3GPP TSG SA WG3 Security — S3#23 **S3-020211**

14 - 17 May 2002

Victoria, Canada

Source:	**Hutchison 3G UK**
Title:	**New SAs and incomplete authentications**
Document for:	**Discussion/Decision**
Agenda Item:	**6.1**

This contribution looks at the issues of enforcing the use of new SAs and incomplete registrations. As the two issues are linked they are contained in one contribution. The contribution is made of the following five files;

S3-020211-att-1 discusses the issues of enforcing the use of new SAs and proposes a solution to the problem

S3-020211-att-2 discusses the inconsistent states possible when a message gets lost during a registration and proposes a solution to this problem.

The remaining files contain proposed CRs to include the solutions in TS 33.203.

3GPP TSG SA WG3 Security — S3#23 **S3-020xxx_att_1**

14 - 17 May 2002

Victoria, Canada

Source: **Hutchison 3G UK**

Title: **Enforcing the use of new SAs**

Document for: **Discussion/Decision**

Agenda Item: **6.1**

The aim of this paper is to describe a security weakness that is introduced by keeping the old pair of security associations after a new authentication.

Suppose an attacker manages to compromise a pair of keys (IK, CK) that are used in some currently valid security association (SA). Clearly this would allow the attacker to access any service of already registered IMPUs and even possibly register further IMPUs (as not all registrations will be challenged). This attack is effectively impossible to stop if not detected, as it appears like normal network behaviour. The defence against such a possibility is to regularly authenticate the subscriber in either a UE or a network-initiated registration procedure.

On its own an authentication is not enough to avoid these vulnerabilities, as the old SA is kept valid and hence the attacker can continue to use the old SAs to forge REGISTER, INVITES etc. The old SA should be kept valid for at least a short time to ensure the smooth transition to the new SA.

To avoid a “forged” registration attempt, the S-CSCF should challenge all protected registrations that were protected by an SA created by any but the latest successful authentication (that is successful from the S-CSCF’s perspective). Similarly once a new SA is created by a successful authentication, the S-CSCF should only accept INVITES etc. (i.e. messages outside the registration procedure) that are protected using an earlier SA for a short time to allow a smooth transfer to the new SAs. The amount of time should be enough for the UE to complete a further authenticated registration, in case a lost message causes the UE to consider the current one to have failed.

Currently the S-CSCF can not make the decisions noted above, as it does not have the necessary information to hand, i.e. whether the particular SA used to protect the message is the latest or not. Suitable information could be appended by the P-CSCF.

Alternatively the responsibility could be placed on the P-CSCF. The security cost of this is to open a small window where the attacks may succeed, i.e. to messages that pass through the P-CSCF protected with an earlier SA before the authentication successful message reaches the P-CSCF. It would also be open if messages get lost between the S-CSCF and P-CSCF (an unlikely event). This alternative (i.e. P-CSCF takes responsibility) would require the following behaviour at the P-CSCF. When the P-CSCF receives a new SA from a successful authentication, it should

- forward REGISTERs protected with earlier SAs to S-CSCF, but indicate no SA was used to protect the REGISTER
- only forward INVITEs etc. that are protected with earlier SAs for a limited amount of time.

The P-CSCF could delete the SA, once it stops forwarding INVITES etc that are protected with it. Alternatively if possible it might be better to return an error message to indicate that the used SA is no longer suitable and the UE should either use a different one or perform an authenticated registration to get a new SA. Currently there is no such mechanism, but if one existed it could network traffic by stopping the UE retransmitting a message and continually protecting it with an SA that is unacceptable to the P-CSCF.

One consequence of only allowing old SAs to be used only for a short time is that the UE must take action if a REGISTER request carrying a RES timeouts without a response. This is because it is possible that the P-CSCF to consider the authentication to be a success, whereas the UE considers it to have failed. This means the UE will continue to uses earlier SAs to protect non-REGISTER messages and the P-CSCF will soon consider this SAs invalid for use and discard the messages.

Hence if the UE receives no response when it returns a RES to the S-CSCF, it should initiate another registration (protected if an SA is available) after the previous REGISTER has timed out to preserve service continuity.

