3GPP TSG SA WG 3 (Security) meeting #11 **S3-000131**
Mainz, Germany, 22-24 February, 2000

DRAFT 3G CHANGE REQUEST

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

33.102 CR 069 Current Version: 3.3.1

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

For submission to TSG		for approval	X	*(only one box should*
list TSG meeting no. here ↑		for information		*be marked with an X)*

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 ☒ UTRAN □ Core Network ☒
(at least one should be marked with an X)

Source: Siemens Atea **Date:** 2000-Feb-20

Subject: Local authentication and connection establishment

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	□

Reason for change:
Re-write 6.4 such that it describes better the signalling procedures and the security features involved in connection set-up and re-authentication during an ongoing connection. At the same time a number of corrections have been made.
The new text includes the changes proposed in Draft CR-058 and Draft CR-059. IT does delete the text that Draft CR-061 proposes to delete. It does not include the changes proposed in Draft CR-060.
This CR proposes when ciphering and integrity protection are started at re-authentication during an on-going connection.

Clauses affected: 6.4

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:

help.doc

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

6.4 Local authentication and connection establishment

6.4.1 General

This clause describes the signalling on the radio link and the security-related functions that are involved when radio connections are established or when authentication and key agreement is performed during an ongoing connection and the newly derived cipher and integrity keys are put into use.

At connection set-up, the security mode negotiation provides local authentication between the user and the service network domain, on the basis of the integrity key IK. Security mode negotiation (and the start of integrity protection) is mandatory, except for the cases detailed in 6.4.2.1.

6.4.2 Scenarios

6.4.2.1 Connection establishment

Figure 6.4.1 provides an overview of the signalling on the radio link and the security-related parameters that may be involved in successful connection establishment.

