3GPP TSG SA WG3 Security — S3#29 **S3-030399**
15 - 18 July 2003
San Francisco, USA

Title:	**SA Lifetimes**
Source:	**3, Ericsson, Lucent**
Document for:	**Discussion/Decision**
Agenda Item:	**7.1**
Attachments:	**Proposed LS to CN and CN1 and a proposed CR to TS 33.203**

Introduction

CN1 and CN have sent SA3 liaisons, S3-030330 and S3-030336 respectively, on the subject of SA lifetimes. CN1 approved some CRs to TS 24.229 on controlling the SA lifetime at the UE and P-CSCF. These CRs were subsequently rejected by CN plenary, as the CRs were not inline with the text in TS 33.203. To resolve this mis-alignment, CN wrote a liaison to SA3 containing some questions for clarification. This contribution propose answers to these question and includes a draft proposed response liaison and a draft CR to TS 33.203 resulting from the answer given in the contribution.

The difference between the SA3 proposed method and the CN1 proposed method is the following. SA3 propose setting the lifetime of a new SA based on the lifetime of the current SA and the expiry time of the new registration, whereas CN1 propose setting the lifetime of the SA based on the lifetime of all registrations. This leads to two main differences, as the CN1 method requires the P-CSCF to store all the registration lifetimes and with the CN1 method the lifetime of an SA could be shortened on de-registrations.

Proposed Answer to CN's questions

In S3-030336, CN asks SA3 several questions on SA handling. This section discusses the issue raised by these questions, proposes text for a reply liaison and also proposes changes for a CR to TS 33.203. A draft liaison and CR are attached to this contribution.

Question 1

In 33.203 section 7.1, bullet point number 8 it states that the SA lifetime should be set to the Registration lifetime. Further, in section 7.4.1a it is stated that the SA lifetime is set to the maximum of the SA lifetime or the registration. Is the correct understanding of these two statements that a) if there are no existing registrations related to an IMPI then 7.1 applies, and b) if there are already existing registrations related to an IMPI then 7.4.1a applies ?

Discussion: The understanding is correct. In fact, given that there are no existing registrations there are no SAs hence in this case the two methods are equivalent. Bullet 8 in section 7 should be removed to avoid confusion.

Proposed text for liaison: The understanding is correct. In fact, given that there are no existing registrations there are no SAs, hence in this case the two methods are equivalent. Bullet 8 in section 7 will be removed to avoid confusion.

Proposal for CR: Delete bullet 8 in section 7.

Question 2

It has also been noted that the definition of the setting of the lifetime is not clear (in 33.203 and 24.229) as the Expires header in a registration is a 'relative' time i.e. the registration will be valid for that time, starting from the registration point. It is possible that a re-registration results in an end time earlier or later than that set by existing registrations, even when this expires value is shorter than one received for a previous registration (e.g. the previous registration may be close to expiry). Can SA3 please confirm that when setting the lifetime of the SA the intent is to utilise the latest end time?

Discussion: The lifetime of the SA must be set to the latest end time to ensure the SA does not expire before all registration have expired as this would make the UE unreachable. The text in TS 33.203 should be changed to read as follows “The UE sets the lifetime of the new SAs such that it either equals the latest lifetime of the old SAs or it will expire shortly after the registration timer in the message, depending which gives the SAs the longer life”. A similar change is necessary for the P-CSCF.

Proposed text for liaison: The lifetime of the SA must be set to the latest end time to ensure the SA does not expire before all registrations have expired, otherwise the UE may become unreachable. The text in TS 33.203 will be changed to read “The UE sets the lifetime of the new SAs such that it either equals the latest lifetime of the old SAs or it will expire shortly after the registration timer in the message, depending which gives the SAs the longer life” with a similar change for the P-CSCF to avoid possible mis-interpretations.

Proposal for CR: The text should be changed as discussed above plus a small additional change to clarify the behaviour at registrations without an authentication.

