3GPP TSG SA WG3 Security — SA3#35 **S3-040721**

October 5-8, 2004, St Paul's Bay, Malta

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.203** **CR** **073** ⌘ **rev** **-** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	**Support of IMS end user devices behind a NA(P)T firewall, and protection of RTP media flows**
Source:	⌘	BT Group plc
Work item code:	⌘	IMS-ASEC
Date:	⌘	24/09/2004
Category:	⌘	**C**
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:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change:	⌘	**Support of IMS end user devices behind a NA(P)T firewall, and protection of RTP media flows**
Summary of change:	⌘	Modifications to implementation of IPsec and SIP on P-CSCF and UE, in order to support detection and traversal of an intervening NAT or PAT, and encapsulation of user data in the same IPsec access tunnel
Consequences if not approved:	⌘	(1) IMS applications behind NAT or PAT firewall will not be supported, and user data will not be protected over access links more vulnerable than GPRS. (2) In its absence, other standards bodies may devise alternative mechanisms, incompatible with TS33.203

Clauses affected:	⌘	New Informative Annex

Other specs affected: ⌘	Y	N	
		X	Other core specifications ⌘
		X	Test specifications
		X	O&M Specifications

Other comments:	⌘	Does not preclude future changes to support Application Layer Gateways on intervening devices

********** BEGIN OF CHANGE**********

Annex K (informative): Support of IMS end user devices behind a NA(P)T firewall, and protection of RTP media flows

When the decision was taken by SA3 to base IMS security on IPSec, it was acknowledged that the solution would not support a UE behind a NAT or PAT firewall router. This is not an issue with the present IMS architecture in 3GPP, but may impose restrictions, as the 3GPP network and service develops. It also presents difficulties with reusing the 3GPP IMS security specification in other contexts, such as WLAN and ADSL access networks, which are likely to incorporate NAT between the end-user device and the SIP server.

This Annex shows how, by making relatively small changes in the way IPsec and SIP protocols are implemented on the SIP Server and UE, it becomes possible to both support NAT/ PAT traversal, and user data encapsulation in the same secure access tunnel.

