

## CHANGE REQUEST

# **33.203** CR **CRNum** # rev **-** # Current version: **5.3.0** #

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

<b>Title:</b>	# INVITE is refused during re-transmission		
<b>Source:</b>	# Nokia		
<b>Work item code:</b>	# IMS-ASEC	<b>Date:</b>	# 04/11/2002
<b>Category:</b>	# <b>F</b>	<b>Release:</b>	# Rel-5
	<i>Use one of the following categories:</i> <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<i>Use one of the following releases:</i> <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>Rel-4</b> (Release 4) <b>Rel-5</b> (Release 5) <b>Rel-6</b> (Release 6)

<b>Reason for change:</b>	# Radio channel deterioration will cause a burst of signals all lost, that makes SIP re-transmission unreliable than in wired world; also roaming in uncovered area will loss all signals.  UE should be allowed to start or receive a SIP session without waiting for re-transmission of successful message of a new SA. Thus UE should send and receive INVITE protected by the old SAs. The P-CSCF should keep the old SAs active to receive INVITE request because of the reason above. The P-CSCF should use the old outbound SAs to send INVITE request since using new SA shall cause UE to delete old SAs; then re-transmission failure would cause UE has to start registration again but unprotected.  If UE starts an unprotected registration due to poweroff, the P-CSCF should remove the old valid SAs. This work assumption is missing from current specification.
<b>Summary of change:</b>	# <ul style="list-style-type: none"> <li>• The P-CSCF should keep the old SAs to send and receive those messages other than those in authentication (e.g. INVITE) request until either the old SAs lifetime are expired, or a further SIP message protected with the new inbound SA is successfully received from the UE; The UE should hold the old inbound SA until either it is expired or further message protected by new SA is received from P-CSCF.</li> </ul>
<b>Consequences if not approved:</b>	# <ul style="list-style-type: none"> <li>• P-CSCF may have no common SA for the UE, due to the deletion of old SAs. INVITE requests protected by old SAs are rejected;</li> <li>• UE may have only old SAs available, if re-transmission is failed. UE can</li> </ul>

not receive any forwarded INVITE and other messages protected by new SA.

**Clauses affected:** ⌘ 7.4.1a, 7.4.2a

	Y	N		
<b>Other specs affected:</b>	⌘	X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

**Other comments:** ⌘

## 7.4 Authenticated re-registration

Every registration that includes a user authentication attempt produces new security associations. If the authentication is successful, then these new security associations shall replace the previous ones. This clause describes how the UE and P-CSCF handle this replacement and which SAs to apply to which message.

If the UE has an already active security association, then it shall use this to protect the REGISTER message. If the S-CSCF is notified by the P-CSCF that the REGISTER message from the UE was integrity-protected it may decide not to authenticate the user by means of the AKA protocol. However, the UE may send unprotected REGISTER messages at any time. In this case, the S-CSCF shall authenticate the user by means of the AKA protocol. In particular, if the UE has an indication that the SA is no longer active at the P-CSCF side, it shall send an unprotected REGISTER message.

Security associations may be unidirectional or bi-directional. This clause assumes that security associations are unidirectional, as this is the general case. For IP layer SAs, the lifetime mentioned in the following clauses is the lifetime held at the application layer. Furthermore deleting an SA means deleting the SA from both the application and IPsec layer. The message numbers, e.g. SM1, used in the following clauses relate to the message flow given in section 6.1.1.

### 7.4.1 Void

#### 7.4.1a Management of security associations in the UE

The UE shall be involved in only one registration procedure at a time, i.e. the UE shall remove any data relating to any previous incomplete registrations or authentications, including any SAs created by an incomplete authentication.

The UE may start a registration procedure with an existing pair of SAs. This will be referred to as the old SAs. The authentication produces a pair of new SAs. These new SAs shall not be used to protect non-authentication traffic until noted during the authentication flow. In the same way, certain messages in the authentication shall be protected with a particular SA. If the UE receives a message protected with the incorrect SA, it shall discard the message.