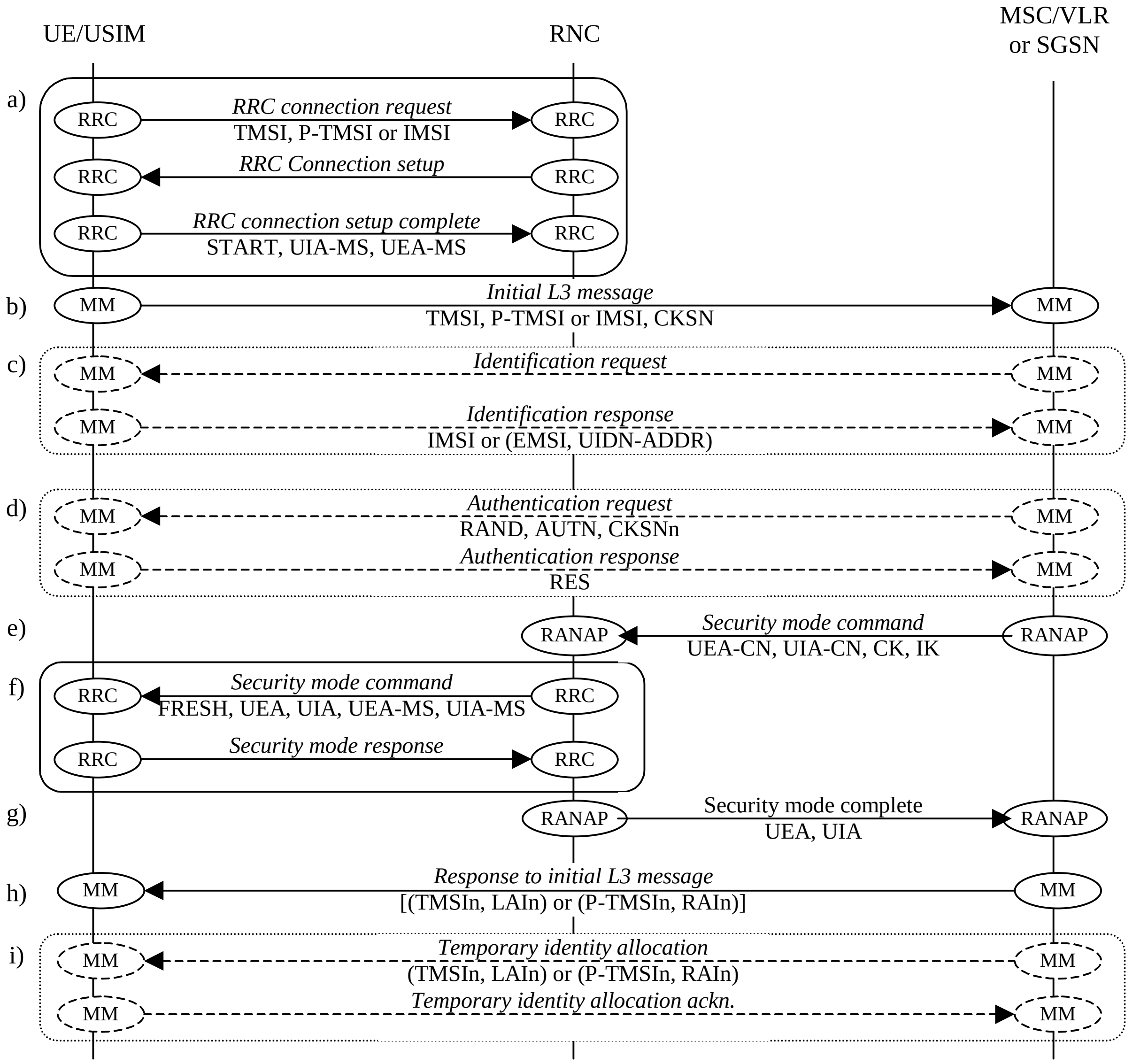


Figure 6.4.1: Signalling procedures at connection establishment

The following signalling procedures shall or may be involved:

a) **RRC connection establishment.** The UE sends the RNC an *RRC connection request*. It includes the establishment cause and a user identity. What user identity is used is defined in 6.1. After receipt of the *RRC connection request*, the RNC sends the UE an *RRC connection set-up*. It assigns a dedicated signalling channel to the user. Finally, the UE sends the RNC an *RRC connection set-up complete*. It includes the initial hyperframe number START (see 6.4.3.3 and 6.4.3.4), the user's integrity capabilities UIA-MS (see 6.4.3.1) and the user's ciphering capabilities UEA-MS (see 6.4.3.2).

b) **The initial L3 message.** The UE sends the MSC/VLR or SGSN the *Initial L3 message*. This can be a *location update request*, a *CM service request*, a *paging response*, a *routing area update request*, an *attach request*, etc. It includes the user's identity and the CKSN (see 6.4.3.7) of the relevant service domain.

In the event the UE has used a temporary identity and the service domain cannot resolve the IMSI, the following procedure shall be executed:

c) **IMSI interrogation to the user.** The MSC/VLR or SGSN may send the UE an *identification request*, requesting the UE for the user's IMSI. Upon receipt of an *identification request*, the UE shall send the MSC/VLR or SGSN a *identification response*. A user without eUIC shall include the user's IMSI (see 6.1). A user with eUIC shall include the user's UIDN address and the encrypted IMSI (see 6.2).

In the event the MSC/VLR or SGSN determines that the network and user do not share cipher and integrity keys (see 6.4.3.7) or because the lifetime of the cipher and integrity keys has expired (see 6.4.3.6) or by an autonomous decision of the serving network operator, the MSC/VLR or SGSN may initiate:

d) **Authentication and key agreement.** The MSC/VLR or SGSN may send the user an *authentication request*. It includes a network challenge RAND, an authentication token AUTN, and a new cipher key sequence number CKSNn. Upon receipt of the *authentication request* the user verifies the data integrity and the freshness of the (RAND, AUTN) pair and computes the user response RES, the cipher key CK and the integrity key IK and sends the MSC/VLR or SGSN an *authentication response* that includes the user response RES. The user updates the current security context to the received CKSNn and the freshly derived CK and IK. Upon receipt of an authentication response, the MSC/VLR or SGSN verifies the user response RES and accordingly updates the current security context to CKSNn and the CK and IK contained in the quintet. For more detail see 6.3.