This contribution proposes adding the described functionality at the P-CSCF, because although this is slightly weaker from a security perspective, it only requires changes to the behaviour of the P-CSCF and the UE as opposed to changing the message flows. The following are proposed texts for TS 33.203 to cover use of the integrity protection indicator under the suggested conditions, only allowing the "old" SA to be used to protect traffic for a limited time after a successful authentication and force the UE to start a new registartion procedure if it does not recieve a reply to an authentication repsones. The proposed text has been included in some prepared CRs.

Integrity protection indicator

In order to decide whether a REGISTER request from the UE needs to be authenticated, the S-CSCF needs to know about the integrity protection applied to the message. The P-CSCF attaches an indication to the REGISTER request to inform the S-CSCF that the message was integrity protected if

- the P-CSCF receives a REGISTER containing an authentication response and the message is protected with the SA created during this authentication procedure ; or
- the P-CSCF receives a REGISTER not containing an authentication response and the message is protected with the SA created by latest successful authentication (from the P-CSCF perspective).

For all other REGISTER requests the P-CSCF attaches an indication that the REGISTER request was not integrity protected or ensures that there is no indication about integrity protection in the message.

Acceptance of non-REGISTER messages protected with old SAs

Once the P-CSCF receives a successful authenticated registration message, the P-CSCF should only forward non-REGISTER messages protected with SAs created by earlier registrations for a short amount of time. After this time it should discard these messages.

UE behaviour on incomplete registrations

If the UE responds to an authentication challenge from a S-CSCF, but does not receive a reply before the request times out, the UE shall start a registration procedure if it still requires any IM services. The first message in this registration should be protected with an SA created by a previous successful authentication if one exists.

3GPP TSG SA WG3 Security — S3#23 **S3-020xxx_att_2**

14 - 17 May 2002

Victoria, Canada

Source: **Hutchison 3G UK**

Title: **Incomplete Authentications**

Document for: **Discussion/decision**

Agenda Item: **6.1**

1 Introduction

The aim of this paper is to propose behaviour of the UE to deal with any possible inconsistent states (between P-CSCF and UE) caused by the loss of messages in a registration procedure. Section 2 discusses the inconsistent states that can be caused by the loss of a message in an authentication. A message is only considered lost after all the re-transmissions. The mostly likely messages to get lost are the ones over the air interface. Section 3 discusses the effects of sending either a protected or unprotected REGISTER during the periods when this inconsistency occurs. It is concluded that without changes to the current network behaviour, the UE will need to send an unprotected REGISTER to get out of the inconsistent state. Section 4 gives some possible new network behaviour to allow the UE to get out of the inconsistent state by using a protected REGISTER. Finally section 5 draws the conclusions.

2 Inconsistent States created by Incomplete Registrations

The behaviour to deal with any inconsistent states created when a UE sends a RES back to the network but does not receive a response, i.e. registration successful, registration failed or a new challenge, has not been given in TS 33.203 (see editor’s note in section 7.3). Figure 1 gives the security association set-up flows from section 7.2 of TS 33.203 for reference.