Question 3

The proposals in the postponed CR’s allow for the SA lifetime to be shortened to match the longest remaining registration. The existing text in 7.4.1a of 33.203 would not result in a shortening of the SA lifetime (it is either lengthened or unchanged) until the final registration is removed, when the SA will be deleted. Do SA3 see an advantage in including a mechanism to allow the SA lifetime to be shortened ?

Discussion: There is no value in decreasing the SA lifetime when there is only one set of SAs. There is value at a re-authentication when there needs to be more than one set of SAs to enable a smooth handover. This cancels the "old" SAs being used for too long after an authentication. Currently TS 33.203 only mandates this at a network initiated re-authentication. If the lifetime is decreased, it should be done for the correct reasons, not just to mirror the registration lifetime that will expire last. The CN1 proposal also seems to mandate the P-CSCF holding registration lifetimes. This is not mandated anywhere else and, in our view, the potential benefits from such a requirement do not warrant the expected storage and processing overhead .

SA3 should re-examine the reasons for mandating the shortening of SA lifetimes only after network initiated re-authentications, vis-à-vis applying this process for all re-authentications. All authentications beyond the initial one, when the first IMPU is registered (and in cases when something has gone wrong), are effectively network initiated as the S-CSCF chooses to authenticate a protected REGISTER. It seems logical that these should be treated the same as network initiated re-authentications and the lifetime of the “old SA” should be reduced accordingly after a successful authentication. To achieve this it would require sentences like the following added to the appropriate place in TS 33.203 “The P-CSCF shall reduce (as necessary) the lifetime of the old SAs to ensure that they are only used for a short time. This reduction in time should still allow the UE enough time to perform a fresh successful authentication in case the final message in an authentication procedure is lost.” It would also require the following sentence deleted from the network initiated re-authentication section “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.”

Proposed text for liaison: SA3 sees no value shortening the lifetime of the SA based on de-registrations. If an SA lifetime is to be shortened, SA3 believe it should be done to old SAs after a successful authentication. To this end SA3 will add the following sentences to TS 33.203. “The P-CSCF shall reduce (as necessary) the lifetime of the old SAs to ensure that they are only used for a short time. This reduction in time should still allow the UE enough time to perform a fresh successful authentication in case the final message in an authentication procedure is lost.”

Proposal for CR: Add the sentences and delete the text as proposed in the discussion section.

Question 4

It has been questioned why the SA needs to be assigned a lifetime at all. It is noted that the SA will be deleted when the last registration related to an IMPI expires in any event (24.229 includes the necessary mechanisms to inform the PCSCF of this event). At other times it will be valid during an ongoing registration, and with the existing 33.203 text the lifetime may be longer than the longest remaining registration. Does SA3 believe that there is a requirement for a defined SA lifetime ?

Discussion: This is an interesting question. There seems to be no need when there is just one set of SAs, except perhaps without a lifetime these SAs are only deleted when all the registrations expire. If it is possible that the P-CSCF will not get the de-registration messages, in cases like a critical failure of the S-CSCF, then the SA lifetimes have value. Furthermore it is a general security principle to give each security association a limited lifetime, as this makes it very clear to which point a particular key can be used to protect data. When there are two sets of SAs, there are two uses of an SA lifetime (or equivalent timer). During an authentication process, the P-CSCF creates SAs when it sends the challenge to the UE. This SA should only live for a short time if the authentication is not successful. After the authentication is complete successfully, the old SAs should have its own lifetime and not always wait until the new SAs are used before it is deleted. At the UE, the same arguments exist. For these reasons it is better to keep the SA lifetime parameter. This is currently no text in TS 33.203 to delete the SAs when all the associated IMPUs are de-registered. It is proposed to add this to the CR.

Proposed text for liaison: SA3 believe there is a need for an SA lifetime. This is particularly true when there are two sets of SAs (because of a re-authentication), as there is a security requirement to not allow the “old” set of SAs to stay valid for too long. SA3 will add text to ensure that the SAs are deleted, once the associated IMPUs are de-registered.

Proposal for CR: Text will be added to both the UE and P-CSCF SA handling sections to ensure that SAs are deleted once all the associated IMPUs are de-registered. .

