**3GPP TSG SA WG3 Security — S3#24** **S3-020416**

**9 - 12 July, 2002**

**Helsinki, Finland**

**Source:** **Nokia**

**Title:** **Common IPsec SA for UDP and TCP sockets**

**Agenda item:** **7.1, IMS**

Document for: **DISCUSSION/APPROVAL**

*Abstract*

*This paper studies the feasibility of sharing common IPsec Security Association (SA) for UDP and TCP sockets for each direction. The issue is investigated from SIP application, socket local binding and IPsec aspects, and no problem found conflicting with the assumption. Therefore a recommendation is proposed that SIP application does not identify two SAs in "SA_table", that is, sharing same SA for both sockets.*

## 1. INTRODUCTION

During last S3 meeting in Victoria, Canada, the IPsec based SA negotiation was discussed intensively for the first hop. It was clear for S3 the needs of requirement, supporting simultaneously TCP other than default UDP socket, so as to handle large message delivery.

The last meeting assumed that both TCP and UDP sockets shall establish individual SA between UE and P-CSCF, the two SAs are not shared despite of the same direction. They are differentiated by different SPI numbers and source port numbers. The contentious view was accepted, but further studying was suggested whether one SA would be sufficient to serve both sockets.

The analysis below shows the feasibility of one SA solution. Thus it is suggested the meeting endorses the proposal and the attached CR against TS 33.203 v5.2.0.

## 2. ANALYSIS

According to IPsec RFCs, IPsec can handle multiple sockets connections via same SA, if the IPsec policy is defined accordingly. When one end selects port number A, A is added to IPsec policy database by the peer as selector of the SA. In P-CSCF IPsec layer, for example, it can handle the SA processing based on SPI number, verifies the policy of SA from that port and IP address, and accepts the datagram regardless whether TCP or UDP header in payload. The same rationale of IPsec is deployed in product such as VPN, where IPsec tunnel does not care what are the applications and how many sockets are used.

When SIP application initiates both TCP and UDP connections, it opens two sockets, which shall bind to local port number. No problem has been found in implementation, for TCP and UDP to bind two sockets to the same local port number. Beside, the sockets can be connected to the same destination address as well. As the consequence, the two sockets opened by TCP and UDP, can point to the same destination.

From SIP application point of view, [IETF_SIP] stated clearly "For any port and interface that a server listens on for UDP, it MUST listen on that same port and interface for TCP. This is because a message may need to be sent using TCP, rather than UDP, if it is too large." When UAC sends a SIP message via UDP socket (UE_protected_port), UAS must prepare to receive a SIP message sent to UE_protected_port, but via TCP stack. Since 3GPP has chosen UDP as default transport, and S3 have specified UE shall send and received protected messages on the *same* port for UDP, this shows that the two sockets MUST share same local port number.

The current spec TS33.203 reads: ”The SIP level in P-CSCF records a SA_table, where each SA is identified by the triple, UE_IP_address, UE_protected_port, transport protocol.” Now that same UE_IP_address and UE_protected_port are used by both sockets, two SAs for each socket is clearly redundant. Similar, SPI number for inbound SA does not need to keep different either.

## 3. PROPOSAL

Analysis has been done from IPsec layer, transport layer and SIP application. The investigation shows a single SA one direction is sufficient to handle all SIP message regardless transport protocol. Therefore we propose the attached CR against TS 33.203 v5.2.0, by adopting an optimised solution for implementers.

## 4. REFERENCE

[IETF_SIP] J. Rosenberg et al., SIP. RFC 3261, IETF. June 2002.

(CR attached)

# CHANGE REQUEST

⌘ **33.203** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*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:*** | ⌘ | One SA for both TCP and UDP sockets | | | |
| ***Source:*** | ⌘ | Nokia | | | |
| ***Work item code:*** | ⌘ | IMS-ASEC | ***Date:*** | ⌘ | 11 July 2002 |
| ***Category:*** | ⌘ | **F** | ***Release:*** | ⌘ | Rel-5 |
| | | *Use one of the following categories:*<br>***F*** *(correction)*<br>***A*** *(corresponds to a correction in an earlier release)*<br>***B*** *(addition of feature),*<br>***C*** *(functional modification of feature)*<br>***D*** *(editorial modification)*<br>Detailed explanations of the above categories can be found in 3GPP TR 21.900. | | | *Use one of the following releases:*<br>*2 (GSM Phase 2)*<br>*R96 (Release 1996)*<br>*R97 (Release 1997)*<br>*R98 (Release 1998)*<br>*R99 (Release 1999)*<br>*Rel-4 (Release 4)*<br>*Rel-5 (Release 5)*<br>*Rel-6 (Release 6)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | The current specification requires two SAs to be established for UDP and TCP each in either direction. This design permits a SPI number modification attack investigated in Tdoc S3-020384. The design also introduces confliction with SIP behaviour defined in RFC3261. |
| ***Summary of change:*** | ⌘ | The new text specifies that two sockets share always the same SA for the same direction. |
| ***Consequences if not approved:*** | ⌘ | • The SPI number modification attack may be allowed,<br>• It can not achieve SIP requirement,<br>• It makes the SA management too complicated,<br>• The resource is half wasted in both UE and P-CSCF. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 7.1, 7.2 | | | | |
| | | **Y** | | | | |
| ***Other specs Affected:*** | ⌘ | **X** | | TS 24.228, 24.229 | ⌘ | |
| | | | | | | |
| | | | | | | |
| ***Other comments:*** | ⌘ | | | | | |

