3GPP TSG SA WG3 Security — S3#23 S3-020292

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, 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 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]~~

7.3.1 Error cases related to IMS AKA

Errors related to IMS AKA failures are specified in section 6.1. However, this section additionally describes how these shall be treated, related to security setup.

~~[Editors Note: It is FFS if this is appropriate taking DoS attacks into account.]~~

7.3.1.1 ~~Integrity check~~User authentication failure ~~in the P-CSCF~~

In this case, SM7 containing a ~~potentially~~ wrong response~~RES~~ fails integrity check by IPsec at the P-CSCF if the ~~(~~IK_{IM} derived from RAND at UE is wrong as well~~).~~ The SIP application at the P-CSCF never receives SM7. It shall delete the temporarily store SA parameters associated with this registration after a time-out.

In case IK_{IM} was derived correctly, but the response was wrong t~~T~~he authentication of the user fails ~~in the network~~at the S-CSCF due to an incorrect RES. ~~The P-CSCF shall discard SM7 and the registration and the authentication procedures shall be aborted (see also clause 6.1.2.1).~~ The S-CSCF will send a 4xx Auth_Failure message SM10, which may pass through an already established SA to the UE as SM12. Afterwards, both, the UE and the P-CSCF delete the new SAs.

7.3.1.2 Network authentication failure

If the UE is not able to successfully authenticate the network, ~~the UE is not able to create the key IK and therefore the SA with the P-CSCF, such that it is not possible to send SM7 in a protected way. Since the P-CSCF already expects SIP messages from the UE to be protected, and is not already aware of any errors, the P-CSCF shall accept such REGISTER messages indicating network authentication failure in the clear.~~

~~So~~ the UE shall send~~s~~ a ~~new~~ REGISTER message ~~SM7~~, indicating a network authentication failure, to the P-CSCF, ~~without protection~~which may pass through an already established SA. ~~SM7 should not contain the security-setup line of the first message.~~ The P-CSCF deletes the new SAs after receiving this message.

7.3.1.3 Synchronisation failure

In this situation, the UE observes that the AUTN sent by the network in SM6 contains an out-of-range sequence number. The UE shall send~~s~~ a ~~new~~ REGISTER message ~~SM7~~ to the P-CSCF, which may pass through an already established SA ~~in the clear~~, indicating the synchronization failure. ~~SM7 should not contain the Security-Setup line of the first message, and the P-CSCF shall keep the security-setup state created after receiving SM1 from the UE.~~ The P-CSCF deletes the new SAs after receiving this message.

7.3.2 Error cases related to the Security-Set-up

7.3.2.1 ~~Unacceptable~~ P~~p~~roposal unacceptable ~~set~~to P-CSCF

In this case the P-CSCF cannot accept the proposal set sent by the UE in the Security-Set-up command of SM1. SM6 shall respond to SM1 with indicating a failure, by sending a 4xx Unacceptable_Proposal.

The P-CSCF therefore shall modify the message SM2 such that the S-CSCF sends a 4xx Unacceptable_Proposal message back to the UE in SM4 and 6 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, IMPU)~~

~~[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.]~~

7.3.2.2 Proposal unacceptable to UE~~Unacceptable algorithm choice~~

If the P-CSCF sends in the security-setup line of SM6 ~~an algorithm~~a proposal that is not acceptable for the UE ~~(i.e. has not been proposed), the UE shall not continue to create a security association with the P-CSCF and~~ shall terminate the registration procedure.

7.3.2.3 Failed consistency check of Security-Set-up lines at the P-CSCF

The P-CSCF shall check whether authentication algorithms list received in SM7 is identical with the authentication algorithms list sent in SM6. If this is not the case the registration procedure is aborted. (Cf. section 7.2) ~~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. The P-CSCF shall respond to the UE by sending a 4xx Unacceptable_Proposal message in SM12. The P-CSCF therefore shall modify the message SM8 such that the S-CSCF sends a 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.]~~

~~7.3.3 Authenticated 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.

7.3.3.3 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.

7.3.3.4 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. For IP layer SAs, it is possible that there needs to be parallel SAs for each available transport protocol. Whenever a user is registered there are **current SAs** at both the P-CSCF and the UE. At the UE, there may alo be either **registration SAs** or inbound **old SAs**. Whilst at the P-CSCF, there may also be **registration SAs** and/or a **valid SAs**. 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.