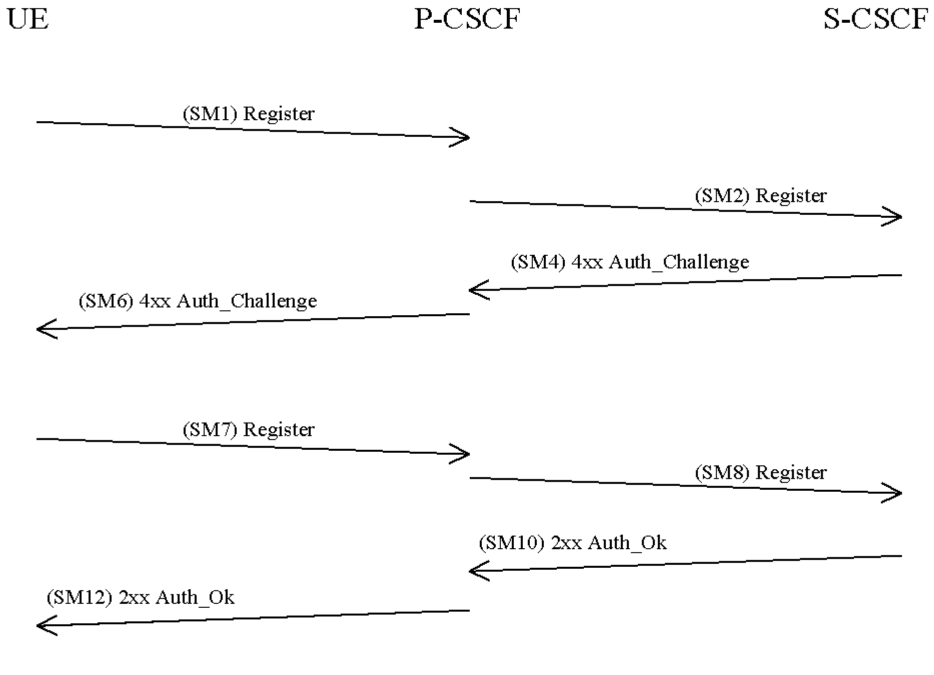

Figure 1: Security Association set-up flows from section 7.2 of TS 33.203

Loss of SM1, SM2, SM4, SM6, SM7 or SM8 does not cause any problems, as all of the S-CSCF, P-CSCF and UE will believe the registration has failed and will “tidy up” accordingly. If SM10 is lost, then the S-CSCF believes the authentication to be a success, while the P-CSCF and UE believe the authentication has failed. If SM12 is lost, then both the S-CSCF and P-CSCF believe the authentication to be a success, while the UE believes the authentication to have failed.

With an unprotected registration when no IMPUs are currently registered, the loss of either SM10 or SM12 causes the network to believe that an IMPU is registered but there is no way for the UE to send or receive protected traffic. If the UE still wants to register that IMPU, it will re-start the registration procedure by sending another independent unprotected REGISTER. As the network must challenge an unprotected REGISTER, the network is treating the UE as unregistered and hence there is no problem when no IMPUs are registered.

The situation is more complicated when there is already an SA in existence. Suppose a UE successfully registers including an authentication IMPU1 for one hour (with no other IMPUs registered). This registration process creates SA1_u and SA1_d, the uplink and downlink security associations respectively. After about 50 minutes, the UE attempts to re-register IMPU1 for another hour. Before the UE attempts this re-registration, the UE, P-CSCF and S-CSCF have the following information

- UE
    - IMPU1 registered with just under 10 minutes left on its expiry timer.
    - SA1_u and SA1_d with roughly 10 minutes left before expiring
- P-CSCF
    - SA1_u and SA1_d with roughly 10 minutes left before expiring
- S-CSCF
    - IMPU1 registered with roughly 10 minutes left on its expiry timer

The UE sends the registration attempt protected with SA1_u. As the registration timer is running low, the S-CSCF challenges the UE. If the authentication is successful until message SM10 is lost, then the S-CSCF has updated the registration expiry time, while the P-CSCF and UE do not believe the registration was a success and will subsequently delete any information relating to that registration transaction. This means the UE, P-CSCF and S-CSCF are left with the following information:

- UE
    - IMPU1 registered with just under 10 minutes left on its expiry timer.
    - SA1_u and SA1_d with roughly 10 minutes left before expiring
- P-CSCF
    - SA1_u and SA1_d with roughly 10 minutes left before expiring
- S-CSCF
    - IMPU1 registered with roughly an hour left on its expiry timer

Similarly if the authentication is successful until message SM12 is lost, then the S-CSCF has updated the registration expiry time and the P-CSCF will keep the new SAs created during the registration. This means the UE, P-CSCF and S-CSCF are left with the following information:

- UE
    - IMPU1 registered with just under 10 minutes left on its expiry timer.
    - SA1_u and SA1_d with roughly 10 minutes left before expiring
- P-CSCF
    - SA1_u and SA1_d with roughly 10 minutes left before expiring
    - SA2_u and SA2_d with roughly an hour left before expiring.
- S-CSCF
    - IMPU1 registered with roughly an hour left on its expiry timer

3 Effects of Possible Behaviour UE

If either SM10 or SM12 gets lost, it is likely that the UE will wish to register IMPU1 again soon. This could be done with either an unprotected registration or a registration protected with SA1_u. Clearly a successful unprotected registration will correct the situation, as the S-CSCF will challenge the UE.

