Avaya Solution & Interoperability Test Lab

Configuring AudioCodes Mediant 3000 Media Gateway 3.0 to use Transport Layer Security (TLS) with Third Party Certificates and Secure Real-time Transport Protocol (SRTP) - Issue 1.0

Abstract

These Application Notes describe the configuration of an AudioCodes Mediant 3000 Media Gateway 3.0 with Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) to secure SIP signaling and media against unauthorized recording or interception. The AudioCodes Mediant 3000 Media Gateway 3.0 is a feature-rich VoIP gateway that offers a broad range of PSTN interfaces and functions, allowing conversion of legacy TDM networks to decentralized IP networks. VoIP security is implemented by using TLS to authenticate hosts, securing the signaling channel. SRTP encrypts the media between endpoints.

Information in these Application Notes has been obtained through Solution Integration compliance testing and additional technical discussions. Testing was conducted at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required to implement Transport Layer Security (TLS) for SIP signaling and Secure Real-time Transport Protocol (SRTP) for media security in an AudioCodes Mediant 3000 Media Gateway 3.0 as part of an Avaya Aura® network solution. TLS adds functionality by enabling clients and servers to exchange verifiable identity certificates (Mutual Authentication) prior to engaging in encrypted communications. This offers the following security advantages:

- TLS prevents identity theft, where an interloper gains access by impersonating a trusted SIP endpoint in the network.

- TLS implements signaling encryption to overcome eavesdropping (packet sniffing) and man-in-the-middle attacks (intruder interrupting the dialog or modifying the signaling data) by negotiating a dynamically generated symmetric key and using ciphers to encrypt TLS handshakes.

TLS identity certificates can be self-signed or signed by a Certificate Authority, the latter is an entity that issues digital certificates which confirm the ownership of a public key by the named subject of the certificate.

The exchange of encrypted data relies on the use of a public/private key pair by each server and client. Encryption parameters and ciphers are offered during the initial TLS handshake. TLS operates on top of TCP, meaning UDP cannot be secured using TLS. To ensure ongoing security, the connection may be renegotiated periodically.

SRTP is a variation of the standard RTP protocol with enhancements to provide message authentication and encryption, adding a layer of security to RTP. SRTP requires endpoints to agree on a cryptographic algorithm and to exchange keys prior to commencing transmission. Once secured, transmission is protected from replay attacks and alteration by unapproved sources. SRTP is independent of TLS; both are often used when Voice over Internet Protocol (VoIP) transmissions must be secured over an unknown network.

SRTP uses the AES cipher to encrypt and decrypt messages and the HMAC-SHA1 algorithm to authenticate the message and protect its' integrity.

The AudioCodes Mediant 3000 Media Gateway 3.0's primary function is to convert SIP messaging into ISDN protocol and vice versa. The AudioCodes Mediant 3000 Media Gateway 3.0 supports several E1 and T1 signaling protocol variants for PSTN access with a capacity of 2000 voice channels.

2. Interoperability Testing

The primary utilization of the AudioCodes Mediant 3000 Media Gateway 3.0 (M3K) is to convert ISDN trunks to SIP trunks, interfacing with a SIP Contact Center or SIP Communications System via Avaya Aura® Session Manager. Using an M3K simplifies system configuration and design; less local resources are needed for TDM to IP conversion.

These Application Notes focus primarily on securing M3K SIP telephony communications with TLS and SRTP in an Avaya Aura® network environment. Securing M3K administration functions (e.g., web management) are also presented where it is desirable to further enhance security.

Intended users of these Applications Notes should be familiar with Avaya installation procedures and necessary operating procedures. It is desirable to carry out procedures during a maintenance window as many configuration changes require restarting equipment and may result in a temporary loss of service. Configuration changes services that are service affecting will be highlighted in the text.

2.1. Test Description and Coverage

Test cases included bi-directional calls between PSTN users and Avaya IP Deskphones registered as SIP users to Session Manager, using SRTP for media, as well as traditional telephony operations and features such as extension dialing, displays, hold/resume, transfer, conferencing, and call forwarding.

In addition, failover testing was performed to verify calls between PSTN users and SIP users registered to both Session Managers were successful when there were network connectivity issues or when the primary Session Manager was unavailable.

2.2. Test Results and Observations

All test cases were successful.

It was observed that if the AudioCodes **Create CSR** button is unintentionally clicked, a new AudioCodes Private Key is immediately generated which will replace the current Private Key. This will automatically activate when AudioCodes is restarted and causes TLS handshakes to fail for all connections.

If the **Create CSR** key is clicked in error, the process must be followed through to the end (i.e., the CSR must be signed and imported into AudioCodes) to get TLS working again.

3. Reference Configuration

Figure 1 shows an AudioCodes Mediant 3000 used in conjunction with an Avaya Aura® Communication Manager/Avaya Aura® Session Manager installation. Session Manager is a SIP proxy; SIP trunks link Communication Manager to Session Manager and also link Session Manager to M3K. Incoming PSTN calls (via an ISDN trunk) terminate on M3K and are converted to VoIP protocol, then sent over a SIP trunk to Session Manager. Session Manager routes the calls to Communication Manager where they terminate at the intended endpoints.

Outgoing PSTN calls are made via the SIP trunk between Communication Manager and Session Manager. Session Manager then routes calls to M3K and onwards to the PSTN. The M3K acts as a PSTN gateway, converting SIP calls to TDM, a function normally performed by an Avaya Media Gateway.

SIP signaling paths are always via Session Manager, media may be direct from M3K to the endpoint (if shuffling is on), else via the Avaya Media Gateway (if shuffling is off).

SIP signaling is built on top of TCP protocol, which is secured using TLS. Media (either from M3K to the Media Gateway or direct from M3K to endpoints) is secured using SRTP.

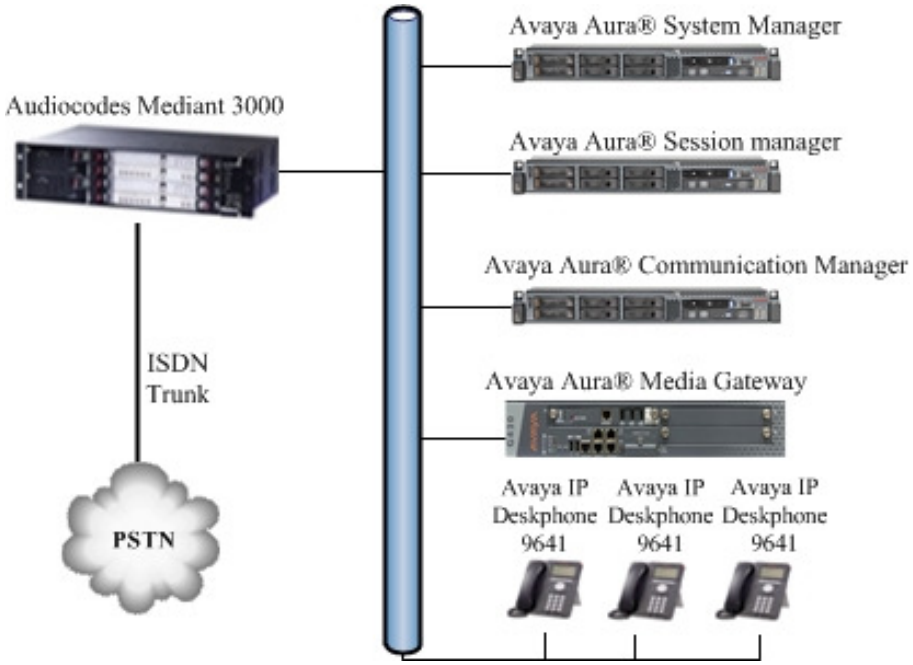


Figure 1: AudioCodes Mediant 3000 Reference Configuration.

.

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® System Manager Avaya S8800 Media Server	Release 6.2, FP2 Version 6.3.2.4.1339
Avaya Aura® Session Manager Avaya S8800 Media Server	Release 6.2, FP2 Build 6.3.2.0.632023
Avaya Aura® Communication Manager Evolution Server • Avaya G430 Media Gateway	Release 6.2, FP2 Version: R016.x.03.0.124.0-20553
Avaya 9600 Series IP Deskphones (with Avaya one-X® SIP firmware)	Release 2.6.10.1 Version 2-6-10-132005
Avaya 96x1 Series IP Deskphone (with Avaya one-X® SIP firmware)	Release 6.2.2.25 Build: 96x1_IPT-SIP-R6_2_2-060613
AudioCodes Mediant 3000 Media Gateway 3.0	R3.0 Firmware Version 6.60A.026.001

5. Configure Avaya Aura® Communication Manager for TLS and SRTP

Prior to configuring AudioCodes Mediant 3000 for TLS/SRTP operation, it is desirable to have previously configured Session Manager and Communication Manager. For detailed administration and configuration instructions for TLS operation with Communication Manager and Session Manager see the additional **Reference [5]** in **Section 11.**

The following is an abbreviated administration guide, listing the tasks necessary to enable TLS/SRTP on Communication Manager:

- Verify Media Encryption is Supported.
- Configure IP Codec Set.
- Configure IP Network Region.
- Verify Initial INVITE with SDP for Secure Calls is enabled.
- Configure SIP Signaling Group.

