3GPP TSG SA WG3 Security — S3#28 **S3-030258**
6 - 9 May 2003, Berlin, Germany

CR-Form-v7

CHANGE REQUEST

⌘	**33.203**	**CR**		⌘ **rev**		⌘ Current version: **5.5.0** ⌘

*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 ☒	Radio Access Network □	Core Network ☒

Title:	⌘	SA set-up procedure		
Source:	⌘	Lucent Technologies		
Work item code:	⌘	IMS	***Date:*** ⌘	28/04/2003
Category:	⌘	**F**	***Release:*** ⌘	***Rel-5***
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	Each re-authentication results in new local port (new "protected port") at the UE, this has a very serious side effect. The SIP protocol employs "source routing" mechanism. Since SIP assumes that the proxies along the routing path may be stateless, the SIP endpoints (i.e., user agents) must specify the entire route and the final target (IP address or FQDN, and destination port) of each request. Whenever, the final target (i.e., (IP address or FQDN, or destination port) for the registered user has changed, this information must be "globally disseminated." Hence, every re-authentication of the registered user specified in the document TS 33.203, will result in an "avalanche of SIP level messages" sent by the SIP level application in the UE.
Summary of change:	⌘	To avoid the problem stated above it is proposed that the source ports be used as a "selector" to identify the associated SAs. Therefore successful re-authentication, in spite of establishing a new SA, shall not result in assignment of new incoming port number at the UE. The proposed changes make explicit the use of the outbound source port as the selector used to identify a particular security association and ensures that the inbound port number is not changed during re-authentication.
Consequences if not approved:	⌘	Implementation of the SA setup procedure specifically relating to re-authentication will cause an unnecessary SIP signalling overhead

Clauses affected:	⌘	7.1,7.2				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

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.

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 a pair 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. The P-CSCF receives messages protected with ESP from any UE on one fixed inbound port (the "protected inbound port") different from the standard SIP port 5060. When the P-CSCF sends protected messages towards the UE, it shall select an outbound port (the "protected outbound port") different from the fixed inbound port, and include it as a source port in the IP packets. The numbers of the inbound and outbound protected ports ~~is~~ are communicated to the UE during the security mode set-up procedure, cf. clause 7.2. For every protected request towards UE, the P-CSCF shall insert the protected inbound port into Via header. No unprotected messages shall be sent from or received on the~~is~~ protected ports. 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 inbound port.

NOTE: The protected inbound port is fixed for a particular P-CSCF, but may be different for different P-CSCFs.

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.

3. For each security association, the UE assigns a local inbound port to ~~send or~~ receive protected messages ~~to and~~ from the P-CSCF ("protected inbound port"), and a local outbound port (the "protected outbound port"), different from the inbound port, to send protected messages to the P-CSCF. No unprotected messages shall be sent to or received on this ports. The UE shall use a single protected inbound port number, and a single protected outbound port number for both TCP and UDP connections. The inbound and outbound port numbers ~~is~~ are 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 outbound port number and send it to the network. If the re-REGISTER request was triggered by the re-authentication request, the UE shall use the old inbound port number. If the UE is not challenged by the network, the new outbound port number shall be obsolete. When the network challenges the UE, the P-CSCF shall always insert a new outbound port number into the challenge message prior to sending it to the UE. Annex H of this specification gives detail how the port numbers ~~is~~ are ~~populated in~~conveyed in the SIP messages. 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.

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

5. For every protected request, the UE shall insert ~~the~~ its protected inbound port ~~of the corresponding SA~~ into the Via header. The P-CSCF shall insure that the response is sent to the UE using the same SA on which the request was received. By including proper source port number in the IP packet, the P-CSCF shall indicate to the UE which SA was used for the response. The UE is allowed to receive only the following messages on an unprotected inbound port:

   - responses to unprotected REGISTER messages;

   - error messages.