It is preferable to protect the registration. Hence we consider what happens if SM12 was lost and the UE sends a new registration of IMPU1 protected with SA1_u. The P-CSCF forwards the message to S-CSCF indicating that it was integrity protected. As IMPU1 has a long time to go on its registration, the S-CSCF does not request an authentication and responds that IMPU is successfully registered for say 59 minutes. This leaves the UE, P-CSCF and S-CSCF with the following information:

- UE
    - IMPU1 registered with just under 59 minute left on its expiry timer.
    - SA1_u and SA1_d with roughly 9 minutes left before expiring
- P-CSCF
    - SA1_u and SA1_d with roughly 9 minutes left before expiring
    - SA2_u and SA2_d with roughly 59 minutes left before expiring (alternatively this might have been deleted).
- S-CSCF
    - IMPU1 registered with roughly 59 minutes left on its expiry timer

In roughly 9 minutes time the UE has a registered IMPU but no SA to communicate with the P-CSCF. The most likely resolution of this situation is the UE sending an unprotected REGISTER request to force the S-CSCF to send a challenge. A similar situation happens, if SM10 gets lost.

This analysis suggests without changes to the network behaviour, sending a protected registration after an incomplete registration could still leave an inconsistent state.

4 Possible network behaviour to allow protected registrations

One possible way of avoiding the problems with losing SM10 or SM12 without the UE sending an unprotected REGISTER request is for the P-CSCF to supply additional information to the S-CSCF about the SA used to protect the REGISTER request. Suppose the P-CSCF informs the S-CSCF of how long the SA that protected the REGISTER has lived for. The S-CSCF could then use the information about the age of the SA to determine whether an authentication is necessary.

Practically it is probably enough to find a method to avoid the inconsistent state created when an SM12 is lost, as losing an SM10 message should be a rare event (particularly in comparison to losing an SM12 message). This can be achieved by the P-CSCF indicating that a REGISTER request was integrity protected only when it was integrity protected by the SA created by the last successful registration (from the P-CSCF perspective). This means that if an “older” SA is used to protect a register, the S-CSCF would believe the REGISTER was unprotected and hence challenge the REGISTER.

5 Conclusions

This document looks at the issue of the possible inconsistent states that are caused by lost messages during an authentication. Without changes to the network behaviour, the UE will need to send an unprotected REGISTER to correct the situation. With some small changes to network behaviour, the UE could send a protected REGISTER. This paper proposes changes to the behaviour of P-CSCF to only indicate integrity protection was applied to a REGISTER request if the latest SA was used.

It is proposed to add the following text to TS 33.203. This text is included in a proposed CR

Integrity protection indicator

In order to decide whether a REGISTER request from the UE needs to be authenticated, the S-CSCF needs to know about the integrity protection applied to the message. The P-CSCF attaches an indication to the REGISTER request to inform the S-CSCF that the message was integrity protected if

- the P-CSCF receives a REGISTER containing an authentication response and the message is protected with the SA created during this authentication procedure ; or
- the P-CSCF receives a REGISTER not containing an authentication response and the message is protected with the SA created by latest successful authentication (from the P-CSCF perspective).

For all other REGISTER requests the P-CSCF attaches an indication that the REGISTER request was not integrity protected or ensures that there is no indication about integrity protection in the message.

3GPP TSG SA WG3 Security — S3#23 **S3-020xxx-att-3**

14 - 17 May 2002

Victoria, Canada

CR-Form-v5

CHANGE REQUEST

⌘ **33.203 CR** ⌘**rev** **-** ⌘ Current version: **5.1.0** ⌘

*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:	⌘	Integrity protection indicator		
Source:	⌘	Hutchison 3G UK		
Work item code:	⌘		***Date:*** ⌘	09/05/02
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:	⌘	The exact use of the integrity protection indicator has not be described yet.
Summary of change:	⌘	Describes the conditions under which the P-CSCF informs the S-CSCF that integrity protection was applied to a REGISTER request
Consequences if not approved:	⌘	The S-CSCF uses the integrity protection indicator to decide whether to challenge a registration or not. Without the text the indicator could be implemented in different ways, which would mean the S-CSCF is not making a consistent choice on whether to authenticate the subscriber or not. This could introduce problem if a message got lost in a previous registration attempt.