For IP layer SAs, the lifetime mentioned in the following clauses is the lifetime held at the application layer. Furthermore deleting an SA means deleting the SA from both the application and network layer. If parallel SAs are needed for more than more transport, the SA management procedures in the following clauses need to be applied for each parallel set of SAs. The message numbers, e.g. SM1, used in the following clauses relate to the message flow given in 6.1.1.

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 shall be deleted. The UE shall delete any SA whose lifetime is exceeded. If the wrong SA is used to protect any message, the message shall be discarded.

When a UE has changed its IP address that it intends to use for subsequent SIP signaling, it should initiate a re-registration procedure.

A successful authentication proceeds in the following steps:

- The UE sends the SM1 message to register with the IMS. It should be integrity-protected using SA_out_cur if it exists.

  If the re-registration was initiated due to the allocation of a new IP address, the UE shall use the old IP address when sending SM1. If the old IP address is no longer usable, SM1 shall not be integrity protected. Inside the SIP message SM1, the UE shall advertise a contact address that it wants to use after the re-registration is complete. This address may be different from the source address used to send SM1 when the UE has allocated a new address. If this is the case, the UE shall also include the old address in SM1 and advertise it to expire immediately.

- The UE receives an authentication challenge in a message (SM6) from the P-CSCF. This message shall be integrity-protected using SA_in_cur if SM1 was integrity-protected.

- If this message SM6 can be successfully processed by the UE, the UE deletes SA_out_old if it exists and creates the new SAs, SA_in_reg and SA_out_reg, which are derived according to section 7.2. The lifetime of the registration SAs should be set to allow enough time to complete the registration procedure. The UE then sends its response (SM7) to the P-CSCF, which shall be protected with SA_out_reg.

  For an IP address change, the IP address of the UE shall be the contact address advertised by UE in SM1 shall be used to create SA_in_reg and SA_out_reg.

- The UE receives an authentication successful message (SM12) from the P-CSCF, which shall be protected using SA_in_reg.

- After the successful processing of this message by the UE, the registration is complete. The UE sets the lifetime 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 authentication means the UE shall delete SA_in_reg and SA_out_reg. If SM1 was protected, the UE shall protect all outbound failure messages in the authentication with SA_out_cur and ensure that SA_in_cur was applied to protect all inbound failure messages in the authentication. If the SM1 was not protected, then no protection shall be applied to the failure 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.

For messages outside an authentication, the UE shall use SA_out_cur to protect all outbound traffic and ensure that all inbound traffic is protected with either SA_in_cur or SA_in_old.

The UE shall use SA_out_cur to protect all outbound traffic

7.4.2 Management of security associations in the P-CSCF

The UE shall delete any SA whose lifetime 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 shall 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 authentication proceeds in the following steps:

- The P-CSCF receives the SM1 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 (SM6) to the UE. This shall be integrity-protected using SA_out_cur, if SM1 was protected.

  For an IP address change if it is to be integrity protected, SM6 shall be sent to the IP address that was used when the SA was originally created, regardless of the contact address advertised by the UE in SM1.

- 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.

  For an IP address change, the IP address of the UE shall be the contact address advertised by UE in SM1 shall be used to create SA_in_reg and SA_out_reg. The UE shall now use the same source address in sending this message as it advertised as its contact address in SM1.

- The P-CSCF receives the message carrying the response (SM7) from the UE. It shall be protected using SA_in_reg.

- The P-CSCF forwards the successful registration message (SM12) 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 SM1 was protected, then SA_out_reg becomes SA_out_val, SA_in_reg becomes SA_in_val (overwriting any previous valid SAs) and the expiry times of SA_in_cur and SA_out_cur should be shortened to allow only enough time for a further authentication in case of lost messages. If SM1 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.

  For an IP address change, SM12 shall be sent to the source address that was used when sending SM7.

A failure in the authentication means the P-CSCF shall delete SA_in_reg and SA_out_reg. If SM1 was protected, the P-CSCF shall protect all outbound failure messages in the authentication with SA_out_cur and ensure that SA_in_cur was

applied to protect all inbound failure messages in the authentication. If the SM1 was not protected, then no protection shall be applied to the failure 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.

For messages outside an authentication, the P-CSCF shall use SA_out_cur to protect all outbound traffic and ensure that all inbound traffic is protected with either SA_in_cur or SA_in_val.