3GPP TSG SA WG3 Security — S3#23 **S3-020240**
14 - 17 May 2002
Victoria, Canada

CR-Form-v4

CHANGE REQUEST

⌘ **33.203** **CR** ⌘ ev **-** ⌘ 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 **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	IP address as SA selector
Source:	⌘	Nokia
Work item code:	⌘	***Date:*** ⌘
Category:	⌘	**B**

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:	⌘	Adding Security negotiation into SA setup procedure.
Summary of change:	⌘	**Adding Security negotiation for IPsec into SA setup procedure.**
Consequences if not approved:	⌘	The SA establishment is rely on the missing function. Without Security negotiation, it may not be able to setup IPsec SA.

Clauses affected:	⌘	
Other specs affected:	⌘	**X** 24.228 **X** 24.229
Other comments:	⌘	

7 Security association set-up procedure

The security association set-up procedure is necessary in order to decide what security services that apply and when the security services start. In the IMS authentication of users is performed during registration as in Section 6.1. Subsequent signaling communications in this session will be integrity and optionally confidentiality protected based on the keys derived during the authentication process.

7.1 Security association parameters

For protecting IMS signaling between the UE and the P-CSCF it is necessary to agree on shared keys provided by IMS AKA, on certain protection methods (e.g. an integrity protection method) and a set of parameters specific to a protection method, e.g. the cryptographic algorithm to be used. The parameters negotiated are typically part of the security association to be used for a protection method.

The security mode setup shall support the negotiation of different protection mechanisms. It shall be able to negotiate or exchange the SA parameters required for these different protection mechanisms. Although the supported protection mechanisms could be quite different, there is a common set of parameters that have to be negotiated for each of them. (This set of parameters ~~includes~~are specified in Annex D.1):

- ~~Authentication (integrity) algorithm, and optionally encryption algorithm;~~
- ~~SA_ID that is used to uniquely identify the SA at the receiving side;~~
- ~~Key length: the length of encryption and authentication (integrity) keys is 128 bits.~~

~~The UE and P-CSCF both have static lists of security mechanisms and parameters they support. The lists do not and cannot change based on input from the other side. There may, however, be several lists for each node.~~

Parameters specifically related to certain protection methods are kept in the annexes describing the protection methods.

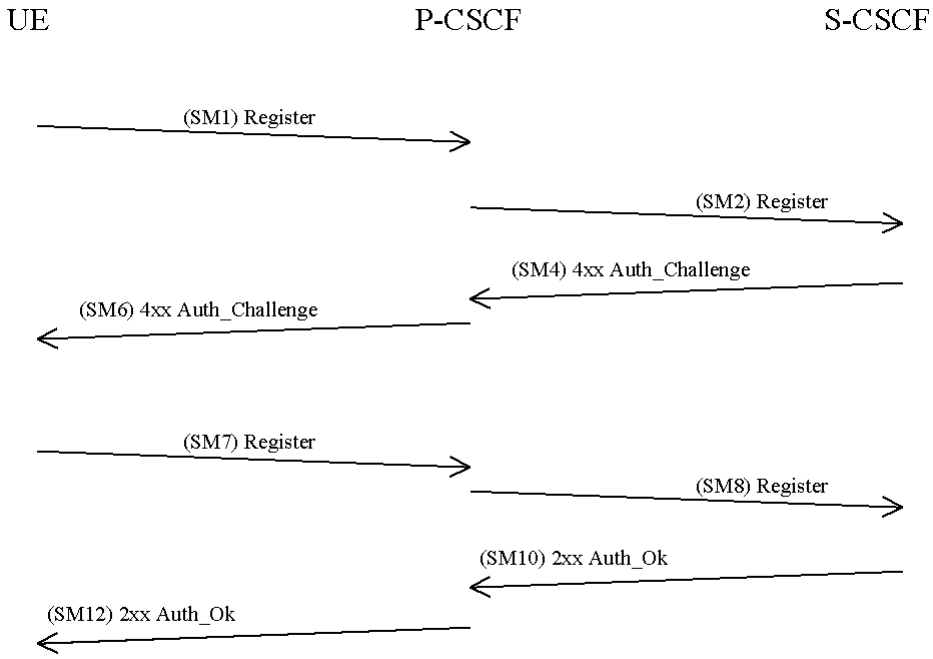
The SA between the UE and the P-CSCF will have a limited lifetime. The lifetime timer shall be the same as the registration timer, which is defined per contact address. When the UE registers the registration timer will be negotiated between the UE, the P-CSCF and the S-CSCF. The S-CSCF will be able to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

The security mechanism negotiation is only applied to the first hop, between UE and P-CSCF to negotiation protection mechanism. Since the IMS architecture relies on home S-CSCF to authenticate UE, the keying protocol and authentication protocol are not negotiable in this phase. During negotiation, UE and P-CSCF both have static lists of security mechanisms and parameters they support. The list does not and cannot be changed based on input from the other side.