K1 Network Setup and Components

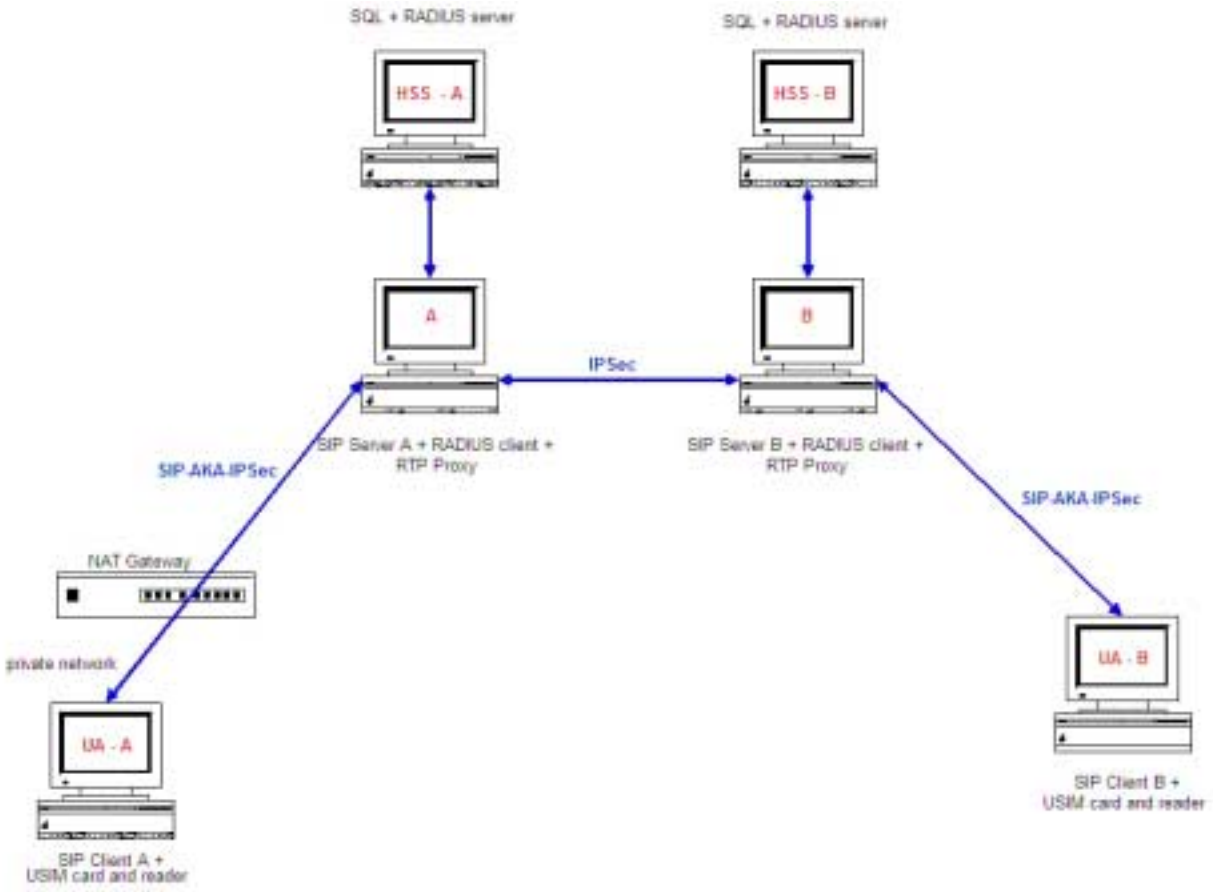

Figure 1 Logical representation of the secure SIP network set-up

For the purposes of this discussion, it is easier to think of the set-up in terms of IPsec endpoints, as in Figure 1.

In practice, the interfaces on all the machines have routable IP addresses on a subnet of the local LAN, with the exception of the machine behind the NAT gateway, which has an RFC 1918 private address. The NAT gateway could be any standard commercial offering, which supports DHCP private addressing, NAT and routing.

To support end user devices behind a NAT firewall and protection of RTP media flows, however, the software components on each node have to be implemented in a specific way. It must be stressed that this does *not* imply normative changes to the underlying standard. These implementation considerations are now described for each node in the logical representation of Figure 1.

- **SIP Server A:** SIP Server in Network A, The following components need to be installed on this node:

1. SIP Proxy
2. Software support for SIP-AKA authentication
3. Radius client, which has, support for AKA and can communicate with the HSS
4. An IPSec client with the necessary hooks to build an IPSec security association, once the SIP client has been successfully authenticated.
   *Note that it may be necessary to extend the proxy to allow the building and updating of an IPSec SA. Many do not have built-in support for IPsec.
   **Also note that it may be necessary to extend the IPsec client, to support UDP encapsulation for clients behind NAT. UDP encapsulation is normally linked to Internet Key Exchange (IKE, the usual mechanism for key management in IPsec). IKE is not used in 3GPP IMS security, so UDP encapsulation must be implemented within AKA instead.
   ***TS33.203 mandates the use of transport mode IPsec. While this will work with UDP encapsulation for NAT traversal, it is recommended that tunnel mode IPsec, with DHCP or similar mechanism for assignment of inner IP address, be used in broadband access environments. This is to avoid conflicts, when NAT routers assign addresses from the same range, e.g. 192.168.0.0
   ****While using tunnel mode IPSec and UDP encapsulation for clients behind NAT, the SIP server needs to see the internal address of the tunnel. Hence once the IPSec SA is established, any NAT traversal support on the SIP server needs to be turned off. Only the initial *unencrypted* registration (SIP-AKA) messages require the NAT traversal support. The SIP server may need to be extended to support this requirement.
5. Support for proxying the RTP media traffic.
6. Support for long-standing IPSec security associations with other SIP related network entities like the HSS and other SIP servers. How these network, as opposed to access level, IPSec SAs are built is assumed to be covered by 3GPP Network Domain security, and are not considered further in this paper.