5.1. Verify Media Encryption is Supported

Logon to Communication Manager and on **Page 4** of **system-parameters customer-options** command; verify the **Media Encryption Over IP?** feature is set to "**y**".

```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                             IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                       ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                         ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                ISDN-PRI? y
              ESS Administration? y               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                    Malicious Call Trace? y
     External Device Alarm Admin? y                  Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                 Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y               Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Configure IP Codec Set

Use the **display ip-codec-set n** command where **n** is the number used to identify the intended codec set. Ensure the necessary audio codecs are listed; use the **change ip-codec-set n** command to alter these if required. In the **Media Encryption** section, ensure that Media Encryption protocol **1-srtp-aescm128-hmac80** is configured.

```
display ip-codec-set 3                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 3

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.729             n         2        20
 3: G.711A            n         2        20
 4:
 5:
 6:
 7:


     Media Encryption
 1: 1-srtp-aescm128-hmac80
 2:
 3:
```

5.3. Configure IP Network Region

Use the **display ip-network-region n** command where **n** is the network region in use. Confirm the **Codec Set** number is the same as the **ip-codec-set** configured in **Section 5.2**.

```
display ip-network-region 1                                     Page   1 of  20
                              IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: silstack.com
    Name: calls to PSTN         Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 3              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 8001
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 0
        Audio PHB Value: 0
        Video PHB Value: 0
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 0
        Audio 802.1p Priority: 0
        Video 802.1p Priority: 0      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 3** of the **ip-network-region** settings, ensure **Allow SIP URI Conversion** is set to "**n**". This settings prevents unsecure media being selected if an endpoints cannot negotiate SRTP successfully.

```
display ip-network-region 1                                     Page   3 of  20
                              IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY
 Incoming LDN Extension:
 Conversion To Full Public Number - Delete:    Insert:
 Maximum Number of Trunks to Use for IGAR:
 Dial Plan Transparency in Survivable Mode? n

BACKUP SERVERS(IN PRIORITY ORDER)    H.323 SECURITY PROFILES
 1                                   1   challenge
 2                                   2
 3                                   3
 4                                   4
 5
 6                                   Allow SIP URI Conversion? n

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
   Near End Establishes TCP Signaling Socket? y
                       Near End TCP Port Min: 61440
                       Near End TCP Port Max: 61444
```

5.4. Verify Initial INVITE with SDP for Secure Calls is enabled

On **Page 19** of **system-parameters features** command, verify the **Initial INVITE with SDP for secure calls** feature is set to "**y**".

```
display system-parameters features                              Page  19 of  20
                        FEATURE-RELATED SYSTEM PARAMETERS
IP PARAMETERS
                   Direct IP-IP Audio Connections? y
                             IP Audio Hairpinning? n
                          Synchronization over IP? n
         Initial INVITE with SDP for secure calls? y
                     SIP Endpoint Managed Transfer? n

   Expand ISDN Numbers to International for 1XCES? n
CALL PICKUP
  Maximum Number of Digits for Directed Group Call Pickup: 4
                   Call Pickup on Intercom Calls? y     Call Pickup Alerting? y
     Temporary Bridged Appearance on Call Pickup? y     Directed Call Pickup? n
                       Extended Group Call Pickup: none
                   Enhanced Call Pickup Alerting? n


                        Display Information With Bridged Call? y
  Keep Bridged Information on Multiline Displays During Calls? y
                  PIN Checking for Private Calls? n
```

5.5. Configure SIP Signaling Group

Use the **display signaling-group n** command, where **n** is the intended signaling group number to be used for TLS/SRTP. On **Page 1**, ensure the following values are used:

- Transport Method: **tls**
- Enforce SIPS URI for SRTP? **y**
- Near-end Listen Port: **5061**
- Far-end Listen Port: **5061**
- Far-end Network Region: **1** (verified in **Section 5.3**)

```
display signaling-group 2                                       Page   1 of   2
                              SIGNALING GROUP

 Group Number: 2             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? y        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

   Near-end Node Name: procr                Far-end Node Name: ASM1
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1

Far-end Domain:
                                          Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? y
         Enable Layer 3 Test? y                  Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 6
```

If multiple Session Managers are in use, ensure each **SIP Signaling Group** should be appropriately configured.

6. Configure Third Party TLS Certificates on Avaya Aura® Communication Manager

Avaya products are supplied with built in TLS certificates which are signed by the Avaya product groups. These may be replaced if required by customer generated or third party certificates. A full description of procedures and protocols associated with the certification process are outside the scope of these Application Notes, see additional **Reference [5]** in **Section 11** for more information.

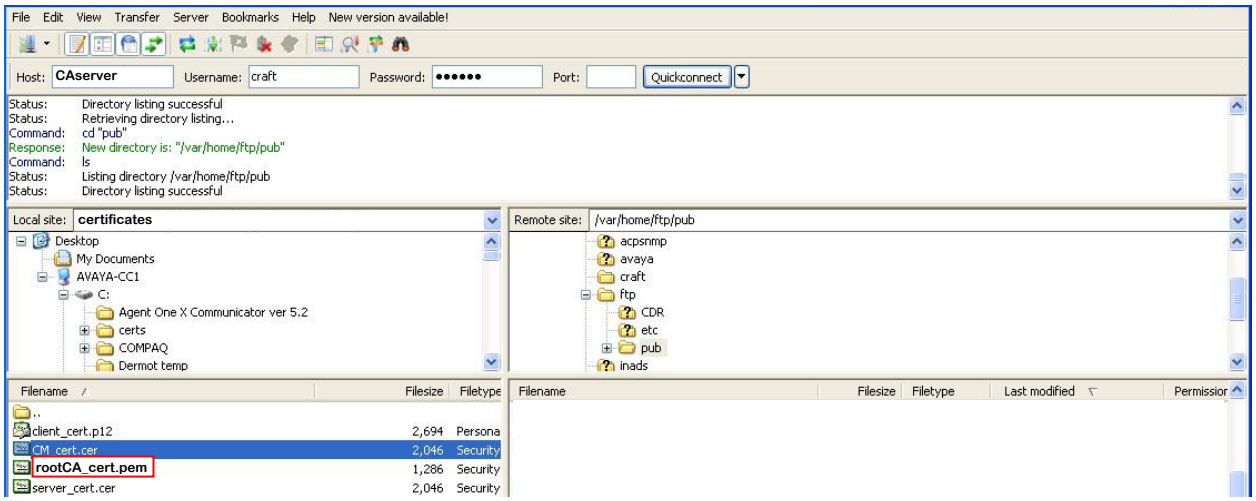
This section focuses on how to replace the default Avaya certificates with new TLS certificates signed by a third party root Certification Authority (CA) server.

6.1. Import a Third Party Root Certificate Authority Certificate

A Third Party root CA certificate is used to verify individual TLS identity certificates. This certificate must be installed on Communication Manager and will be used to verify the identity of endpoints which seek to communicate with Communication Manager.

Obtain a copy of the third party root CA certificate (in .pem format) on a USB pen drive, attach this to Communication Manager, mount the pen drive and use the Linux shell to copy the certificate file to the **/var/home/ftp/pub** location.

Alternatively, from the root CA server use a Secure File Transfer Protocol (SFTP) client, such as Filezila or WinSCP, to connect to the Communication Manager IP address. Copy the third-party Root CA certificate from the CA server to the location **/var/home/ftp/pub** on Communication Manager. See the following screenshot, copy file **rootCA_cert.pem** (highlighted) to /var/home/ftp/pub.



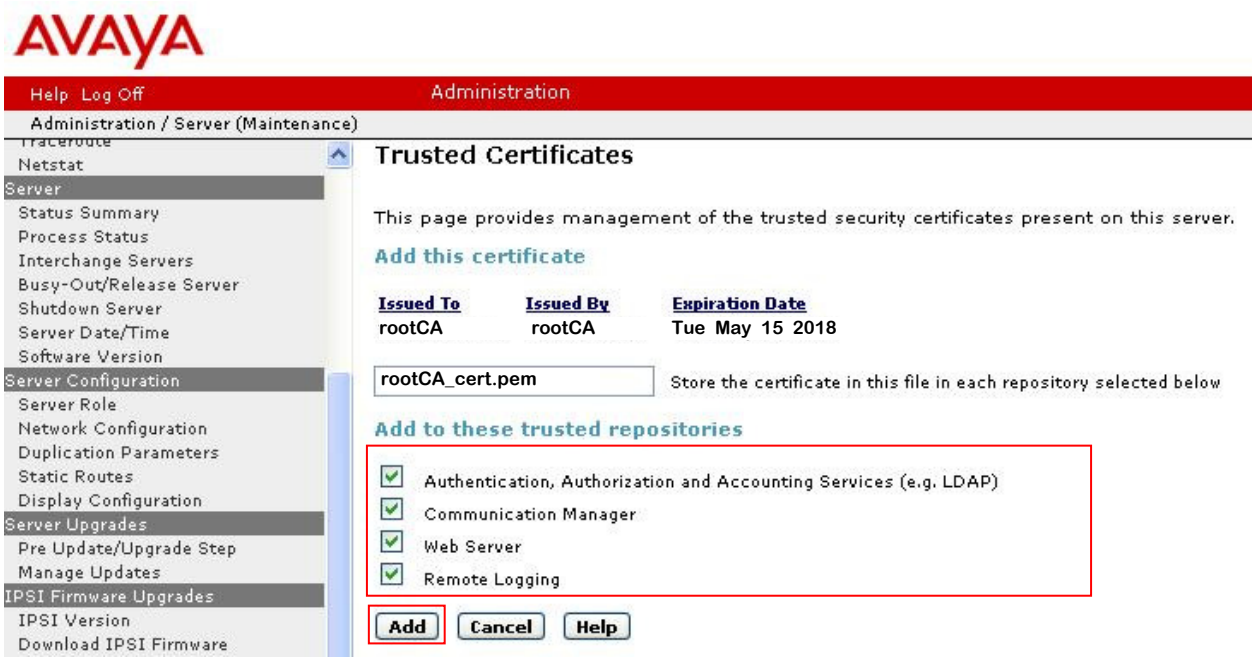
Using a web browser (Microsoft Internet Explorer or Firefox supported) logon to Communication Manager using the system username and password (not shown).