~~[Editors Note: The support of different mechanisms is FFS.]~~

7.2 Set-up of security associations (successful case)

In this section the normal case is specified i.e. when no failures occurs. Note that for simplicity some of the nodes and messages have been omitted. Hence there are gaps in the numbering of messages, as the I-CSCF is omitted.



The UE sends a Register message towards the S-CSCF to register the location of the UE and to set-up the security mode. This has been described in 6.1. In order to start security mode setup the UE shall include a *Security-~~setup~~Mechanism:* line in this message, including the list of supported security mechanisms: the protection method, the proposed set of integrity algorithms, the proposed set of confidentiality algorithms (optional), the SA_~~ID and an optional *info* field. The *info* field is reserved for method specific use, so any method supported by the security mode set-up must specify whether and how to use the *info* field~~. The SA_ID_U shall be chosen so that it uniquely identifies the (unidirectional) inbound SA at the UE side.

~~Elements in [...] are optional.~~

SM1:
REGISTER(IMPI , Security-setup = to-uri, from-uri, ~~*integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list],*~~ *mech_list_UE* ~~*SA_ID_U, [info]),~~ ~~IMPI, IMPU~~*)*

Explanation:

- To_uri and from-uri are SIP URI defined in [Sec-agree], the receiver and initiator's identifier.
- Mech_list_UE is the supported algorithm listed by UE. It encapsulates the detail of each mechanism to be negotiated. In IPsec case, it may be expressed as: mech=ipsec-man;pref=1;SA_ID_U=ABCD; Suite=1. The attribute fields are extensible.
- The IPsec without automatic key algorithm (IKE) is named as 'ipsec-man'.
- Preference is 1 means the IPsec is the first preferred choice.
- Suite indicates the UE supported suite definition.

The P-CSCF shall announce a list of its supported security mechanisms in response to the UE in SM6. The P-CSCF shall add its list to the response even if there were no common security mechanisms in the UE's and P-CSCF's list. The P-CSCF's list shall not depend on the UE's list.In particular, the list shall contain the IPsec parameters, such as SA_ID_P.

schoose exactly one of the proposed mechanisms respectively and exactly one of the proposed algorithms respectively based on the policies that applies and send the selected mechanisms and algorithms to the UE in SM6.

The SA_ID_P shall be chosen in such a way that it uniquely identifies the (unidirectional) inbound SA at the P-CSCF side, within the P-CSCF.

[Editors Note: It is FFS if the HN shall take part in the negotiation of algorithms.]

SM6:
4xx Auth_Challenge(IMPI , Security-setup = to-uri, from-ui, *integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list]mech_list_Proxy, SA_ID_P, [info], IMPI)*

Explanation:

- Mech_list_Proxy is the mechanism list offered by Proxy. In detail format, IPsec mechanism is elaborated as mech=ipsec-man;pref=1; SA_ID_P=CDEF;Suite=1
- Pre=1 means that mechanism IPsec without IKE is first preference in this P-CSCF.

The UE shall select and use the first matching security mechanism from the P-CSCF's list. According to the mechanisms chosen the UE shall in SM7 start the integrity protection in SM7 – and optionally the confidentiality protection – of the whole SIP-message by setting up security associations according to mechanisms and the parameters negotiated in SM1 and SM6, and applying the corresponding protection to the SIP- message. Furthermore the Security-setup: line sent by the P-CSCF sent to the UE in SM61 shall be includedrepeated:

SM7:
REGISTER(IMPI , Security-setup = to-uri, from-ui, *mech_list_Proxy)*Security-setup = *integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_PU, [info],* IMPI)

After receiving SM7 from the UE, the P-CSCF shall check that the list repeated in SM7 corresponds to its static list of supported security mechanisms. compare the Security-Setup line of this message with the Security-Setup line received in SM1. The P-CSCF shall in SM8 include information to the S-CSCF that the received message from the UE was integrity protected. The P-CSCF shall add this information to all subsequent messages received from the UE that have successfully passed the integrity check in the P-CSCF.

SM8:
REGISTER(Integrity-Protection = *Successful,* IMPI*)*

The P-CSCF finally sends SM12 to the UE. SM12 does not contain information specific to security mode setup (i.e. a Security-setup line), but with sending SM12 not indicating an error the P-CSCF confirms that security mode setup has been successful. After receiving SM12 not indicating an error, the UE can assume the successful completion of the security-mode setup.