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

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_inbound_port, P-CSCF_protected_outbound_port, SPI, IMPI, IMPU1, ... , IMPUn, lifetime) 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 ~~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 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_outbound_port), where the UE_IP_address is the source IP address in the packet header and the protected outbound 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 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 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 (UE_IP_address, UE_protected_outbound_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 SA which has been established and has not expired, the SIP application at the UE stores at least the following data: (~~UE~~P-CSCF_protected_outbound_port, SPI, lifetime) 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 a new pair of SAs (cf. clause 6.3) the SIP application at the UE shall ensure that the ~~selected~~ P-CSCF_protected_outbound_port number~~ for the protected port~~, 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 inbound 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 source port in the IP packet, that contains the P-CSCF protected_outbound_port identifies the SA ~~is identified by 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.

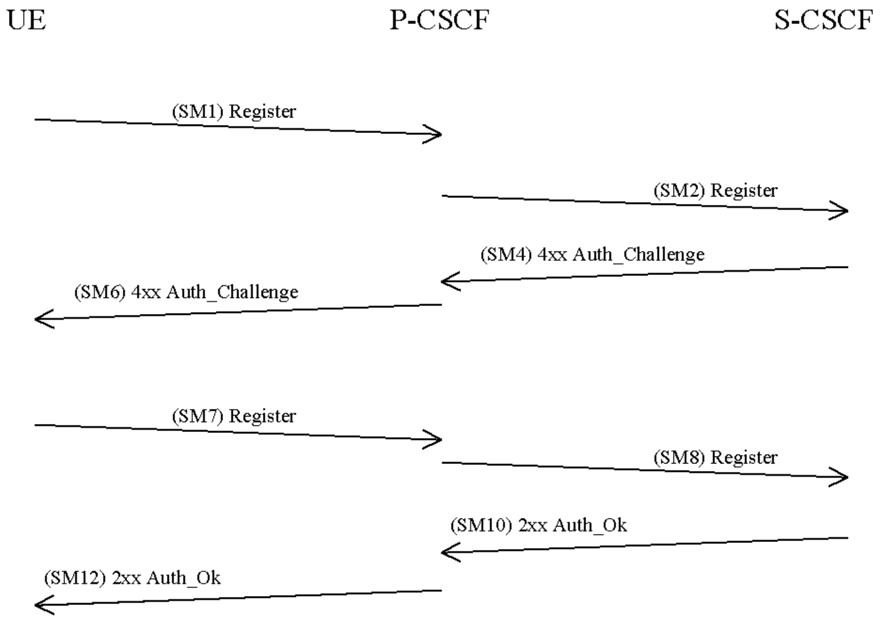
8. The UE shall insure that the response is sent to the P-CSCF using the same SA on which the request was received. By including proper source port number in the IP packet, the UE shall indicate to the P-CSCF which SA was used for the response.

9~~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 value and the protected inbound port and protected outbound port 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, Inbound Port_U, Outbound Port_U, UE integrity algorithms list)*

SPI_U is the symbolic name of the SPI value (cf. section 7.1) spi that the UE selects. The syntax of spi is defined in Annex H.

Inbound Port_U is the symbolic name of a ~~pair of~~ inbound port number~~s~~ (port1~~, port2~~) where port1 defines the destination port number for inbound messages at the UE that are protected, and Outbound Port_U is the symbolic name of a outbound port number (port2) where port2 defines the source port number for outbound messages at the UE that are protected. The syntax of port1 and 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 an outbound port number and the SPI for the inbound SA. 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 pair of SAs in the local security association database.

The *Security-setup*-line in SM6 contains the SPI assigned by the P-CSCF, the protected outbound port, and the fixed number of the protected inbound 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, Inbound_ Port_P*, *Outbound_ Port_P, P-CSCF integrity algorithms list)*

SPI_P is the symbolic name of the SPI value (cf. section 7.1) spi that the P-CSCF selects. The syntax of spi is defined in Annex H.

