The IMS: IP Multimedia Concepts And Services, Second Edition

PREV
Authentication

NEXT
SIP Security Mechanism Agreement

10.7. ACCESS SECURITY – IPSEC SAS

10.7.1. Overview

Section 3.8.4 describes how access security works in principle. Security via the Gm interface is achieved by means of IPsec SAs, which require specific handling at the SIP signalling level. This section describes how the UE and P-CSCF negotiate the security mechanism, how IPsec-related parameters are exchanged and how SAs are established and handled.

As the establishment of IPsec SAs is based on authentication of the user, new SAs are established during every re-authentication process. Consequently, new pairs of IPsec SAs have to be established between the UE and the P-CSCF.

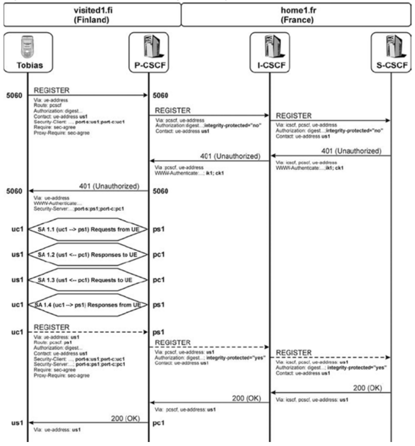
10.7.2. Establishing an SA during initial registration

The initial REGISTER request as well as the 401 (Unauthorized) response are sent between the UE and the P-CSCF without any kind of protection. These two messages transport information that allows the UE and the P-CSCF to negotiate the security mechanism and to agree on the parameters and ports that will be used for the SAs.

During the registration process two pairs of IPsec SAs are established between the UE and the P-CSCF. Unless otherwise stated, such a set of two pairs of SAs is referred to as a "set of SAs", while a single or specific IPsec SA from these four is referred to as an "SA".

The four IPsec SAs are not static connections (e.g., TCP connections). They can be regarded as logical associations between the UE and the P-CSCF that allow the secure exchange of SIP messages.

Figure 10.5. SA establishment during initial registration.


visited1.fi (Finland)
home1.fr (France)
Tobias
P-CSCF
I-CSCF
S-CSCF
5060
REGISTER
Via: ue-address
Route: pcscf
Authorization: digest...
Contact: ue-address us1
Security-Client: ..., port-s:us1;port-c:uc1
Require: sec-agree
Proxy-Require: sec-agree
5060
REGISTER
Via: pcscf, ue-address
Authorization:digest...;integrity-protected="no"
Contact: ue-address us1
REGISTER
Via: icscf, pcscf, ue-address
Authorization: digest...;integrity-protected="no"
Contact: ue-address us1
401 (Unauthorized)
Via: icscf, pcscf, ue-address
WWW-Authentcate:...;ik1; ck1
401 (Unauthorized)
Via :pcscf, ue-address
WWW-Authenticate:...; ik1; ck1
5060
401 (Unauthorized)
5060
Via: ue-address
WWW-Authenticate:...
Security-Server:...;port-s:ps1;port-c:pc1
uc1
SA 1.1 (uc1 --> ps1) Requests from UE
ps1
us1
SA 1.2 (us1 <-- pc1) Responses to UE
pc1
us1
SA 1.3 (us1 <-- pc1) Requests to UE
pc1
uc1
SA 1.4 (uc1 --> ps1) Responses from UE
ps1
uc1
REGISTER
ps1
Via: ue-address: us1
Route: pcscf: ps1
Authorization: digest...
Contact: ue-address us1
Security-Client: ..., port-s:us1;port-c:uc1
Security-Server:...; port-s:ps1;port-c:pc1
Require: sec-agree
Proxy-Require: sec-agree
REGISTER
Via: pcscf, ue-address: us1
Authorization: digest...; integrity-protected="yes"
Contact: ue-address us1
REGISTER
Via: icscf, pcscf, ue-address: us1
Authorization: digest...; integrity-protected="yes"
Contact: ue-address us1
200 (OK)
Via: icscf, pcscf, ue-address: us1
200 (OK)
Via: pcscf, ue-address: us1
us1
200 (OK)
pc1
Via: ue-address: us1

A set of SAs facilitates four ports:

- the protected client port at the UE (uc1);
- the protected server port at the UE (us1);

These ports are negotiated between the UE and the P-CSCF during initial registration (Figure 10.5) by using the Security-Client, Security-Server and Security-Verify headers of the SIP Security Mechanism Agreement (see Section 10.8).