[Editors Note: It is FFS if the HN shall take part in the negotiation process.]

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 failure in the P-CSCF

In this case, SM7 containing a potentially wrong RES fails integrity check at P-CSCF (IK derived from RAND at UE is wrong as well). The authentication of the user fails in the network due 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).

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 sends a new register message SM7, indicating a network authentication failure, to the P-CSCF, without protection. SM7 should not contain the security-setup line of the first 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 sends a new register message SM7 to the P-CSCF 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.

7.3.2 Error cases related to the Security-Set-up

7.3.2.1 Unacceptable proposal set

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 Unacceptable algorithm choice

If the P-CSCF sends in the security-setup line of SM6 an algorithm 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

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.]

Annex B (informative): Mechanisms for IPSec based solution

[Editors Note: If the IPSec solution is finally chosen the chapters below shall be moved into the main body of this TS in the corresponding sections.]

B.1 [6.2] Confidentiality mechanisms

IPsec ESP may optionally be implemented for providing confidentiality of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. If ESP confidentiality is used, it shall be applied in transport mode between UE and P-CSCF. If ESP confidentiality is provided, it is always provided in addition to ESP integrity protection.

The SAs that are required for ESP shall be derived from the 128-bit integrity key CK_{IM} generated through IMS AKA, as specified in chapter 6.1.

If confidentiality is required, for each direction, there is one ESP SA for both confidentiality and integrity that shall be used between the UE and the P-CSCF. The encryption transform is identical for the two SAs in either direction. The encryption key for the SA inbound from the P-CSCF is CK.

The encryption key for the SA inbound from the P-CSCF is CK_{IM_in}. The encryption key for the SA outbound from the P-CSCF is $CK_{IM\_out.}$

The encryption keys are derived as $CK_{IM\_in} = h1(CK_{IM})$ and $CK_{IM\_out} = h2(CK_{IM})$ using suitable key derivation functions h1 and h2.

The encryption key derivation on the user side is done in the ISIM. The encryption key derivation on the network side is done in the P-CSCF.

The method to set up ESP security associations during the SIP registration procedure is specified in chapter 7.

B.2 [6.3] Integrity mechanisms

IPsec ESP shall provide integrity protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. ESP integrity shall be applied in transport mode between UE and P-CSCF.

The SAs that are required for ESP shall be derived from the 128-bit integrity key IK generated through IMS AKA, as specified in chapter 6.1. The transform used for the ESP SA shall be negotiated as specified in chapter 7. ESP shall use two unidirectional SAs between the UE and the P-CSCF, one in each direction. The integrity algorithm is identical for both SAs.

The integrity key for the SA inbound from the P-CSCF is IK_{IM_in}. The integrity key for the SA outbound from the P-CSCF is $IK_{IM\_out.}$

The integrity keys are derived as $IK_{IM\_in} = h1(IK_{IM})$ and $IK_{IM\_out} = h2(IK_{IM})$ using suitable key derivation functions h1 and h2. (They may be the same as those in section 6.2.)

The integrity key derivation on the user side is done in the ISIM. The integrity key derivation on the network side is done in the P-CSCF.

The method to set up ESP security associations during the SIP registration procedure is specified in chapter 7.

Annex D (informative):
Set-up procedures for IPSec based solution

[Editors Note: If the IPSec solution is finally chosen the chapters below shall be moved into the main body of this TS in the corresponding sections.]

This section is based on section 7 and provides additional specification for the support of IPsec ESP.

D.1 Security association parameters

The SA parameters, identifiers and attributes that shall be negotiated between UE and P-CSCF, are

- SA Suite number. Suite is pre-defined algorithms and parameters used for SA establishment. It contains information:
  - ESP transform identifier
  - Authentication (integrity) algorithm
  - Life type: the life type is always seconds
  - SA duration: the SA duration has a fixed length.
  - Key length: the length of encryption and authentication (integrity) keys is 128 bits.

One example of suite is defined as:

Suite 1:

a) IPsec protocol

Protocol id=PROTO_IPSEC_ESP

ESP Transform Identifiers= ESP_NULL

b) SA attributes

Situation=SIT_INTEGRITY

SA Life Type=seconds

SA Life Duration=32s

Authentication Algorithm= HMAC_MD5

Encapsulation Mode=Transport

Keying= AKA

key lengths=128 bits

The other ephemeral parameters to be negotiated are:

- SPI or SA_ID from both directions
- Port number for protected messages

Further parameters:

- ~~Life type: the life type is always seconds~~
- ~~SA duration: the SA duration has a fixed length of 2^{32}-1.~~
- ~~Key length: the length of encryption and authentication (integrity) keys is 128 bits.~~

Selectors:

