CR-Form-v7

CHANGE REQUEST

⌘ TS 33.102 CR 182 ⌘rev - ⌘ Current version: 5.2.0 ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Mitigation against a man-in-the-middle attack associated with early UE handling
Source:	⌘	SA WG3
Work item code:	⌘	LATE_UE
Date:	⌘	19/09/2003
Category:	⌘	C
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	If an unprotected IMEISV is used to establish security without ciphering (i.e. with UEA0) for UEs which have faulty UEA1 implementations then a man-in-the-middle attack is possible. A mechanism to mitigate against this attack needs to be specified.
Summary of change:	⌘	Add a mechanism to mitigate against a man-in-the-middle attack associated with early UE handling.
Consequences if not approved:	⌘	A man-in-the-middle attacker would be able to disable ciphering for UEs which are capable of ciphering.

Clauses affected:	⌘	2, 6.4.5			
Other specs affected:	⌘	Y: Other core specifications	⌘	24.008, 25.413	
		N: Test specifications			
		N: O&M Specifications			
Other comments:	⌘				

***** Start of change *****

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2] 3GPP TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[3] 3GPP TR 21.905: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications (Release 1999)".

[4] 3GPP TS 23.121: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Architecture Requirements for Release 99".

[5] 3GPP TS 31.101: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics".

[6] 3GPP TS 22.022: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Personalisation of UMTS Mobile Equipment (ME); Mobile functionality specification".

[7] 3GPP TS 23.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Security Mechanisms for the (U)SIM application toolkit; Stage 2".

[8] ETSI GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[9] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[10] ISO/IEC 9798-4: "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function".

[11] 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications".

[12] 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification".

[13] 3GPP TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementers' test data".

[14] 3GPP TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data".

[15] 3GPP TS 31.111: "3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT)".

[16] 3GPP TS 22.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Security Mechanisms for the (U)SIM Application Toolkit; Stage 1".

[17] 3GPP TS 25.331: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RRC Protocol Specification".

[18] 3GPP TS 25.321: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; MAC protocol specification".

[19] 3GPP TS 25.322: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RLC Protocol Specification".

[20] 3GPP TS 31.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Characteristics of the USIM Application".

[21] 3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Service principles".

[22] 3GPP TS 23.195 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Provision of User Equipment Specific Behaviour Information (UESBI) to network entities".

***** End of change *****

***** Start of change *****

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and VLR/SGSN. The four exceptions when it is not mandatory to start integrity protection are:

- If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.
- If there is no MS-VLR/SGSNsignalling after the initial L3 signalling message sent from MS to VLR/SGSN, i.e. in the case of deactivation indication sent from the MS followed by connection release.
- If the only MS-VLR/SGSN signalling after the initial L3 signalling message sent from MS to VLR/SGSN, and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.
- If the call is an emergency call teleservice as defined in TS 22.003, see section 6.4.9.2 below.

When the integrity protection shall be started, the only procedures between MS and VLR/SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to VLR/SGSN) and before the security mode set-up procedure are the following:

- Identification by a permanent identity (i.e. request for IMSI), and
- Authentication and key agreement.

