3GPP TSG SA WG3 Security — S3#29 **S3-030418**
15 - 18 July 2003, San Francisco, USA

CR-Form-v7

CHANGE REQUEST

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

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Security association handling, behaviour of SIP over TCP and re-authentication
Source:	⌘	Lucent / Siemens
Work item code:	⌘	IMS
Date:	⌘	07/07/2003
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	1) The establishment of security associations in a registration described in TS 33.203 v5.6.0 does not adequately take into account the communication behaviour of SIP over TCP. *2)* The change of security association in a re-authentication described in TS 33.203 v5.6.0 may lead to a change of UE server ports during an ongoing dialogue. It must be avoided to have to communicate this change to the remote entity.
Summary of change:	⌘	1. Establish two pairs of security associations, instead of one, to account for two different TCP connections. 2. Security associations in a re-authentication shall leave server ports fixed and change only client ports.
Consequences if not approved:	⌘	Lack of alignment with SIP RFC 3261.

Clauses affected:	⌘	Section 6 and 7

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

Other comments:	⌘	

***** Begin of Change ****

6 Security mechanisms

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 two pairs of (unilateral)~~a~~ security associations (SAs) ~~is~~ are 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~~ two pairs of SAs shall be active between the UE and the P-CSCF. This two pairs of SAs ~~single SA~~ shall be updated when a new successful authentication of the subscriber has occurred, cf. section 7.4.

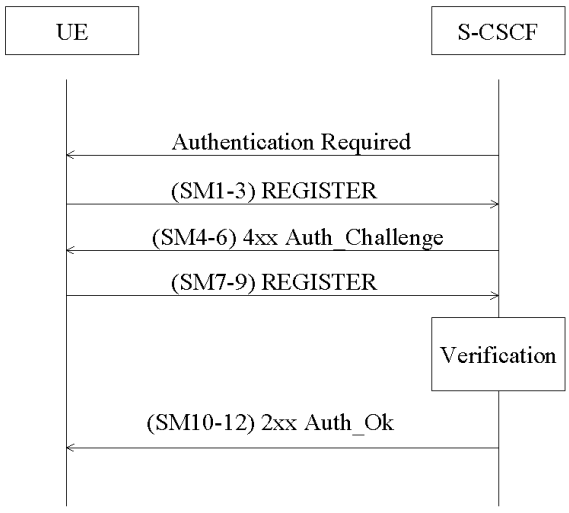
It is the policy of the HN that decides if an authentication shall take place for the registration of different IMPUs e.g. belonging to same or different service profiles. Regarding the definition of service profiles cf. [3].

***** End of Change ****

***** Begin of Change ****

6.1.4 Network Initiated authentications

In order to authenticate an already registered user, the S-CSCF shall send a request to the UE to initiate a re-registration procedure. When received at the S-CSCF, the re-registration shall trigger a new IMS AKA procedure that will allow the S-CSCF to re-authenticate the user.



Both the UE and the P-CSCF shall shorten the lifetime of the old SA pairs generated from the last successful authentication, so as to guarantee that the new SA pairs shall be used.

The UE shall initiate the re-registration on the reception of the Authentication Required indication. In the event that the UE does not initiate the re-registration procedure after the request from the S-CSCF, the S-CSCF may decide to de-register the subscriber or re-issue an Authentication-Required.

6.1.5 Integrity protection indicator

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

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

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

6.2 Confidentiality mechanisms

No confidentiality mechanism is provided in this specification, cf. clause 5.1.3.

6.3 Integrity mechanisms

IPsec ESP as specified in reference [13] shall provide integrity protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. IPSec ESP general concepts on Security Policy management, Security Associations and IP traffic processing as described in reference [14] shall also be considered. ESP integrity shall be applied in transport mode between UE and P-CSCF.

The method to set up ESP security associations (SAs) during the SIP registration procedure is specified in clause 7. As a result of an authenticated ~~the~~ registration procedure, two~~a~~ pairs of unidirectional SAs between the UE and the P-CSCF, all shared by TCP and UDP, shall be established in the P-CSCF and later in the UE. One SA pair is for traffic ~~from~~ between a client port at the UE ~~to~~ and a server port at the P-CSCF ~~(inbound SA at the P-CSCF)~~ and the other SA is for traffic ~~from~~ between a client port at the P-CSCF ~~to~~ and a server port at the UE ~~(outbound SA at the P-CSCF)~~. For a detailed description of the establishment of these security associations see section 7.

