3GPP TSG SA WG3 Security — S3#11 **S3-000149**

22-24 February, 2000

Mainz, Germany

Source: **Nokia**

Title: **Draft CR on 33.102 about local authentication**

Document for: **Decision**

Agenda Item:

The draft CR addresses the 'man-in-the-middle' scenario, where an intruder steals capacity from radio bearers. The problem was raised in the 3GPP S3#10 meeting in Antwerp.

In this threat scenario, the man-in-the-middle represents a base station + RNC for a legal mobile station and simultaneously represents a mobile station for a legal base station (and RNC). This scenario works well only if ciphering is not used in the radio interface and if the mobile station stays within an area of one base station. In this case it is possible that the 'man-in-the-middle' could send and receive its own data using the user plane radio bearer(s) set up by the legal entities. All data packet (RLC) headers between the legal peer entities would be manipulated by the 'middle-man' so that the peer entities could not notice that something is wrong. The legal user would be able to notice this only afterwards from his/her bill.

The integrity protection as such cannot prevent the attack, since integrity protection is used only in the control plane. However, if the amount of data sent and received is periodically compared between the RNC and the UE, addition of fake data is noticed soon. The comparison messages are integrity protected, hence they cannot be modified.

This procedure serves also as a periodic local authentication during a connection.

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 | Current Version: 3.3.1

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

For submission to TSG	SA #7	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: *(at least one should be marked with an X)*	USIM		ME	X	UTRAN	X	Core Network	

Source:	SA 3	**Date:**	2000-Feb-22
Subject:	Local Authenication 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	X
	D	Editorial modification	

Reason for change:	A periodic local authentication procedure is added because it provides the RNC and the UE means to verify the amount of data sent during the connection. This is needed in order to prevent intruders from stealing capacity of the network.
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 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.