3GPP TSG-WG3 Meeting #29
San Francisco, USA, 15th–18th July 2003

Tdoc ⌘S3-030xxx_att_2

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.203** **CR** **CRNum** ⌘**rev** ⌘ Current version: **5.6.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Clarifications on the security association lifetime management
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	02/07/2003
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:	⌘	Some of the current security association lifetime management is unclear and inconsistent. A security weakness has been identified in only shortening the old SAs lifetime after network initiated re-authentications, rather than all re-authentications.
Summary of change:	⌘	The setting of the A lifetime in section 7.1 is removed, as it is covered in section 7.4.1a. The method of setting of the new security associations lifetime is made more explicit. The lifetime of the old SA is shortened after all re-authentications rather than just after network initiated re-authentications.
Consequences if not approved:	⌘	Inconsistence and unclear statements would be left in the specification, which could possibly cause incompatible implementations. A security weakness will be left in the specification.

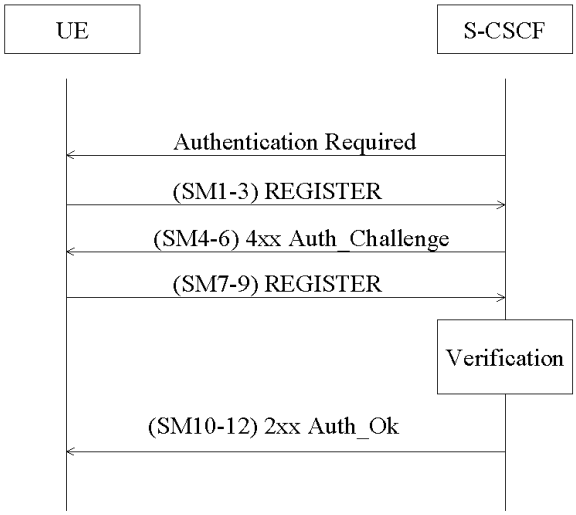
Clauses affected:	⌘	6.1.4, 7.1, 7.4.1a, 7.4.2a

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		TS 24.229, TS 24.228
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

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.

7.1 Security association parameters

For protecting IMS signaling between the UE and the P-CSCF it is necessary to agree on shared keys that are provided by IMS AKA, and a set of parameters specific to a protection method. The security mode setup (cf. clause 7.2) is used to negotiate the SA parameters required for IPsec ESP with authentication, but without confidentiality.

The SA parameters that shall be negotiated between UE and P-CSCF in the security mode set-up procedure, are:

- **Integrity algorithm**

NOTE: What is called "authentication algorithm" in [13] is called "integrity algorithm" in this specification in order to be in line with the terminology used in other 3GPP specifications and, in particular, to avoid confusion with the authentication algorithms used in the AKA protocol.

The integrity algorithm is either HMAC-MD5-96 [15] or HMAC-SHA-1-96 [16].

Both integrity algorithms shall be supported by both, the UE and the P-CSCF as mandated by [13]. In the unlikely event that one of the integrity algorithms is compromised during the lifetime of this specification, this algorithm shall no longer be supported.

NOTE: If only one of the two integrity algorithms is compromised then it suffices for the IMS to remain secure that the algorithm is no longer supported by any P-CSCF. The security mode set-up procedure (cf. clause 7.2) will then ensure that the other integrity algorithm is selected.

- **SPI (Security Parameter Index)**

The SPI is allocated locally for inbound SAs. The triple (SPI, destination IP address, security protocol) uniquely identifies an SA at the IP layer. The UE shall select the SPIs uniquely, and different from any SPIs that might be used in any existing SAs (i.e. inbound and outbound SAs). The SPIs selected by the P-CSCF shall be different than the SPIs sent by the UE, cf. section 7.2.

NOTE: This allocation of SPIs ensures that protected messages in the uplink always differ from protected messages in the downlink in, at least, the SPI field. This thwarts reflection attacks. When several applications use IPsec on the same physical interface the SIP application should be allocated a separate range of SPIs.