The integrity key IK_{ESP} is the same for the two pairs of simultaneously established SAs. The integrity key IK_{ESP} is obtained from the key IK_{IM} established as a result of the AKA procedure, specified in clause 6.1, using a suitable key expansion function. This key expansion function depends on the ESP integrity algorithm and is specified in Annex I of this specification.

The integrity key expansion on the user side is done in the UE. The integrity key expansion on the network side is done in the P-CSCF.

The anti-replay service shall be enabled in the UE and the P-CSCF on all established SAs.

***** End of Change ****

***** Begin of Change ****

7 Security association set-up procedure

The security association set-up procedure is necessary in order to decide what security services to apply and when the security services start. In the IMS authentication of users is performed during registration as specified in clause 6.1. Subsequent signaling communications in this session will be integrity 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, and a set of parameters specific to a protection method. The security mode setup (cf. clause 7.2) is used to negotiate the SA parameters required for IPsec ESP with authentication, but without confidentiality.

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

- **Integrity algorithm**

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

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

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

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

- **SPI (Security Parameter Index)**

The SPI is allocated locally for inbound SAs. The triple (SPI, destination IP address, security protocol) uniquely identifies an SA at the IP layer. The UE shall select the SPIs uniquely, and different from any SPIs that might be used in any existing SAs (i.e. inbound and outbound SAs). The SPIs selected by the P-CSCF shall be different than the SPIs sent by the UE, cf. section 7.2. In an authenticated registration, the UE and the P-CSCF each select two SPIs, not yet associated with existing inbound SAs, for the new inbound security associations at the UE and the P-CSCF respectively.

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

The following SA parameters are not negotiated:

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

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

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

Selectors:

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

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

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

- The transport protocol selector shall allow UDP and TCP.
- Ports:

1. ~~1.~~ The P-CSCF associates two ports, called *port_ps* and *port_pc*, with each pair of security assocations established in an authenticated registration. The ports *port_ps* and *port_pc* are different from the standard SIP ports 5060 and 5061. No unprotected messages shall be sent from or received on the ports *port_ps* and *port_pc*. From a security point of view, unprotected messages may be received on any port which is different from the ports *port_ps* and *port_pc*. The number of the ports *port_ps* and *port_pc* are communicated to the UE during the security mode set-up procedure, cf. clause 7.2. These ports are used with both, UDP and TCP. The use of these ports may differ for TCP and UDP, as follows:
   UDP case: t~~T~~he P-CSCF receives requests and responses ~~messages~~ protected with ESP from any UE on ~~one fixed~~the port *port_ps* (the"protected server port") ~~different from the standard SIP port 5060~~. The P-CSCF sends requests and responses protected with ESP to a UE on the port *port_pc* (the "protected client port"). ~~The number of the protected port is communicated to the UE during the security mode set-up procedure, cf. clause 7.2.~~ For every protected request towards the UE, the P-CSCF shall insert the protected server port *port_ps* into the Via header. The protected responses from the UE are then sent to port_ps at the P-CSCF. ~~No unprotected messages shall be sent from or received on this port. From a security point of view, the P-CSCF may receive unprotected messages from any UE on any port which is different from the protected port.~~
   TCP case: the P-CSCF receives requests and sends responses protected with ESP from and to any UE on the port *port_ps*. The P-CSCF sends requests and receives responses protected with ESP to and from a UE on the port *port_pc* (the "protected client port").

NOTE: The protected server port *port_ps* stays fixed for a UE until all IMPUs from this UE are de-registered. It may be ~~is~~ fixed for a particular P-CSCF over all UEs, but there is no need to fix the same protected server port ~~may be different~~ for different P-CSCFs.

NOTE: The distinction between the UDP and the TCP case reflects the different behaviour of SIP over UDP and TCP, as specified in RFC 3261, section 18.

