TSG-RAN Working Group 3 meeting #7 *TSGR3#7(99)B55*
Sophia Antipolis, France, 20th – 24th of September 1999

Agenda Item: 10.3

Source: **Ericsson**

Title: Security Mode Control Procedure for RANAP

Document for: Decision

1. Introduction

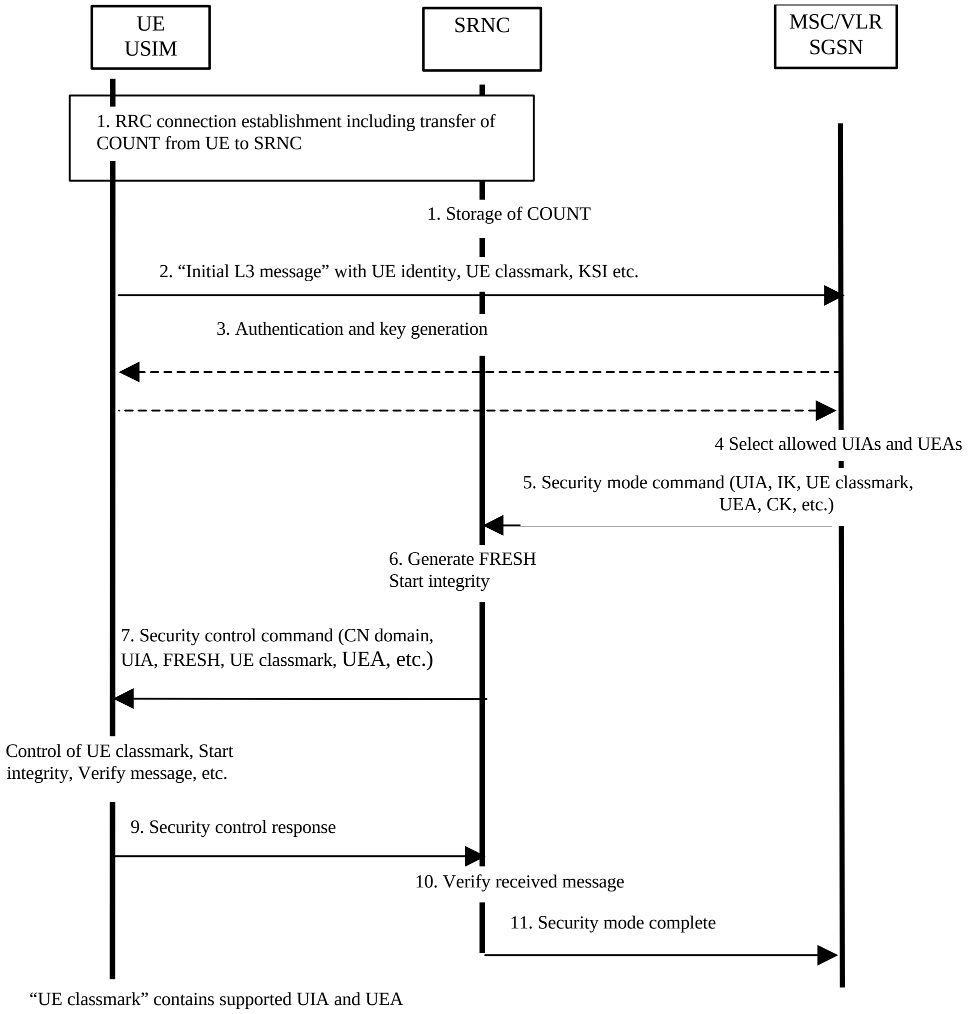
Ref. 1 so far only includes Cipher Mode Control as security function. It is, however, a requirement to also handle Integrity Protection which is a mandatory function (see Ref. 2). This contribution thus proposes a common RANAP procedure for handling of both Ciphering and Integrity Protection.

2. Background

See App. A for background information on the Integrity Algorithm.

3. Discussion on Integrity Protection

With one common "Security mode control" procedure for both ciphering and integrity protection, the message sequence flow below describes the information transfer at initial connection establishment, authentication and start of integrity protection.


UE
USIM
SRNC
MSC/VLR
SGSN
1. RRC connection establishment including transfer of COUNT from UE to SRNC
1. Storage of COUNT
2. "Initial L3 message" with UE identity, UE classmark, KSI etc.
3. Authentication and key generation
4 Select allowed UIAs and UEAs
5. Security mode command (UIA, IK, UE classmark, UEA, CK, etc.)
6. Generate FRESH
Start integrity
7. Security control command (CN domain, UIA, FRESH, UE classmark, UEA, etc.)
Control of UE classmark, Start integrity, Verify message, etc.
9. Security control response
10. Verify received message
11. Security mode complete
"UE classmark" contains supported UIA and UEA

Note 1:
The network must have the "UE security capability" information, which is part of the "UE Classmark", before the integrity protection can start, i.e. the "UE Classmark" must be sent to the network in an unprotected message. Returning the "UE Classmark" later on to the UE in a protected message will give UE the possibility to verify that it was the correct "UE Classmark" 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 UE to RNC of the COUNT parameter to be used as one of the input parameters for the integrity algorithm. The COUNT parameter is stored in the SRNC.

