3GPP TSG SA WG3 Security — S3#23 **S3-020235**

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 **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	Requested Changes for SIP integrity
Source:	⌘	Siemens AG
Work item code:	⌘	***Date:*** ⌘
Category:	⌘	**C**

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Release: ⌘ Rel-5

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	The CR implements SA3's decision to use IPsec without IKE as the mechanism for SIP integrity. It also reflects changes in draft-IETF-sip-sec-agree on which the mechanism for SIP integrity relies. It further resolves some open issues and provides clarifications and editorial changes.
Summary of change:	⌘	The requested changes are described in detail in a companion contribution by Siemens to SA#23. The main changes are: - move Annexes B and D to main body; - replace generic text in section 7 with text specific for IPsec; - revise section 7.2 to reflect changes in draft-IETF-sip-sec-agree; - delete most of the text SA handling in section 7.3 as it is now contained in section 7.4 - treat security associations for TCP and UDP independently; - counter reflection attacks by unidirectional SPIs; - propose a key expansion function for HMAC-SHA-1-96.
Consequences if not approved:	⌘	The specification will not be complete, and not in line with IETF.

Clauses affected:	⌘	5.1.4, 6.3, 7.1, 7.2, 7.3 Annex B, Annex D
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

5.1.4 Integrity protection

Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signaling, as specified in section 6.3. The following mechanisms are provided.

1. The UE and the P-CSCF shall negotiate the integrity algorithm that shall be used for the session, as specified in chapter 7.

2. The UE and the P-CSCF shall agree on ~~a~~ security associations, which include ~~identifyies~~ the integrity keys, ~~IK~~ that shall be used for the integrity protection. The mechanism is based on IMS AKA and specified in chapter 6.1.

3. The UE and the P-CSCF shall both verify that the data received originates from a node, which has the agreed ~~session~~ integrity key~~, IK~~. This verification is also used to detect if the data has been tampered with.

4. The UE and the P-CSCF shall both verify the freshness of the message such that both replay attacks and reflection attacks are mitigated.

Integrity between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [5].

6.3 Integrity mechanisms

~~*[Editor's note: At this stage both Annex B and Annex C provides with potential measures for integrity protection. One of these solutions will be the normative solution.]*~~
[Editorial note to be removed when implementing this CR: The text in this section is the text from Annex B.2 in TS 33.203 v510. Only the changes with respect to former Annex B.2 are marked.]

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 method to set up ESP security associations (SAs) during the SIP registration procedure is specified in chapter 7.~~The transform used for the ESP SA shall be negotiated as specified in chapter 7. ESP shall use~~ As a result of the registration procedure, two pairs of unidirectional SAs between the UE and the P-CSCF, ~~one in each direction~~one pair for TCP and one pair for UDP, shall be simultaneously established. Each pair consists of an SA for traffic from the UE to the P-CSCF (inbound SA at the P-CSCF) and an SA for traffic from the P-CSCF to the UE (outbound SA at the P-CSCF). ~~The integrity algorithm is identical for both SAs.~~

The integrity key IK_{ESP} is the same for the ~~SA~~ four simultaneously established SAs.~~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 key IK_{ESP} is~~s~~ are derived from the key IK_{IM} established as a result of the AKA procedure, as specified in chapter 6.1. ~~as $IK_{IM\_in} = h1(IK_{IM})$ and $IK_{IM\_out} = h2(IK_{IM})$~~ using a suitable key ~~derivation~~expansion function~~s h1 and h2~~. ~~(They may be the same as those in section 6.2.)~~This key expansion function depends on the ESP authentication algorithm and is specified in Annex Y of this specification.

The integrity key ~~derivation~~expansion on the user side is done in the ~~ISIM~~UE. The integrity key ~~derivation~~expansion 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.*~~

7 Security association set-up procedure

The security association set-up procedure is necessary in order to decide what security services ~~that~~ to apply and when the security services start. In the IMS, authentication of users is performed during registration as specified 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 that are 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~~is used to negotiate ~~or exchange~~ the SA parameters required for IPsec ESP with authentication, but without confidentiality.~~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:~~

- ~~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.~~

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

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

- ~~ESP transform identifier~~
- Authentication (integrity) algorithm. The authentication algorithm is either HMAC-MD5-96 [rfc2403] or HMAC-SHA-1-96 [rfc2404]. Both authentication algorithms shall be supported by both, the UE and the P-CSCF as mandated by rfc2406. In the unlikely event that one of the authentication algorithm is compromised during the lifetime of this specification, this algorithm shall no longer be supported.

