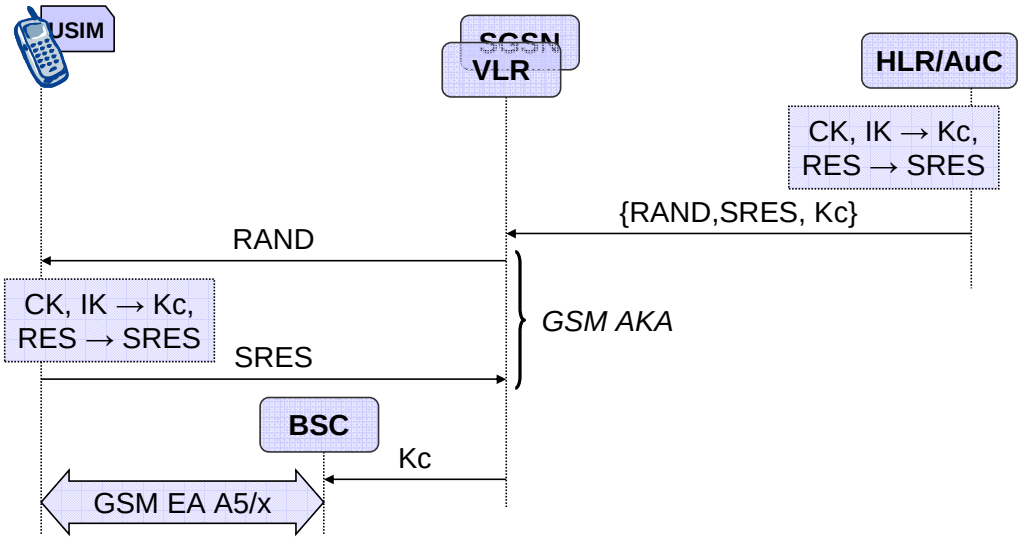

Figure 24 User attached to GSM BSS (VLR/SGSN R99-)

Fig. 25 shows the different scenarios that can occur with UMTS subscribers in a mixed network architecture.

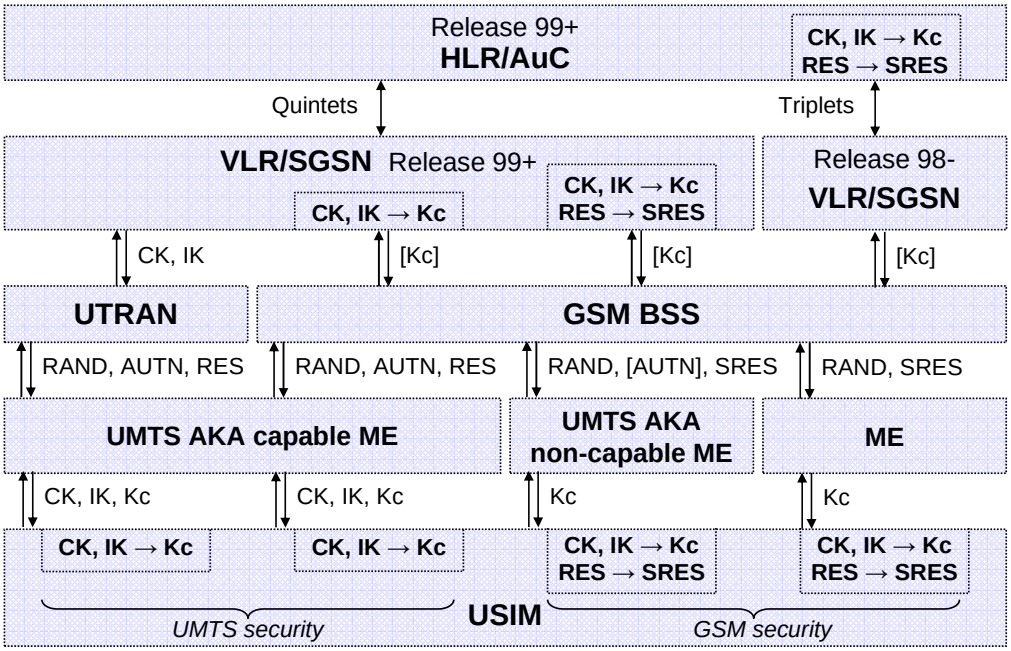

Figure 25 Authentication and key agreement of UMTS subscribers

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.

