Technical Specification Group Services and System Aspects **TSGS#19(03)0102**

Meeting #19, Birmingham, UK, 17-20 March 2003

Source: **SA WG3**

Title: **1 CR to 33.203: Ensuring the deletion of unwanted SA's (Rel-5)**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CR was approved by SA WG3 meeting #27 and is hereby presented to TSG SA#19 for approval.

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-030102	33.203	037	-	Rel-5	Ensuring the deletion of unwanted SA's	F	5.4.0	IMS-ASEC	S3-030124

3GPP TSG SA WG3 Security — S3#27 **S3-030124**
25- 28 February 2003, Sophia Antipolis, France

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **037** ⌘ **rev** **-** ⌘ Current version: **5.4.0** ⌘

*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 **X**

Title:	⌘	Ensuring the deletion of unwanted SAs
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	19/02/2003
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 P-CSCF does not curently remove unwanted SAs (if they exist) from an incomplete authentication process when the P-CSCF sends an SM12 message in a subsequent authentication. This could cause the P-CSCF to hold three sets of SAs and prevent the successful completion of an authentication
Summary of change:	⌘	Ensure the P-CSCF deletes the SAs from an incomplete authentication when a subsequent authentication completes (from the P-CSCF perspective)
Consequences if not approved:	⌘	If the last message in an authentication gets lost (after SIP layer re-transmissions) twice between sucessful authentications, then (unless one of the SA lifetime expires) the P-CSCF will contain three pairs of SAs for one UE and will not create another pair (rule 3 in section 7.1 forbids the P-CSCF to have more than 3 pairs of SAs) and an authentication with that UE cannot complete sucessfully until one of the SAs lifetime expires and it is removed.

Clauses affected:	⌘	7.4.2a			
Other specs affected:	⌘	**Y** / **N**	Other core specifications	⌘	24.229
		Y /	Other core specifications		
		/ **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 ~~a~~ previously completed authentications. 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 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 equal to the maximum of registration timer in the message and the lifetime of the old SAs.
- After SM12 is sent, t~~T~~he P-~~-~~CSCF handles the UE related SAs according to following rules:
  - 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.
  - If SM1 is protected with an old ~~valid~~ SA~~s~~, the P-~~-~~CSCF keeps thi~~s~~e inbound SA and the corresponding outbound S~~old S~~A~~s~~ with the UE active, and continues to use them. Any other old SAs are deleted. The kept 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 can occur for several reasons. If the SM1 was not protected, then no protection shall be applied to the failure messages, except the user authentication failure message which shall be protected with the new SA. If SM1 was protected, the old SAs shall be used to protect the failure messages. In both cases, after processing the failure message, the P-~~-~~CSCF shall delete the new SAs.

The P-~~-~~CSCF shall monitor the expiry time of registrations without authentication and adjust the lifetime of SAs it holds to ensure that they live longer than the expiry time given in the registration.

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