3GPP TSG SA WG3 Security — S3#26 **S3-020702**
19- 22 November 2002,
Oxford, UK

Title:	Liaison on (IMS) SA handling and the lifetime of old SA pair in Network Initiated Authentication
Response to:	None.
Source:	SA3
To:	CN1
Cc:	-

Contact Person:

Name:	Tao Haukka
Company:	Nokia Corporation
Tel. Number:	+358 40 5170079
E-mail Address:	**tao.haukka@nokia.com**

Attachments: S3-020701, Open issues in SA handling

1. Overall Description:

SA3 has approved the attached CR regarding to the SA handling during re-authentication. SA3 observed that the latest specification of CN1 is in line with the attached CR, except the consideration of shortening lifetime of old SA pair in Network Initiated Authentication case.

SA3 would like to point out this improves the security level of IMS accessing. An attacker impersonates valid subscriber by a spoofed old session key can be soon rejected by the network.

2. Actions:

To CN1 group:

SA3 kindly asks CN1 to consider the issue, and update corresponding specification to be in line with the S3 approved CR.

3. Date of next SA3 Meetings:

SA3#27	25 - 28 Feb. 2003	Sophia Antipolis, France
SA#28	06 - 09 May 2003	Berlin, Germany

3GPP TSG SA WG3 Security — S3#26 **S3-020701**
19- 22 November 2002, Oxford, UK

CR-Form-v7

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 ☒

Title:	⌘	Open issues in SA handling		
Source:	⌘	Nokia		
Work item code:	⌘	IMS-ASEC	***Date:*** ⌘	21/11/2002
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: ⌘

Before the UE receives confirmation by 200 OK (SM12), UE should use the old SA for non-authentication messages, because it can be sure neither a) the authentication would be successful, nor b) does it know if 200OK would be received eventually. In case a), If UE uses new SA to send any non-authentication messages before the new SA is confirmed by 200 OK (SM12), it may fail due to

1. Authentication failure
2. Integrity failure
3. Sequence number out of synchronization

It is likely the network may attempt to challenge the UE again in these scenarios. Meanwhile the user should be still allowed to use IMS service. Also P-CSCF should continue to forward INVITE to the UE, since it's still a valid subscriber during this phase.

In case b), if re-transmission is failed, UE's new SAs will be quickly deleted, yet P-CSCF removes old SAs once successful authentication is forwarded. This causes no common SA available between the peer, yet each one assumes it holds valid SAs toward the peer. If UE tries old SAs, it won't get response.
It won't solve the problem if P-CSCF adopts new SA to forward INVITE to the UE. Since UE may deleted new SAs already, or pretty soon; if the INVITE can't reach the UE due to same reason, then the problem in last paragraph still remains.

Therefore the issues described atop must be resolved before the deadline of R5 frozen.

On the other hand, to guarantee the Network Initiated Authentication shall abandon the old SA pair quickly, the proposed change is to shorten the lifetime of old SA pair in both UE and P-CSCF, and expect the authentication procedure is done during the window. This operation should follow the regular authentication procedure as close as possible.

Summary of change: ⌘

During SA refreshing phase but before authentication result is received, the old SAs shall be used for those non-authentiation messages. This is valid for both UE and P-CSCF;

After forwarding successful message 200OK, the P-CSCF shall keep the old SAs active towards the UE, until either the old SAs are expired, or further message protected by new SA is received from the UE. The P-CSCF shall move to new SAs.
After receiving 200OK, the UE shall delete the old outbound SA, and keep the old inbound SA to receive from P-CSCF properly. Further outbound traffic in UE shall be protected by new outbound SA.

An side issue: If UE starts an unprotected registration due to poweroff, the P-CSCF should remove the old valid SAs. This is work assumption that has been missing from

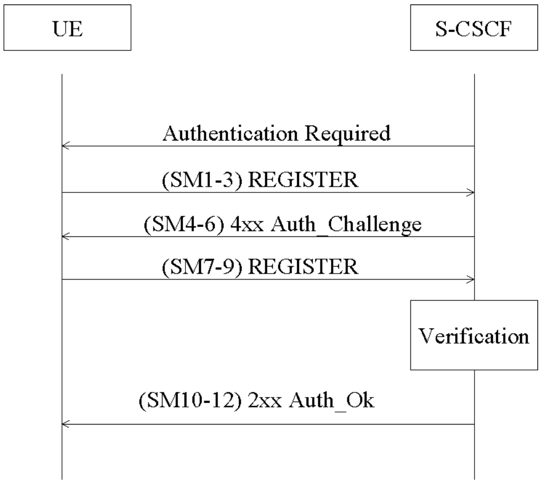
		current specification. In the Network Initiated Authentication case, the P-CSCF and the UE both shorten the old SA pair before registration (SM1) is issued from the UE.
Consequences if not approved:	⌘	• In case of conflict between UE's INVITE request protected by new SAs and deletion of them in the P-CSCF due to case a), the service is rejected to a valid subscriber; • In case of conflict between UE's response to an INVITE which is protect by new SA, and the deletion of new SAs in P-CSCF due to case a), the phone call is lost. • More impact on DoS when user encounters replay attack. Spoofing attack will also prohibit user invites or to be invited. • In case of re-transmission failure, no common SA available between the peer, yet each one assumes it holds valid SAs toward the peer. • In case of re-transmission failure, forwarded INVITE which is protected by new SA may never be received by the UE due to deletion of new SAs.

Clauses affected:	⌘	6.1.4, 7.4.1a, 7.4.2a				
		Y	**N**			
Other specs Affected:	⌘	**X**		Other core specifications	⌘	24.228, 24.229
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

********* First Change ***********

6.1.4 Network Initiated authentications

In order to authenticate an already registered user, the S-CSCF shall send a request to the UE to initiate a re-registration procedure. When received at the S-CSCF, the re-registration shall trigger a new IMS AKA procedure that will allow the S-CSCF to re-authenticate the user.



Both the UE and the P-CSCF shall shorten the lifetime of the old SA pair generated from the last successful authentication, so as to guarantee that the new SA pair shall be used.

The UE shall initiate the re-registration on the reception of the Authentication Required indication. In the event that the UE does not initiate the re-registration procedure after the request from the S-CSCF, the S-CSCF may decide to de-register the subscriber or re-issue an Authentication-Required.

********* Next Change ***********

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 by 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.~~ Meanwhile, if SM1 was protected, the UE shall use the old SAs for messages other than those in the authentication, until a successful message of new authentication is received (SM12); if SM1 was unprotected, the UE is not allowed to use IMS service until it receives an authentication successful message (SM12). ~~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~~ SA is~~are~~ 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~~ old SAs ~~can now be~~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 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:

    - 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 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.