From the top menu bar select **Administration→Server (Maintenance)** (not shown).

On the side menu select **Security →Trusted Certificates**.
A new page opens showing the installed trusted certificates. Click the **Add** button (highlighted).

A new page opens. Type the root CA certificate name (**rootCA_cert.pem**) and click the **Open** button (highlighted).

A new page opens showing some root CA certificate information to confirm it is the required certificate. Type the root CA certificate name in the text box (**rootCA_cert.pem**) and select each service under **Add to these trusted repositories** that will use this certificate to verify incoming connections. Click the **Add** button when ready.



The Trusted Certificates page re-opens, showing the newly added root CA certificate.

6.2. Generate a Certificate Signing Request and Private Key for Avaya Aura® Communication Manager

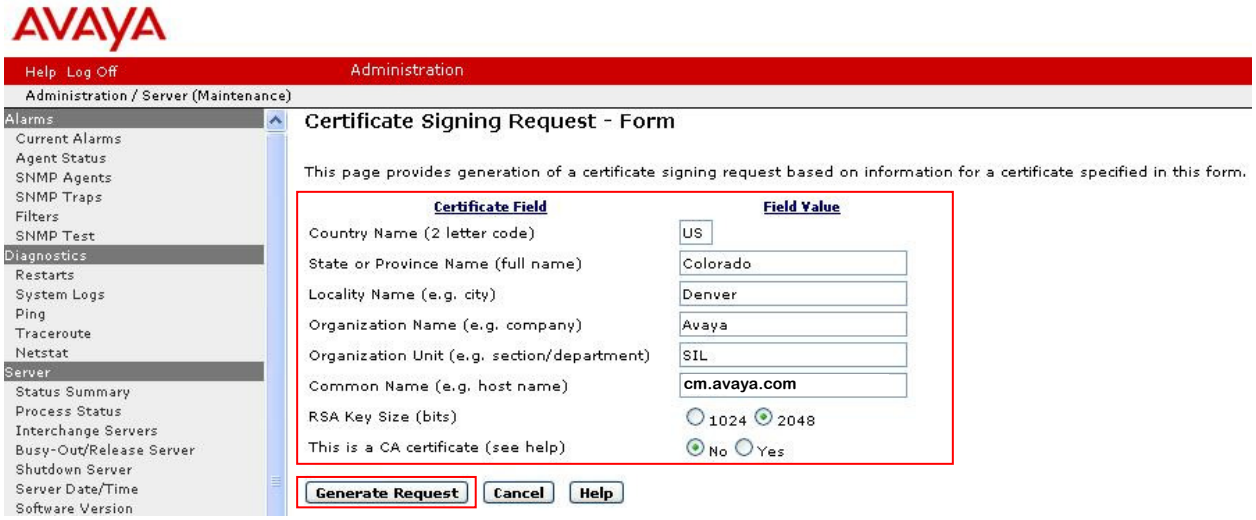
If the default Avaya root CA certificate for Communication Manager is changed, the default Communication Manager identity certificate must also be changed. This requires access to an enterprise or equivalent root CA certificate server which will validate the new Communication Manager identity certificate. To replace the default Communication Manager identity certificate, the following steps are required:

- Generate a certificate signing request (CSR) on Communication Manager
- Submit the certificate signing request to the root CA server.
- Import the signed identity certificate to Communication Manager

Generate a CSR using the by logging on to Communication Manager (see **Section 6.1**), navigate to **Security→Certificate Signing Request**. Click on the **New Request** button (not shown), a CSR form opens. Enter appropriate information for your organization in the **Field Values text boxes**. Ensure the Communication Manager server Fully Qualified Domain Name (FQDN) is entered for **Common Name**. The **RSA Key Size (bits)** should be 2048. Confirm the **This is a CA certificate (see help)** radio button has **No** checked.

When ready, click on the **Generate Request** button. The CSR test is printed on a new screen (not shown). Copy all the text from **`-----BEGIN CERTIFICATE REQUEST-----`** up to and including **`-----END CERTIFICATE REQUEST-----`**

This text will be submitted to the root CA server for signing. The text can be pasted into a text editor and saved (if required).



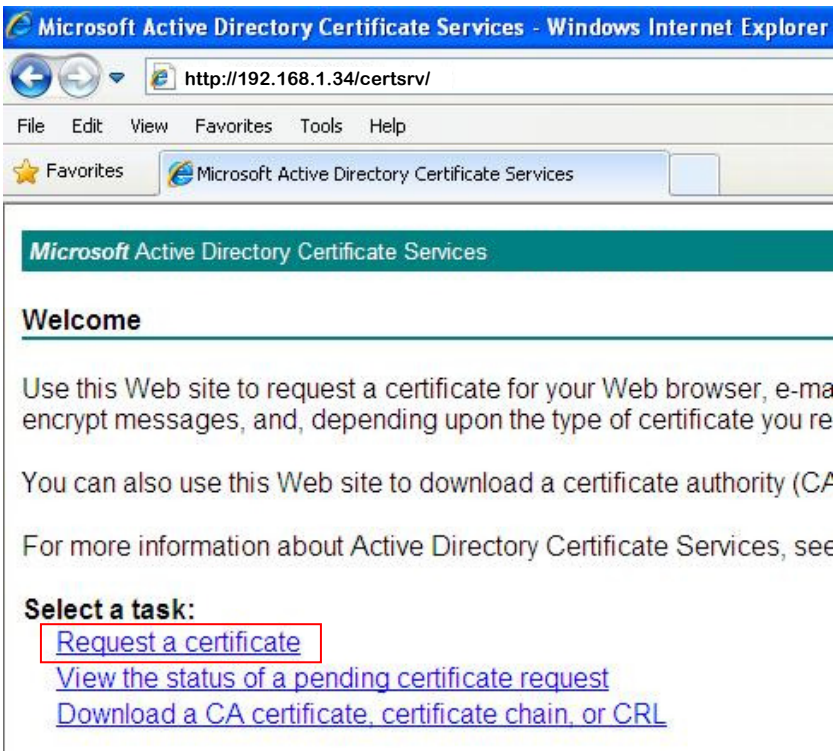
6.3. Sign the Certificate Signing Request on Certificate Authority

The CSR from **Section 6.2** must be sent to the root CA server for signing. The CSR text will be pasted into the root CA server. In this example a Microsoft Windows 2008 Server Enterprise CA is used.

Using Internet Explorer, browse to the **Microsoft Active Directory Certificate Services** on the CA server.

http://<IPaddressOfCAserver>/certsrv/
where <IPaddressOfCAserver> is the IP address or FQDN of the Microsoft Windows 2008 CA.

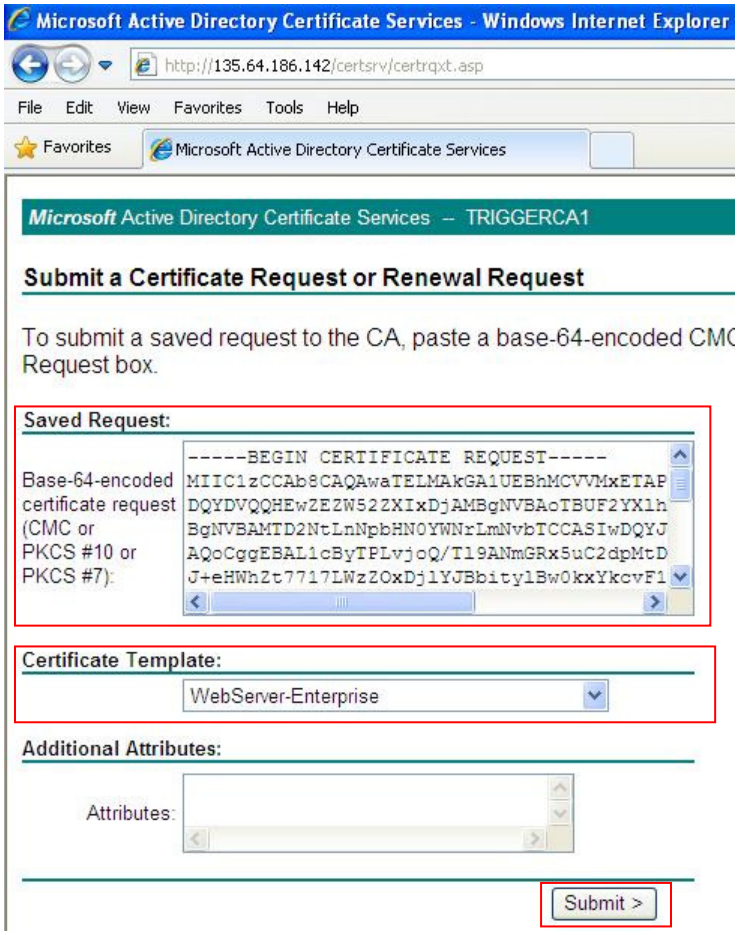
Click on **Request a certificate.**



A new page displays (not shown). Click on the **advanced certificate request** link.