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

2~~3~~. The UE associates two ports, called *port_us* and *port_uc*, with each pair of security assocations established in an authenticated registration. The ports *port_us* and *port_uc* are different from the standard SIP ports 5060 and 5061. No unprotected messages shall be sent from or received on the ports *port_us* and *port_uc*. From a security point of view, unprotected messages may be received on any port which is different from the ports *port_us* and *port_uc*. The number of the ports *port_us* and *port_uc* are communicated to the P-CSCF during the security mode set-up procedure, cf. clause 7.2. These ports are used with both, UDP and TCP. The use of these ports may differ for TCP and UDP, as follows:
   UDP case: the UE receives requests and responses protected with ESP on the port *port_us* (the"protected server port"). The UE sends requests and responses protected with ESP on the port *port_uc* (the "protected client port"). For every protected request towards the P-CSCF, the UE shall insert the protected server port

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

NOTE: The protected server port *port_us* stays fixed for a UE until all IMPUs from this UE are de-registered.

NOTE: The distinction between the UDP and the TCP case reflects the different behaviour of SIP over UDP and TCP, as specified in RFC 3261, section 18.

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

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

- responses to unprotected REGISTER messages;
- error messages.

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

The following rules apply:

1. For each unidirectional 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, P-CSCF_protected_port, SPI, IMPI, IMPU1, ... , IMPUn, lifetime) in an "SA_table". The pair (UE_protected_port, P-CSCF_protected_port) equals either (*port_uc*, *port_ps*) or (*port_us*, *port_pc*).

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

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

3. The SIP application at the P-CSCF shall check upon receipt of an initial REGISTER message that the pair (UE_IP_address, ~~UE_protected_port~~UE_protected_client_port), where the UE_IP_address is the source IP address in the packet header and the protected client port is sent as part of the security mode set-up procedure (cf. clause 7.2), has not yet been associated with entries in the "SA_table". Furthermore, the P-CSCF shall check that, for any one IMPI, no more than ~~three~~ six SAs per direction are stored at any one time. If these checks are unsuccessful the registration is aborted and a suitable error message is sent to the UE.

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

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

5. For each unidirectional SA which has been established and has not expired, the SIP application at the UE stores at least the following data: (UE_protected_port, P-CSCF_protected_port, SPI, lifetime) in an "SA_table". The pair (UE_protected_port, P-CSCF_protected_port) equals either (*port_uc*, *port_ps*) or (*port_us*, *port_pc*).

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

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

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

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

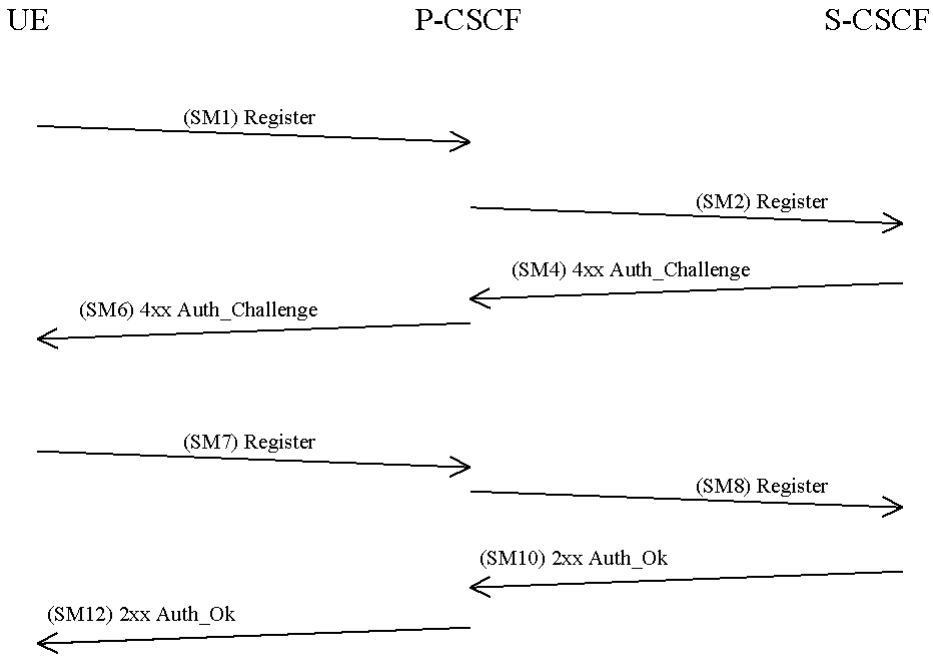
NOTE: If the integrity check of a received packet fails then IPsec will automatically discard the packet.