Inbound_Port_P is the symbolic name of the port number port1, where port1 defines the destination port number for inbound messages at the P-CSCF that are protected. Outbound_Port_P is the symbolic name of the port number port2, where port2 defines the source port number for outbound messages at the P-CSCF sent towards the UE that are protected ~~The port number port2 of the P-CSCF shall be absent in Port_P.~~ The syntax of 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 another pair of SAs in the local SAD.

The UE shall integrity-protect SM7 and all following SIP messages. Furthermore the integrity algorithms list received in SM6 shall be included:

SM7:
REGISTER(Security-setup = *P-CSCF integrity algorithms list)*

After receiving SM7 from the UE, the P-CSCF shall check whether the integrity algorithms list received in SM7 is identical with the integrity algorithms list sent in SM6. 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. 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.

3GPP TSG SA WG3 Security — S3#28 **S3-030xxx**
6 - 9 May 2003
Berlin, Germany

Source:	**Lucent Technologies**
Title:	**Security association set-up procedure**
Document for:	**Discussion**
Agenda Item:	**7.1**
WI/Topic:	**IMS**

1. Introduction

Prior to receiving IM services, the user has to register with the IMS as described in the documents TS 24.229 and TS 33.203. There are three functions that are performed during the initial registration, i.e.:

1. Mutual authentication between the subscriber and the network (i.e., UE and S-CSCF),
2. Establishment of Security Association (SA) between the UE and P-CSCF, and
3. Conveying the UE contact information to the S-CSCF indicating where the subscriber can be reached.

The scheme for mutual authentication and key agreement in the IMS is IMS AKA, and the associated challenge/response procedure is described in the documents TS 24.229 and TS 33.203. The procedure of setting up the SA between the UE and the P-CSCF is described in the document TS 33.203. The mechanism to convey the contact information (IP address or FQDN, port number, and transport protocol) for the indicated public user identities is described in the document TS 24.229. It should be mentioned that all three functions listed above are performed concurrently during the initial unprotected registration, subsequent challenge (401 response), and followed by the protected re-registration.

2. Discussion

2.1 Problem Statement

The document TS 33.203 identifies which SA parameters are negotiated between the UE and P-CSCF. At the UE or P-CSCF, the Security Parameter Index (SPI) that is locally allocated for the inbound Security Association (SA), will, in conjunction with the destination IP address and security protocol, uniquely identify to which SA the incoming IP packet pertains. In addition, the document TS 33.203 also identifies the "selectors" that should be employed when handling the inbound and outbound IP packets, and selecting the proper SA. The identified "selectors" are: the source and destination IP addresses, transport protocols that share the SA, and source and destination ports. These "selectors" are bound to a SA. For example, prior to sending the SIP message to the P-CSCF, the UE uses the "selector-values" as a pointer to the table (e.g., Security Policy Database) that specifies which SA should be employed when sending the message. Likewise, for the incoming IP packet arrives at the UE on a given incoming SA, the UE uses the "selector-values" as a pointer to the table (e.g., Security Policy Database) to verify that the proper SA was used. Subsequently, the message is delivered to the indicated port at the UE. The same procedure applies at the P-CSCF.

When a new SA is established in the UE (in addition to the old SA), new "selector-values" have to be bound to the new SA. However, since the document TS 33.203 assumes that the source and destination IP addresses, transport protocols, and P-CSCF's (protected) port, are fixed during the duration of UE registration, the only remaining "selector" that can be employed to identify the new SA is the local port in the UE. Therefore, the document TS 33.203 mandates that a new (different) local port number in the UE is assigned to point to the new SA. Likewise, when the P-CSCF sends an IP packet to the UE, it will, by specifying the UE's port number, indicate which SA was used to transfer the IP packet. Hence, the TS 33.203 document states:

> "*For each security association, the UE assigns a local port to send or receive protected messages to and from the P-CSCF ("protected port")………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."*

However, if the UE is challenged, the new port number will identify the new SA.