The following SA parameters are not negotiated:

- Life type: the life type is always seconds;
- SA duration: the SA duration has a fixed length of 2^{32}-1;

NOTE: The SA duration is a network layer concept. From a practical point of view, the value chosen for "SA duration" does not impose any limit on the lifetime of an SA at the network layer. The SA lifetime is controlled by the SIP application as specified in clause 7.4.

- Mode: transport mode;
- Key length: the length of the integrity key IK_{ESP} depends on the integrity algorithm. It is 128 bits for HMAC-MD5-96 and 160 bits for HMAC-SHA-1-96.

Selectors:

The security associations (SA) have to be bound to specific parameters (selectors) of the SIP flows between UE and P-CSCF, i.e. source and destination IP addresses, transport protocols that share the SA, and source and destination ports.

- IP addresses are bound to a pair of SAs, as in clause 6.3, as follows:
  - inbound SA at the P-CSCF:
    The source and destination IP addresses associated with the SA are identical to those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

- outbound SA at the P-CSCF:
  the source IP address bound to the outbound SA equals the destination IP address bound to the inbound SA;
  the destination IP address bound to the outbound SA equals the source IP address bound to the inbound SA.

NOTE: This implies that the source and destination IP addresses in the header of the IP packet in which the protected SIP REGISTER message was received by the P-CSCF need to be the same as those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

- The transport protocol selector shall allow UDP and TCP.

- Ports:

1. The P-CSCF receives messages protected with ESP from any UE on one fixed port (the"protected port") different from the standard SIP port 5060. The number of the protected port is communicated to the UE during the security mode set-up procedure, cf. clause 7.2. For every protected request towards UE, the P-CSCF shall insert the protected port into Via header. No unprotected messages shall be sent from or received on this port. From a security point of view, the P-CSCF may receive unprotected messages from any UE on any port which is different from the protected port.

NOTE: The protected port is fixed for a particular P-CSCF, but may be different for different P-CSCFs.

2. For protected or unprotected outbound messages from the P-CSCF (inbound for the UE) any source port number may be used at the P-CSCF from a security point of view.

3. For each security association, the UE assigns a local port to send or receive protected messages to and from the P-CSCF ("protected port"). No unprotected messages shall be sent to or received on this port. The UE shall use a single protected port number for both TCP and UDP connections. The port number is communicated to the P-CSCF during the security mode set-up procedure, cf. clause 7.2. When the UE sends a re-REGISTER request, it shall always pick up a new port number and send it to the network. If the UE is not challenged by the network, the port number shall be obsolete. Annex H of this specification gives detail how the port number is populated in SIP message. From a security point of view, the UE may send or receive unprotected messages to or from the P-CSCF on any ports which are not the protected ports.

4. The P-CSCF is allowed to receive only REGISTER messages on unprotected ports. All other messages not arriving on the protected port shall be discarded by the P-CSCF.

5. For every protected request, the UE shall insert the protected port of the corresponding SA into Via header. The UE is allowed to receive only the following messages on an unprotected port:

   - responses to unprotected REGISTER messages;

   - error messages.

   All other messages not arriving on a protected port shall be discarded by the UE.

The following rules apply:

1. For each SA which has been established and has not expired, the SIP application at the P-CSCF stores at least the following data: (UE_IP_address, UE_protected_port, SPI, IMPI, IMPU1, ... , IMPUn, lifetime) in an "SA_table".

NOTE: The SPI is only required when initiating and deleting SAs in the P-CSCF. The SPI is not exchanged between IPsec and the SIP layer for incoming or outgoing SIP messages.

2. The SIP application at the P-CSCF shall check upon receipt of a protected REGISTER message that the pair (source IP address, source port) in the packet headers coincide with the UE's address pair (IP address, source port) inserted in the Via header of the protected REGISTER message. If the Via header does not explicitly contain the UE's address pair, but rather a symbolic name then the P-CSCF shall first resolve the symbolic name by suitable means to obtain an address pair.