2. The UE sends the Initial L3 message (Location update request, CM service request, Routing area update request, etc.) to the relevant CN domain. This message contains relevant MM information and also the UE classmark IE, which includes information on the UIA(s) and UEA(s) supported by the UE. 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 use.
   Note 2: The assumption is that the selection of algorithms is done in the same way as for GSM. This has to be agreed with RAN WG3, RAN WG2 and CN WG1.

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

6. The SRNC decides which algorithms to use, generates a random value FRESH and initiates the downlink integrity protection.

7. The SRNC generates the RRC message Security control command. The message includes the UE classmark IE, the UIA and FRESH to be used and possible also the UEA to be used. Additional information (e.g. related to 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 UE, 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 UE controls that the UE classmark IE received is equal to the UE classmark IE sent in the initial message. The UE computes XMAC-I on the message received by using the indicated UIA, the stored COUNT and the received FRESH parameter. The UE verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

9. If all controls are successful, the UE compiles the RRC message Security control command response and generates the MAC-I for this message.

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 from SRNC to the CN node ends the procedure.

The Security mode command to UE starts the downlink integrity protection, i.e. also all following messages sent to the UE are integrity protected. The Security mode command response from UE starts the uplink Integrity protection, i.e. also all following messages sent from the UE are integrity protected.

4. Security Mode Control

4.1 Successful Operation

The security mode control procedure allows the CN to pass cipher and integrity mode information to the UTRAN. UTRAN uses this information to select and load the encryption device for the user and signalling data with the appropriate parameters and also to store the appropriate parameters for the integrity algorithm. This is achieved by sending the UTRAN a SECURITY MODE COMMAND message. Receipt of the message at the UTRAN shall trigger the execution of the corresponding radio interface procedure and, if applicable, invoke the encryption device and start stream ciphering and also start the integrity protection.

In the SECURITY MODE COMMAND the CN shall specifiy which ciphering and integrity protection algorithms that may be used by the UTRAN. The UTRAN shall then internally select appropriate algorithms, taking into account the UE/UTRAN capabilities. The SECURITY MODE COMPLETE message returned to the CN indicates the chosen algorithms. The set of permitted algorithms specified in the SECURITY MODE COMMAND shall remain applicable for subsequent RAB Assignments and Intra-UTRAN Relocations.

When the execution of the radio interface procedure is successfully finished, UTRAN shall return a SECURITY MODE COMPLETE message to the CN.

The SECURITY MODE COMMAND and SECURITY MODE COMPLETE messages are sent as connection oriented messages via the appropriate signalling connection.

In case of a UE with Radio Access Bearers towards both core networks, the RABs towards CS shall always be ciphered according to the information received from CS and the RABs towards PS with the information received from PS. The signalling data shall always be ciphered with the last received ciphering information and integrity protected with the last received integrity protection information.

The signalling flow of the successful Security mode control procedure is shown in Figure 1.

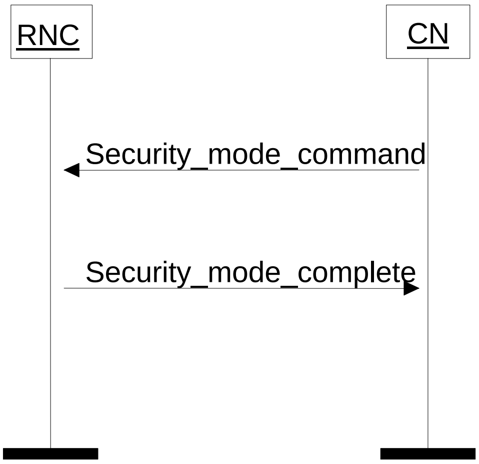


Figure 1. Security Mode Control procedure, successful case.

4.2 Unsuccessful Operation

If the UTRAN or the UE is unable to support the ciphering and/or integrity protection algorithms specified in the SECURITY MODE COMMAND message, then the UTRAN shall return to CN a SECURITY MODE REJECT message with a cause value saying that requested ciphering and/or integrity protection algorithms are not supported". A SECURITY MODE REJECT message shall also be returned if a CN requests a change of ciphering and/or integrity protection algorithms for a UE when ciphering or integrity protection is already active for that CN. A cause value shall indicate that ciphering and/or integrity protection is already active.
Note: Re-authentication is being discussed in S3, which may result in that changing of algorithms will be allowed. Guidance from S3 is needed.

If the radio interface Security Control Procedure fails, SECURITY MODE REJECT shall be sent to CN with a cause value indicating failure in the radio interface procedure.

The signalling flow of the Security mode control procedure in case of unsuccessful operation is shown in Figure 2.

