3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010098**

14 September, 2001

Sophia Antipolis, France

Source: **Siemens**

Title: **IPsec SA set-up procedures between UE and P-CSCF**

Document for: **Discussion and Decision**

Agenda Item:

1 Abstract

This contribution assumes that IPsec provides integrity protection and optional encryption between the UE and the P-CSCF to secure SIP signalling within the IMS.

After identifying the required SA parameters to be negotiated, a procedure is described how security mode set-up, as proposed in [S3-010326] and included in TS 33.203 v050, can be detailed to support the negotiation of IPsec SAs, instead of just negotiating the integrity protection mechanism and algorithms.

It is proposed to first read the companion contribution to the IMS ad hoc meeting, entitled "IPsec for Integrity protection between UE and P-CSCF", also by Siemens.

2 Required SA parameters

The standard mechanism to negotiate IPsec SAs, is IKE. The set of parameters that are negotiable for IPsec within a run of IKE, are given in the IP security domain of interpretation (RFC 2407). For an ESP SA, these are ESP transform identifiers, SA attributes and selectors like IP addresses and ports. In addition, an SPI (security parameters index) has to be exchanged to uniquely identify the SA.

To ensure basic interoperability, RFC 2407 lists the attributes SA life type/SA duration and Auth Algorithm to be supported by all implementations. The attribute SA life type specifies whether the SA duration is expressed in seconds or Kbytes.

In the context of the IMS, ESP SAs between the UE and the P-CSCF do not require a lifetime negotiation, since the maximum lifetime of a specific SA is already limited by the lifetime of the IMS registration. A new IPsec SA for an existing registration is generated by a new run of the IMS AKA in a re-registration with authentication. With a de-registration of a UE, it is required anyway that the according SAs are removed from the local SADBs.

Support for a life type negotiation is not required here, this can be assumed as always being seconds.

It is proposed to set the SA duration to the fixed length of 2^{32}-1 seconds, requiring four octets. This means that the lifetime of an SA will never expire before the IMS registration expires. Note that the IKE DoI specifies SA duration as being of variable length (RFC 2407, section 4.5). Therefore, implementations conforming with the standard are able to support this SA duration.

The length of encryption and authentication keys is 128 bits. Different keys are needed for incoming and outgoing traffic to avoid reflection attacks as the IP addresses are not protected by ESP and there is no direction bit. It is proposed to use the keys CK_{IM}, IK_{IM} as derived from the IMS AKA in one direction and a suitable modification of CK_{IM}, IK_{IM} in the other direction. An example of a suitable modification is a rotation of the key bits by n bits, where n remains to be determined.
It is true that reflection attacks would fail at the SIP level as the addresses in the SIP header would allow to detect that the message should have been sent in the other direction, but it was deemed better to block attacks as early as possible.

Therefore, the SA parameters, identifiers and attributes that shall be negotiable between UE and P-CSCF, are

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

Selectors:

The security associations have to be bound to specific 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.

At SA3#19, Ericsson showed in [S3-010347] that the following way can be used to bind the SAs to the SIP flows:

1. *We allow servers to use any port number for sending/receiving SIP packets. Typical OSes support such behaviour easily.*
2. *On the UE side, we require the SIP clients to use the same port for both sending and receiving. Typical OSes support such behaviour easily.*
3. *If there are multiple independent SIP clients in one UE – perhaps corresponding to several persons – they should use different ports of course.*

Since a requirement arises for a fixed port where the P-CSCF accepts certain messages in the clear (for a rationale, see 3.3.2), we propose to use this method with the following minor modification:

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.

Note: (This note applies no matter whether integrity is provided by IPsec or at SIP level.)
It needs further investigation, and perhaps LSs to the appropriate groups, to determine whether case 3 can actually occur. Case 3 would imply that several users, each with an ISIM, are active on one terminal at the same time. (This is a scenario which in the past has always been rejected by SA3.) It is further to be clarified whether several UAs can be active for the same user (with one ISIM). This is not a problem as long as the different UAs on one UE always are attached to the same P-CSCF (this needs to be confirmed) as then the same security association can be used. Otherwise, different security associations would be required which would be possible, but additional specification would be needed for the handling of these security associations in the ISIM and the UE.