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

c2: $SRES_{[GSM]} = XRES^*_1 \oplus XRES^*_2 \oplus XRES^*_3 \oplus XRES^*_4$

c3: $Kc_{[GSM]} = CK_1 \oplus CK_2 \oplus IK_1 \oplus IK_2$

XRES* is 16 octets long and XRES* = XRES if XRES is 16 octets long and XRES* = XRES || 0...0 if XRES is shorter than 16 octets,

XRES*i are all 4 octets long and XRES* = XRES*1 || XRES*2 || XRES*3 || XRES*4,

CKi and IKi are both 64 bits long and CK = CK1 || CK2 and IK = IK1 || IK2.

Figure 26 Conversion functions

GSM subscribers connected to UTRAN

For GSM subscribers, GSM AKA is always used. When in an UTRAN, the UMTS CK and IK are derived from the GSM cipher key Kc by the ME and the VLR/SGSN, both R99+ entities.

Fig. 28 shows the different scenarios that can occur with GSM subscribers using either R98- or R99+ ME in a mixed network architecture.

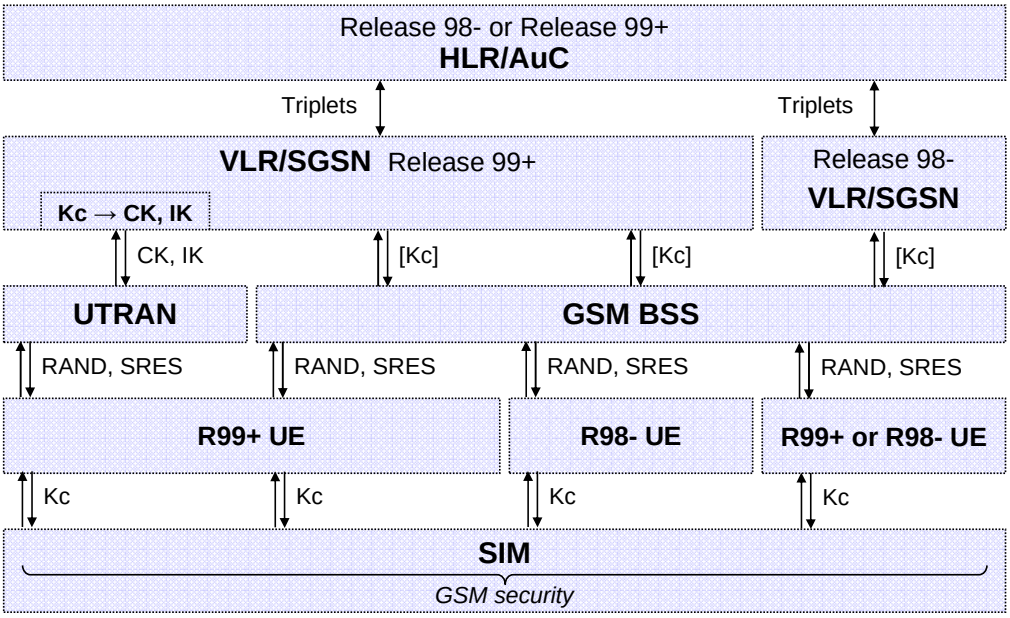

Fig 27 Authentication and key agreement for GSM subscribers

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:

c4: $CK_{[UMTS]}$ = Kc || Kc

c5: $IK_{[UMTS]}$ = $Kc_1 \oplus Kc_2$ || Kc || $Kc_1 \oplus Kc_2$

Kc_i are both 32 bits long and Kc = Kc1 || Kc2

Figure 28 Conversion functions

CS handover (UTRAN to GERAN)

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 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.

At the network side the MSC/VLR derives the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK used before the intersystem handover

(using the conversion function c3) and sends Kc to the target BSC (which forwards it to the BTS).

At the user side, the ME applies the derived GSM cipher key Kc from the key set which was used before the intersystem handover.

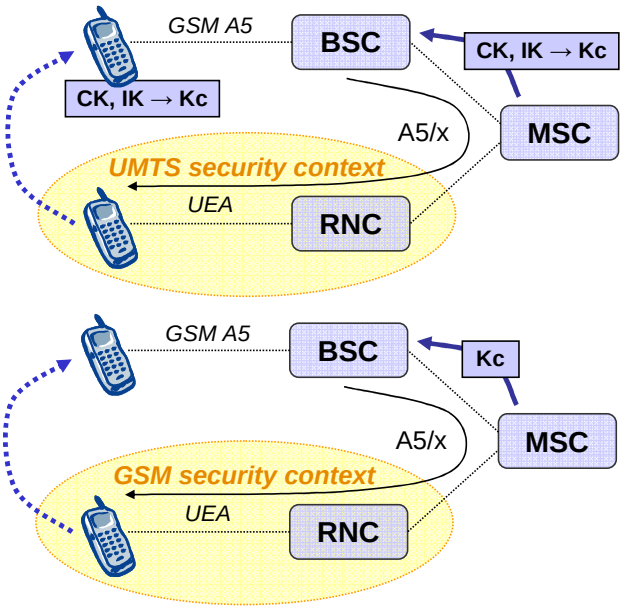

Figure 29 CS handover (UTRAN to GSM BSS)

The conversion is only needed if before the handover the UMTS security context was established (USIM in the ME). The conversion is not needed in case when before the handover the GSM security context was established (SIM in the ME).