The following three protocols steps initiate integrity protection and select the ciphering mode. They are mandatorily executed at each connection establishment, with the following exceptions:

– If the only purpose of the signalling connection establishment is a periodic location update, i.e., no change of any registration information;

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

– If the only UE- CN signalling after the initial L3 message, except possibly message for IMSI interrogation and authentication and key agreement, is a reject message followed by a connection release.

In all other cases, security mode negotiation is mandatory and the only procedures allowed between UE and VLR (resp. between UE and SGSN), after the initial L3 message, and before the security mode negotiation procedure are:

– IMSI interrogation to the user.

– Authentication and key agreement.

The protocol steps for security mode negotiation are:

e) **(RANAP) Security mode command.** The MSC/VLR or SGSN sends the RNC a *security mode command*. It contains the integrity modes UIA-CN allowed by the CN (see 6.4.3.1), the ciphering modes UEA-CN allowed by the CN (see 6.4.3.2), the integrity key IK and the cipher key CK. Upon receipt of the *security mode command*, the RNC generates a random value FRESH and initialises the integrity sequence number COUNT-I (see 6.4.3.3) and the ciphering sequence number COUNT-C (see 6.4.3.4). The RNC then selects an integrity mode UIA (see 6.4.3.1) and a cipher mode UEA (see 6.4.3.2).

f) **(RRC) Security mode command/response.** The RNC sends the UE a *security mode command*. It includes the random value FRESH, the selected integrity mode UIA and the selected cipher mode, and a copy of the user's integrity and ciphering capabilities UIA-MS and UEA-MS. *Security mode command* is the first integrity protected message. Upon receipt of the *security mode command*, the UE stores the random value FRESH and initialises the ciphering sequence number COUNT-C and the integrity sequence number COUNT-I, selects the integrity mode UIA and the cipher mode UEA. The UE sends the RNC a *security mode complete*. *Security mode complete* is the first encrypted message (if encryption is enabled).

g) **(RANAP) Security mode complete.** Upon receipt of the *security mode complete*, the RNC sends the MSC/VLR or SGSN a *security mode complete* message. It includes the ciphering capability UEA and the integrity capability UIA in use.

The remaining steps:

h) **Response to the initial LR message.** The MSC/VLR or SGSN then sends a response to the initial L3 message. In case of a location update in a new location area (or a routing area update in a new routing area), the response shall include a new temporary identity and location/routing area identification.

In case the response to the initial L3 message did not contain a new temporary identity and location/routing aea identification, the MSC/VLR or SGSN may initiate

i) **Temporary identity allocation.** For more detail see 6.1.

6.4.2.2 Authentication and key agreement during an ongoing connection

Figure 6.4.2 provides an overview of the signalling on the radio link and the security-related parameters that is involved in authentication and key agreement during an ongoing connection.