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

7.2 Set-up of security associations (successful case)

The set-up of security associations is based on [21]. Annex H of this specification shows how to use [21] for the set-up of security associations.

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. clause 6.1. In order to start the security mode set-up procedure, the UE shall include a *Security-setup*-line in this message.

The *Security-setup-line* in SM1 contains the Security Parameter Index values and the protected ports selected by the UE. It also contains a list of identifiers for the integrity algorithms which the UE supports.

SM1:
REGISTER(Security-setup = *SPI_U, Port_U, UE integrity algorithms list)*

SPI_U is the symbolic name of ~~the~~ a pair of SPI values (cf. section 7.1) (*spi_uc, spi_us*) that the UE selects. *spi_uc* is the SPI of the inbound SA at the UE's protected client port, and *spi_us* is the SPI of the inbound SA at the UE's protected server port. The syntax of *spi_uc* and *spi_us* ~~spi~~ is defined in Annex H.

Port_U is the symbolic name of a pair of port numbers (*port_uc, port_us*) as defined in section 7.1. ~~(port1, port2) where port1 defines the destination port number for inbound messages at the UE that are protected, and port2 defines the source port number for outbound messages at the UE that are protected.~~ The syntax of *port_uc* ~~port1~~ and *port_us* ~~port2~~ is defined in Annex H.

Upon receipt of SM1, the P-CSCF temporarily stores the parameters received in the *Security-setup-line* together with the UE's IP address from the source IP address of the IP packet header, the 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. The P-CSCF shall define the SPIs such that they are unique and different from any SPIs as received in the *Security-setup-line* from the UE.

NOTE: This rule is needed since the UE and the P-CSCF use the same key for inbound and outbound traffic.

In order to determine the integrity algorithm the P-CSCF proceeds as follows: the P-CSCF has a list of integrity algorithms it supports, ordered by priority. The P-CSCF selects the first integrity algorithm on its own list which is also supported by the UE.

The P-CSCF then establishes ~~another~~ two new pairs of SAs in the local security association database.

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

SM6:
4xx Auth_Challenge(Security-setup = SPI_P, Port_P, *P-CSCF integrity algorithms list)*

SPI_P is the symbolic name of the pair of SPI values (cf. section 7.1) (*spi_pc, spi_ps*) ~~spi~~ that the P-CSCF selects. The syntax of *spi_pc* and *spi_ps* ~~spi~~ is defined in Annex H.

Port_P is the symbolic name of the port numbers (*port_pc, port_ps*) as defined in section 7.1. *spi_pc* is the SPI of the inbound SA at the P-CSCF's protected client port, and *spi_ps* is the SPI of the inbound SA at the P-CSCF's protected server port. ~~port1, where port1 defines the destination port number for inbound messages at the P-CSCF that are protected. The port number port2 of the P-CSCF shall be absent in Port_P.~~ The syntax of Port_P~~port1~~ is defined in Annex H.

Upon receipt of SM6, the UE determines the integrity algorithm as follows: the UE selects the first integrity 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 two new ~~another~~ pairs of SAs in the local SAD.

The UE shall integrity-protect SM7 and all following SIP messages. Furthermore the integrity algorithms list, *SPI_P,* and *Port_P* ~~-~~received in SM6, and *SPI_U, Port_U sent in SM1* shall be included:

SM7:
REGISTER(Security-setup = *SPI_U, Port_U, SPI_P, Port_P, P-CSCF integrity algorithms list)*

After receiving SM7 from the UE, the P-CSCF shall check whether the integrity algorithms list, *SPI_P,* and *Port_P* received in SM7 is identical with the ~~integrity algorithms list~~corresponding parameters sent in SM6. It further checks whether *SPI_U* and *Port_U* received in SM7 are identical with those received in SM1. If this is not the case the registration procedure is aborted. The P-CSCF shall include in SM8 information to the S-CSCF that the received message from the UE was integrity protected as indicated in clause 6.1.5. The P-CSCF shall add this information to all

subsequent REGISTER 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.

