3GPP TSG SA WG3 Security — S3#25 **S3-020527**

8 - 11 October 2002

Bristol, UK

Source: **Hutchison 3G**

Title: **Registration and SA lifetimes**

Document for: **Discussion/Decision**

Agenda Item:

Introduction

At the last meeting S3-020372 (attached) raised the issue of some problems with using the registration expiry timer to set the SA lifetime.

There are two suggested ways to cover the problem with a registration without authentication:

1) Limit the expiry time of registrations (without authentications) to the maximum time that an IMPU is currently registered (this does not stop the network requesting an authentication to register the IMPU for longer).
2) Extend the lifetime of the SA to ensure that it lives longer than the registration.

There were issues identified with each approach that stopped them being accepted. The decision was not resolved during an email discussion after the meeting. The following sections contain a summary of the advantages and disadvantages of each approach.

For registrations with authentications, S3-020372 suggested ensuring that the lifetime of the new SA was at least as long as that of the old SA to avoid having an IMPU registered for longer than the SA will live. The author is not aware of another suggestion to deal with this case.

Limiting the expiry lifetime

The main advantage of this method from the security perspective is that there is a clear SA lifetime, which is negotiated at the start and never changed. It also seems to be inline with the text that was in v5.1.0 of the TS 33.203

"*The SA between the UE and the P-CSCF will have a limited lifetime. The lifetime timer shall be the same as the registration timer, which is defined per contact address. When the UE registers the registration timer will be negotiated between the UE, the P-CSCF and the S-CSCF. The S-CSCF will be able to accept, decrease or increase the proposed expiration time from the UE and the final value is sent in the response to the UE. The expiry time in the UE will be shorter than the expiry time in the S-CSCF, such that the UE is able to re-register. For each new successful authentication the SA shall be updated.* ***The S-CSCF shall align the expiration of subsequent registrations with any existing registration timer.*** *The SA is deleted if the registration timers expires in the P-CSCF or in the S-CSCF.*"

This text got removed in the update to include the IP layer integrity mechanism. This method results in each authentication meaning that any IMPU for the authenticated IMPI can be registered without a further authentication until the expiry time of the registration with the authentication. To register an IMPU past this time requires a new authentication.

The disadvantage of this method is that it places a restriction on the policy in the S-CSCF as it puts a limit on the time that an IMPU can be registered without an authentication. This is not much of a restriction if the UEs offer the network large registration times, so the network could space authentications out. It is more of a restriction if the UE only offer short registration times (as the S-CSCF can not extend the time). Of course the UE can send unprotected registers and force an authentication from the network.

Extending the SA lifetime

The major disadvantage of extending the SA lifetime was the idea that this creates an indefinitely extendable SA in the UE while it believes it is connected to the network, unless some other mechanism is introduced into UE to remove/replace it. Currently the SA would be deleted if the UE is switched off or de-registers all its IMPUs.

The advantage of this method is that there is no restriction on the local policy of the S-CSCF. If this is the selected method, there seems to be little use for the lifetime of an SA.

Conclusion

This paper reviews the discussion so far on the binding between SA and registration lifetimes, in order to help SA3 reach a consensus on one of the discussed solutions or perhaps an alternative.

A CR to cover each possible case is attached to this contribution.

3GPP TSG SA WG3 Security — S3#24 **S3-~~020xxx~~020372**

9 - 12 July 2002

Helsinki, Finland

Source: **Hutchison 3G UK**

Title: **SA and registration lifetimes**

Document for: **Discussion/Decision**

Agenda Item: **7.1~~x.x~~**

Introduction

This contribution looks at the relationship between the ~~l~~expiry ~~ife~~times of registrations and the lifetimes of SAs at the P-CSCF and UE.

T~~SA3 has been using the working assumption that t~~he expiry time~~r~~ of a registration will be used to set the lifetime of an SA. Without some further clarification, this can cause the problems described in the next section. ~~, although there is no explicit text to describe exactly how this relation happens (careful here there may be some text, probably stronger than a working assumption).~~

Timing Issues

Whatever mechanism is selected to handle registration lifetimes and the expiry time of SAs~~ lifetimes~~, it is important to ensure ~~never end up in the position~~ that an IMPU is never registered for longer than ~~the lifetime of~~ the SA that will be used to protect the ~~-~~traffic to/from that IMPU will live, as a registered UE will become unreachable.~~.~~

~~This document does not consider possible inconsistent states between the UE, P-CSCF and S-CSCF caused by losing (even after re-transmissions) messages.~~

There are two processes that affect at least one of the expiry time of registrations and the lifetime~~s~~ of ~~registrations and~~ SAs, that is, registrations without authentications and registrations with authentications.

Firstly we consider a registration without an authentication. Suppose a subscriber has already registered IMPU1 until time X and the P-CSCF and UE contain a corresponding SA that will also expiry at time X. The subscriber then tries to register IMPU2. The S-CSCF accepts this registration attempt without an authentication and sets the registration of IMPU2 to expire at time Y (see below diagram).