The security associations (SA) have to be bound to specific parameters (selectors) of the SIP flows between UE and P-CSCF, i.e. IP addresses and ports. Both sides have to use the same policy here, but since the required selectors will be known from the SIP messages, there is no need to negotiate them. However, it is critical to keep the source IP address and source port number, the selector pair unique in P-CSCF. The P-CSCF must reject any REGISTER message sent from a valid SA's selector pair corresponding to a different IMPI than the one that is bound to this selector pair. The only parameter that shall be negotiated, is a fixed port for specific unprotected SIP messages at the P-CSCF:

1. For the inbound SA at the P-CSCF (outbound for the UE) the P-CSCF shall use a fixed port. This may be port 5060 as the standard SIP port, or any other fixed port where the server accepts SIP messages from the UE. In addition, another port for specific unprotected SIP messages from the UE to the server is fixed.
   For the outbound SA at the P-CSCF (inbound for the UE) ANY port number shall be allowed at the P-CSCF.
2. On the UE side, the SIP UAs shall use the same port for both sending and receiving SIP signalling to the P-CSCF.
3. If there are multiple SIP UAs belonging to different ISIMs in one UE they shall use different SAs and bind them to different ports on the UE side.
4. The UE may send only the following messages to the fixed port for unprotected messages:
   - initial REGISTER message;
   - REGISTER message with network authentication failure indication;
   - REGISTER message with synchronization failure indication.

   All other messages incoming on this port must be discarded by the SIP application on the P-CSCF.

[Editors' note:It is ffs whether case 3 can actually occur.]

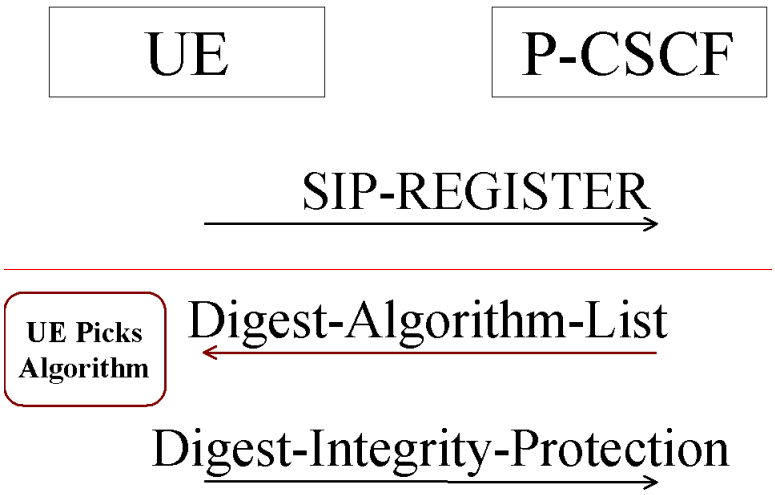
For each incoming message the SIP application must verify that the correct inbound SA associated with the public ID (IMPU) given in the SIP message has been used. This shall be done by verifying that the correct source IP address and source port bound to the public ID (IMPU) of the SIP message have been used for sending the message.

~~Annex F (informative):~~
~~Bidding down protection~~

~~This annex contains the Bidding Down Protection mechanism which is an extension to HTTP Digest i.e. [12]. The purpose with this Annex is to keep track on the development of the Bidding Down Protection and to have it as a fallback solution if Security Mode Setup is not available in time from IETF.~~

~~[Editors note: This text is FFS but it has to be further developed describing the mechanism in more detail. It is also FFS how to ensure that the UE picks the strongest algorithm and what algorithms should be mandatory.]~~

~~The extended HTTP Digest can negotiate what integrity algorithm to use. The general scheme is described in the figure below.~~



~~This security mode set-up looks different to the current requirements defined in clause 7 where the P-CSCF chooses the algorithm. A proposed mechanism for bidding down protection is to utilise a nonce, which will have a meaning for the client. The nonce-value in this case is not longer only a random number it will include the integrity algorithm and quality of protection along with the traditional nonce value. The nonce in this case could look like:~~

~~Nonce = base64 encoding (auth-algorithms, auth-extd-int, time-stamp || Hash(time-stamp, Request URI, private-key))~~

~~The server (in the IMS profile the server will be the P-CSCF) issues a list of supported mechanisms like e.g. MD5 and SHA-1. The client (in the IMS profile the client is the UE) picks the strongest algorithm it supports i.e. SHA-1 and protects the following messages with this algorithm. A man in the middle could not degrade the proposed list since the client shall repeat the nonce value which in this case includes the proposed list of algorithms as suggested above. The server or the P-CSCF can check that the list is correct but it does not have to store the suggested list.~~