3. The SIP application at the P-CSCF shall check upon receipt of an initial REGISTER message that the pair (UE_IP_address, UE_protected_port), where the UE_IP_address is the source IP address in the packet header and the protected port is sent as part of the security mode set-up procedure (cf. clause 7.2), has not yet been associated with entries in the "SA_table". Furthermore, the P-CSCF shall check that, for any one IMPI, no more

than three SAs per direction are stored at any one time. If these checks are unsuccessful the registration is aborted and a suitable error message is sent to the UE.

NOTE: According to clause 7.4 on SA handling, at most three SAs per direction may exist at a P-CSCF for one user at any one time.

4. For each incoming protected message the SIP application at the P-CSCF shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by the pair (UE_IP_address, UE_protected_port) in the "SA_table". The SIP application at the P-CSCF shall further check that the IMPU associated with the SA in the "SA_table" and the IMPU in the received SIP message coincide. If this is not the case the message shall be discarded.

5. For each SA which has been established and has not expired, the SIP application at the UE stores at least the following data: (UE_protected_port, SPI, lifetime) in an "SA_table".

NOTE: The SPI is only required to initiate and delete SAs in the UE. The SPI is not exchanged between IPsec and the SIP layer for incoming or outgoing SIP messages.

6. When establishing a new pair of SAs (cf. clause 6.3) the SIP application at the UE shall ensure that the selected number for the protected port, as well as SPI number, do not correspond to an entry in the "SA_table".

NOTE: Regarding the selection of the number of the protected port at the UE it is generally recommended that the UE randomly selects the number of the protected port from a sufficiently large set of numbers not yet allocated at the UE. This is to thwart a limited form of a Denial of Service attack. UMTS PS access link security also helps to thwart this attack.

7. For each incoming protected message the SIP application at the UE shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by UE_protected_port in the "SA table". The source port selector is set to be a wildcard in the UE's IPsec database.

NOTE: If the integrity check of a received packet fails then IPsec will automatically discard the packet.

~~8. The lifetime of an SA at the application layer between the UE and the P-CSCF shall equal the registration period.~~

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 be~~y~~ 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. 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).
- 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~~such that it either equals the latest lifetime of the old SAs or it will expire shortly after the registration timer in the message, depending which gives the SAs the longer life. For further traffic sent from UE, the new outbound SA is used. The old outbound 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 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 UE shall delete the new SAs.

The UE shall monitor the expiry time of registrations without an authentication and if necessary increase ~~adjust~~ the lifetime of the SAs such that it will expire shortly after the registration timer in the message~~it holds to ensure that they live longer than the expiry time given in the registration~~.

The UE shall delete any SA whose lifetime is exceeded. The UE shall delete all SAs it holds once all the IMPUs are de-registered.

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 existing SAs from 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 such that they either equals the latest lifetime of the old SAs or it will expire shortly after the registration timer in the message, depending which gives the SAs the longer life~~equal to the maximum of registration timer in the message and the lifetime of the old SAs~~.
- After SM12 is sent, the P-CSCF handles the UE related SAs according to following rules:
  - If there are old SAs, 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, the P-CSCF keeps this inbound SA and the corresponding outbound SA with the UE active, and continues to use them. Any other old SAs are deleted. The P-CSCF shall reduce (as necessary) the lifetime of the stored old SAs to ensure that they are only used for a short time. This reduction in time should still allow the UE enough time to perform a new successful authentication in case the final message in an authentication procedure is lost. 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 an authentication and if necessary increase ~~adjust~~ the lifetime of SAs such that it will expire shortly after the registration timer in the message~~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. The P-CSCF shall delete all SAs it holds that are associated with a particular IMPI once all the associated IMPUs are de-registered.

3GPP TSG-SA WG3 Security – S3#29 **S3-030xxx_att_1**
San Francisco, USA, 15th – 18th July 2003.