The set of SAs needs to be established with a shared key. Unfortunately, the P-CSCF knows nothing about the security parameters that are shared between Tobias's ISIM application and the HSS in the home network. Therefore, the S-CSCF sends the IK and the CK to the P-CSCF within the WWW-Authenticate header in the 401 (Unauthorized) response. The P-CSCF must remove these two keys from the header and store them locally before sending the 401 (Unauthorized) response toward the UE. The IK is then used by the P-CSCF as the shared key for the set of SAs. The UE at the other end of the Gm interface calculates the IK from the received challenge in the 401 (Unauthorized) response and also uses it as the shared key (see Section 10.6.6).

By means of the IK, the P-CSCF and the UE can then establish the set of SAs between the four ports that were exchanged beforehand in the initial REGISTER request and its response:

- between uc1 and ps1 for sending SIP requests from the UE to the P-CSCF;
- between us1 and pc1 for sending SIP responses from the P-CSCF to the UE;
- between us1 and pc1 for sending SIP requests from the P-CSCF to the UE; and
- between uc1 and ps1 for sending SIP responses from the UE to the P-CSCF.

After their establishment the set of SAs gets assigned a temporary lifetime. Although the UE will send all subsequent requests and responses via this temporary set of SAs, the set of SAs cannot be taken into use until the authentication procedure between the UE and the S-CSCF has been finished. This is done in order to ensure that the security mechanism between the UE and the P-CSCF is based on successful authentication of the user.

When sending the 200 (OK) response to the UE, the P-CSCF will update the lifetime of the set of SAs by giving it the lifetime of the registration (as indicated in the expires value of the Contact header) plus 30 seconds. The UE will do the same after receiving the 200 (OK) response.

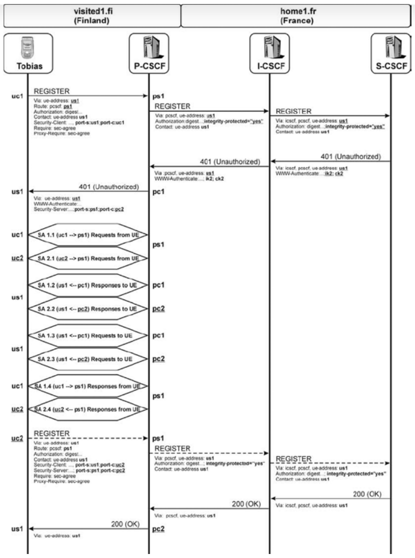
In the case of initial registration (as described here), both ends (i.e., P-CSCF and UE) will immediately afterwards take this set of SAs into use. This means that the P-CSCF will send all SIP messages that are directed toward the UE via the established set of SAs. The UE will in the same way send all SIP messages via the established set of SAs.

10.7.3. Handling of multiple sets of SAs in case of re-authentication

We have now seen how the first set of SAs is established during initial registration. As the establishment of a set of SAs is based on the authentication data that are sent from the S-CSCF in the 401 (Unauthorized) response, every re-authentication will generate a new set of SAs between the UE and the P-CSCF. Re-authentication procedures are described in Section 10.13. After successful re-authentication the UE and the P-CSCF will maintain two sets of SAs (Figure 10.6):

- the set of SAs that was already established and taken into use before the re-registration took place, which is now called the "old set of SAs"; and
- a new set of SAs that was established based on re-authentication, which is now called the "new set of SAs".

Figure 10.6. Two sets of SAs during re-authentication.