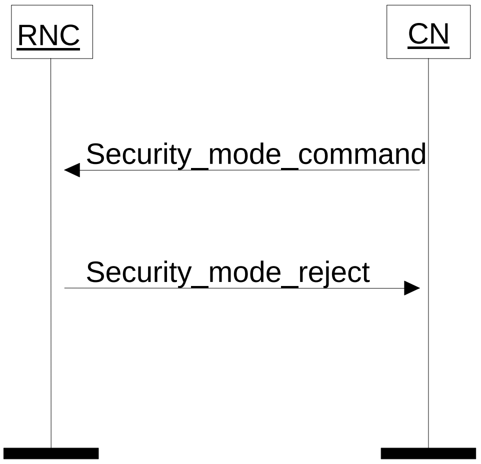


Figure 2. Security Mode Control procedure, unsuccessful case.

4.3 Abnormal Conditions

If CN, after having sent SECURITY MODE COMMAND, receives RELOCATION REQUIRED the security procedure shall be interrupted and resumed later after completed relocation, towards the RNC that then has the role of serving RNC.

In the source RNC, incoming security control messages shall be ignored during relocation, i.e. from sending of RELOCATION REQUIRED until relocation is terminated.

5. Information to transfer during Relocation

Information needed to continue the integrity protection and ciphering also after a relocation, must be transferred from source RNC to target RNC during relocation. The following information shall be included:

UIA, IK, COUNT, FRESH for integrity protection and

UEA, CK, COUNT, BEARER for ciphering.

Note: It is FFS whether this information can all be sent transparently or if some must be possible to modify by the CN.

6. SECURITY MODE COMMAND

Information element	**Reference**	**Type**
Message type		M
Integrity Protection Information		M (1)
UE Classmark		M
Encryption Information		O (1)

(1) Integrity and Encryption information include key(s) and permitted algorithms.

Note 1. It is FFS whether NAS information should be included in this message.

Note 2. The possibility to cipher only some of the RABs is FFS.

Note 3: The need for including UE Classmark has to be agreed with RAN WG2.

7. SECURITY MODE COMPLETE

Information element	**Reference**	**Type**
Message type		M
Chosen Integrity Protection Algorithm		M
Chosen Encryption Algorithm		O

Note 1. It is FFS whether NAS information should be included in this message.

8. SECURITY MODE REJECT

Information element	Reference	Type
Message type		M
Cause		M

9. Conclusion and Proposal

It is possible to replace the Cipher Mode Control procedure with a new procedure called Security Mode Control. This procedure will handle both ciphering and integrity protection.

It is thus proposed to replace the contents in chapter 8.1 in Ref. 1 with the contents of chapter 4 in this document and also to replace chapters 9.1.9 to 9.1.11 in Ref. 1 with chapters 6 to 8 in this document.

The contents in chapter 5 shall be used as input when defining which information that needs to be transferred from Source RNC to Target RNC during relocation.

10. References

[1] TS 25.413 UTRAN Iu Interface RANAP Signalling

[2] TS 33.102 Security Architecture

Appendix A

The following is copied from the 3G TS 33.102:

The UMTS Integrity Algorithm (UIA) shall be implemented in the UE and in the RNC.

Figure 13 illustrates the use of the UIA to authenticate the data integrity of a signalling message.

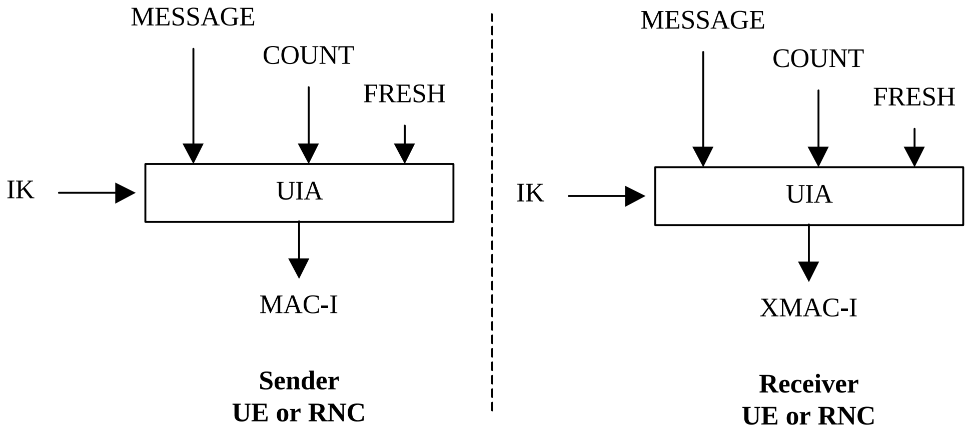


Figure 13: Derivation of MAC-I (or XMAC-I) on a signalling message

The input parameters to the algorithm are the Integrity Key (IK), a time dependent input (COUNT), a random value generated by the network side (FRESH) and the signalling data (MESSAGE). Based on these input parameters the user computes message authentication code for data integrity (MAC-I) using the UMTS Integrity Algorithm (UIA). 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 input parameter COUNT protects against replay during a connection. It is a value incremented at both sides of the radio access link every 10 ms layer 1 frame. Its initial value is sent by the user to the network at connection set-up. The user stores the last used COUNT value from the previous connection and increments it by one. In this way the user is assured that no COUNT value is re-used (by the network) with the same integrity key.

The input parameter FRESH protects network against replay of signalling messages by the user. At connection set-up the network generates a random value FRESH and sends it to the user. 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.