A new page opens (not shown), click on **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

A new page displays. Paste the CSR into the **Saved Request** area. Ensure a **Certificate Template** is selected that matches network requirements; contact your systems administrator if required. When ready, click on the **Submit** button.



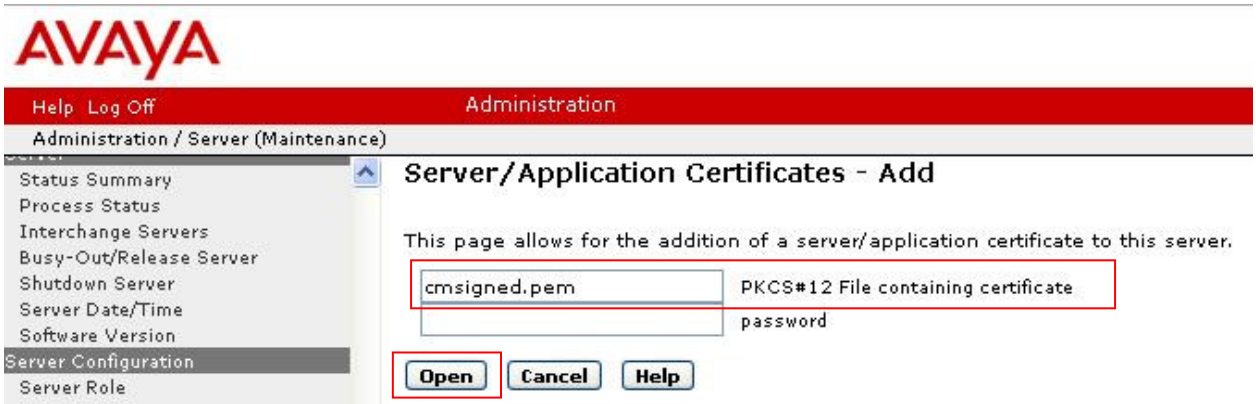
The **Certificate Issued** page opens. Ensure the **Base 64 Encoded** radio button is checked. Click the **Download certificate** link, a file selector opens allowing the file to be saved. Save the file with a **.pem** extension and a descriptive name, e.g., **cmsigned.pem**. Copy the certificate to Communication Manager using SFTP into the **/var/home/ftp/pub** directory.

6.4. Install the Third-Party Signed Identity Certificate into Avaya Aura® Communication Manager

On the Communication Manager web interface, browse to **Security→Server/Application Certificates**.

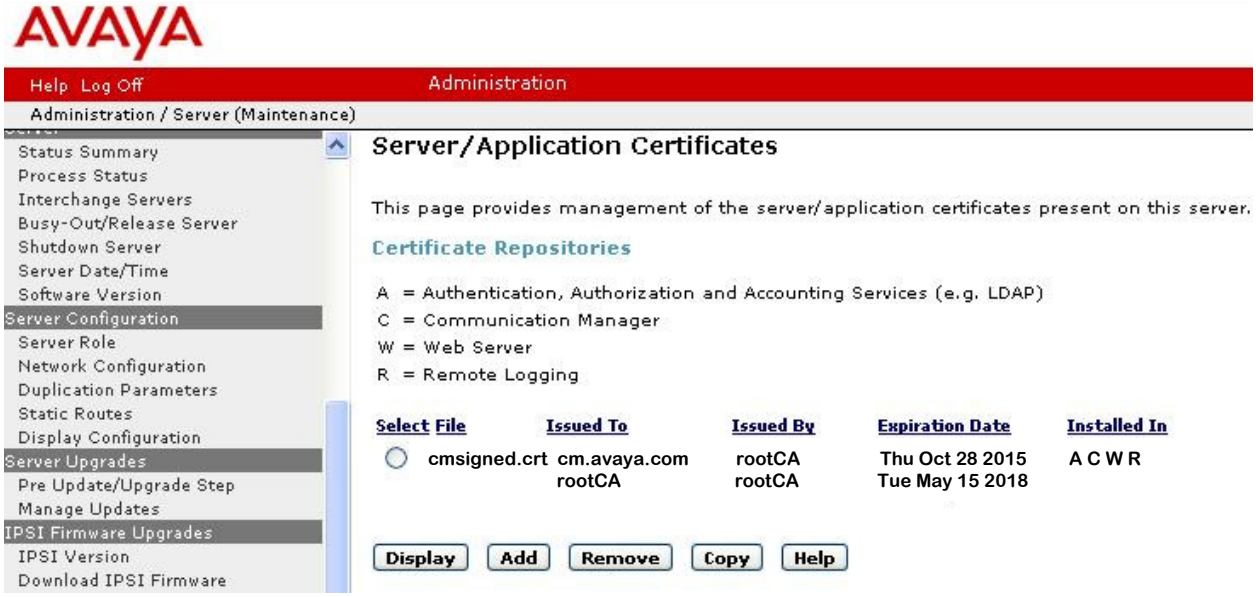
The **Server/Application Certificates** page opens (not shown), click the **Add** button (not shown).

The **Server/Application Certificates – Add** page opens. Type the name of the recently signed certificate (cmsigned.pem) into the **PKCS#12 File containing certificate** text box (no password required). Click the **Open** button.



The certificate is loaded and summary information is shown. Select the checkboxes for each certificate repository. Click the **Add** button.

The new identity certificate is installed.



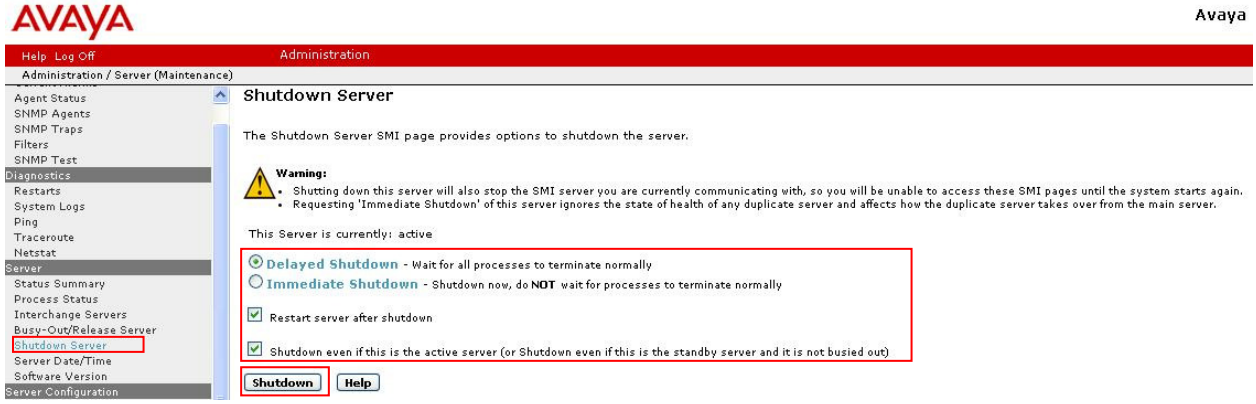
6.5. Restart Avaya Aura® Communication Manager

Before the new root CA certificate can be activated, Communication Manager must be restarted.

Logon to Communication Manager using a SSH client using the craft account and issue the **SAT** command. Issue the **save trans** command. Logout from the SAT application.

Using the web browser, select **Server→Shutdown Server** from the side menu. Select **Delayed Shutdown**, check the box beside **Restart Server after Shutdown,** check **Shutdown even if this is the active server (or Shutdown even if this is the standby server and it is not busied out).** Click the **Shutdown** button. Communication Manager will now restart.

The newly added root CA certificate is automatically copied to the inactive Communication Manager server if the installation is a High Availability (HA) Installation.



7. Configure Avaya Aura® Session Manager for TLS operation with AudioCodes Mediant 3000

Avaya Aura® Session Manager is a SIP based proxy that provides routing services for Communication Manager and other (third party) SIP based equipment. M3K connects directly to Session Manager, which manages all SIP traffic to and from the PSTN. Session Manager monitors the link to M3K to detect outages.