Clauses affected:	⌘	6.1.5	
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments:	⌘		

6.1.5 Integrity protection indicator

In order to decide whether a REGISTER request from the UE needs to be authenticated, the S-CSCF needs to know about the integrity protection applied to the message. The P-CSCF attaches an indication to the REGISTER request to inform the S-CSCF that the message was integrity protected if

- the P-CSCF receives a REGISTER containing an authentication response and the message is protected with the SA created during this authentication procedure ; or
- the P-CSCF receives a REGISTER not containing an authentication response and the message is protected with the SA created by latest successful authentication (from the P-CSCF perspective).

For all other REGISTER requests the P-CSCF attaches an indication that the REGISTER request was not integrity protected or ensures that there is no indication about integrity protection in the message.

3GPP TSG SA WG3 Security — S3#23 **S3-020xxx_att_4**

14 - 17 May 2002

Victoria, Canada

CR-Form-v5

CHANGE REQUEST

⌘ **33.203 CR** ⌘ **rev** **-** ⌘ Current version: **5.1.0** ⌘

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:	⌘	UE and P-CSCF Behaviour on an Incomplete Authentication		
Source:	⌘	Hutchison 3G UK		
Work item code:	⌘		***Date:*** ⌘	
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:	⌘	The behaviour of the UE, P-CSCF and S-CSCF after an incomplete registration is not currently specified. This leaves an incomplete specification. The change also removes an Editor's note.
Summary of change:	⌘	Describes the behaviour of the UE, P-CSCF and S-CSCF after an incomplete authentication.
Consequences if not approved:	⌘	The specification will not be complete, which may lead to implementations that do not operate successfully together.

Clauses affected:	⌘	6.1.2.3, 7.3, 7.3.1.4		
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘	
Other comments:	⌘			

************* FIRST CHANGED SECTION **************

6.1.2.3 Incomplete authentication

If the S-CSCF does not receive a response to an authentication within an acceptable time, it considers the authentication to have failed. If the IMPU was not already registered, the S-CSCF shall send a Cx-Put to the HSS to set the registration-flag for that IMPU to *unregistered* (see message CM3 in clause 6.1.2.2). If the IMPU was already registered, the S-CSCF does not change the registration-flag.

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

7.3 Error cases in the set-up of security associations

~~Whenever an expected message is not received after a time-out the receiving entity considers the registration to have failed.~~

~~[Editor's note: Clarify, how SIP registration handles the inconsistent state that is created by a lost SM12 message]~~

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

7.3.1.4 Incomplete authentication

If the UE responds to an authentication challenge from a S-CSCF, but does not receive a reply before the request times out, the UE shall start a registration procedure if it still requires any IM services. The first message in this registration should be protected with an SA created by a previous successful authentication if one exists.

If the P-CSCF deletes a registration SA due to its lifetime being exceeded, the P-CSCF should delete any information relating to that registration procedure.

3GPP TSG SA WG3 Security — S3#23 **S3-020xxx-att-5**

14 - 17 May 2002

Victoria, Canada

CR-Form-v5

CHANGE REQUEST

⌘	**33.203**	**CR**		⌘ **rev**	**-**	⌘	Current version:	**5.1.0** ⌘

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:	⌘	Hutchison 3G UK		
Work item code:	⌘		***Date:*** ⌘	10/05/2002
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. The SA handling procedures are also moved from a section describing error behaviour
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:	⌘	6.1, 7.3.3, 7.4		
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘	
Other comments:	⌘			

************* FIRST CHANGED SECTION **************

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~~3.3~~.

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. Regarding the definition of service profiles cf. [3].

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

7.3.3 Error cases relating to a~~A~~uthenticated re-registration

~~If the registration is a re-registration, a pair of security associations between UE and P-CSCF is already active. 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.]~~

~~7.3.3.1 Handling of security associations in authenticated re-registrations (successful case)~~

~~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.~~

~~7.3.3.2 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.~~

7.3.3.1~~3~~ Error cases related to IMS AKA

User authentication failure

The S-CSCF will send a 4xx Auth_Failure message SM10, which will pass through the already established SA to the UE as SM12. Afterwards, both, the UE and the P-CSCF delete the new SAs.