visited1.fi
(Finland)
home1.fr
(France)
Tobias
P-CSCF
I-CSCF
S-CSCF
uc1
REGISTER
Via: ue-address: us1
Route: pcscf: ps1
Authorization: digest...
Contact: ue-address us1
Security-Client: ..., port-s:us1;port-c:uc1
Require: sec-agree
Proxy-Require: sec-agree
ps1
REGISTER
Via: pcscf, ue-address: us1
Authorization:digest...;integrity-protected="yes"
Contact: ue-address us1
REGISTER
Via: icscf, pcscf, ue-address: us1
Authorization: digest...;integrity-protected="yes"
Contact: ue-address us1
401 (Unauthorized)
Via: icscf, pcscf, ue-address: us1
WWW-Authenticate:...:ik2; ck2
401 (Unauthorized)
Via :pcscf, ue-address: us1
WWW-Authenticate:...; ik2; ck2
us1
401 (Unauthorized)
pc1
Via: ue-address: us1
WWW-Authenticate:...
Security-Server:....;port-s:ps1;port-c:pc2
uc1
SA 1.1 (uc1 --> ps1) Requests from UE
ps1
uc2
SA 2.1 (uc2 --> ps1) Requests from UE
SA 1.2 (us1 <-- pc1) Responses to UE
pc1
us1
SA 2.2 (us1 <-- pc2) Responses to UE
pc2
SA 1.3 (us1 <-- pc1) Requests to UE
pc1
us1
SA 2.3 (us1 <-- pc2) Requests to UE
pc2
uc1
SA 1.4 (uc1 --> ps1) Responses from UE
ps1
uc2
SA 2.4 (uc2 <-- ps1) Responses from UE
uc2
REGISTER
ps1
Via: ue-address: us1
Route: pcscf: ps1
Authorization: digest...
Contact: ue-address us1
Security-Client: ..., port-s:us1;port-c:uc2
Security-Server:...; port-s:ps1;port-c:pc2
Require: sec-agree
Proxy-Require: sec-agree
REGISTER
Via: pcscf, ue-address: us1
Authorization: digest...; integrity-protected="yes"
Contact: ue-address us1
REGISTER
Via: icscf, pcscf, ue-address: us1
Authorization: digest...; integrity-protected="yes"
Contact: ue-address us1
200 (OK)
Via: icscf, pcscf, ue-address: us1
200 (OK)
Via: pcscf, ue-address: us1
us1
200 (OK)
pc2
Via: ue-address: us1

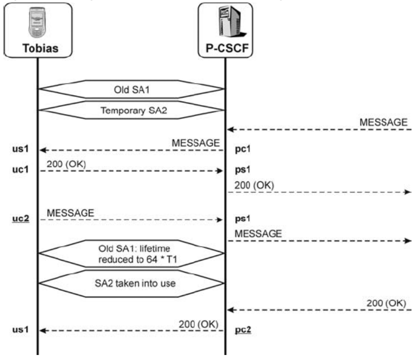
The major complication in this situation is that the P-CSCF cannot be sure whether the 200 (OK) response for the second REGISTER request has been received by Tobias's UE, as SIP defines no acknowledgement mechanism for received responses for any request other than an INVITE. If the UE has not received the 200 (OK) response for the second REGISTER, then it will not take the new set of SAs into use. Therefore, it has to wait until the UE sends a new request on the new set of SAs before it can take them into use. This means that, as long as the P-CSCF does not receive a request from the UE on the new set of SAs, it will:

- send incoming requests to the UE over the old set of SAs (i.e., from its protected client port pc1 to the UE's protected server port us1); and
- keep both sets of SAs active until one or both of them either expires or a new request from the UE is received.

In our example we assume that the UE has received the 200 (OK) for the second REGISTER request and, therefore, is aware that the authentication procedure was successful and the new set of SAs can be used. Unfortunately, the P-CSCF does not know this and will send incoming requests to the UE over the old set of SAs; therefore, the UE also needs to maintain both sets of SAs.

When the UE needs to send out a new request, it will send it by means of the new set of SAs, which will confirm to the P-CSCF that the new set of SAs can be taken into full use (Figure 10.7). Furthermore, at this moment the old set of SAs will not be immediately dropped, as the UE might have received or sent a request over it, which the remote end has not yet responded to. Therefore, the old set of SAs is kept for another 64 * T_1 seconds (usually 128 seconds in an IMS environment), before it is dropped.

Figure 10.7. Taking a new set of SAs into use and dropping an old set of SAs.



Note also that the UE cannot take the new set of SAs into use by sending a response – e.g., a 200 (OK) response – for a request – e.g., a MESSAGE response to the same port and over the same set of SAs as the request was received.

Whenever a set of temporary SAs is established the UE will drop all other SAs, other than the one over which it sent the last REGISTER request. Consequently, the UE never needs to handle more than two sets of SAs at the same time.

10.7.4. SA lifetime

During an ongoing authentication procedure the lifetime of a temporary set of SAs is restricted to 4 minutes. This guarantees that the authentication procedure can be finished. After successful authentication the lifetime of the new set of SAs is set to:

- Either the expiration time of the concluded registration plus 30 seconds. The expiration time of the registration is indicated in the expires parameter that is returned in the Contact header of the 200 (OK) response to the REGISTER.
- Or, if another set of SAs does already exist, to the lifetime of that already-existing set of SAs as long as its lifetime is longer than the expiration time of the just-concluded registration plus 30 seconds.