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

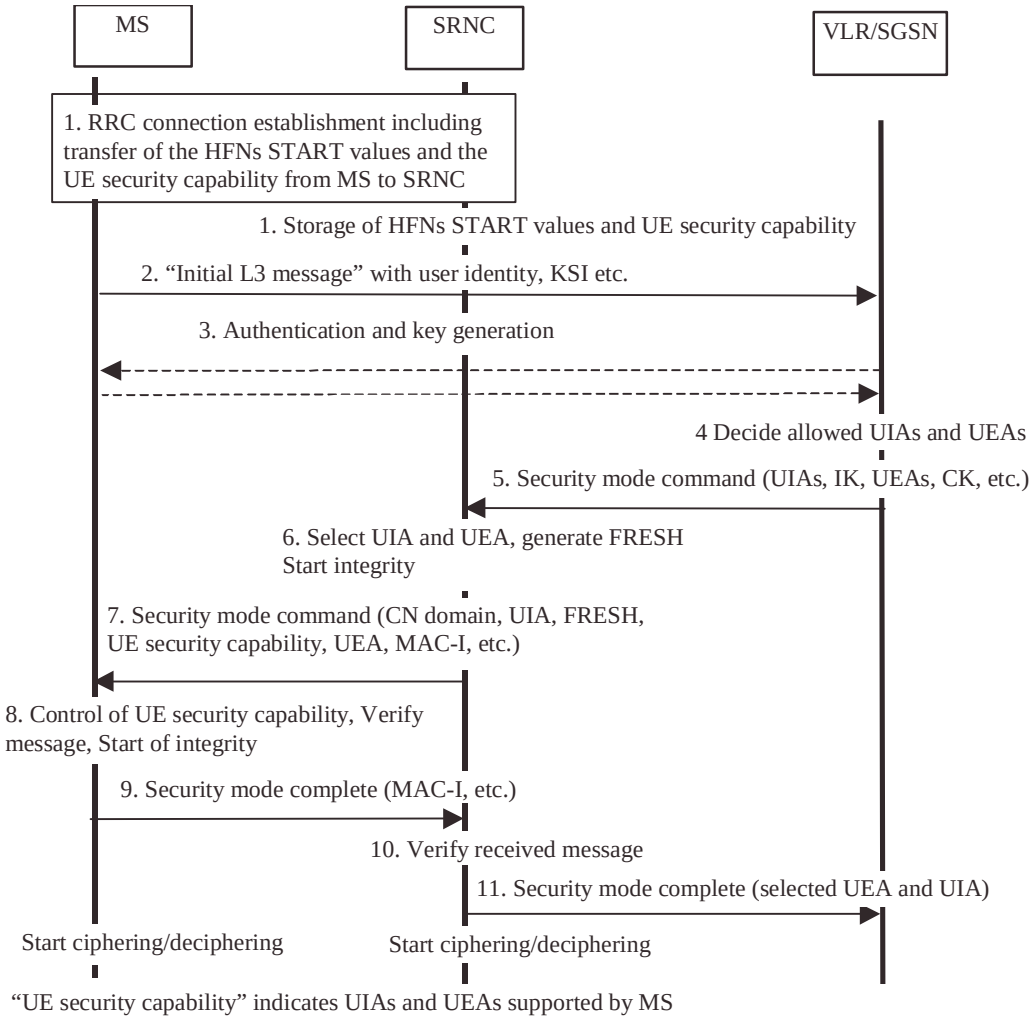

Figure 14: Local authentication and connection set-up

NOTE 1: The network must have the "UE 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.

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the ME security capability optionally the GSM Classmarks 2 and 3 and the START values for the CS service domain respective the PS service domain. The UE security capability information includes the ciphering capabilities (UEAs) and the integrity capabilities (UIAs) of the MS. The START values and the UE security capability information are stored in the SRNC. If the GSM Clasmarks 2 and 3 are transmitted during the RRC Connection establishment, the RNC must store the GSM ciphering capability of the UE (see also message 7).

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 VLR/SGSN. This message contains e.g. the user identity and the KSI. The included KSI (Key Set Identifier) is the KSI allocated by the CS service domain or PS service domain at the last authentication for this CN domain.

3. User identity request may be performed (see 6.2). Authentication of the user and generation of new security keys (IK and CK) may be performed (see 6.3.3). A new KSI will then also be allocated.

4. The VLR/SGSN determines which UIAs and UEAs that are allowed to be used in order of preference.

5. The VLR/SGSN initiates integrity and ciphering by sending the RANAP message Security Mode Command to SRNC. This message contains an ordered list of allowed UIAs in order of preference, and the IK to be used. If ciphering shall be started, it contains the ordered list of allowed UEAs in order of preference, and the CK to be used. If a new authentication and security key generation has been performed (see 3 above), this shall be indicated in the message sent to the SRNC. The indication of new generated keys implies that the START value to be used shall be reset (i.e. set to zero) at start use of the new keys. Otherwise, it is the START value already available in the SRNC that shall be used (see 1. above).

6. The SRNC decides which algorithms to use by selecting the highest preference algorithm from the list of allowed algorithms that matches any of the algorithms supported by the MS (see 6.4.2). The SRNC generates a random value FRESH and initiates the downlink integrity protection. If the requirements received in the Security mode command can not be fulfilled, the SRNC sends a SECURITY MODE REJECT message to the requesting VLR/SGSN. The further actions are described in 6.4.2.

7. The SRNC generates the RRC message Security mode command. The message includes the ME security capability, optionally the GSM ciphering capability (if received during RRC Connection establishment), the UIA and FRESH to be used and if ciphering shall be started also the UEA to be used. Additional information (start of ciphering) may also be included. 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.

8. At reception of the Security mode command message, the MS controls that the "UE security capability" received is equal to the "UE security capability" sent in the initial message. The same applies to the GSM ciphering capability if it was included in the RRC Connection Establishment. 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 mode complete and generates the MAC-I for this message. If any control is not successful, the procedure ends in 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 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.

Mechanisms are defined to allow networks to overcome early UE implementation faults [22]. A potential early UE implementation fault could be a faulty UEA1 implementation. To allow networks to handle early UEs which have faulty UEA1 implementations, the SGSN/VLR may configure the security mode command based on the UE's IMEISV so that certain UEs which claim to support UEA1 shall have security established without ciphering (i.e. with UEA0), while other UEs which claim to support UEA1 shall have security established with ciphering (i.e. with UEA1). This procedure shall involve the SGSN/VLR retrieving the IMEISV from the UE before the security mode set-up procedure has started.

If the above procedure to handle UEs which have faulty UEA1 implementations is implemented and the security mode set-up procedure results in security being established without ciphering (i.e. with UEA0) then the SGSN/VLR shall request the IMEISV from the UE for a second time immediately after the security mode set-up procedure has been completed. This second IMEISV request is integrity protected. If the IMEISV request is not successful, or if the second IMEISV received is different from the IMEISV received before the security mode set-up procedure was started then the connection shall be released.

***** End of change *****