The use of the two pairs of unidirectional SAs is illustrated in the figure below with a set of example message exchanges protected by the respective IPsec SAs where the INVITE and following messages are assumed to be carried over TCP.

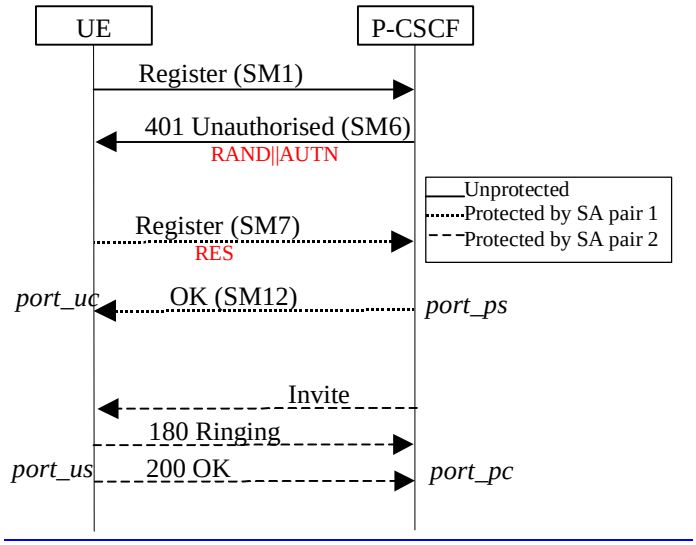


Figure 1

***** End of Change ****

***** Begin of Change ****

7.4 Authenticated re-registration

Every registration that includes a user authentication attempt produces new security associations. If the authentication is successful, then these new security associations shall replace the previous ones. This clause describes how the UE and P-CSCF handle this replacement and which SAs to apply to which message.

When security associations are changed in an authenticated re-registration then the protected server ports at the UE (*port_us*) and the P-CSCF (*port_ps*) shall remain unchanged, while the protected client ports at the UE (*port_uc*) and the P-CSCF (*port_pc*) shall change. For the definition of these ports see section 7.1.

If the UE has an already active pair of security associations, then it shall use this to protect the REGISTER message. 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 authenticate 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. In particular, if the UE considers the SAs no longer active at the P-CSCF, e.g., after receiving no response to several protected messages, then the UE should send an unprotected REGISTER message.

Security associations may be unidirectional or bi-directional. This clause assumes that security associations are unidirectional, as this is the general case. 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 IPsec layer. The message numbers, e.g. SM1, used in the following clauses relate to the message flow given in section 6.1.1.

7.4.1 Void

7.4.1a Management of security associations in the UE

The UE shall be involved in only one registration procedure at a time, i.e. the UE shall remove any data relating to any previous incomplete registrations or authentications, including any SAs created by an incomplete authentication.

The UE may start a registration procedure with ~~an~~ two existing pairs of SAs. These~~is~~ will be referred to as the old SAs. The authentication produces two ~~a~~ pairs of new SAs. These new SAs shall not be~~y~~ used to protect non-authentication traffic until noted during the authentication flow. In the same way, certain messages in the authentication shall be protected with a particular SA. If the UE receives a message protected with the incorrect SA, it shall discard the message.

A successful authentication proceeds in the following steps:

- The UE sends the SM1 message to register with the IMS. If SM1 was protected, it shall be protected with the old outbound SA.
- The UE receives an authentication challenge in a message (SM6) from the P-CSCF. This message shall be protected with the old inbound SA if SM1 was protected and unprotected otherwise.
- If this message SM6 can be successfully processed by the UE, the UE creates the new SAs, which are derived according to section 7.1. The lifetime of the new SAs shall be set to allow enough time to complete the registration procedure. The UE then sends its response (SM7) to the P-CSCF, which shall be protected with the new outbound SA. Meanwhile, if SM1 was protected, the UE shall use the old SAs for messages other than those in the authentication, until a successful message of new authentication is received (SM12); if SM1 was unprotected, the UE is not allowed to use IMS service until it receives an authentication successful message (SM12).
- The UE receives an authentication successful message (SM12) from the P-CSCF. It shall be protected with the new inbound SA.
- After the successful processing of this message by the UE, the registration is complete. The UE sets the lifetime of the new SAs using the maximum of registration timer in the message and the lifetime of the old SAs. For further ~~traffic~~ requests sent from UE, the new outbound SAs ~~is~~ are used. Responses received over an old SA are still sent over the old SA. When no more responses are to be sent over an old SA, t~~T~~he old outbound SAs ~~is~~ are are now deleted. The old inbound SAs ~~is~~ are kept for receiving messages from P-CSCF. In particular, responses to requests sent over the old SA shall be received over the old SA.~~It~~ They shall be deleted when either lifetime is expired, or a further SIP message protected with ~~the~~ a new inbound SA is successfully received from the P-CSCF, and no more responses to be received over the old SA are expected.. The new SAs are used to protect all traffic.