Whenever a re-registration takes place and is successful the P-CSCF and the UE have to update the lifetime of all existing SAs with the expiration time of the concluded re-registration plus 30 seconds, if that value is bigger than the already-assigned lifetime of the SAs.

Consequently, the SAs between the UE and the P-CSCF will be kept 30 seconds longer than Tobias is registered to the IMS network.

When the P-CSCF becomes aware that Tobias is no longer registered (e.g., by receiving a NOTIFY with Tobias's registration-state information which indicates network-initiated de-registration – see Section 10.14.3), the P-CSCF will drop all SAs toward the UE after 64 * T_1 seconds.

10.7.5. Port setting and routing

Special attention has to be paid when it comes to the usage of SA ports, as they heavily influence the routing between the P-CSCF and the UE. As shown in Figure 10.6, Tobias's UE:

- will send all requests from its protected client port (2468);
- expects all responses to be received on its protected server port (1357);
- expects all requests to be received at its protected server port (1357);
- will send all responses to received requests from its protected client port (2468).

The P-CSCF, on the other hand:

- will send all requests toward the UE from its protected client port (8642);
- expects to receive all responses from the UE at its protected server port (7531);
- expects to receive all requests from the UE at its protected server port (7531); and
- will send all responses toward the UE from its protected client port (8642).

To ensure that all requests are sent via IPsec SAs:

- The UE will set its protected server port as part of its address:
  - in the Contact header of every request (including all REGISTER requests);
  - in the Via header of every request, besides the initial REGISTER.
- The UE will set the protected server port of the P-CSCF as part of the outbound proxy (i.e., P-CSCF) address in the Route header of every initial request that it sends.
- The P-CSCF will set its protected server port as part of its address:
  - in the Record-Route header of every initial request that is sent toward the UE;

ting of port numbers in the Record-Route header see Section 11.3).

10.7.5.1. Port setting during registration

For example, Tobias's UE initially registers with the following information:

```
REGISTER sip:home1.fr SIP/2.0
Via: sip:[5555:1:2:3:4];branch=0uetb
Route: <sip:[5555::a:b:c:d];lr>
Security-Client: digest, IPsec-3gpp; alg=hmac-sha-1-96
                 ;spi-c=23456789 ;spi-s=12345678
                 ;port-c=2468; port-s=1357
Contact: sip:[5555::1:2:3:4]:1357
```

This means that the UE:

- Is going to establish IPsec SA with:
  - port 2468 as the protected client port (port-c parameter of the Security-Client header);
  - port 1357 as the protected server port (port-s parameter of the Security-Client header).
- Expects all incoming requests to be routed to its protected server port (port value in the Contact header).
- Will send this initial REGISTER request to the unprotected port 5060 of the P-CSCF, as no port value is given in the Route header.
- Will await all responses to this initial REGISTER request on unprotected port 5060, as no port value is given in the Via header.

The 401 (Unauthorized) response that is received afterwards by the UE will look like this:

```
SIP/2.0 401 Unauthorized
Via: sip:[5555:1:2:3:4];branch=0uetb
Security-Server: tls ;q=0.2, IPsec-3gpp; q=0.1
                 ;alg=hmac-sha-1-96
                 ;spi-c=98765432 ;spi-s=87654321
                 ;port-c=8642 ;port-s=7531
```

This means that the P-CSCF is going to establish an IPsec SA with:

- port 8642 as the protected client port (port-c parameter of the Security-Server header); and
- port 7531 as the protected server port (port-s parameter of the Security-Server header).

After this exchange the UE and the P-CSCF will set up the temporary set of SAs and the UE will then send the second REGISTER request already protected, which then will look like:

```
REGISTER sip:home1.fr SIP/2.0
Via: sip:[5555:1:2:3:4]:1357;branch=1uetb
Route: <sip:[5555::a:b:c:d]:7531;lr>
Contact: sip:[5555::1:2:3:4]:1357
```

Note that the Security-Client and Security-Verify headers are also included in this request (see Section 10.8), but, as they no longer have any influence on SA establishment and routing, they are not shown here. This means that the UE:

- expects all incoming initial requests to be routed to its protected server port (port value in the Contact header);
- sends this REGISTER request already over the temporary IPsec SA (i.e., to the protected server port of the P-CSCF – port value in the Route header); and
- expects all responses to this REGISTER request to be sent via the temporary IPsec SA (i.e., on its protected server port 1357 – port value in the Via header).