UE	**P-CSCF**	**S-CSCF**
IMPU1 registered until time X		IMPU1 registered until time X
SA that lives until time X	SA that lives until time X	

-------------------------------- Registration of IMPU2 without an authentication -----------------------------------

IMPU1 registered until time X		IMPU1 registered until time X
IMPU2 registered until time Y		IMPU2 registered until time Y
SA that lives until time X	SA that lives until time X	

If Y is later than X, then the SA will expire before the registration and a registered IMPU could become unreachable.

This problem can be avoided by applying one (and only one is necessary) of the following rules in the network

1. For registrations without authentication, the expiry timer of the registration shall be set to no longer than the longest remaining time of all the currently registered IMPUs for that IMPI.
2. The P-CSCF monitors the expiry timer of all registrations without authentication for an IMPI and increases the lifetime of the latest SA for that IMPI to ensure the SA lives longer than any registration.

From a security perspective, the first rule seems to be the most sensible. Put another way, the rule says if that the latest a user has IMPU registered until is time X and it wants to register an IMPU until time Y later than X, it requires an authentication. This also avoids the need for P-CSCF to monitor the lifetimes of all registrations without authentications and adjust the lifetimes of SAs accordingly.

Secondly we consider a registration with an authentication. Suppose a subscriber has already registered an IMPU with expiry time X and the P-CSCF and UE contain a corresponding SA that has will also expiry after time X. The subscriber then tries to register a further IMPU. The S-CSCF accepts this registration attempt only after an authentication and set the expiry timer of this registration to Y (see the below diagram)

UE	**P-CSCF**	**S-CSCF**
IMPU1 registered until time X		IMPU1 registered until time X
SA that lives until time X	SA that lives until time X	

-------------------------------- Registration of IMPU2 with an authentication -----------------------------------

IMPU1 registered until time X		IMPU1 registered until time X
IMPU2 registered until time Y		IMPU2 registered until time Y
SA that lives until time Y	SA that lives until time Y	

Note: the previous SA may be kept for a short time to enable smooth handover

If Y is less than X, then the SA will expire before the registration and a registered IMPU could become unreachable.

The sensible way to avoid this problem is to set the lifetime of the SA to expire at least as late as the registration and of the previous SA.

~~The problem can be avoided by either stopping the problem from happening by putting restrictions on the registration lifetimes (rule a) or taking corrective action on the SA lifetimes at the P-CSCF and UE (rule b).~~

~~A registration without authentication increases the lifetime of a registration, this suggests that one of two rules should be applied;~~

~~1a) the expiry time of the registration is not allowed to more than the lifetime of the current SA.~~

~~1b) the lifetime of the SA needs to be increased (if necessary) to at least that of the expiry time of the registration~~

~~An authentication requires one of the following rules to be applied;~~

~~2a) the registration timer of the new registration must be longer than any current registration timer.~~

~~2b) the expiry time of the new SA must be at least as long as the previous SA.~~

~~Comparison of Rules 1a and 1b~~

~~Rule 1a puts a restriction on the lifetimes of registrations. It also requires the S-CSCF to keep a timer for each IMPI. It means that to register an IMPU for a long time may require an authentication. This would probably only an issue, if getting towards the end of all registration lifetimes in the S-CSCF. Without a detailed analysis it seems that this method would force more registrations without authentication and authentications. It is hard to say exactly to what extent there will be additional registrations and authentications.~~

~~Perhaps the strongest arguments in favour of rule 1a are negative implications on the selection of rule 1b.~~

~~Rule 1b means that an SA lifetime will be extended (possibly only at the application layer). This means the P-CSCF will need to look at the expiry time of every registration in order to update the lifetime of the SA. This could seem odd in the sense that an SA is negotiated for a certain lifetime (at the application layer) and then the lifetime gets extended (at the application layer). An alternative view is that an SA is negotiated for an effectively limitless lifetime (at the network layer) but with a (changeable) expiry time at the application layer.~~

~~One issue that was raised in the IMS drafting session of the last SA3 meeting was that with the IP layer SAs held effectively at two layers, it is possible to have an SA left at the network layer after it is deleted from the application layer (e.g. failure at application layer or bad implementation). Using rule 1b means that the lifetime of the SA needs to be continually extended, whereas with Rule 1a it is set after the authentication is successful and left until the SA is deleted (due to either the expiry time being exceeded or the SA becoming obsolete). This means that if Rule 1a is selected, it is less likely to have an SA left at the network layer given that it is possible to update the expiry time of the SA at the network layer once the authentication is successful. This could be done by either updating the expiry time only of the SA or deleting the odd version of the SA and adding a new version of the SA with updated expiry time.~~

~~The best rule here is ………..~~

~~Comparison of Rules 2a and 2b~~

~~Rule 2a puts a limitation on setting registration timers and the storage variable in the S-CSCF to know the expiry time of the previous SA.~~

~~Rule 2b requires some small amount of processing once the authentication is successful.~~

~~Clearly Rule 2b seems the most sensible.~~

Proposed Text to Cover Suggested Functionality~~ext for TS 33.102~~

This section proposes some text to cover the above decisions. The exact text, where to put the text into the document and potentially even which document the text should be in needs to be decided once there is agreed text for the SA handling.