CS handover (GERAN to UTRAN)

If ciphering has been started when an intersystem handover occurs from GSM BSS to UTRAN, the necessary information (e.g. CK, IK, START 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 intersystem handover will imply a change of ciphering algorithm from a GSM A5 to a UEA.

The integrity protection of signalling messages is started immediately after the intersystem handover from GSM BSS to UTRAN is completed.

At the network side, the MSC/VLR derives, the UMTS cipher/integrity keys CK and IK from the key set used before the intersystem handover.

At the user side, the ME applies the UMTS cipher/integrity keys CK and IK from the key set which was used before the intersystem handover.

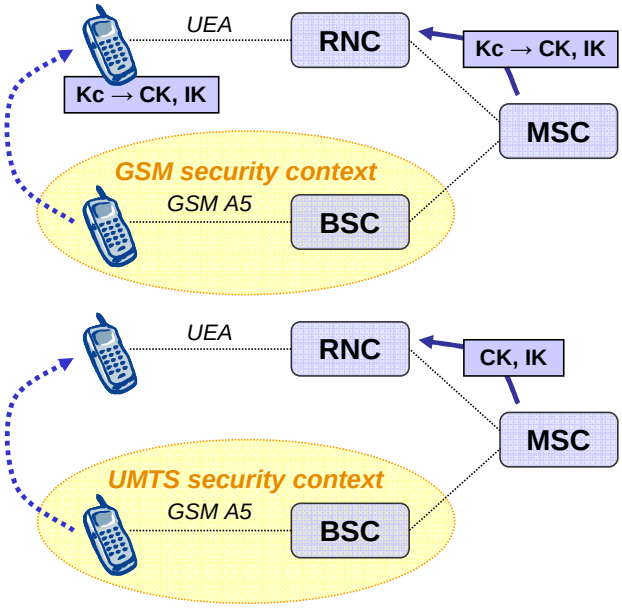

Figure 30 CS handover (GSM BSS to UTRAN)

The conversion is only needed if before the handover the GSM security context was established (e.g. SIM in the ME). The conversion is not needed in case when before the handover the UMTS security context was established (USIM in the ME).

PS system change (UTRAN to GERAN)

In case of an intersystem change to a GSM BSS, the SGSN derives the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK agreed during the latest AKA procedure and applies it.

At the user side, the ME applies the derived GSM cipher key Kc received from the USIM/SIM during the latest AKA procedure.

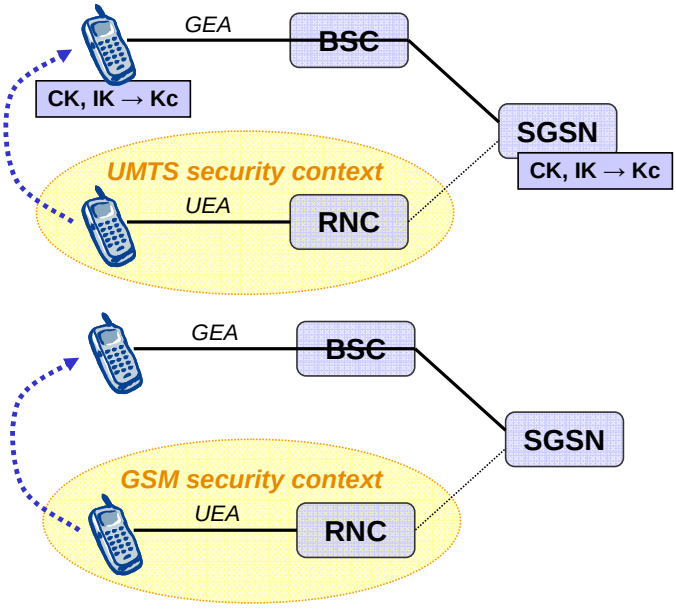

Figure 31 PS system change (UTRAN to GSM BSS)

The conversion is only needed if before the handover the UMTS security context was established (USIM in the ME). The conversion is not needed in case when before the handover the GSM security context was established (SIM in the ME).

PS system change (GERAN to UTRAN)

UMTS security context

In case of an intersystem change to a UTRAN, the SGSN, the UMTS cipher/integrity keys CK and IK agreed during the latest UMTS AKA procedure are sent to the target RNC.