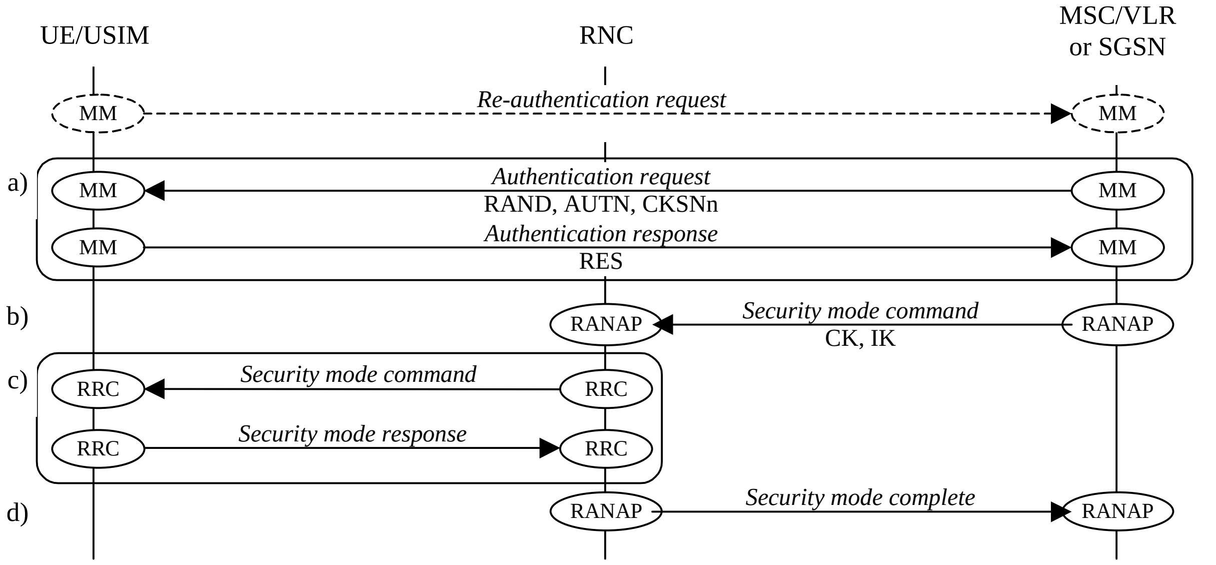


Figure 6.4.2: Authentication and key agreement during an ongoing connection

Authentication and key agreement during an ongoing connection can be caused by a *re-authentication request* sent by the UE (when the START has passed THRESHOLD) or by an a autonomous decision of the MSC/VLR or SGSN.

The protocol steps are as follows:

a) **Authentication and key agreement.** The MSC/VLR or SGSN sends the user an *authentication request*. It includes a network challenge RAND, an authentication token AUTN, and a new cipher key sequence number CKSNn. Upon receipt of the *authentication request* the user verifies the data integrity and the freshness of the (RAND, AUTN) pair and computes the user response RES, the cipher key CK and the integrity key IK and sends the MSC/VLR or SGSN an *authentication response* that includes the user response RES. The user updates the current security context to the received CKSNn and the freshly derived CK and IK. Upon receipt of an authentication response, the MSC/VLR or SGSN verifies the user response RES and accordingly updates the current security context to CKSNn and the CK and IK contained in the quintet. For more detail see 6.3.

b) **(RANAP) Security mode command.** The MSC/VLR or SGSN sends the RNC a *security mode command*. It only contains the integrity key IK and the cipher key CK. It is not allowed to change the integrity mode and/or the cipher mode of an on-going connection. Upon receipt of the *security mode command* initialises the integrity sequence number COUNT-I (see 6.4.3.3) and the ciphering sequence number COUNT-C (see 6.4.3.4).

c) **(RRC) Security mode negotiation.** The RNC sends the UE a *security mode command*. *Security mode command* is the first message protected using the new integrity key and the new COUNT-I (it is ciphered using the old cipher key and the old COUNT-C). Upon receipt of the *security mode command* initialises the ciphering sequence number COUNT-C and the integrity sequence number COUNT-I and selects the new cipher and integrity keys. The UE verifies the integrity of the received command using the new integrity key. The UE sends the RNC a *security mode complete*. *Security mode complete* is the first message encrypted with the new cipher key (if encryption is enabled).

d) **(RANAP) Security mode complete.** The RNC acknowledges to the MSC/VLR that the new cipher and integrity keys are being used.

6.4.3 Mechanisms

6.4.3.1 Integrity mode negotiation

In the *RRC connection setup complete* message the UE sends the RNC the integrity modes supported by the user UIA-MS. In the security mode command the MSC/VLR or SGSN sends the RNC the integrity modes supported by the core network UIA-CN. The RNC then selects an integrity mode UIA ∈ UIA-MS ∩ UIA-RNC ∩ UIA-CN supported by all. If no common UIA can be found, the radio connection is released. The RNC initiates integrity protection with integrity mode UIA. In the security mode command the RNC then sends the user the selected integrity mode UIA and the user's integrity capabilities UIA-MS. The UE verifies the integrity of the received message and verifies whether the received UIA-MS equals the UIA-MS sent to the RNC beforehand. If the integrity cannot be verified, the connection is released.

Both service domains (CS and PS) that belong to the same serving network shall allow the same integrity modes, i.e., UIA-CN_{CS} = UIA-CN_{PS}. When a connection is already established with a first service domain, it is not allowed that the integrity mode for the connection with the second service domain is different.