3 Proposed mechanism for SA setup

The proposed registration message flow is based on the message flow given in [S3-010326] and now included in TS 33.20 v050 by Ericsson and Nokia.

3.1 Successful case

1) This first message is sent from the UE to the P-CSCF.

The user initially sends a SIP Register request to the P-CSCF (which will forward this), to start both the authentication and the security mode setup:

REGISTER sip:… SIP/2.0
Authorization: eap base64_eap_identity_response
Security-Setup: { esp | integrity algorithms list | [confidentiality algorithms list] |SPI }
…

For example, the UE proposes hmac_sha1 and hmac_md5 as possible integrity algorithms (and optionally a list of confidentiality algorithms). The SPI shall be chosen in such a way that it uniquely identifies the (unidirectional) inbound SA at the UE side, within the UE.

2) This second message is sent from the P-CSCF to the UE in the case that no errors occurred. For error cases see the subsections below.

The P-CSCF will process the Security Set-up part of the first request message received, choose an integrity algorithm and optionally a confidentiality algorithm, and come up with the following response:

SIP/2.0 401 Unauthorized
WWW-Authenticate: eap base64_eap_aka_challenge_request
Security-Setup: {esp | integrity algorithm | [confidentiality algorithm] | SPI | unprotected_port }
…

Here the network sends the selected integrity and confidentiality algorithm, e.g. hmac_sha1 and AES_CBC. The SPI shall be chosen in such a way that it uniquely identifies the (unidirectional) inbound SA at the P-CSCF side, within the P-CSCF. The *unprotected_port* specifies the port where the P-CSCF is willing to accept unprotected messages sent by the UE.

In the case of an unacceptable proposal set sent by the UE the P-CSCF sends a response indicating an error, as specified in 3.4.1.

3) This third message is sent from the UE to the P-CSCF in the case that no errors occurred. For error cases see the subsections below.

The third message should be already integrity-, and optionally confidentiality-, protected, since the UE is able to derive the integrity key IK_{IM}, and all other parameters necessary to set up the required IPsec SA.

If no error occurred up to this point, the terminal therefore starts integrity, and optionally confidentiality, protection and sends the second register message to the P-CSCF, protected under the new ESP SA:

ESP(
    REGISTER sip:… SIP/2.0
    Authorization: eap base64_eap_aka_challenge_response
    Security-Setup: *{ esp | integrity algorithms list | | [confidentiality algorithms list] | SPI}*
    …
)

To verify the Security-Setup parameters initially sent by the terminal, this message repeats the Security Set-up line, now protected under the ESP SA, so the consistency can be checked by the P-CSCF.

(Another option, as already described in [S3-010326], is to repeat these as part of the next message from the P-CSCF to the UE. But, it seems to be sensible to reduce the workload for the terminal, and to do this verification as early as possible.)

If the UE cannot authenticate the network side, it shall continue as specified in 3.3.2.

If the UE observes that the AUTN sent by the network contains an out-of-range sequence number, it shall continue as specified in 3.3.3

If the UE cannot accept an algorithm chosen by the P-CSCF, it shall continue as specified in 3.4.3.

4) After receiving the third message from the UE, the P-CSCF shall compare the Security-Setup line of this message with the Security Set-up line received in the first register message sent by the UE. These lines must be identical, otherwise any of the parameters could have been modified by an attacker.

In the successful case, a fourth message is sent from the P-CSCF to the UE. It does not contain anything related to the Security Set-up in the successful case.

```
ESP(
    SIP/2.0 200 OK
    WWW-Authenticate: eap base64_eap_aka_success
    …
)
```

If the P-CSCF cannot authenticate the UE after receiving message 3, it shall continue as specified in 3.3.1.

If the P-CSCF cannot verify the Security-Setup line after receiving message 3, it shall continue as specified in 3.4.3.

3.2 Error cases related to SIP registration

Whenever an expected message is not received after a time-out the receiving entity considers the registration to have failed.