- **SIP Server B:** This machine is an exact replica of SIP Server A, the only difference being that it represents a different operator or SIP domain

- **HSS A and HSS B:** This server stores the subscriber information, including the master secret that the RADIUS server will use to generate the AKA quintuplets. No changes are required to support the additional features of NAT traversal and access link protection. However, the Generic Authentication Architecture (GAA) concept, and the BootStrapping Function (BSF) within it, could be used to provide *separate* secure IPsec access tunnels for SIP messaging and RTP media flows, for each host requiring SIP services, This would require the implementation of the Zn interface to the BSF, rather than a direct connection to the HSS.

- **SIP Client A:** This machine sits behind a NAT gateway, and requires a SIP Client with support for SIP-AKA authentication and an IPSec client with support for UDP encapsulation, and with the necessary hooks to build an IPSec SA once the SIP Client has been successfully authenticated. It may be necessary to extend the SIP

client to allow the building and updating an IPSec SA,if IPsec client functionality is not built-in. The following protocol will also need to be implemented:

1. When the access link IPSec SAs have been successfully set up at both ends, SIP Client A shall send at least one packet (ICMP ping for example) to the SIP server. This will create a pinhole on the NAT gateway, which will allow UDP encapsulated IPSec traffic, coming from the SIP Server, to pass through the NAT gateway. In the absence of a NAT pinhole, any incoming packets would be dropped by the gateway (unknown destination).

2. Once the pinhole is created, it may be kept alive by periodic keep-alive messages (either a SIP layer message, or an ICMP packet) sent either by SIP Server A, or by SIP Client A.

3. Note that since IPSec UDP encapsulation is used for NAT traversal, once the IPSec SA is established, any SIP/RTP layer support for NAT traversal is no longer required. Consequently, symmetric RTP support, for example, is no longer required (use of the same port number for sending and receiving the RTP traffic). Symmetric RTP is a proposed NAT traversal solution for media traffic, in the absence of any NAT traversal support from the lower layers.

- **SIP Client B:** This machine is an exact replica of SIP Client A, but is identified by a different SIP URL, and has a routable IP address. Thus NAT traversal support is unnecessary. SIP Server B is the registration server for client B.

No changes were required to the UICC and USIM application, or to the IMS application itself. (Any SIP-based application would suffice.)

K2 Operation without NAT

Figure 2 describes how SIP-AKA works between SIP Client B and SIP Server B, when there is no NAT gateway between the two.