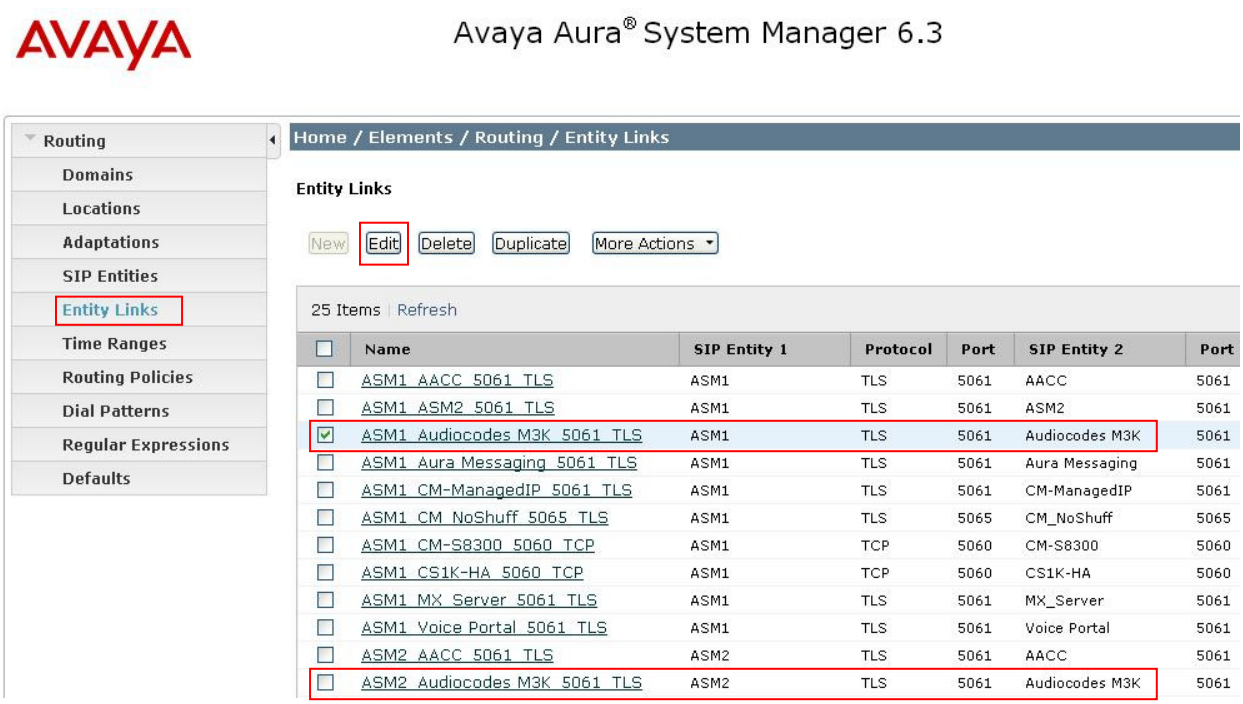
It is assumed Session Manager TLS configuration has already been performed for M3K; the following procedures will show how to change Session Manager default TLS certificates for third party certificates. For detailed information on how to setup TLS links on Session Manager, see additional **Reference [5]** in **Section 11**.

7.1. Modify AudioCodes Entity Links to enable TLS

Using a web browser (Microsoft Internet Explorer supported), logon to Avaya Aura® System Manager (not shown). Under the **Elements** list, click on the **Routing** link (not shown).

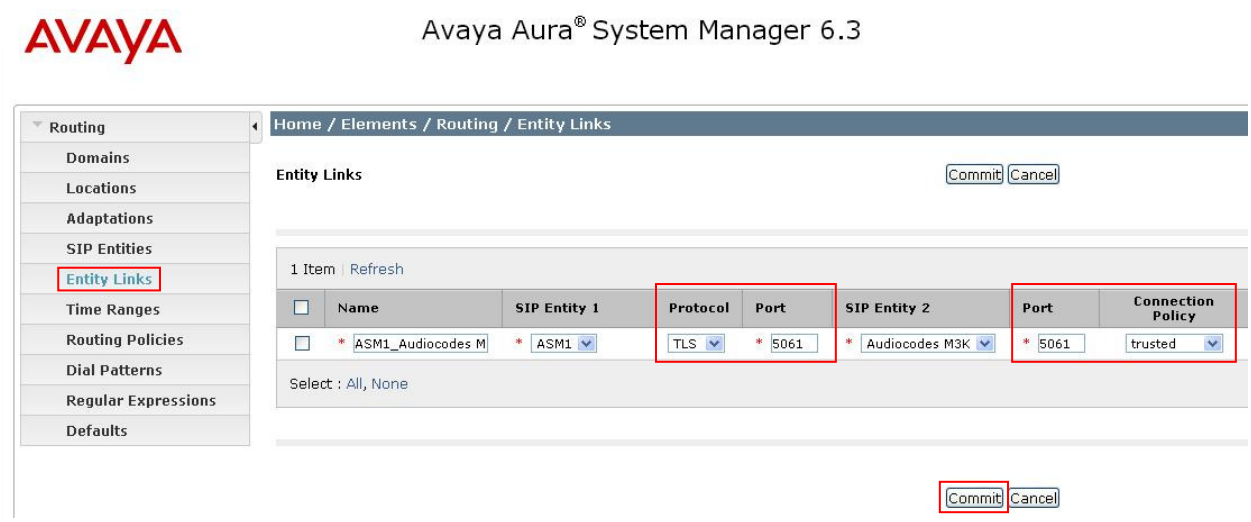
Click on **Entity Links** in the side menu. A page of configured Entity Links opens. Locate the M3K entry (highlighted) and click the checkbox beside it. Click the **Edit** button (highlighted).

Note: if the installation contains more than one Session Manager, there may be more than one Entity Link for M3K as shown below.



A new page opens. Select **TLS** from the **Protocol** drop down list. Ensure both **Port** settings are **5061**. Confirm **Connection Policy** is set to **trusted**. Click the **Commit** button when ready.

Repeat this step for the other M3K entity link (if required).



7.2. Install a Third Party root Certificate in Avaya Aura® System Manager

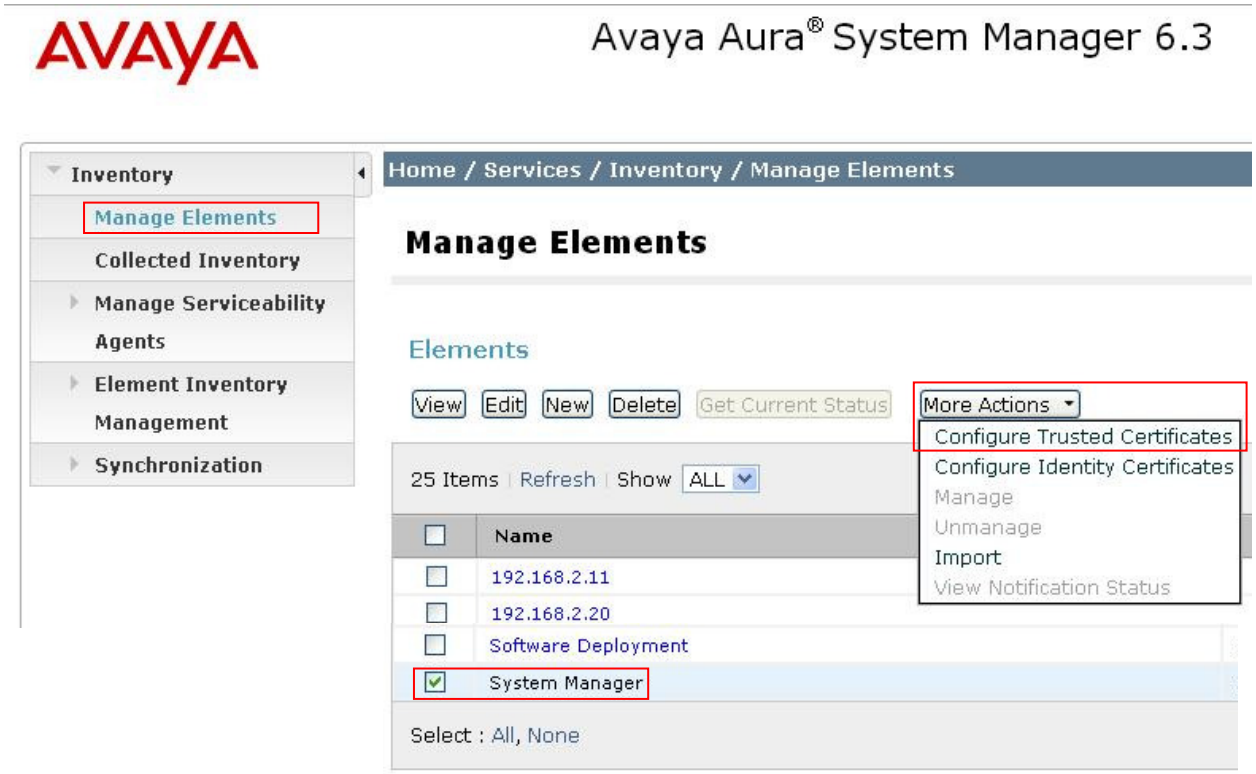
Prior to installing new trusted root certificates in Session Manager, the new certificates must be installed in System Manager. This step is required to preserve trust between System Manager and Session Manager.