For registrations without an authentication, the proposed text is as follows:~~rule 1x we need text along the following lines:~~

~~“……………………..”~~ “For registrations without authentication, the S-CSCF shall set the expiry timer of the registration to be not larger than the largest current expiry timer of all registered IMPU related (via their IMPI) to the IMPU being registered”

For registrations with an authentication, the proposed text is as follows: ~~rule 2b we need text along the following lines:~~

“Once the P-CSCF/UE considers the authentication to be successful, it sets the SA lifetime to be using the largest of the registration expiry and the time left before the ~~qual to the maximum of the~~ previous ~~SA’s lifetime and the registration~~ expires~~y lifetime~~.”

~~Generic text (maybe not needed)~~

~~“If the UE has an SA with only short lifetime and a registration with a longer lifetime, then the UE should send an unprotected register.”~~

3GPP WSG – SA3 Meeting #25
Munich, Germany, 8th – 11th October

Tdoc ⌘S3-020527_att2

CR-Form-v7

CHANGE REQUEST

⌘	**33.203**	**CR**		⌘ **rev**	**-**	⌘	Current version:	**5.3.2** ⌘

*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: ⌘	Registration and SA lifetimes			
Source: ⌘	Hutchison 3G			
Work item code: ⌘	IMS-ASEC		***Date:*** ⌘	03/11/2002
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: ⌘	The current method for handling the combination of registration and SA lifetimes could leave an IMPU registered but with no SA available to contact the UE
Summary of change: ⌘	Ensures that any new SA created lives at least as long as the previous SA and that the expiry time of any registration without authentication does not exceed the SA lifetime.
Consequences if not approved: ⌘	A registered IMPU may be unreachable causing a loss of service.

Clauses affected: ⌘	6.1, 7.4.1a, 7.4.2a			
	Y	**N**		
Other specs affected: ⌘	**Y**		Other core specifications ⌘	24.229
		N	Test specifications	
		N	O&M Specifications	
Other comments: ⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.1 Authentication and key agreement

The scheme for authentication and key agreement in the IMS is called IMS AKA. The IMS AKA achieves mutual authentication between the ISIM and the HN, cf. Figure 1. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI, cf. [3]. The HSS and the ISIM share a long-term key associated with the IMPI.

The HN shall choose the IMS AKA scheme for authenticating an IM subscriber accessing through UMTS. The security parameters e.g. keys generated by the IMS AKA scheme are transported by SIP.

The generation of the authentication vector AV that includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in [1]. The ISIM and the HSS keep track of counters SQN_{ISIM} and SQN_{HSS} respectively. The requirements on the handling of the counters and mechanisms for sequence number management are specified in [1]. The AMF field can be used in the same way as in [1].

Furthermore a security association is established between the UE and the P-CSCF. The subscriber may have several IMPUs associated with one IMPI. These may belong to the same or different service profiles. Only one SA shall be active between the UE and the P-CSCF. This single SA shall be updated when a new successful authentication of the subscriber has occurred, cf. section 7.4.

It is the policy of the HN that decides if an authentication shall take place for the registration of different IMPUs e.g. belonging to same or different service profiles. If the registration is not authenticated, then the expiry time will be limited to maximum expiry time of any currently registered IMPU. Regarding the definition of service profiles cf. [3].

********************* NEXT CHANGED SECTION *******************

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. 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 maximum of registration timer in the message and the lifetime of the old SAs. 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 SAs can now be 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, 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.

3GPP WSG – SA3 Meeting #25
Munich, Germany, 8th – 11th October

Tdoc ⌘S3-020527_att3

CR-Form-v7

CHANGE REQUEST

⌘	**33.203**	**CR**		⌘ **rev**	**-**	⌘	Current version:	**5.3.2** ⌘

*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: ⌘	Registration and SA lifetimes		
Source: ⌘	Hutchison 3G		
Work item code: ⌘	IMS-ASEC	***Date:*** ⌘	03/11/2002
Category: ⌘	**F** *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.	***Release:*** ⌘	Rel-5 *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 current method for handling the combination of registration and SA lifetimes could leave an IMPU registered but with no SA available to contact the UE
Summary of change: ⌘	Ensures that any new SA created lives at least as long as the previous SA and the SA lifetime is updated if the expiry time of a registartion without an authentication exceeds the current lifetime.
Consequences if not approved: ⌘	A registered IMPU may be unreachable causing a loss of service.

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

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

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. 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 maximum of registration timer in the message and the lifetime of the old SAs. 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 monitor the expiry time of registrations without authentication and adjust the lifetime of SAs it hold to ensure that they live longer than the expiry time given in the registration.

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 SAs can now be 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, 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 monitor the expiry time of registrations without authentication and adjust the lifetime of SAs it hold 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.