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

- ~~–~~ SPI (Security Parameter Index). The SPI is allocated locally for inbound SAs. The triple (SPI, destination IP address, transport protocol) uniquely identifies an SA. The most significant bit of any SPI allocated by the P-CSCF shall be "0" and the most significant bit of any SPI allocated by the UE shall be "1".

Note: this allocation of SPIs ensures that protected messages in the uplink always differ from protected messages in the downlink in, at least, the SPI field. This thwarts reflection attacks.

~~Further~~ SA parameters that need not be negotiated:

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

  Note: The SA lifetime is controlled by the application, cf. section 7.4 on SA handling.

- Mode: transport mode

- Key length: the length of ~~encryption and~~the authentication (integrity) keys IK_{ESP} depends on the authentication algorithm. It is 128 bits for HMAC-MD5-96 and 160 bits for HMAC-SHA-1-96.

Selectors:

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

- The source and destination IP addresses associated with the SA are those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

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

[Editor's note: If the condition in the above note seems to be too restrictive then the source and destination IP addresses associated with the SA could also be negotiated as part of the security mode set-up procedure. CN1 should say whether there is a need for this.]

- The transport protocol is either TCP or UDP.

- Ports:

1. The P-CSCF receives messages protected with ESP from any UE on one fixed port (the "protected port") different from the standard SIP port 5060. The number *Port_P* of the protected port is communicated to the UE during the security mode set-up procedure, cf. section 7.2. No unprotected messages must be sent to or received on this port. The P-CSCF may receive unprotected messages from any UE on any port which is different from the protected port.

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

3. For each security association, the UE assigns a port to send or receive messages to and from the P-CSCF protected with ESP ("protected port"). The number *Port_U* of this port is communicated to the P-CSCF during the security mode set-up procedure, cf. section 7.2. No unprotected messages must be sent to or received on this port. The UE may use different port numbers for TCP and UDP. The UE may send or receive unprotected messages to or from the P-CSCF on any ports which are not protected ports.

[Editor's note: The condition that the UE sends and receives protected messages on the same port is not necessary from a security point of view. These ports could be made different, at the expense of one more parameter to be negotiated in the security mode set-up procedure, but they have to be fixed in the registration procedure.]

~~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 P-CSCF ~~may~~ is allowed to ~~send~~ receive only the following messages on unprotected ports: ~~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~~not arriving on the protected port must be discarded by ~~the SIP application on~~ the P-CSCF.

5. The UE is allowed to ~~may~~ receive only the following messages on an unprotected port ~~other than a port for protected messages~~:

   - response to unprotected REGISTER message;

   - error messages.

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

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

The following rules apply:

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

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

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

[Editor's note: it is required that the UE's IP address is always bound to the IPsec security association. This can be done as in rule 2 above by deriving the UE's IP address from the contact header in a protected REGISTER message. The contact header must be always present when a user registers via a P-CSCF. An alternative way of binding the UE's IP address to the IPsec SA would be provided by including it in the security mode set-up procedure. (This is not yet covered in section 7.2.) This alternative would also allow to bind a range or a small number of UE IP addresses to the SA, if required.]

3. The SIP application at the P-CSCF shall check upon receipt of a REGISTER message that the triples (UE_IP_address, UE_protected_port, transport protocol), proposed in the security mode set-up (cf. section 7.2) have not yet been associated with entries in the "SA_table". If they already have been associated with an entry the registration is aborted and a suitable error message is sent to the UE. Furthermore, the P-CSCF shall check that, for one IMPI, no more than three SAs per direction and per transport protocol are stored at any one time.

Note: according to section 7.4 on SA handling, at most three SAs per direction and per transport protocol need to exist at a P-CSCF for one user at any one time.

4. For each incoming protected message the SIP application at the P-CSCF must verify that the correct inbound SA ~~associated with the public ID (IMPU) given in the SIP message~~ according to section 7.4 on SA handling has been used,. ~~This shall be done by verifying that the correct~~The SA is identified by the triple (UE_IP_address, UE_protected_port, transport protocol) in the SA table. ~~source IP address and source port bound~~ The SIP application at the P-CSCF must further check that the IMPU associated with the SA in the SA-table and the IMPU in the received SIP message coincide. ~~to the public ID (IMPU) of the SIP message have been used for sending the message.~~ If this is not the case the message must be discarded.

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

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

6. When establishing two new pairs of SAs (cf. section 6.3) the SIP application at the UE shall ensure for each transport protocol that the selected number for the protected port does not correspond to an entry in the "SA_table".