Using a web browser (Microsoft Internet Explorer supported), navigate to the System Manager web console by entering:

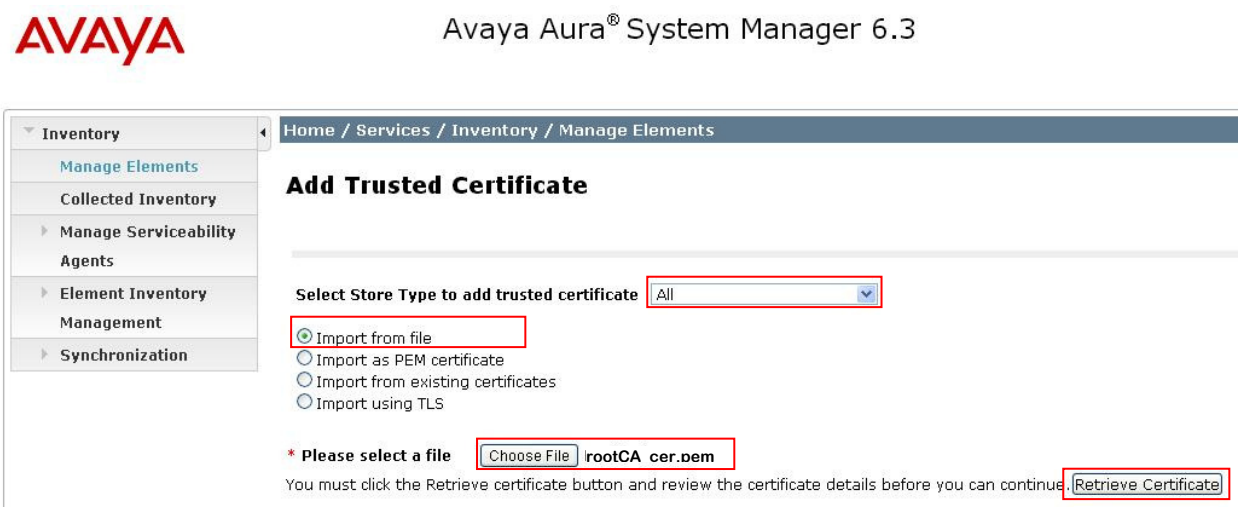
https://<SMGRFQDN>, where <SMGRFQDN> is the IP address or Fully Qualified domain name of System Manager. Enter the admin username and password.

Under the **Services** list**,** click **Inventory** (not shown).

The **Inventory** page opens. Click **Manage Elements** from the left navigation pane and select the checkbox beside **System Manager**. Click on the **More Actions** drop-down menu and select **Configure Trusted Certificates**.



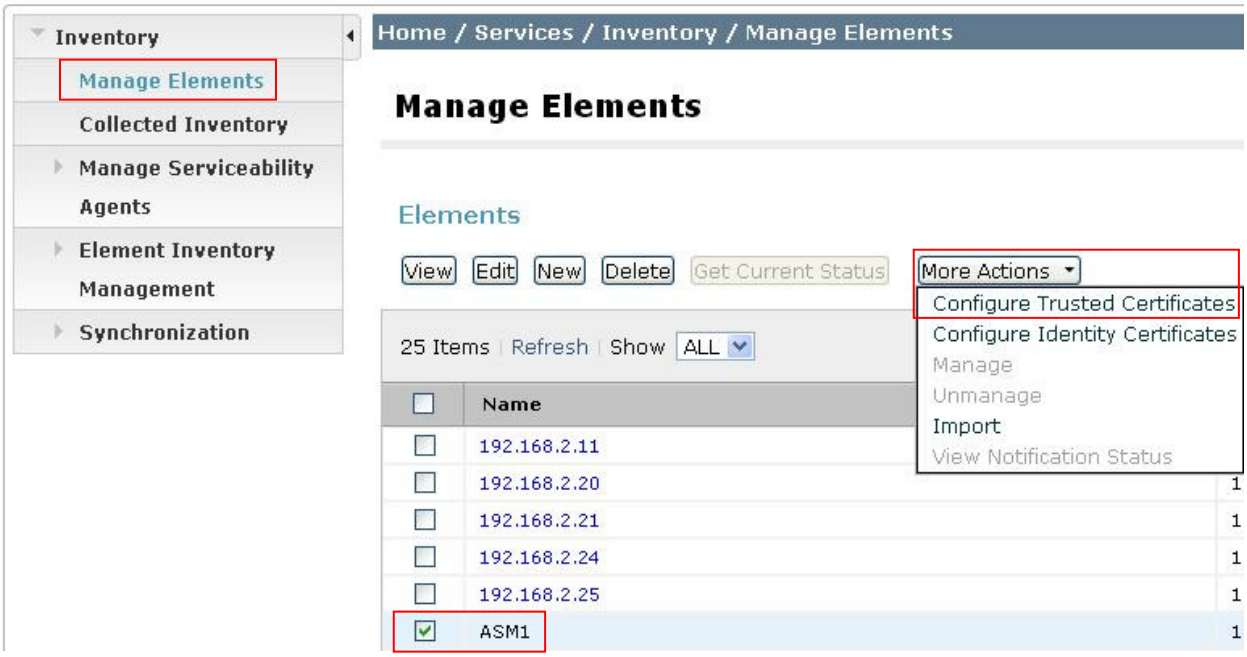
Click **Add** (Not Shown). On **Add Trusted Certificate** page, select **All** for the **Select Store Type to add trusted certificate** drop-down menu. Select the radio button beside **Import from file**. Click **Choose File** to locate the third-party CA root certificate file (**rootCA_cert.pem)** on the local PC and select **Retrieve Certificate** and then **Commit** (not shown). Click **Done** (not shown).



7.3. Install a Third Party root Certificate in Avaya Aura® Session Manager

The third-party root CA certificate must be added to the Session Manager trusted certificate store. This certificate will be used to confirm other SIP endpoints identity by validating the signature of TLS identity certificates presented during TLS handshake negotiations.

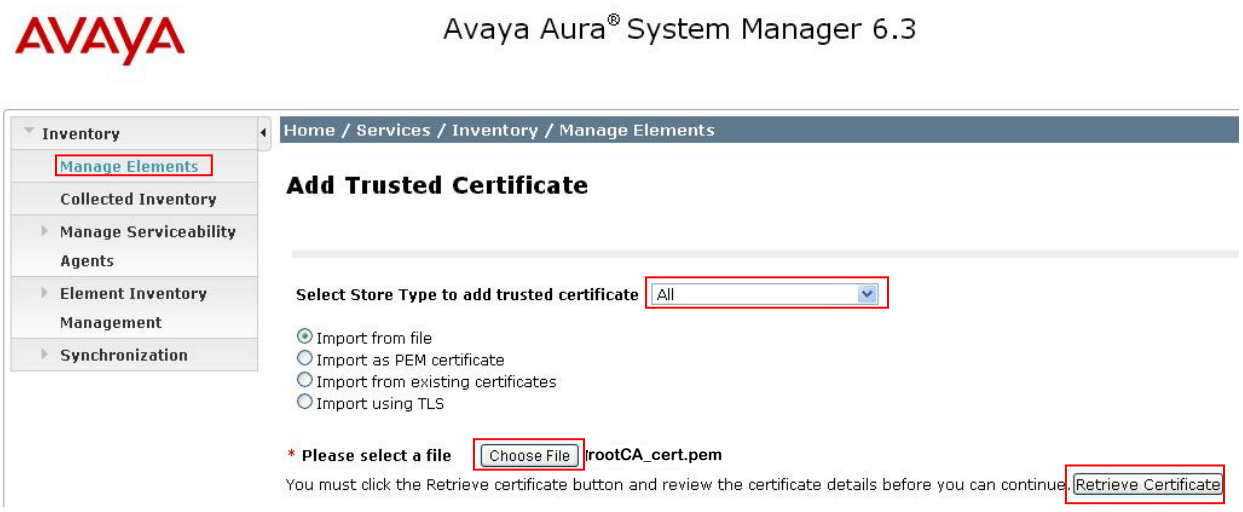
On the System Manager web console, under **Services**, click **Inventory** (not shown).
Click **Manage Elements** from the left navigation pane and select the checkbox beside the Session Manager element (ASM1 in the screenshot). Click the **More Actions** drop down list and select **Configure Trusted Certificates**.



On the trusted certificates page, click **Add** (not shown). On the **Add Trusted Certificate** page, select **All** for the **Select Store Type to add trusted certificate** drop-down menu.

Select **Import from File** then click the **Choose File** button, a standard file selector opens. Navigate to the third-party CA root certificate file location (**rootCA_cert.pem** – see **Section 6.1**), click the **Open** button on the file selector. The web page refreshes and shows the selected file name. Click the **Retrieve Certificate** button and then **Commit** (not shown).

Click **Done** (not shown).



Access Session Manager CLI via SSH as craft and change to the root user. Execute the following command to restart the Session Manager services;

#restart all

Repeat **Section 7.3** if there are more than one Session Managers in the configuration.

Access System Manager CLI via SSH, log in as craft and then switch user to root. Execute the following command;

#sh $SPIRIT_HOME/scripts/configureSpiritSecurity.sh

```
[root@smgr ~]# $SPIRIT_HOME/scripts/configureSpiritSecurity.sh
Stopping SPIRIT Agent Application 1.0-1.0...
Stopped SPIRIT Agent Application 1.0-1.0.
Starting SPIRIT Agent Application 1.0-1.0...
```

7.4. Create a Certificate Signing Request on Avaya Aura® Session Manager

Generating a Certificate Signing request for Session Manager is not possible using the System Manager web interface. Instead, the task must be done using the Session Manager command line interface. Logon to Session Manager using a SSH (putty or similar) using the craft account and change to the root account. The procedure will use **openSSL** to generate a CSR. However, the default openSSL profile must first be edited to change some important settings.