At the user side, in both cases, the ME applies the UMTS cipher/integrity keys CK and IK received from the USIM during the latest UMTS AKA procedure.

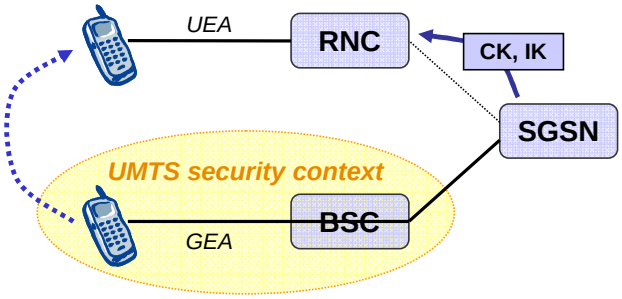

Figure 32 PS system change (GERAN to UTRAN) - UMTS security context

GSM security context

Established for a UMTS subscriber

A GSM security context for a UMTS subscriber is established in case the user has a R99+ ME but the SGSN is R98. As result, in case of intersystem change to a UTRAN controlled by another R99+ SGSN, the initial R98- SGSN sends the GSM Kc agreed during the latest GSM AKA procedure 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 quintets is then established between the R99+ SGSN and the USIM. The new SGSN becomes the new anchor point for the service.

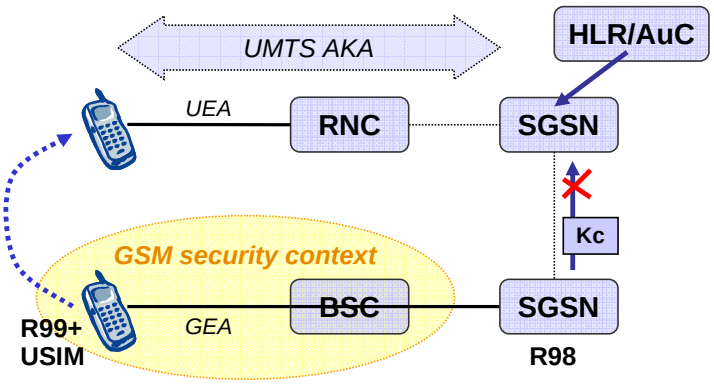

Figure 33 PS system change (GERAN to UTRAN) - GSM security context for UMTS subscriber

Established for a GSM subscriber

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 GSM cipher key Kc (using the conversion functions c4 and c5) agreed during the latest GSM AKA procedure and sends them to the target RNC.

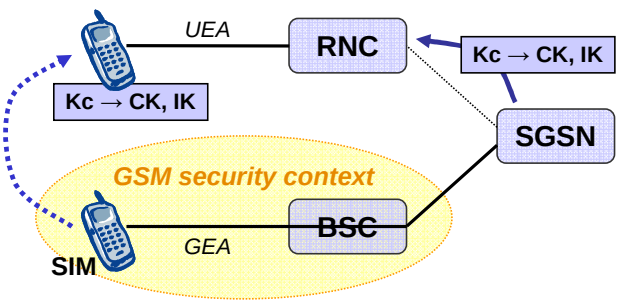

Figure 34 PS system change (GERAN to UTRAN) - GSM security context for GSM subscriber (same SGSN)

b) In case of an intersystem change from a R99+ SGSN to a UTRAN controlled by another SGSN, the initial SGSN sends the GSM Kc agreed during the latest GSM AKA procedure 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.

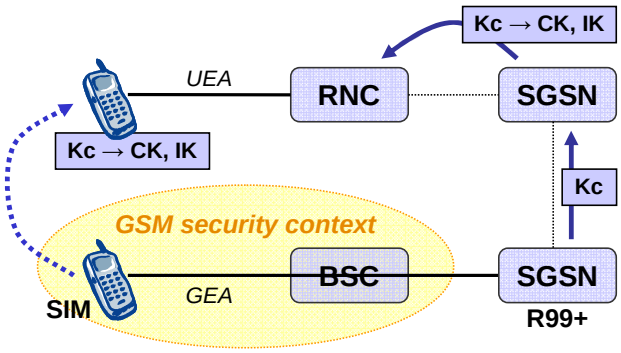

Figure 35 PS system change (GERAN to UTRAN) - GSM security context for GSM subscriber (SGSN R99+ to another SGSN)

c) In case of an intersystem change from an R98- SGSN to a UTRAN controlled by another SGSN, the initial SGSN sends the GSM cipher key Kc agreed during the latest GSM AKA procedure 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+ ME is coming from a R98-SGSN.

