<div style="border:1px solid;">

CR-Form-v7

CHANGE REQUEST

⌘	**33.203 CR**	⌘**rev**	**-**	⌘	Current version:	**5.7.0**	⌘

</div>

*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 **X**

Title: ⌘	SA procedures	
Source: ⌘	Nokia	
Work item code:⌘	IMS-ASEC	***Date:*** ⌘ 08/10/2003
Category: ⌘	**F**	***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: ⌘	The SA management procedures are clarified.
Summary of change:⌘	'is' was changed to 'belonging to the same registration procedure, was'
Consequences if not approved: ⌘	Misunderstanding of the procedures, therefore vendor interoperability problems.

Clauses affected: ⌘	7.4.2	

Other specs affected: ⌘	Y	N		⌘
	X		Other core specifications	24.229
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘	

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 existing SAs from previously completed authentications. It may also contain two existing pairs of SAs from an incomplete authentication. These will be referred to as the old and registration SAs respectively. The authentication produces two pairs 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 old SAs are 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 such that they either equals the latest lifetime of the old SAs or it will expire shortly after the registration timer in the message, depending which gives the SAs the longer life.

-   After SM12 is sent, the P-CSCF handles the UE related SAs according to following rules:

    -   If there are old SAs, but SM1 belonging to the same registration procedure ~~is~~was 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.

    -   If SM1 belonging to the same registration procedure was ~~is~~ protected with an old valid SA, the P-CSCF keeps this inbound SA and the corresponding three SAs created during the same registration with the UE active, and continues to use them. Any other old SAs are deleted. When a further SIP message protected with a new inbound SA is successfully received from the UE, the P-CSCF starts to use the new SAs for outbound messages with the following exception: when a SIP message is part of a pending SIP transaction it is still sent over the old SA. A SIP transaction is called pending if it was started using an old SA. The old SAs are then deleted as soon as all pending SIP transactions have been completed, or have timed out. The old SAs are always deleted when the old SAs lifetime are expired. This completes the SA handling procedure for the P-CSCF.