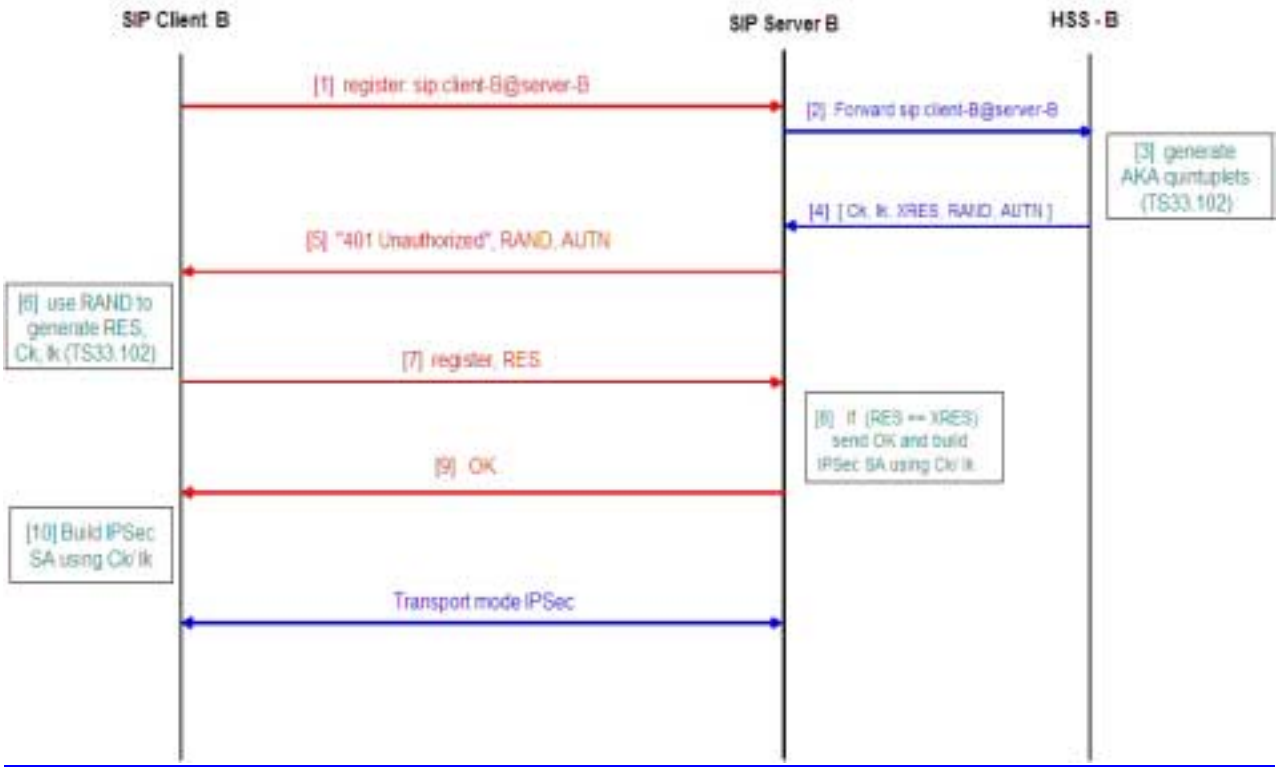

Figure 2 SIP-AKA without NAT

Step-by-step explanation:

1. SIP Client B sends a SIP REGISTER message to SIP Server B.
2. SIP Client B hasn't been authenticated. Therefore SIP Server B forwards the SIP Client B SIP URL to HSS B, via RADIUS.
3. HSS B uses the SIP URL to locate the user in its database, and to generate the necessary AKA quintuplets.
4. HSS B returns {CK, IK, XRES, RAND, AUTN} quintuplet to SIP Server B.
5. SIP Server B sends a "401 Unauthorized" SIP message to SIP Client B, along with RAND and AUTN which it received from HSS B.
6. The UMTS SIM card on UA B uses RAND to generate CK, IK and RES.
7. SIP Client B resends the SIP REGISTER message, along with RES to SIP Server B.
8. SIP Server B compares if RES is equal to XRES.
9. If they are equal, SIP Server B sends an OK message to SIP Client B and builds the required IPSec SA, using CK/IK keying material.
10. SIP Client B, on receiving the OK message, builds the corresponding IPSec SA in the reverse direction, using the same CK/IK keying material.

When the registration period expires, the user agent *must* re-register. So the same process as shown in Figure 2 is repeated, but this time all the SIP registration traffic goes encrypted. A successful re-registration results in both ends updating the IPSec Security Associations. When the SIP Client de-registers, IPSec Security Associations are deleted at both the client and the server ends.

K3 Operation with NAT

Figure 3 describes how SIP-AKA works between SIP Client A and SIP Server A, when there is a NAT Gateway between the two.