Create a new openSSL configuration file or edit the default file located in **/etc/pki/tls/openssl.cnf** on Session Manager. Important edits are highlighted in **bold** with comments;

```
# Extension copying option: use with caution.
copy_extensions = copy
[ req ]
default_bits            = 2048 # Smaller values are insecure
default_md              = sha1
default_keyfile         = private.key # This is the private key file
distinguished_name      = req_distinguished_name
attributes              = req_attributes
req_extensions          = v3_req # Needed for some extensions


[ req_distinguished_name ]
countryName             = Country Name (2 letter code)
countryName_default     = US # Only used if no input from user
countryName_min         = 2
countryName_max         = 2

stateOrProvinceName           = State or Province Name (full name)
stateOrProvinceName_default   = Colorado # Only used if no input from user

localityName                  = Locality Name (e.g., city)
localityName_default          = Denver # Only used if no input from user

0.organizationName            = Organization Name (e.g., company)
0.organizationName_default    = Avaya # Only used if no input from user
[ v3_req ]

# Extensions to add to a certificate request

basicConstraints = CA:FALSE # This is not a Certificate Authority cert
keyUsage = nonRepudiation, digitalSignature, keyEncipherment,
dataEncipherment, keyAgreement
extendedKeyUsage=serverAuth, clientAuth
subjectAltName= @alt_names

[alt_names]
DNS.1 = asm1.avaya.com # This is the Session Manager FQDN
```

Save the file as **openssl.cnf**.

On the Session Manager command line, type **openssl** (press the **Enter** key).
This puts the terminal into openssl mode, the shell prompt will change to **OpenSSL>.**

Enter the following command to generate the Session Manager CSR;

req –out asm1.csr –new –newkey rsa:2048 –nodes –keyout asm1.key –config /etc/pki/tls/openssl.cnf

This command requests input to populate certificate parameters such as:
country code, organization, Organization Unit, etc. Ensure the relevant information is available before generating the CSR.

In this example, the Common Name (CN) = **asm1.silstack.com**, which is the FQDN of the Session Manager. The administrator will be prompted to enter a challenge password for the private key; this should be noted for future use.

This example uses a 2048 bit private key length, smaller values are insecure.
The resulting CSR file is saved as **asm1.csr**.
Verify the CSR file contains the correct information by entering the following:

req –text –noout –verify –in asm1.csr

Examine the output in the terminal window, confirm the values are as expected.
To exit the **OpenSSL>** mode, type **exit**.

At the shell prompt, type **cat asm1.csr** (**press Enter**). The CSR contents are printed in the terminal window, similar to the example below.


```
-----BEGIN CERTIFICATE REQUEST-----
MIIDNDCCAhwCAQAwazELMAkGA1UEBhMCSUUxETAPBgNVBAgTCENvbm5hY2h0MQ8w
DQYDVQQHEwZHYWx3YXkxDjAMBgNVBAoTBUF2YXlhMQwwCgYDVQQLEwNTSUwxGjAY
BgNVBAMTEWFzbTEuc2lsc3RhY2suY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAv/iM1or94I5vDonMcL6OTUgT7z9hiL2Nya9KjNjbynOXE1jhfEsq
N69Gr6JGvtsF4r4p/lH4jlAZ9N1TNRuCcNmXAYBx9UAl9moj4EO93WC1nKcxkn2B
L0bxMTpRQwwc3CalEqcG4ogtv1edfTxQI85hpHMuIbYzJQfaNX7SkolsmRC+O9bW
ACsaXpHPhpmsc6ecmSPPKbFOjIWdVzbSwdPBqX9QjMPWqk/rRd5s01ivMbQFd5nL
UZpc5IgI068=
-----END CERTIFICATE REQUEST-----
```


The CSR must be submitted to a root CA server to be signed before it can be imported into Session Manager. Copy all the text from **-----BEGIN CERTIFICATE REQUEST-----** up to and including **-----END CERTIFICATE REQUEST-----**.

Use the procedure in **Section 6.3** to sign the Session Manager CSR. Save the file with a **.pem** extension and a descriptive name, e.g., **asm1signed.pem**. Copy the certificate to Session Manager using SFTP into the **/home/craft** directory.

7.5. Package the Avaya Aura® Session Manager Private key and Signed Certificate into a PKCS#12 certificate bundle

Session Manager can only import signed TLS identity certificates in PKCS#12 format. The signed certificate is in .pem format, it must be combined with the Session Manager private key into a PKCS#12 bundle. Ensure the private key file used in **Section 7.4** (**asm1.key**) is copied to the **/home/craft** folder. On a Session Manager terminal window (putty client or similar), issue the following command to create a PKCS#12 bundle;

openssl pkcs12 –export –out asm1.p12 –inkey asm1.key –in asm1signed.pem

When prompted, enter the challenge password from **Section 7.4** to complete exporting this PKCS#12 bundle. Using an SFTP client or USB key, copy file **asm1.p12** to the local PC used to administer System Manager.

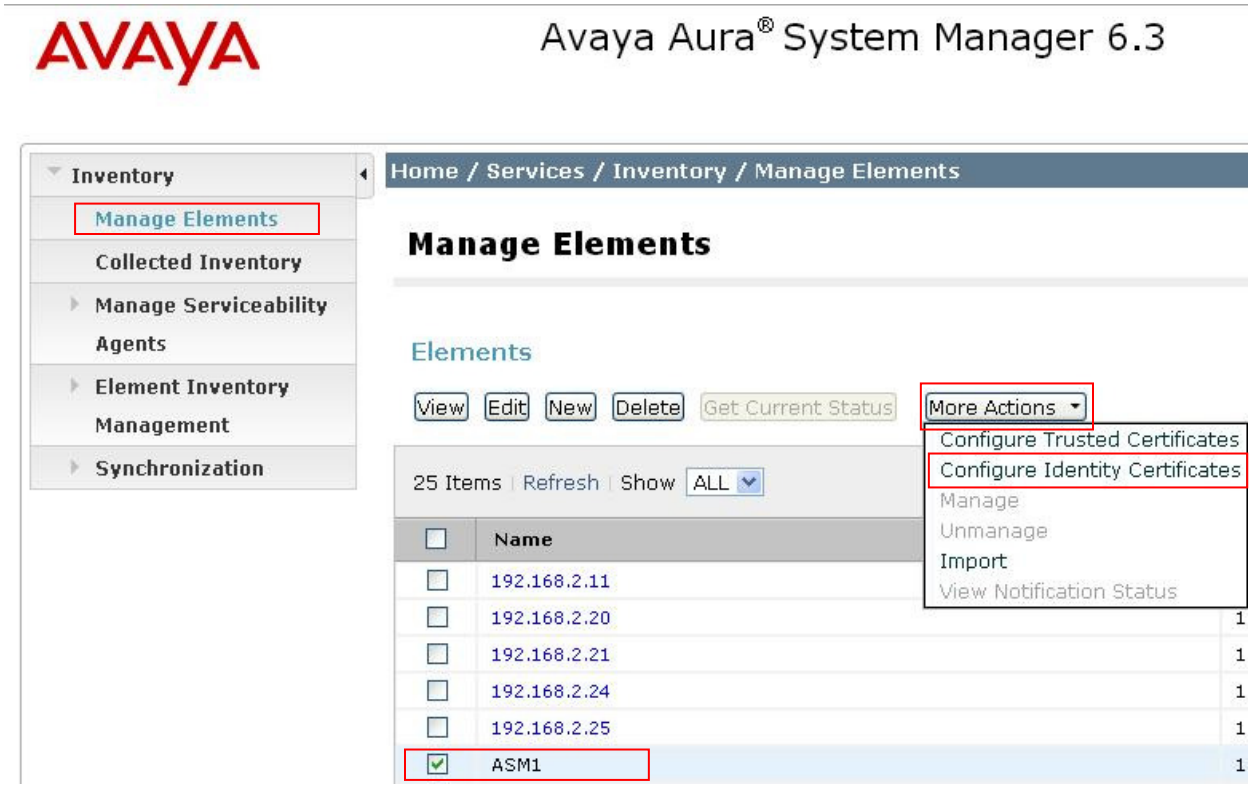
Repeat the procedures in **Section 7.4** and **Section 7.5** for the subsequent Session Managers.