Note 1: if the registration protocol goes well up to the last message (message 4 in section 3.1), and the last message is sent by the P-CSCF, but not received by the UE , then an inconsistent state results: the network side believes that the registration was successul whereas the UE considers it failed. This inconsistency could be resolved by the UE attempting another registration, as described in the SIP specification [sipbis04], section 14.3.1, but note that this may not be possible (e.g. due to loss of connectivity). It should be also noted that the occurence of this inconsistency has nothing to do with security.

However, in order to be able to specify how security should deal with this case the UE behaviour should be clarified.

Note 2: if unprotected REGISTER messages were not allowed then the UE could be permanently locked out if the UE lost state. In order to prevent that the possibility of a fresh start is necessary. This seems to mandate the use of a system-wide fixed port on the P-CSCF for specific unprotected messages.

3.3 Error cases related to IMS AKA

3.3.1 User authentication failure

In this case the authentication of the user fails in the network due an incorrect RES. The S-CSCF will send a 401 Unauthorized message, which will pass through the already established SA to the UE.

Note, that this failure will already occur in the third message, when the UE does not use the correct integrity key IK_{IM}. In this situation, the P-CSCF will receive IPsec protected packets that cannot be verified and therefore will be discarded.

In order to handle this situation, the P-CSCF shall implement a timer for the authentication process. When a message is received that passes the ESP integrity check and successfully completes the authentication, it is immediately processed. However, if during the registration timer the P-CSCF receives ESP 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.

(this behaviour has been proposed in [S3-010326])

3.3.2 Network authentication failure

If the UE is not able to successfully authenticate the network, the UE is not able to create the key IK_{IM} and therefore the ESP SA with the P-CSCF, such that it is not possible to send this REGISTER message in a protected way. Since the P-CSCF already expects SIP messages from the UE to be protected by an ESP SA, and is not already aware of any errors, the P-CSCF shall accept such REGISTER messages indicating network authentication failure on a different port, the unprotected port, in the clear.

So the UE sends a new register message, indicating a network authentication failure, to the P-CSCF, without protection. This register message should not contain the Security-Set-up line of the first message.

The P-CSCF shall only accept SIP messages indicating this error, and errors due to a synchronisation failure, on this specific port.

3.3.3 Synchronisation failure

In this situation, the UE observes that the AUTN sent by the network contains an out-of-range sequence number. It is still able to create the key IK_{IM}. Nevertheless, the UE behaviour shall be according to the network authentication failure case specified in 3.3.2.

So the UE sends a new register message to the P-CSCF error port in the clear, indicating the synchronisation failure. This register message should not contain the Security-Setup line of the first message, and the P-CSCF shall keep the Security-Setup state from the first register message received from the UE.

The P-CSCF shall only accept SIP messages indicating this error, and errors due to network authentication failure, on this specific port.

3.4 Error cases related to the Security-Setup

3.4.1 Unacceptable proposal set

In this case the P-CSCF cannot accept the proposal set sent by the UE in the Security-Set-up command. The second message shall respond to the first REGISTER message with indicating a failure, by sending a 403 Forbidden error message.

3.4.2 Unacceptable algorithm choice

If the P-CSCF sends in the second message's Security-Set-up line an algorithm that is not acceptable for the UE (i.e. has not been proposed), the UE shall not continue to create a security association with the P-CSCF and shall terminate the registration procedure.

3.4.3 Failed consistency check of Security-Set-up lines

This is the case if the Security-Setup line in the second register message from the UE to the P-CSCF cannot be verified, so the Security-Setup line of the first, unprotected register and the Security-Setup line of the second, protected register do not match. In this case the P-CSCF shall respond to the UE by sending a 403 Forbidden error message.

3.5 Authenticated re-registration

If the registration is a re-registration, a pair of security associations between UE and P-CSCF is already active. These SAs shall protect the first two messages of the authenticated re-registration, i.e. the first register message and the response. (Otherwise these messages would be rejected as the parties involved expect protected messages.)