6.4.3.2 Cipher mode negotiation

In the *RRC connection setup complete* message the UE sends the RNC the cipher modes supported by the user UEA-MS. In the security mode command the MSC/VLR or SGSN sends the RNC the cipher modes supported by the core network UEA-CN. The RNC then selects a cipher mode UEA ∈ UEA-MS ∩ UEA-RNC ∩ UEA-CN supported by all. If no common UEA can be found, the radio connection is released. The RNC initiates integrity protection with integrity mode UEA. In the security mode command the RNC then sends the user the selected cipher mode UEA and the user's cipher capabilities UEA-MS. The UE verifies the integrity of the received message and verifies whether the received UEA-MS equals the UEA-MS sent to the RNC beforehand. If the integrity cannot be verified, the connection is released.

Both service domains (CS and PS) that belong to the same serving network shall allow the same cipher modes, i.e., UEA-CN_{CS} = UEA-CN_{PS}. When a connection is already established with a first service domain, it is not allowed that the cipher mode for the connection with the second service domain is different.

6.4.3.3 Initiation of integrity protection

At connection set-up, *security mode command* is the first integrity protected message using the integrity key IK, the newly generated network challenge FRESH and the integrity sequence number COUNT-I initialised using START.

At re-authentication during an ongoing connection, *security mode command* is the first integrity protected message using the new integrity key IK and the integrity sequence number COUNT-I initialised at 0. The network challenge FRESH that was in use remains in use.

6.4.3.4 Initiation of encryption

At connection set-up, *security mode response* is the first ciphered message using the cipher key CK, the newly generated network challenge FRESH and the ciphering sequence number COUNT-C initialised using START.

At re-authentication during an ongoing connection, *security mode response* is the first ciphered message using the new cipher key CK and the ciphering sequence number COUNT-C initialised at 0.

6.4.3.5 Authentication and key agreement

Authentication and key agreement is the procedure that allows the user and the service domain to agree on a cipher key CK and an integrity key IK. Authentication and key agreement is described in 6.3.

Authentication and key agreement may be initiated by the service domain as often as the network operator wishes.

Authentication and key agreement requires that the identity of the user (i.e. IMSI) be known by the service domain. At the network end, the established cipher key and integrity key are stored in the MSC/VLR or SGSN and transferred to the RNC when they are needed. At user end, the cipher key and integrity key are stored in the USIM and transferred to the UE where they are applied.

If an authentication and key agreement procedure is performed during a data transfer in the PS mode, the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the UE as part of the security mode negotiation that follows the authentication and key agreement procedure.

6.4.3.6 Cipher key and integrity key lifetime

Authentication and key agreement is not mandatory at connection set-up. Unlimited re-use of cipher and integrity is however not allowed.

The MSC/VLR or SGSN shall initiate authentication and key agreement, at connection set-up when the cipher and integrity keys are already more than 24 hours in use.

The MSC/VLR or SGSN should initiate authentication and key agreement, during an on-going connection when the cipher and integrity keys are already more than 24 hours in use.

In addition, a mechanism is provided in the UE/USIM that ensures that a cipher key and integrity key are not used to protect an unlimited amount of data. To that extent the UE and the USIM keep track of the accumulated amount of data that the cipher key has been applied to (START value). Each time an RRC connection is released the highest value START of the hyperframe number (the most significant part of COUNT-C, see 6.6) 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.

The USIM shall trigger a authentication and key agreement at connection set-up when the START value in the USIM exceeds a certain threshold. The UE shall indicate that an authentication and key agreement is required by setting the value of CKSN to the value "111" in the initial L3 message.

The UE shall trigger a re-authentication during an ongoing connection when the START value in the UE exceeds a certain threshold. The UE shall indicate that a re-authentication is required by sending a re-authentication request to the MSC/VLR or SGSN.

6.4.3.7 Cipher key and integrity key identification

The cipher key sequence number CKSN is a number which is associated with the cipher and integrity keys derived during authentication and key agreement.

The user indicates the CKSN associated to the cipher and integrity keys stored the in the initial L3 message. If the user has no cipher and integrity keys, or wishes to trigger authentication and key agreement, it sends the value "111".