10.7.5.2. Port setting during re-authentication

As said before, every re-authentication will result in a new pair of IPsec SAs. When exchanging the security parameter indexes and protected port numbers for the new set of SAs according to the SIP Security Mechanism Agreement, the P-CSCF and the UE only change their protected client

- the UE receives requests and responses for both sets of SAs via its protected server port (us1);
- the P-CSCF receives requests and responses for both sets of SAs via its protected server port (ps1);
- the UE uses a new protected client port (uc2) for sending requests and responses toward the P-CSCF over the new set of SAs; and
- the P-CSCF also uses a new protected client port (pc2) for sending requests and responses toward the UE over the new set of SAs.

This is due to the fact that two sets of SAs must not use the same port parameters. Furthermore, if the protected server ports change, this would cause major problems and would mean that:

- the UE would need to perform re-registration, as its registered contact includes the protected server port;
- the UE would need to send re-INVITE on all established sessions, as its contact information that was sent to the remote end includes the protected server port;
- the P-CSCF would receive from the UE all subsequent requests to every already-established dialog (including all subscriptions of the UE) on the P-CSCF's old, protected server port, as there is no possibility in SIP to change the route information for an already-established dialog.

This list is not complete, but it shows that changing the protected server port would cause a lot of problems for SIP routing. Therefore, it is essential that this value is not changed as long as the user stays registered.

10.7.5.3. Port settings for SIP requests other than REGISTER

The setting of the protected ports in non-REGISTER requests is described in more detail in Section 11.3.

10.7.5.4. Usage of ports with UDP and TCP

The previous sections showed how requests and responses are routed via one or more sets of SAs. In the chosen example, only UDP was used as a transport protocol. For TCP, however, there is a slight difference in these procedures.

When a request is sent out via UDP (Figure 10.8) the Via header indicates the IP address and port number to which all related responses should be routed. When TCP is used to send the request (Figure 10.9) the information in the Via header is overridden and the response is routed back to the same address and port that the request was received from. This draws attention to the nature of TCP as a connection-oriented transport protocol. By applying this rule it is ensured that no additional TCP connection needs to be opened to send the response to a request that was received via TCP. This causes the routing of SIP messages between the P-CSCF and the UE to behave differently. The UE will set its protected server port (us1) in the Via header of every request that it sends out, regardless of whether UDP or TCP is used. All requests will originate from the UE's protected client port (uc1).

Figure 10.8. Request and response routing between UE and P-CSCF over UDP.

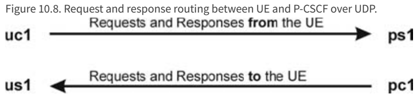
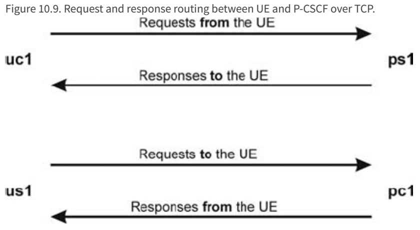

uc1
Requests and Responses from the UE
ps1
us1
Requests and Responses to the UE
pc1

Figure 10.9. Request and response routing between UE and P-CSCF over TCP.



In the case of UDP the responses to such a request will be sent to the UE's protected server port (us1), as indicated in the Via header.

In the case of TCP the responses to such a request will be sent to the UE's protected client port (uc1), as the request originated from there. The same is true in the other direction (i.e., for requests sent from the P-CSCF toward the UE and their responses).

3GPP TS 33.102	Security architecture.
3GPP TS 33.203	Access security for IP-based services.
3GPP TS 33.210	Network Domain Security (NDS); IP network layer security.
RFC2401	Security Architecture for the Internet Protocol.
RFC2403	The Use of HMAC-MD5-96 within ESP and AH.
RFC2404	The Use of HMAC-SHA-1-96 within ESP and AH.
RFC2451	The ESP CBC-Mode Cipher Algorithms.

Resource Centers / Playlists / History / Topics / Settings / Get the App / Sign Out

PREV
Authentication

NEXT
SIP Security Mechanism Agreement