A successful authentication proceeds in the following steps:

- The UE sends the SM1 message to register with the IMS. If SM1 was protected, it shall be protected with the old outbound SA.
- The UE receives an authentication challenge in a message (SM6) from the P-CSCF. This message shall be protected with the old inbound SA if SM1 was protected and unprotected otherwise.
- If this message SM6 can be successfully processed by the UE, the UE creates the new SAs, which are derived according to section 7.1. The lifetime of the new SAs shall be set to allow enough time to complete the registration procedure. The UE then sends its response (SM7) to the P-CSCF, which shall be protected with the new outbound SA. If SM1 was protected, the new SAs can now be used to protect messages other than those in the authentication. Furthermore for outbound traffic, the new SA shall be used.
- The UE receives an authentication successful message (SM12) from the P-CSCF. It shall be protected with the new inbound SA.
- After the successful processing of this message by the UE, the registration is complete. The UE sets the lifetime of the new SAs using the registration timer in the message. For further traffic sent from UE, the new outbound SA is used. The old outbound SAs are is now deleted. The old inbound SA is kept for receiving messages from P-CSCF. It shall be deleted when either lifetime is expired, or a further SIP message protected with the new inbound SA is successfully received from the P-CSCF. ~~The new SAs are used to protect all traffic.~~

A failure in the authentication means the UE shall delete the new SAs. If the SM1 was not protected, then no protection shall be applied to the failure messages. If SM1 was protected, the old SAs shall be used to protect these messages.

The UE shall delete any SA whose lifetime is exceeded.

## 7.4.2 Void

### 7.4.2a Management of security associations in the P-CSCF

When the S-CSCF initiates an authentication by sending a challenge to the UE, the P-CSCF may already contain an existing pair of SAs from a previously completed authentication. It may also contain an existing pair of SAs from an incomplete authentication. These will be referred to as the old and registration SAs respectively. The authentication produces a pair of new SAs. These new SAs shall not be used to protect non-authentication traffic until noted during the authentication flow. Similarly certain messages in the authentication shall be protected with a particular SA. If the P-CSCF receives a message protected with the incorrect SA, it shall discard the message.

The P-CSCF associates the IMPI given in the registration procedure and all the successfully registered IMPUs related to that IMPI to an SA.

A successful authentication proceeds in the following steps:

- The P-CSCF receives the SM1 message. If SM1 is protected, it shall be protected with the old inbound SA.
- The P-CSCF forwards the message containing the challenge (SM6) to the UE. This shall be protected with the old outbound SA, if SM1 was protected and unprotected otherwise.
- The P-CSCF then creates the new SAs, which are derived according to section 7.1. The expiry time of the new SAs shall be set to allow enough time to complete the registration procedure. The registration SAs shall be deleted if they exist.
- The P-CSCF receives the message carrying the response (SM7) from the UE. It shall be protected using the new inbound SA. ~~If SM1 was protected, the new SAs can now be used to protect messages other than those in the authentication.~~
- The P-CSCF forwards the successful registration message (SM12) to the UE. It shall be protected using the new outbound SA. This completes the registration procedure for the P-CSCF. The P-CSCF sets the expiry time of the new SAs equal to the registration timer in the message. ~~and deletes the old SAs. The new SAs are used to protect all traffic.~~
- The P-CSCF handles the UE related SAs according to following rules:
  - o If there are old SAs valid, but SM1 is received unprotected, the P-CSCF considers error cases happened, and assumes UE does not have those old SAs for use. In this case the P-CSCF shall remove the old SAs.
  - o If SM1 is protected with old valid SAs, the P-CSCF keeps the old SAs with the UE active, and continues to use them. The old SAs are deleted when either the old SAs lifetime are expired, or a further SIP message protected with the new inbound SA is successfully received from the UE. Then further messages are protected with new SAs. This completes the SA handling procedure for the P-CSCF.

A failure in the authentication means the P-CSCF shall delete the new SAs. If the SM1 was not protected, then no protection shall be applied to the failure messages. If SM1 was protected, the old SAs shall be used to protect these messages.

The P-CSCF shall delete any SA whose lifetime is exceeded.