Upon receipt of the initial L3 message, the VLR or SGSN verifies whether the CKSN sent by the user corresponds with the CKSN stored in VLR or SGSN. If this is the case, the network may skip authentication and key agreement and the key stored at both ends are used.

The network may initiate authentication and key agreement. In that case, the CKSN is included in the authentication request sent to the user and the user and the VLR or SGSN store and use the new CKSN.

The CKSN is three bits long. Seven values "000" through "110" are used to identify the cipher and integrity key set. A value of "111" is used by the user to indicate that no valid key is available for use. The value "111" in the other direction from network to the user is reserved.

~~6.4 Local authentication and connection establishment~~

~~6.4.1 Cipher key and integrity key setting~~

~~Mutual key setting is the procedure that allows the MS and the RNC to agree on the key IK used to compute message authentication codes using algorithm UIA. Authentication and key setting is 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. TMUI or IMUI) is known by the SN/VLR. The key IK is stored in the SN/VLR and transferred to the RNC when it is needed. The key IK is stored in the USIM until it is updated at the next authentication.~~

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

~~6.4.2 Cipher key 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 message 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 the cipher and imust be stored in the RNC and the integrity of the classmark with the newly generated IK and this value is transmitted to the RNC after the authentication procedure is complete.~~

~~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.~~

~~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 USIM 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.~~

~~This mechanism will ensure that a cipher/integrity key set cannot be reused more times than the limit set by the operator.~~

~~6.4.4 Cipher key and integrity key identification~~

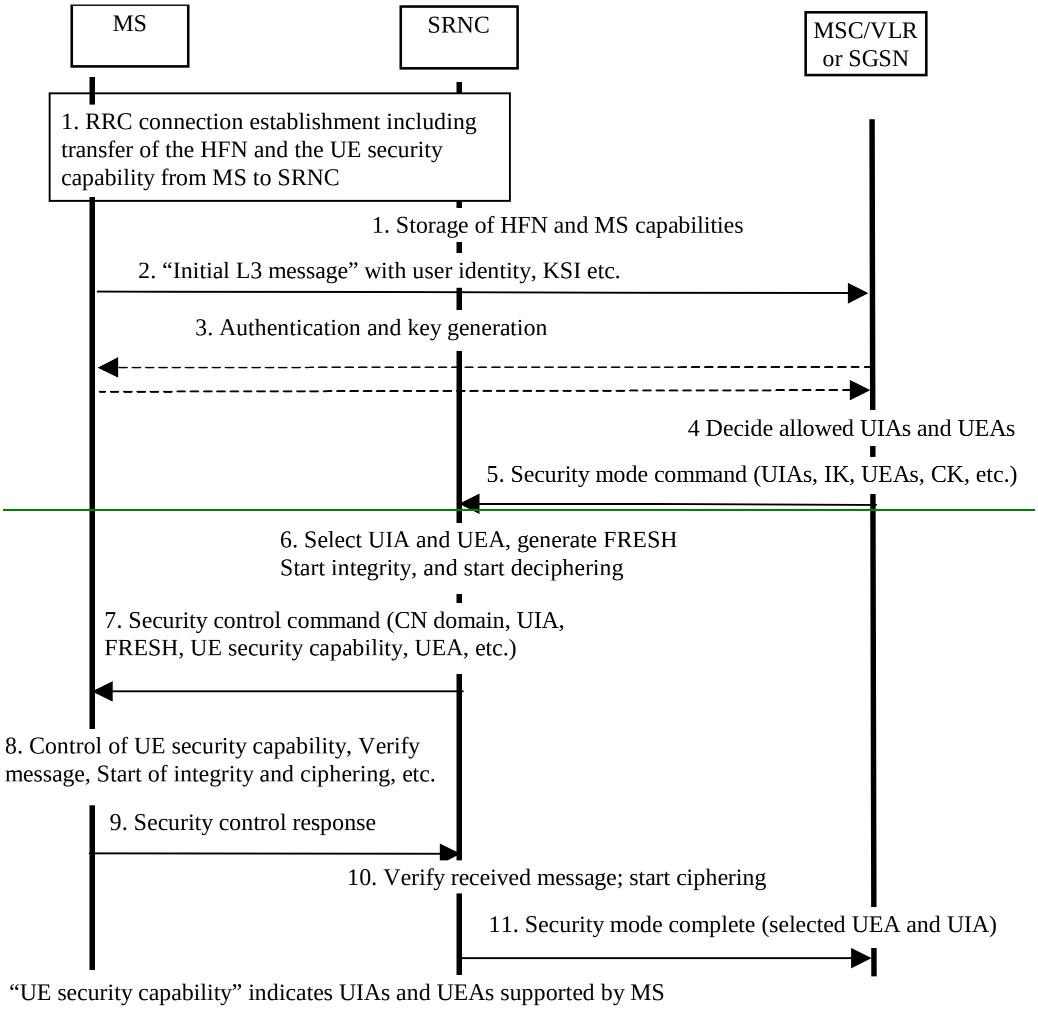
~~The key set identifier (KSI) is a number which is associated with the cipher and integrity keys derived during authentication. The key set identifier is allocated by the network and sent with the authentication request message to the mobile station where it is stored together with the calculated cipher key CK and integrity key IK.~~

