CR-Form-v5

CHANGE REQUEST

⌘ 33.203 CR ⌘rev - ⌘ Current version: 5.2.0 ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Update of SA handling procedures
Source:	⌘	Ericsson, Hutchison 3G
Work item code:	⌘	IMS-ASEC
Date:	⌘	12/7/2002
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)

Reason for change:	⌘	Current security association (SA) handling procedures do not cover all the possible cases that can occur
Summary of change:	⌘	Update the way the P-CSCF handles security associations to deal with some cases that are not already covered. Also describes the behaviour of the UE and P-CSCF in isolation of each other.
Consequences if not approved:	⌘	Some behaviour of the P-CSCF is not described, which means that different P-CSCF may take different action possibly causing the UE to become unreachable.

Clauses affected:	⌘	7.4
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ 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 ~~registration is a re-registration, a pair of security associations between~~ UE has an ~~and P-CSCF is~~ already active security association, then it should use this to protect 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 authentication 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. ~~The authenticated re-registration shall initially utilize the existing SA. This is the normal case. However, in the event the UE originates the (SM1) Register message using no protection, the P-CSCF shall still accept it and forward the request to the S-CSCF, indicating that the register message was not integrity protected. This shall trigger the S-CSCF to challenge the subscriber with the execution of a new IMS-AKA authentication procedure as described in clause 6.1.1.~~

~~[Editors Note: The exact mechanism for changing SAs is currently under investigation.]~~

~~Before SM7 is sent by the UE, both peers shall replace the existing SA by the new SA negotiated during these first two messages.~~

~~[Editors Note: The exact mechanism when to change SA1 to SA2 under certain error conditions is FFS.]~~

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 network layer. The message numbers, e.g. SM1, used in the following clauses relate to the message flow given in 6.1.1.

7.4.1 ~~7.4.1~~ Management of security associations in the UE ~~Handling of security associations in authenticated re-registrations (successful case)~~

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

The UE may start an authentication procedure with a 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. Similarly certain messages in the authentication shall be protected with a particular SA. If the UE receives a message protected with the incorrect SA, it should discard the message.

A successful authentication proceeds in the following steps:

- The UE sends the SM1 message to register with the IMS. If 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 should 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. For outbound traffic the new SA shall be used in preference to the old SA.
- 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 may be used to protect these messages.

The UE shall delete any SA whose lifetime is exceeded.

~~Before re-registration begins the following SAs exist:~~

- ~~SA1 from UE to P-CSCF;~~
- ~~SA2 from P-CSCF to UE.~~

~~The re-registration then is as follows:~~

~~1) The UE sends SM1 to re-register with the IMS, using the existing SA1 to the P-CSCF. As in the case of a new registration, a list of parameters to be negotiated in a security association set-up is included.~~

~~[Editors Note: It is FFS if the SA1 shall be used for SM1 or not]~~

~~2) The P-CSCF waits for the response SM4 from the S-CSCF and then sends SM6 to the UE, using SA2. As in the case of a new registration, the parameters selected for the new security associations are included. The P-CSCF then creates two new security associations, in parallel to the existing ones, in its database:~~

- ~~SA11 from UE to P-CSCF;~~
- ~~SA12 from P-CSCF to UE.~~

~~3) If SM6 could be successfully processed by the UE, the UE also creates the new SAs SA11 and SA12 in its database. The UE then sends SM7 to the P-CSCF. As in the case of a new registration, the authentication response and the list of parameters repeated from message 1 are included. SM7 is protected with the new SA11.~~

~~4) The P-CSCF waits for the response SM10 from the S-CSCF and then sends SM12 to the UE, using the new SA 12.~~

~~5) After the reception of SM12 by the UE, the re-registration is complete.~~

~~The UE now uses the new SAs for all subsequent messages. The old (outbound) SA1 is deleted. The old (inbound) SA2 must be kept until a further SIP message protected with the new inbound SA12 is successfully received from the P-CSCF.~~

~~The P-CSCF keeps all four SAs with the UE active until a further SIP message protected with the new inbound SA11 is successfully received from the UE. In the meantime, the P-CSCF continues to use the old SA2 for outbound traffic to the UE.~~

7.4.2 Management of security associations in the P-CSCF~~Error cases related to authenticated re-registration~~

~~Whenever an expected message is not received after a time-out the receiving entity considers the registration to have failed. The receiving entity then deletes any new security associations it may have established and continues to use the old ones if they have not yet expired.~~

~~If the registration protocol goes well up to the last message SM12, and SM12 is sent by the P-CSCF, but not received by the UE , then the UE has only the olds SAs available (after the time-out), but the P-CSCF cannot know this. Therefore, the P-CSCF continues to use the old SA2 for outbound traffic to the UE, but keeps both, old and new SAs. The new SAs are deleted when a message is received from the UE which is protected with the old SA, or if a REGISTER message is received on the port where the P-CSCF accepts specific unprotected messages.~~

The P-CSCF may enter an authentication procedure with a pair of SAs from a previously completed authentication. It may also contain a 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 should 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 it is protected, it should 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 should 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. For outbound traffic the old SA shall be used in preference to the new SA.

- The P-CSCF forwards the successful registration message (SM12) to the UE. It shall be protected using the new inbound 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.

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 may be used to protect these messages.

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