Note: regarding the selection of the number of the protected port at the UE it is generally recommended that the UE randomly selects the number of the protected port from a sufficiently large set of numbers not yet allocated at the UE. This is to thwart a limited form of a Denial of Service attack.

7. For each incoming protected message the SIP application at the UE must verify that the correct inbound SA according to section 7.4 on SA handling has been used. The SA is identified by the pair (UE_protected_port, transport protocol) in the SA table.

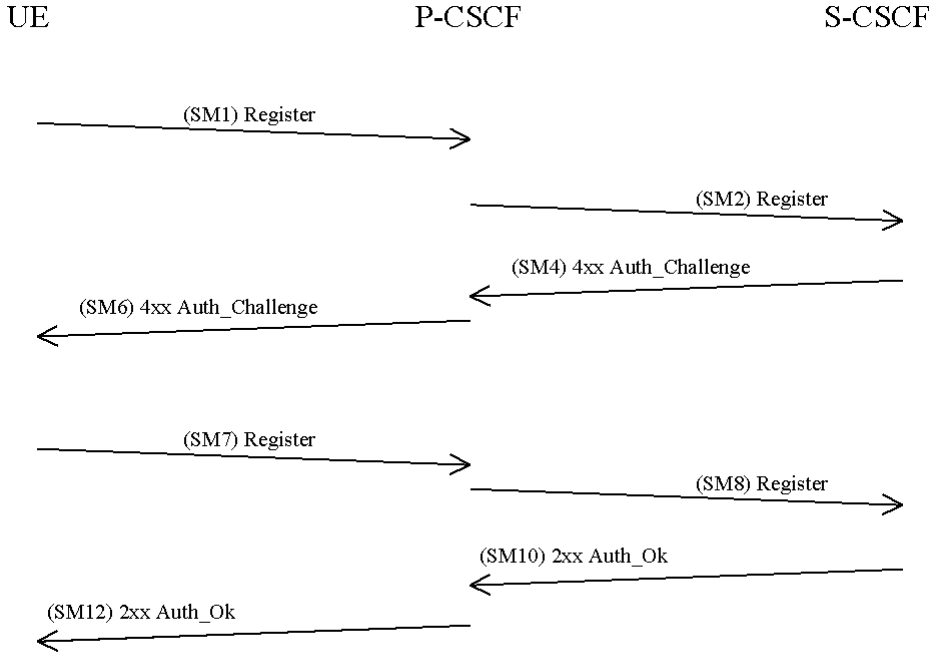
8. The lifetime of an SA between the UE and the P-CSCF shall be equal to the registration period.

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

7.2 Set-up of security associations (successful case)

The stage 3 specification of this information flow [tba] is based on [draft-IETF-sip-sec-agree]. Annex X of this specification shows how to use [draft-IETF-sip-sec-agree] for security mode set-up.

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, cf. section 6.1. ~~This has been described in 6.1.~~ In order to start the security mode set-up procedure the UE shall include a *Security-setup:* line in this message.~~,~~ ~~including 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.~~

The *Security-setup:* line in SM1 contains the SPIs and the numbers of the protected ports assigned by the UE for the SAs for TCP and UDP. It also contains a list of identifiers for the authentication algorithms which the UE supports.

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

SM1:
REGISTER(Security-setup = *SPI_U_TCP, SPI_U_UDP, Port_U_TCP, Port_U_UDP, UE authentication algorithms list)*
~~integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info]), IMPI, IMPU)~~

Upon receipt of SM1, the P-CSCF temporarily stores the parameters received in the *Security-setup:* line together with the UE's IP address, IMPI and IMPU. Upon receipt of SM4, the P-CSCF adds the key IK_{IM} received from the S-CSCF to the temporarily stored parameters. The P-CSCF then selects the SPIs for the inbound SAs for TCP and UDP.
In order to determine the authentication algorithm the P-CSCF proceeds as follows: the P-CSCF has a list of authentication algorithms it supports, ordered by priority. If HMAC-MD5-96 is supported it shall have the highest priority on the list. The P-CSCF selects the first authentication algorithm on its own list which is also supported by the UE.
The P-CSCF then establishes the two pairs of SAs in the local security association database.
~~The P-CSCF shall choose 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.]~~

The *Security-setup:* line in SM6 contains the SPIs assigned by the P-CSCF for the SAs for TCP and UDP and the fixed number of the protected port at the P-CSCF. It also contains a list of identifiers for the authentication algorithms which the P-CSCF supports.