~~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 is 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.~~

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


MS
SRNC
MSC/VLR or SGSN
1. RRC connection establishment including transfer of the HFN and the UE security capability from MS to SRNC
1. Storage of HFN and MS capabilities
2. "Initial L3 message" with user identity, KSI etc.
3. Authentication and key generation
4 Decide allowed UIAs and UEAs
5. Security mode command (UIAs, IK, UEAs, CK, etc.)
6. Select UIA and UEA, generate FRESH Start integrity, and start deciphering
7. Security control command (CN domain, UIA, FRESH, UE security capability, UEA, etc.)
8. Control of UE security capability, Verify message, Start of integrity and ciphering, etc.
9. Security control response
10. Verify received message; start ciphering
11. Security mode complete (selected UEA and UIA)
"UE security capability" indicates UIAs and UEAs supported by MS

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

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

~~Detailed description of the flow above:~~

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

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

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

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

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

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

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

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

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

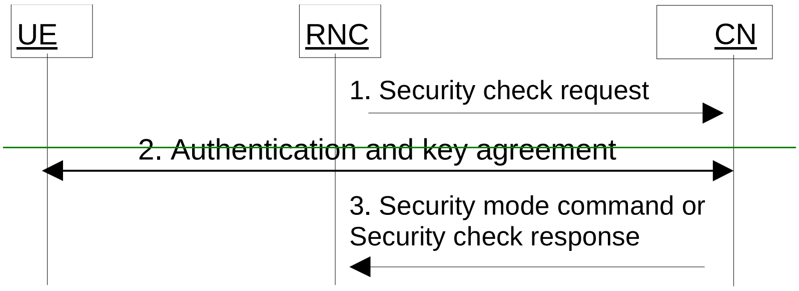
10. ~~At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.~~

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

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

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

~~The following procedure is used by the RNC to request the CN to perform an authentication and to provide a new CK and IK in case of unsuccessful integrity check. This can happen on the RNC side or in the UE side. In the latter case the UE sends a SECURITY CONTROL REJECT message to the RNC.~~


UE
RNC
CN
1. Security check request
2. Authentication and key agreement
3. Security mode command or
Security check response

~~Figure 15: Procedures at unsuccessful integrity check~~

~~RNC detects that new security parameters are needed. This may be triggered by (repeated) failure of integrity checks (e.g. COUNT-I went out of synchronisation), or at handover the new RNC does not support an algorithm selected by the old RNC, etc.~~

1. ~~RNC sends a SECURITY CHECK REQUEST message to CN (indicating cause of the request).~~
2. ~~The CN performs the authentication and key agreement procedure.~~
3. ~~If the authentication is successful, the CN sends a Security mode command to RNC. This will restart the ciphering and integrity check with new parameters. If the authentication is not successful, the CN sends a SECURITY CHECK RESPONSE (Cause) to RNC.~~
4. ~~If the failure situation persists, the connection should be dropped.~~