The S-CSCF may authenticate an already registered user at ant time by requesting the UE to initiate a re-registration procedure. Every registration that includes a user authentication attempt produces new SAs. If the authentication is successful, then these new SAs and associated local port at the UE (new "protected port") will replace the previous SAs and associated local port (old "protected port").

The mechanism described in the document TS 33.203, where each re-authentication results in new local port (new "protected port") at the UE, has a very serious side effect. The SIP protocol employs "source routing" mechanism. Since SIP assumes that the proxies along the routing path may be stateless, the SIP endpoints (i.e., user agents) must specify the entire route and the final target (IP address or FQDN, and destination port) of each request. Whenever, the final target (i.e., (IP address or FQDN, or destination port) for the registered user has changed, this information must be "globally disseminated." Hence, every re-authentication of the registered user specified in the document TS 33.203, will result in an " avalanche of SIP level messages" sent by the SIP level application in the UE. The following activities will be triggered:

1. The UE has to re-register all currently registered public user identities specifying new contact information (IP address or FQDN, new port number).
2. For each current dialog with associated multimedia session, the UE will have to send a re-INVITE request specifying new contact information (IP address or FQDN, new port number).
3. The UE will have to be re-SUBSCRIBE with all notifiers to inform them about the new contact information (IP address or FQDN, new port number).
4. The UE will have to re-subscribe to its registration-event package with the S-CSCF to inform the S-CSCF about its new contact information (IP address or FQDN, new port number).
5. Every re-registration (as indicated in 1. above) will cause the S-CSCF to send a NOTIFY request to all entities that have subscribed to the UE registration-event package (e.g., P-CSCF).
6. For Release 6, since it supports presence service, presence notification has to be sent to all watchers every time that the UE contact changes.

There are additional problems that may be caused by the indicated procedure. For example, when the UE responds to the challenge (i.e., 401 response), with the re-register request which port should it specify in the Contact header? The new port should not be specified, since this port should be used only if the new SA has been successfully established and the UE has been authenticated. However, if the old port was specified, and the 200 OK indicate that the new SA has been successfully established and the UE has been authenticated, then the S-CSCF will have to be informed about the new port through an additional registration.

2.2 Proposed Solution

To avoid the problem stated above it is proposed that the source ports be used as a "selector" to identify the associated SAs. The successful re-authentication, in spite of establishing a new SA, shall not result in assignment of new incoming port number at the UE. The following approach is proposed:

For each SA, the UE assigns an inbound local port (UE_inbound port), and an outbound local port (UE_outbound port) to send or receive protected messages to and from the P-CSCF. The UE_inbound port number is different then the UE_outbound port number. The UE_inbound port number and the UE_outbound port number are communicated to the P-CSCF during the security mode set-up procedure (in the Security-Client header). When the UE sends a re-REGISTER request, it shall always pick up a new UE_outbound port number and send it to the P-CSCF. If the UE is not challenged by the network, the UE_outbound port number shall be obsolete. When the UE sends a re-REGISTER request that is triggered by the re-authentication, the UE_inbound port is never modified.

For each SA, the P_CSCF has a fixed inbound local port (P-CSCF_inbound port), and assigns an outbound local port (P-CSCF_outbound port) to send or receive protected messages to and from the UE. The fixed P-CSCF_inbound port number is different then the P-CSCF_outbound port number. The fixed P-CSCF_inbound port number and the P-CSCF_outbound port number are communicated to the UE during the security mode set-up procedure (in the Security-Server header). When the P-CSCF sends a 401 response to the UE, it shall always pick up a new P-CSCF_outbound port number and send it to the UE.

The source port in the received IP packet (that contains the P-CSCF_outbound port number) shall identify the SA at the UE. The source port in the received IP packet (that contains the UE_outbound port number) shall identify the SA at the P-CSCF. The UE and P-CSCF shall insure that the response is always sent using the same SA on which the request was received.

3. Proposal

It is proposed that the SA3 WG discussed the identified problem, and adopts the SA set-up procedure proposed in this contribution. The companion CR provides the necessary changes to reflect the proposed procedure.