Title:	**[DRAFT]** Response LS on Security Association Lifetime Management
Response to:	LS (S3-030336 = NP-030308) on Security Association Lifetime Management and LS (S3-030330 and LS (S3-030330 = NP-030918) on Security Association Lifetimes
Release:	5
Work Item:	IMS-CCR
Source:	SA3
To:	CN, CN1
Cc:	

Contact Person:
Name: Adrian Escott
Tel. Number: +44 7782 325254
E-mail Address: adrian.escott@three.co.uk

Attachments: Agreed CR

---

1. Overall Description:

SA3 would like to thank CN and CN1 for their liaisons on Security Association Lifetimes.

In their liaison CN ask SA3 several questions to get some clarifications to enable CN1 to apply the correct changes to TS 24.229. SA3 have considered the questions and agreed on the following answers.

Q1*. In 33.203 section 7.1, bullet point number 8 it states that the SA lifetime should be set to the Registration lifetime. Further, in section 7.4.1a it is stated that the SA lifetime is set to the maximum of the SA lifetime or the registration. Is the correct understanding of these two statements that a) if there are no existing registrations related to an IMPI then 7.1 applies, and b) if there are already existing registrations related to an IMPI then 7.4.1a applies ?*

Answer: The understanding is correct. In fact, given that there are no existing registrations there are no SAs, hence in this case the two methods are equivalent. Bullet 8 in section 7 will be removed to avoid confusion.

Q2*. It has also been noted that the definition of the setting of the lifetime is not clear (in 33.203 and 24.229) as the Expires header in a registration is a 'relative' time i.e. the registration will be valid for that time, starting from the registration point. It is possible that a re-registration results in an end time earlier or later than that set by existing registrations, even when this expires value is shorter than one received for a previous registration (e.g. the previous registration may be close to expiry). Can SA3 please confirm that when setting the lifetime of the SA the intent is to utilise the latest end time ?*

Answer: The lifetime of the SA must be set to the latest end time to ensure the SA does not expire before all registrations have expired, otherwise the UE may become unreachable. The text in TS 33.203 will be changed to read "The UE sets the lifetime of the new SAs such that it either equals the latest lifetime of the old SAs or it will expire shortly after the registration timer in the message, depending which gives the SAs the longer life" with a similar change for the P-CSCF to avoid possible mis-interpretations.

Q3*. The proposals in the postponed CR's allow for the SA lifetime to be shortened to match the longest remaining registration. The existing text in 7.4.1a of 33.203 would not result in a shortening of the SA lifetime (it is either lengthened or unchanged) until the final registration is removed, when the SA will be deleted. Do SA3 see an advantage in including a mechanism to allow the SA lifetime to be shortened ?*

Answer: SA3 sees no value shortening the lifetime of the SA based on de-registrations. If an SA lifetime is to be shortened, SA3 believe it should be done to old SAs after a successful authentication. To this end SA3 will add the following sentences to TS 33.203. "The P-CSCF shall reduce (as necessary) the lifetime of the old SAs to ensure that they are only used for a short time. This reduction in time should still allow the UE enough

time to perform a fresh successful authentication in case the final message in an authentication procedure is lost."

***Q4**. It has been questioned why the SA needs to be assigned a lifetime at all. It is noted that the SA will be deleted when the last registration related to an IMPI expires in any event (24.229 includes the necessary mechanisms to inform the PCSCF of this event). At other times it will be valid during an ongoing registration, and with the existing 33.203 text the lifetime may be longer than the longest remaining registration. Does SA3 believe that there is a requirement for a defined SA lifetime ?*

Answer: SA3 believe there is a need for an SA lifetime. This is particularly true when there are two sets of SAs (because of a re-authentication), as there is a security requirement to not allow the "old" set of SAs to stay valid for too long. SA3 will add text to ensure that the SAs are deleted, once the associated IMPUs are de-registered.

SA3 hope that the answers the above questions will enable CN1 to make the necessary changes to their specifications to align with the operation agreed by SA3.

2. Actions:

To CN1:
CN1 are kindly requested to consider the above responses to the questions raised by CN and the attached CR when implementing changes to their specifications.

3. Date of Next TSG-SA WG3 Meetings:

TSG-SA WG3 Meeting #30	6th – 10th October 2001	TBD
TSG-SA WG3 Meeting #31	18th – 21st November 2001	TBD