Network authentication failure

If the UE is not able to successfully authenticate the network, it does not establish a new SA. The UE sends a REGISTER message SM7 indicating a network authentication failure to the P-CSCF, using the already established SA. The P-CSCF deletes the new SAs after receiving this message.

Synchronisation failure

If the UE notices a synchronisation failure it does not establish a new SA. The UE sends a message SM7, indicating the synchronisation failure, to the P-CSCF, using the already established SA. The P-CSCF deletes the new SA after receiving this message.

7.3.3.2~~4~~ Error cases related to the Security-Setup

Unacceptable proposal set

The message SM6 shall respond to the first REGISTER message SM1 with a 4xx Unacceptable_Proposal, using the already established SA. Neither side establishes a new SA.

The P-CSCF therefore shall modify the message SM2 such that the S-CSCF sends the 4xx Unacceptable_Proposal message back to the UE in SM4and SM6 and the registration process is finished.

SM2:
REGISTER(Security-setup = *integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info],* Failure = *NoCommonIntegrityAlgorithm,* IMPI)

[Editors Note: It is FFS how the exact mechanism shall be for the Unacceptable proposal set case. The editor believes that the S-CSCF is the registrar and hence the P-CSCF should only be able to modify the headers and not send back responses. The failure response should be sent by the S-CSCF. This however has not been agreed.]

Failed consistency check of Security-Set-up lines

This is the case if the Security-Setup line in SM7 from the UE to the P-CSCF cannot be verified, so the Security-Setup line of the unprotected SM1 and the Security-Setup line of the protected SM7 do not match. In this case the P-CSCF shall respond to the UE by sending a 4xx Unacceptable_Proposal message in SM12 using the already established SA. Both sides delete the new SAs.

The P-CSCF therefore shall modify the message SM8 such that the S-CSCF sends the 4xx Unacceptable_Proposal message back to the UE in SM10 and SM12 and the registration process is finished.

SM8:
REGISTER(Security-setup = *integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info],* Failure = *NoCommonIntegrityAlgorithm),* IMPI)

[Editors Note: It is FFS how the exact mechanism shall be for the Unacceptable proposal set case. The editor believes that the S-CSCF is the registrar and hence the P-CSCF should only be able to modify the headers and not send back responses. The failure response should be sent by the S-CSCF. This however has not been agreed.]

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

7.4 Management and Use of Security Associations

Every successful registration procedure that includes a user authentication produces a new pair of security associations (SAs). These new SAs shall then replace the previous SAs. This section describes how the UE and P-CSCF shall handle this replacement and which SA to apply to which message. Security associations may be unidirectional or bi-directional. This section assumes that security associations are unidirectional, as this is the general case. Whenever a user is registered there is a **current SA** for each direction at both the P-CSCF and the UE. In addition there may be either a **registration SA** for each direction or an inbound **old SA** at the UE and either a **registration SA** or a **valid SA** for each direction or rarely both at the P-CSCF. They are denoted as follows:

SA_in_cur	current inbound SA
SA_out_cur	current outbound SA
SA_in_reg	registration inbound SA
SA_out_reg	registration outbound SA
SA_in_old	old inbound SA (in UE only)
SA_in_val	valid inbound SA (in P-CSCF only)
SA_out_val	valid outbound SA (in P-CSCF only)

This notation has local significance only. That means that SA_in_cur at the UE is not always the same as SA_out_cur at the P-CSCF and similarly for other SAs. The SAs shall be distinguished by different SA_IDs.

7.4.1 Management of security associations in the UE

The UE shall be involved in only one registration procedure at a time. Upon starting a new registration procedure, any existing registration SAs are deleted. The UE shall delete any SA whose expiry time is exceeded. If the wrong SA is used to protect any message, the message should be discarded.

A successful registration with authentication proceeds in the following steps:

- The UE sends the initial message to register with the IMS. It should be integrity-protected using SA_out_cur if it exists.