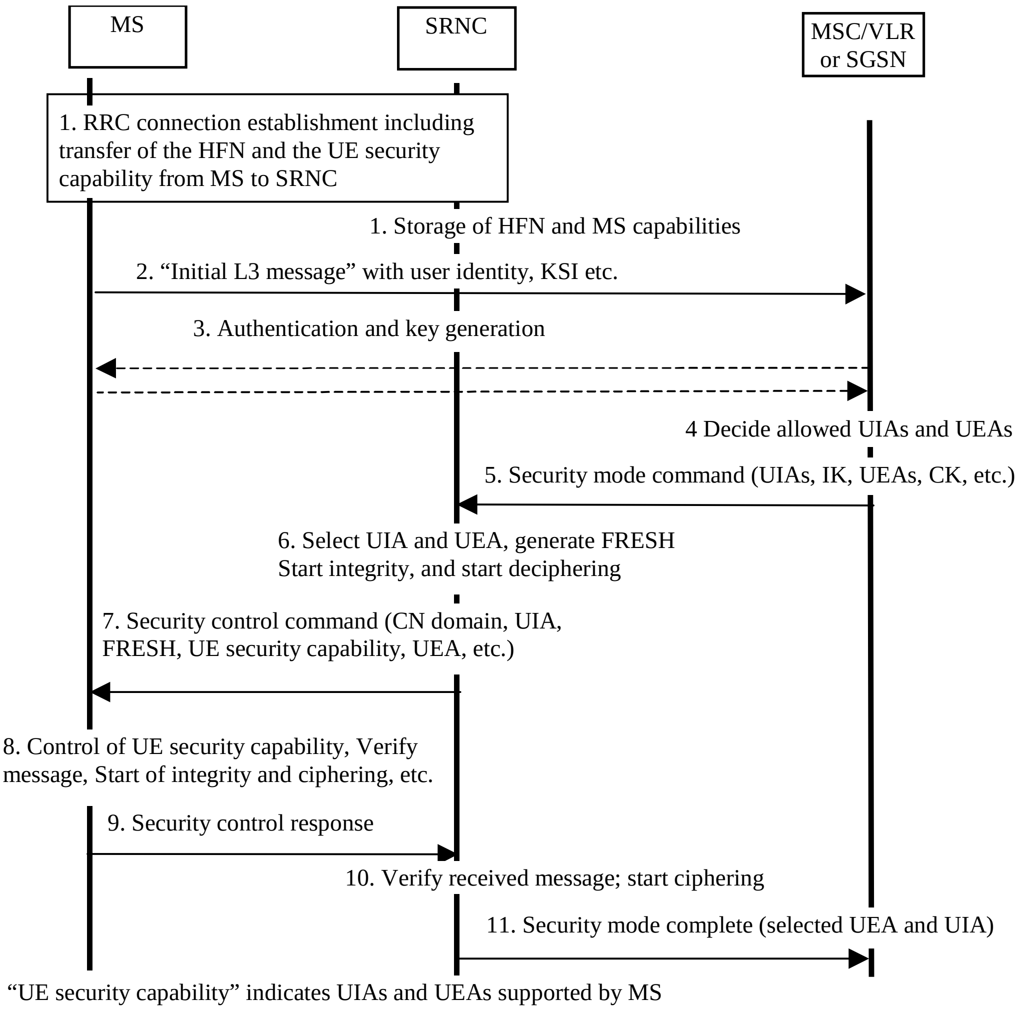


Figure 14: Local authentication and connection set-up

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.

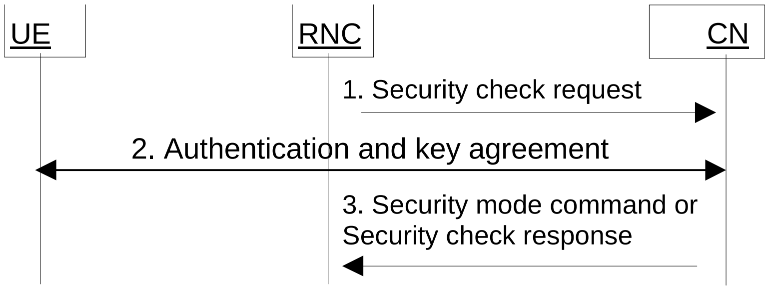


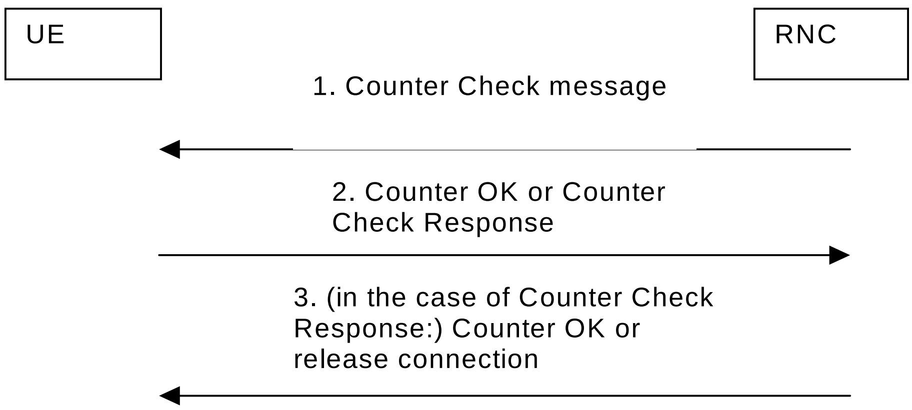
Figure 15: Procedures at unsuccessful integrity check

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.

6.4.7 Signalling procedure for periodic local authentication

The following procedure is used by the RNC to periodically perform a local authentication. At the same time, the amount of data sent during the RRC connection is periodically checked by the RNC and the UE. The RNC is monitoring the COUNT 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.



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

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

3. In case the RNC receives the 'Counter OK' message the procedure is completed. In case the RNC receives the Counter Check response it compares the counter values indicated in it to counter values in the RNC. If there is no difference or if

the difference is acceptable then the RNC completes the procedure by sending the 'Counter OK' message. Otherwise, the connection is released.

6.5 Access link data integrity

6.5.1 General

Most RRC, MM and CC signalling information elements are considered sensitive and must be integrity protected. A message authentication function shall be applied on these signalling information elements transmitted between the MS and the SN.

The UMTS Integrity Algorithm (UIA) shall be used with an Integrity Key (IK) to compute a message authentication code for a given message.

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

- Notification
- Paging Type 1
- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete
- RRC Connection Reject
- All System Information messages.