A failure in the authentication can occur for several reasons. If the SM1 was not protected, then no protection shall be applied to the failure messages, except the user authentication failure message which shall be protected with the new SA. If SM1 was protected, the old SAs shall be used to protect the failure messages. In both cases, after processing the failure message, the UE shall delete the new SAs.

The UE shall monitor the expiry time of registrations without authentication and adjust the lifetime of SAs it holds to ensure that they live longer than the expiry time given in the registration.

The UE shall delete any SA whose lifetime is exceeded.

7.4.2 Void

7.4.2a Management of security associations in the P-CSCF

When the S-CSCF initiates an authentication by sending a challenge to the UE, the P-CSCF may already contain existing SAs from previously completed authentications. It may also contain ~~an~~ two existing pairs of SAs from an incomplete authentication. These will be referred to as the old and registration SAs respectively. The authentication produces two~~a~~ pairs of new SAs. These new SAs shall not be used to protect non-authentication traffic until noted during the authentication flow. Similarly certain messages in the authentication shall be protected with a particular SA. If the P-CSCF receives a message protected with the incorrect SA, it shall discard the message.

The P-CSCF associates the IMPI given in the registration procedure and all the successfully registered IMPUs related to that IMPI to an SA.

A successful authentication proceeds in the following steps:

- The P-CSCF receives the SM1 message. If SM1 is protected, it shall be protected with the old inbound SA to .
- The P-CSCF forwards the message containing the challenge (SM6) to the UE. This shall be protected with the old outbound SA , if SM1 was protected and unprotected otherwise.
- The P-CSCF then creates the new SAs, which are derived according to section 7.1. The expiry time of the new SAs shall be set to allow enough time to complete the registration procedure. The registration SAs shall be deleted if they exist.
- The P-CSCF receives the message carrying the response (SM7) from the UE. It shall be protected using the new inbound SA. If SM1 was protected, the old SAs are used to protect messages other than those in the authentication.
- The P-CSCF forwards the successful registration message (SM12) to the UE. It shall be protected using the new outbound SA. This completes the registration procedure for the P-CSCF. The P-CSCF sets the expiry time of the new SAs equal to the maximum of registration timer in the message and the lifetime of the old SAs.
- After SM12 is sent, the P-CSCF handles the UE related SAs according to following rules:
  - If there are old SAs, but SM1 is received unprotected, the P-CSCF considers error cases happened, and assumes UE does not have those old SAs for use. In this case the P-CSCF shall remove the old SAs.
  - If SM1 is protected with an old valid SA, the P-CSCF keeps this inbound SA and the corresponding ~~outbound~~ three SAs created during the same registration with the UE active, and continues to use them. In particular, responses to requests sent/received over the old SA shall be received/sent over the old SA. Any other old SAs are deleted. The kept old SAs are deleted when either the old SAs lifetime are expired, or a further SIP message protected with ~~the~~ a new inbound SA is successfully received from the UE, and no more responses to be sent or received over the old SAs are expected.. Then further messages are protected with new SAs. This completes the SA handling procedure for the P-CSCF.

A failure in the authentication can occur for several reasons. If the SM1 was not protected, then no protection shall be applied to the failure messages, except the user authentication failure message which shall be protected with the new SAs. If SM1 was protected, the old SAs shall be used to protect the failure messages. In both cases, after processing the failure message, the P-CSCF shall delete the new SAs.

The P-CSCF shall monitor the expiry time of registrations without authentication and adjust the lifetime of SAs it holds to ensure that they live longer than the expiry time given in the registration.

The P-CSCF shall delete any SA whose lifetime is exceeded.

******End of Change ***