- The UE receives an authentication challenge in a message from the P-CSCF. This message shall be integrity-protected using SA_in_cur if the UE’s initial message was integrity-protected.

- If this message can be successfully processed by the UE, the UE creates the new SAs, SA_in_reg and SA_out_reg, which are derived according to section 7.2. The expiry time of the registration SAs should be set to allow enough time to complete the registration procedure. The UE then sends its response to the P-CSCF, which shall be protected with SA_out_reg.

- The UE receives a registration successful message from the P-CSCF, which shall be protected using SA_in_reg.

- After the successful processing of the registration successful message by the UE, the registration is complete. The UE sets the expiry time of the registration SAs equal to the registration timer in the message. SA_in_cur becomes the new SA_in_old, SA_out_reg becomes the new SA_out_cur and SA_in_reg becomes the new SA_in_cur.

A failure in the registration means the UE should delete SA_in_reg and SA_out_reg. If the first message in a registration procedure is protected, the UE shall protect all other outbound messages in that registration procedure with SA_out_cur or ensure that SA_in_cur was applied to protect all other inbound messages in that registration procedure, for example synchronization failure messages. If the first message was not protected, then no protection shall be applied to the other messages.

When a SIP message protected with SA_in_cur is successfully received from the P-CSCF, the UE shall delete SA_in_old if it exists.

Outisde registration procedures, the UE shall use SA_out_cur to protect all outbound traffic. Furthermore the UE shall ensure that all inbound traffic is protected with either SA_in_cur or SA_in_old.

7.4.2 Management of security associations in the P-CSCF

The P-CSCF shall delete any SA whose expiry time is exceeded. If the current SAs are deleted and there exist valid SAs, then the P-CSCF makes the SA_out_val the new SA_out_cur and SA_in_val the new SA_in_cur, and removes the valid SAs. If the wrong SA is used to protect any message, the message should be discarded.

The P-CSCF associates the IMPI and IMPU given in the registration procedure with the registration SAs created during that registration procedure. The P-CSCF associates the IMPI given in the registration procedure and all the successfully registered IMPUs related to that IMPI with current and valid SAs.

A successful registration with the first message protected proceeds in the following steps:

- The P-CSCF receives the first register message. If it is protected, it should be integrity-protect using SA_in_cur or SA_in_val.

- The P-CSCF forwards the message containing the challenge to the UE. This shall be integrity-protected using SA_out_cur, if the initial message was protected.

- The P-CSCF then creates the new SAs, SA_in_reg and SA_out_reg, which are derived according to section 7.2. The expiry time of the registration SAs should be set to allow just enough time to complete the registration procedure.

Editor's note: there can exist 3 sets of SAs at this point.

- The P-CSCF receives the message carrying the response from the UE. It shall be protected using SA_in_reg.

- The P-CSCF forwards the successful registration message to the UE, which shall be protected using SA_out_reg. This completes the registration procedure for the P-CSCF. The P-CSCF sets the expiry time of the registration SAs equal to the registration timer in the message. If the first register message was protected, then SA_out_reg becomes SA_out_val and SA_in_reg becomes SA_in_val (overwriting any previous valid SAs) and the expiry times of SA_in_cur and SA_out_cur are set to allow only enough time for an authentication. If the first register message was unprotected, then SA_out_reg becomes SA_out_cur and SA_in_reg becomes SA_in_cur, and all valid and registration SAs are deleted.

A failure in the registration means the P-CSCF should delete SA_in_reg and SA_out_reg. If the first message in a registration procedure is protected, the P-CSCFshall protect all other outbound message in a registration procedure with SA_out_cur or ensure that SA_in_cur was applied to protect all other inbound messages in a registration procedure, for example synchronization failure messages. If the first message was not protected, then no protection shall be applied to the other messages.

When the P-CSCF successfully receives a SIP message protected with SA_in_val from the UE, then SA_in_val and SA_out_val becomes the new SA_in_cur and SA_out_cur respectively, and there are no more valid SAs.

Outside registration procedures, the P-CSCF shall use SA_out_cur to protect outbound traffic. Furthermore the P-CSCF shall ensure that inbound traffic is protected with either SA_in_cur or SA_in_val. If the wrong SA is used, the message should be discarded.