Before the third message is sent by the UE, both peers shall replace the existing SA by the new SA negotiated during these first two messages.

Before we can proceed to specify how security associations are set up for ESP in particular we have to generally specify how SAs are handled in the case of re-registrations, independent of the particular mechanism for integrity and confidentiality protection.

The main problem originates from the fact that a failed re-registration cannot simply lead to the user's current registration being deleted. Because in the IMS the re-registration procedure is started by the user, an attacker could perform a Denial of Service attack by faking a re-registration attempt, and the ensuing failure would lead to the de-registration of the bona fide user. Therefore, for user-initiated re-registrations, the current registration, and the corresponding security associations, have to remain valid for a certain period, even if a re-registration attempt fails. The policy may be different for network-initiated re-registrations (see corresponding contribution by Siemens), but even in that case an operator may want to give a user another try before de-registering him. An additional difficulty, compared to the CS and PS domains of UMTS, arises from the fact that in the IMS registration, authentication and security association set-up are now all combined in one procedure.

3.5.1 Handling of security associations in authenticated re-registrations (successful case)

The following part of the description is independent of the particular mechanism for integrity and confidentiality protection.

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 message 1 (REGISTER) 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.

2) The P-CSCF waits for the response from the S-CSCF and then sends message 2 to the UE, using SA2. As in the case of a new registration, the parameters selected for the new security association 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 message 2 could be successfully processed by the UE, the UE also creates the new SAs SA11 and SA12 in its database. The UE then sends the third message (REGISTER) 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. The third message is protected with the new SA11.

4) The P-CSCF waits for the response from the S-CSCF and then sends the OK to the UE, using the new SA 12.

5) After the reception of the fourth message 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. The reason for this behaviour becomes clear from the failure cases.

Aspects specific to the use of IPsec/ESP:

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 first REGISTER message in the list of parameters to be negotiated in a security association set-up. (If it is desired to use identical messages for new registrations and re-registrations then a new port can also be included in the first message for new registrations although it is not strictly needed there.)

The reason for using a new port for the new SAs is that in this way the SIP application can control which security associations, old or new, are used, as ports are visible to the application.

3.5.2 Error cases related to SIP 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. (see Note 1 in section 3.2 as well).

If the registration protocol goes well up to the last message (message 4 in section 3.5.1), and the last message 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.

3.5.3 Error cases related to IMS AKA

3.5.3.1 User authentication failure

The S-CSCF will send a 401 Unauthorized message, which will pass through the already established SA to the UE. Afterwards, both, the UE and the P-CSCF delete the new SAs.

3.5.3.2 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 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.

3.5.3.3 Synchronisation failure

If the UE notices a synchronisation failure it does not establish a new SA. The UE sends a message, indicating the synchronisation failure, to the P-CSCF, using the already established SA. The P-CSCF deletes the new SA after receiving this message.

3.5.4 Error cases related to the Security-Setup

3.5.4.1 Unacceptable proposal set

The second message shall respond to the first REGISTER message with a 403 Forbidden error message, using the already established SA. Neither side establishes a new SA.

3.5.4.2 Failed consistency check of Security-Set-up lines

This is the case if the Security-Setup line in the second register message from the UE to the P-CSCF cannot be verified, so the Security-Setup line of the first, unprotected register and the Security-Setup line of the second, protected register do not match. In this case the P-CSCF shall respond to the UE by sending a 403 Forbidden error message using the already established SA. Both sides delete the new SAs.

4 References:

[S3-010326] 3GPP TSG SA WG3 Security: "Security mode setup for the IMS registration", Ericsson, Nokia, and Nortel, SA3#19, July 4-6, 2001.

[S3-010347] 3GPP TSG SA WG3 Security: "Integrity protection for SIP signalling", Ericsson, SA3#19, July 4-6, 2001.

[S3-xxxxxx] TS 33.203 v050

[sipbis04] Handley M, Schulzrinne H, Schooler E, Rosenberg J., "SIP, Session Initiation Protocol", draft-ietf-sip-rfc2543bis-04.txt, Work in Progress.