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

S3-020606

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:	⌘	Authenticaton errors cause SA handling in conflict with INVITE		
Source:	⌘	Nokia		
Work item code:	⌘	IMS-ASEC	***Date:*** ⌘	04/11/2002
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:	⌘	When UE is in re-authentication procedure, i.e. there are old SAs valid, the UE should be accepted to start or receive a SIP session, since the UE is still an authenticated subscriber with valid (old) SAs. Authentication failure or integrity failure should prohibit the user to use new SAs but not old SAs. In case of a conflict between UE sending INVITE and P-CSCF sending failure of authentication, IMS service should not be refused by the network.
Summary of change:	⌘	During SA refreshing phase and before authentication result is received, the old SAs should not be deleted; instead they should be used for those message not in authentiation.
Consequences if not approved:	⌘	• There is conflict case, no response for the INVITE will come back to the UE according to current spec, because P-CSCF already deleted the new SA; • If P-CSCF forwards INVITE protected with new SA, and deletes new SA because of authentication failure, the response from UE can not be received due to conflict. • More impact on DoS when user encounters replay attack. Spoofing attack will also prohibit user invites or to be invited.

Clauses affected:	⌘	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:	⌘					

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. The old SAs are now deleted. 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.

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.