## 7.1 Security association parameters

******************************************omitted********************************************

3. 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 ~~may~~ shall use ~~different~~ a single protected port numbers for both TCP and UDP connections. The~~ numbers of~~ ~~these~~ port number ~~s~~ ~~are~~ is communicated to the P-CSCF during the security mode set-up procedure, cf. clause 7.2. 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.

~~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.~~

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

5. 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 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, lifetime) in an "SA_table".

NOTE 8: 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 of the protected REGISTER message. 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.

3. The SIP application at the P-CSCF shall check upon receipt of an initial REGISTER message that, ~~for each transport protocol,~~ the ~~triple~~ pair (UE_IP_address, UE_protected_port, ~~transport protocol~~), where the UE_IP_address is the source IP address in the packet header and the protected 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 and per transport protocol 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 9: According to clause 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 shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by the ~~triple~~ pair (UE_IP_address, UE_protected_port~~, transport protocol~~) 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_protected_port, ~~transport protocol,~~ SPI, lifetime) in an "SA_table".

NOTE 10: 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~~ a new pair~~s~~ of SAs (cf. clause 6.3) the SIP application at the UE shall ensure that~~, for each transport protocol,~~ the selected number for the protected port as well as SPI number do~~es~~ not correspond to an entry in the "SA_table".

NOTE 11: 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.

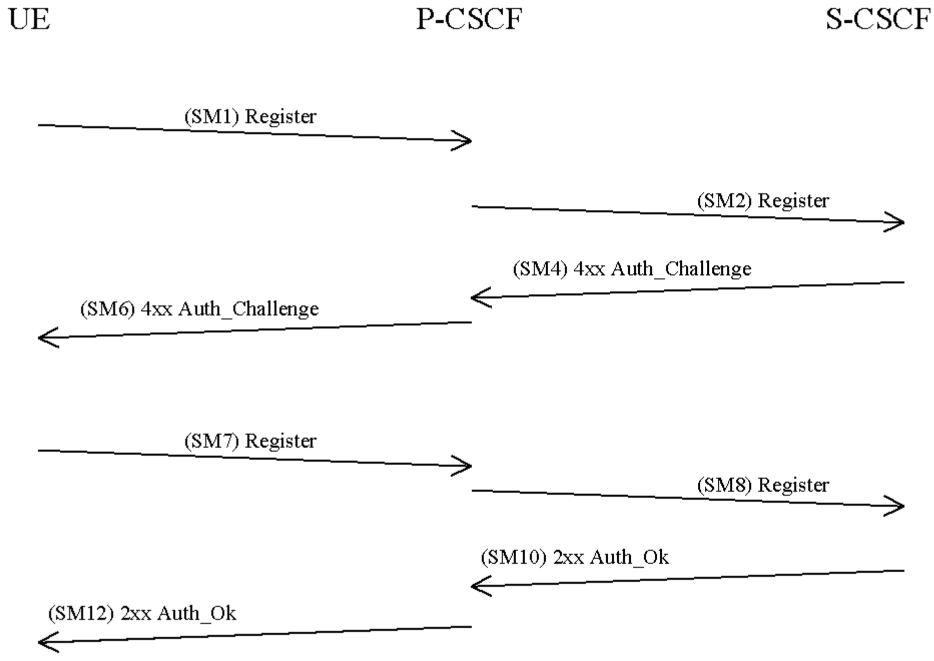
7. For each incoming protected message the SIP application at the UE shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by the ~~pair (~~UE_protected_port~~, transport protocol)~~ in the "SA table".

NOTE 12: 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 [draft-IETF-sip-sec-agree]. Annex H of this specification shows how to use [draft-IETF-sip-sec-agree] 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 SPI~~s~~ ~~and the~~ numbers and ~~of~~ the protected ports ~~assigned~~ selected by the UE ~~for the SAs for TCP and UDP~~. It also contains a list of identifiers for the integrity algorithms which the UE supports.

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

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 SPI~~s~~ for the inbound SA~~s for TCP and UDP~~.

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 the ~~two~~ another pair~~s~~ of SAs in the local security association database.

The *Security-setup*-line in SM6 contains the SPI~~s~~ 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 integrity algorithms which the P-CSCF supports.

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

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 the ~~two~~ another pair~~s~~ 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.