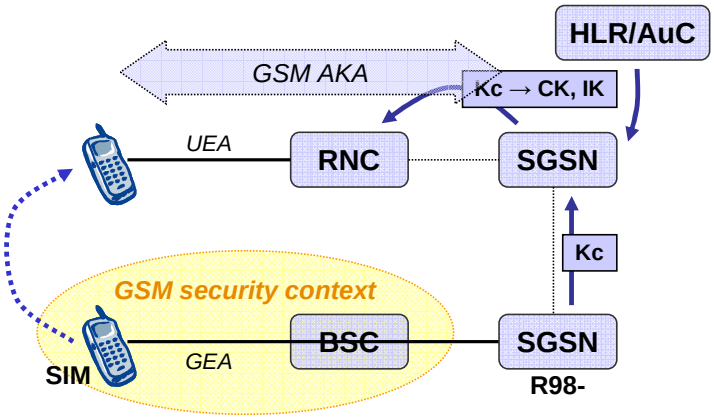

Figure 36 PS system change (GERAN to UTRAN) - GSM security context for GSM subscriber (SGSN R98- to another SGSN)

At the user side, in all cases, the ME derives the UMTS cipher/integrity keys CK and IK from the GSM cipher key Kc (using the conversion functions c4 and c5) received from the SIM during the latest GSM AKA procedure and

applies them. In case c) these keys will be over-written with a new CK, IK pair due to the new AKA.

Acronyms and Abbreviations

3G	Third Generation
AK	Anonymity Key
AKA	Authentication and Key Agreement
AMF	Authentication Management Field
AUC	Authentication Centre
AUTN	AUthentication TokeN
AUTS	Automatic Update Transaction System
AV	Authentication Vector
BSC	Base Station Controller
BSS	Base Station System
BTS	Base Transceiver Station
CK	Ciphering Key
CKSN	Ciphering Key Sequence Number
CN	Core Network
CS	Circuit Switching / Convergence Sublayer / Coding Scheme
FIFO	First In, First Out
GERAN	GSM/EDGE Radio Access Network
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HE	Home Environment
HLR	Home Location Register
IK	Integrity Protection Key
IMSI	International Mobile Subscriber Identity
LA	Location Area / Link Adaptation
LAI	Location Area Identity
MAC	Media Access Control / Message Authentication Code
MAC-I	Message Authentication Code for Integrity
ME	Mobile Equipment
MS	Mobile Station
PS	Packet Switching / Presence Service
P-TMSI	Packet TMSI
RA	Routing Area
RAI	Routing Area Identity
RAN	Radio Access Network
RANAP	RAN Application Part
RAND	Random Number
RES	authentication RESponse
RLC	Radio Link Control

RNC	Radio Network Controller
RRC	Radio Resource Control
SEQ	Sequence Number
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SN	Serving Network / Subscriber Number
SQN	SeQuence Number
SRNC	Serving Radio Network Controller
TMSI	Temporary Mobile Subscriber Identity
UEA	User Encryption Algorithm
UMTS	Universal Mobile Telecommunication System
USIM	UMTS Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access network
VLR	Visitor Location Register
XRES	eXpected RESponse

References

This section contains the locations of various specifications, document references and useful information where you can learn more about this subject.

[1] 33.102 3G security; Security architecture

[2] 25.331 Radio Resource Control (RRC); Protocol specification

[3] 25.321 Medium Access Control (MAC) protocol specification

[4] 25.322 Radio Link Control (RLC) protocol specification

[5] 25.413 UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling

[6] 24.301 Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3

Disclaimer

This document is based on Leliwa training materials.

Information in this document is subject to change without notice. Leliwa assumes no responsibility for any errors that may appear in this document.

This document may be freely redistributed. You can store it on any servers and make it available for public download. In such case it must be clearly indicated that it comes from Leliwa website www.leliwa.com

If you received only this file, you can download more Leliwa Technical Bulletins from the following address:

http://www.leliwa.com/downloads

If you want to be informed when the new bulletins are uploaded, please send a blank e-mail with Subject="Update_request" to bulletins@leliwa.com or click this link: bulletins@leliwa.com

Leliwa Sp. z o.o.

Plebiscytowa 1.122
PL-44-100 Gliwice
Poland
GPS: N50.2981°, E018.6561°

telephone: +48 32 376 63 05
fax: +48 32 376 63 07
Skype: leliwa_poland
email: info@leliwa.com

Leliwa Telecom AB

Orrpelsvägen 66
SE-167 66 BROMMA
Sweden
GPS: N59.3260°, E17.9464°

telephone: +46 8 4459430
email: info@leliwa.com