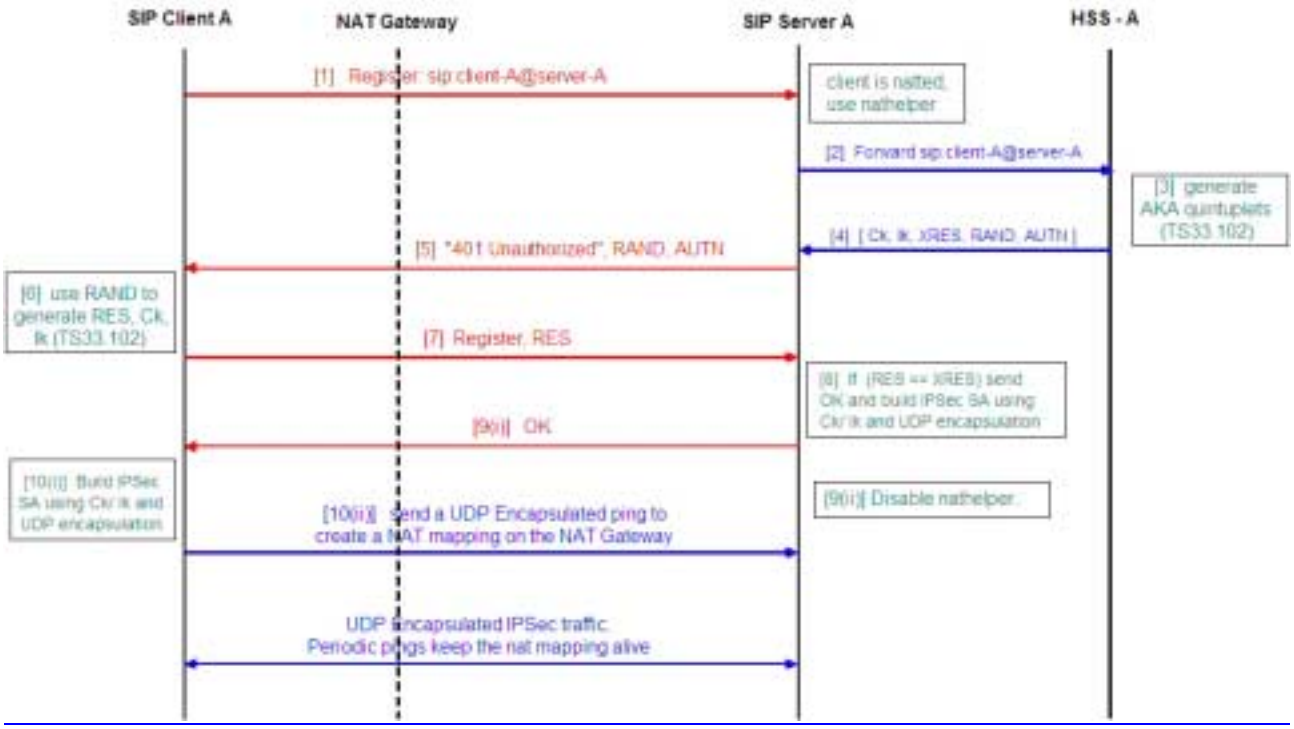

Figure 3 SIP-AKA with NAT

Step-by-step explanation:

1. SIP Client A sends a SIP REGISTER message to SIP Server A

2. SIP Server A sees a request coming in from a client behind a NAT (IP address in header and SIP contents do not coincide), and so turns on the NAT detection and traversal functionality for this client, for example nathelper within Linux. As the client has not been authenticated, SIP Server A again forwards the SIP Client A SIP URL to HSS A, for example using the RADIUS protocol.

3. HSS A uses the SIP URL to locate the user in its database, and to generate the necessary AKA quintuplets.

4. HSS A returns {CK, IK, XRES, RAND, AUTN} to SIP Server A.

5. SIP Server A sends a “401 Unauthorized” SIP message to UA A, along with RAND and AUTN which it received from HSS A.

6. The UMTS SIM card on SIP Client A uses RAND to generate CK, IK and RES.

7. SIP Client A resends the SIP REGISTER message along with RES to SIP Server A.

8. SIP Server A compares RES to XRES (the expected response).

9. (i) If they are equal, SIP Server A sends an OK message to SIP Client A, and builds the required IPSec SA, using CK/IK keying material. An important distinction is that UDP encapsulation for NAT traversal is now turned on.
   (ii) SIP Server A switches off NAT traversal for SIP Client A.

10. (i) SIP Client A on receiving the OK message, builds the IPSec SA, using the same CK/IK keying material.
    (ii) SIP Client A sends a UDP-encapsulated ICMP ping to SIP Server A. This will create a pinhole in the NAT gateway, which will allow any incoming packets to get through the NAT. A keep-alive message sent periodically by SIP Client A keeps the NAT mapping alive. Note that the keep-alive message can come from either end. In this implementation the client is the sender.

When the registration period expires, the SIP Client must re-register. So the same process as shown in **Figure 3** is repeated, but this time all the SIP registration traffic is encrypted. A successful re-registration results in the both ends updating their respective IPSec security associations. When the SIP Client de-registers, the IPSec security association is deleted at both the client and the server ends.

Annex L (informative): Change history

********** END OF CHANGE**********