SM6:
401 Unauthorized response ~~4xx Auth_Challenge~~(Security-setup = *SPI_P_TCP, SPI_P_UDP, Port_P, P-CSCF authentication algorithms list)*
~~*integrity mechanism, [confidentiality mechanism], integrity algorithm, [confidentiality algorithm], SA_ID_P, [info],* IMPI)~~

Upon receipt of SM6, the UE determines the authentication algorithm as follows: the UE selects the first authentication algorithm on the list received from the P-CSCF in SM 6 which is also supported by the UE.
The UE then proceeds to establish the two pairs of SAs in the local SAD.

The UE shall ~~in~~ integrity-protect SM7 and all following messages.~~start the integrity protection – 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 in SM6~~1~~ shall be included:

SM7:
REGISTER(Security-setup = *P-CSCF authentication algorithms list)*
~~*integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info],* IMPI)~~

After receiving SM7 from the UE, the P-CSCF shall ~~compare~~ check whether authentication algorithms list ~~the Security-Setup line of~~ received in ~~this message~~SM7 is identical with the authentication algorithms list ~~Security-Setup line received~~ sent in SM6~~1.~~. If this is not the case the registration procedure is aborted. The P-CSCF shall include 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~~User authentication failure ~~in the P-CSCF~~

In this case, SM7 containing a ~~potentially~~ wrong RES fails integrity check by IPsec at the P-CSCF if the ~~(~~IK_{IM} derived from RAND at UE is wrong as well~~).~~ The 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 RES 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).~~

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 unprotected 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 unprotected 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~~ 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~~ are already active. The authenticated re-registration ~~shall initially utilize~~should then use the existing SAs. If the S-CSCF is notified by the P-CSCF that the REGISTER message from the UE was integrity-protected it may decide not to authentication the user by means of the AKA protocol. However, the UE may send unprotected REGISTER messages at any time. In this case, the S-CSCF shall authenticate the user by means of the AKA protocol. ~~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 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~~

- ~~ESP transform identifier~~
- ~~Authentication (integrity) algorithm~~
- ~~SPI~~

~~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.~~

~~D.2 Security mode setup for IPsec ESP~~

~~This section describes how the security mode setup described in chapter 7 shall be used for negotiating ESP as protection mechanism and setting up the parameters required by ESP.~~

~~D.2.1 General procedures specific to the ESP protection mechanism~~

~~The integrity and encryption mechanisms both have the value "esp". The fields SA_ID_U and SA_ID_P carry the SPI values to be exchanged, to identify the ESP SAs.~~

~~The P-CSCF shall use an unprotected port to be able to receive specific unprotected messages. This unprotected port has to be communicated to the UE, by using the *info* field of message SM6. This unprotected port is required, when an IPsec SA is already in place at the P-CSCF, but the UE due to any reason is not able to use this SA. In this case, the UE shall send error messages or a new REGISTER message in the clear to the P-CSCF port received in the *info* field within SM6. Otherwise at the P-CSCF side, ESP would simply drop all IP packets from the UE that fail the integrity check.~~

~~The error messages that shall be sent in the clear from the UE to the P-CSCF are these for network authentication failures (sections 7.3.1.2) and synchronization failures (section 7.3.1.3).~~

~~D.2.2 Handling of user authentication failure~~

~~(This extends the content of chapter 7.3.1.1 and 7.3.3.3 for IPsec ESP)~~

~~In the case of a user authentication failure, the user will usually not be able to use a security association with the correct key material. Therefore, when using ESP for integrity protection and encryption, this will cause SM7 to be dropped at the P-CSCF IP(sec) layer due to a failed integrity check within ESP processing.~~

~~As SM7 will not reach the P-CSCF IMS application, the P-CSCF shall implement a timer for the authentication process. When a message is received that passes the integrity-check and successfully completes the authentication, it is immediately processed. However, if during the registration timer the P-CSCF receives packets that cannot be verified, it discards them. At the end of the registration timer, it reports an authentication failure back to the home network.~~

~~D.2.3 Authenticated re-registration procedures specific to the ESP protection mechanism~~

~~The new security associations SA11 and SA12 shall be bound to a new port on the UE side. This new port shall be communicated by the UE in the *info* field of the first REGISTER message SM1.~~

Annex X (normative): The use of [draft-IETF-sip-sec-agree] for security mode set-up

tba

Annex Y (normative): Key expansion functions for IPsec ESP

If the selected authentication algorithm is HMAC-MD5-96 then $IK_{ESP} = IK_{IM}$.

If the selected authentication algorithm is HMAC-SHA-1-96 then IK_{ESP} is obtained from IK_{IM} by appending the 32 most significant bits of IK_{IM} to IK_{IM}.