7.6. Replace the Default Avaya Aura® Session Manager Identity Certificate

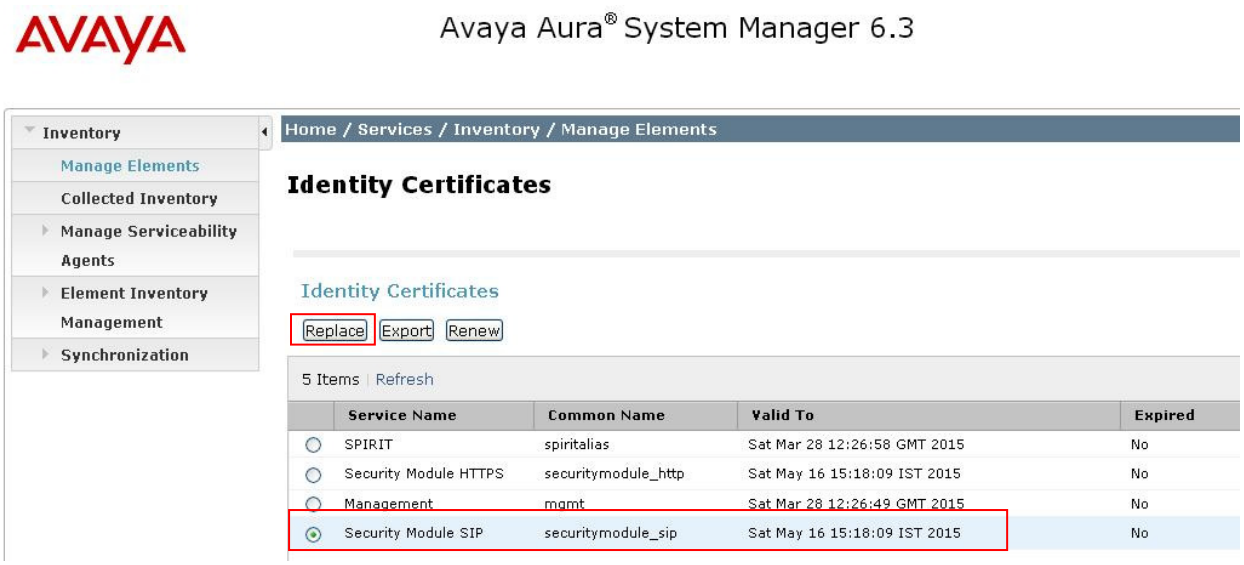
Session Manager contains a default Identity certificate with a hardcoded Common Name (CN) of **sm100** used solely for SIP communication. Each Session Manager will need to be changed to use a third-party signed identity certificate with its unique FQDN as the Common Name on the certificate.

On the System Manager web console, navigate to **Services→ Inventory → Manage Elements** (not shown). Select the check box beside the Session Manager element, which is **ASM1** in the sample configuration.

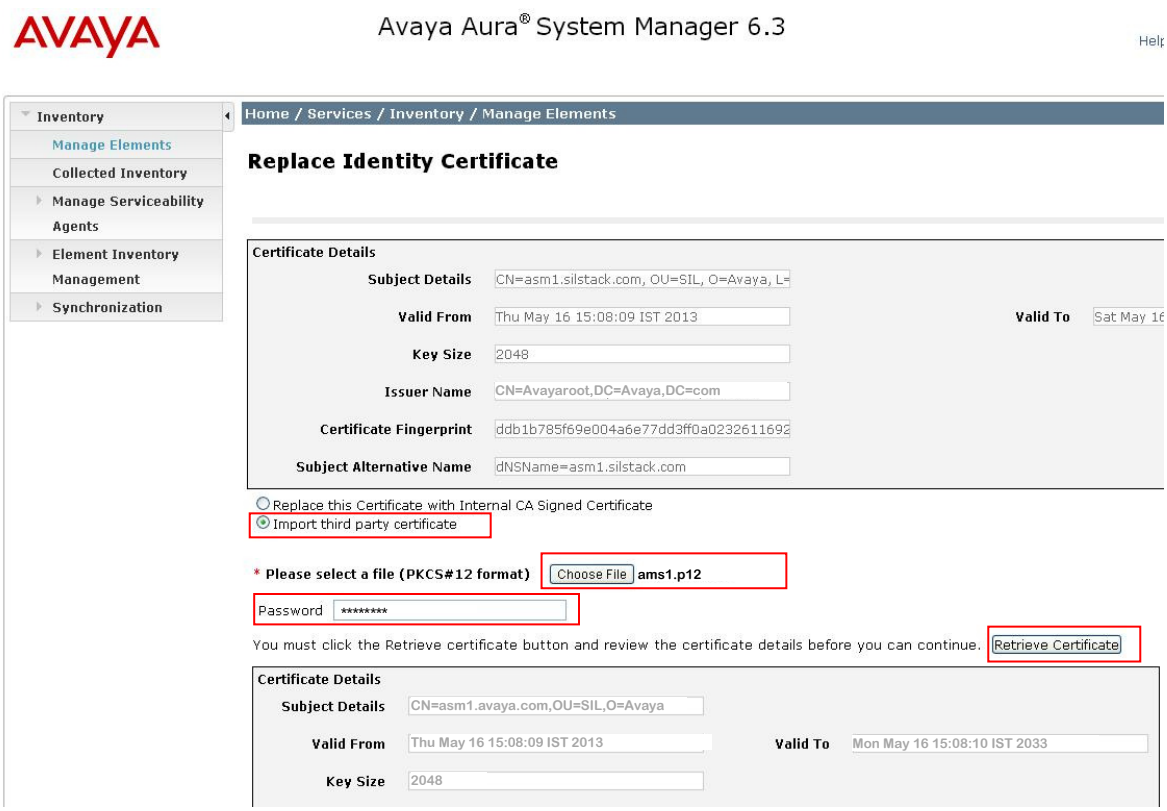
Select **Configure Identity Certificates** from **More Actions** menu as shown below.



Select the radio button beside **Security Module SIP**. The details of the default Session Manager Security certificate are shown. Note **SM100** as the CN. Click on the **Replace** button.



In the new screen, click the **Import third party certificate** radio button. Click **Choose File** to locate the PKCS#12 file created in **Section 7.5** (i.e. **asm1.p12**), enter the key import password and click **Retrieve Certificate**. Click on **Commit** and **Done** on the following screen (not shown).



PPM data exchange with Session Manager occurs over HTTPS, port 443. TLS certificate exchange for PPM should also use the third-party certificates. See additional **Reference [8]** in **Section 11.**

Navigate back to **Manage Elements** (not shown). Select the check box beside the Session Manager element ASM1 (not shown). Select the radio button beside **Security Module HTTPS** as shown below. The details of the default Session HTTPS Manager Security certificate are made available (not shown here). Note **SM100** is the CN. Click on the **Replace** button in order to replace this default identity certificate.

In the new screen, click the **Import third party certificate** radio button. Click **Choose File** to locate the PKCS#12 file created in **Section 7.5** (i.e. **asm1.p12**), enter the key import password and click **Retrieve Certificate**. Click on **Commit** and **Done** on the next screen (not shown).

Repeat the procedure in **Section 7.6** for any other Session Manager.

Access Session Manager CLI via SSH as craft and change to the root user. Execute the following command to restart the Session Manager services;

#restart all

Repeat the steps described in **Section 7.6** for all Session Managers in the network**.**

8. Configure AudioCodes Mediant 3000 Media Gateway 3.0 to use Third Party Certificates

The following procedure assumes the basic configuration steps have been performed on the AudioCodes Mediant 3000 Media Gateway. The procedure will highlight the changes required to enable TLS and SRTP. Replacement of the default AudioCodes certificates with new third party certificates will also be shown. The following steps are required:

- Change default AudioCodes HTTPS cipher and private key size in the 'ini'settings
- Enable TLS and select ports.
- Enable secure media.
- Generate a new AudioCodes TLS identity certificate
- Sign the AudioCodes TLS identity certificate.
- Import the signed certificate together with the root CA certificate.

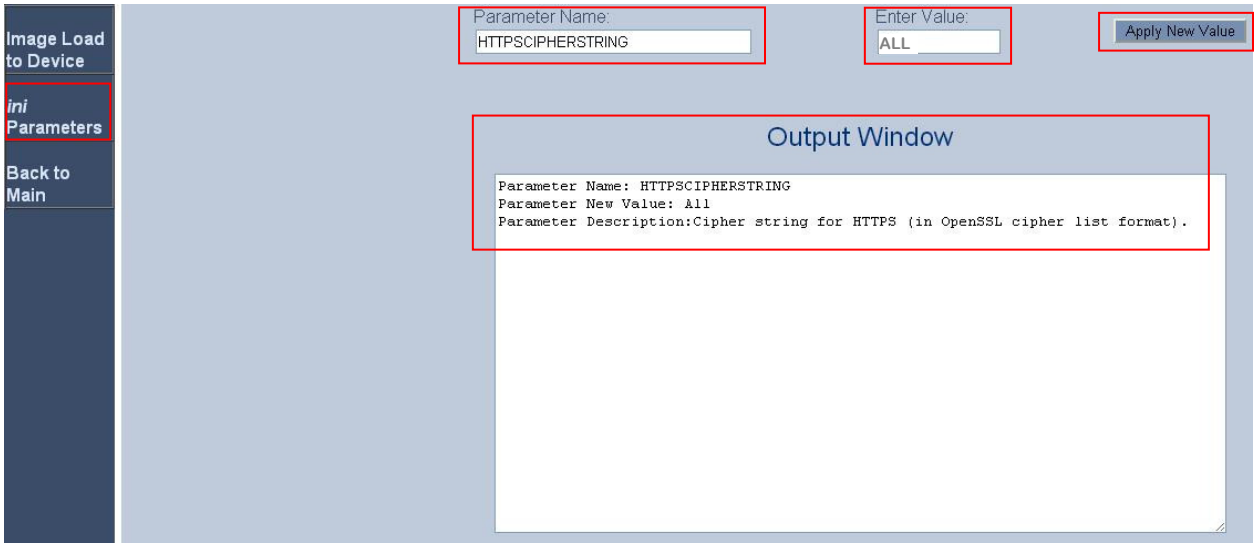
8.1. Change the default AudioCodes HTTPS Cipher and Private Key bit size

Logon to AudioCodes using a web browser (not shown - Internet Explorer, Firefox supported) using the administration credentials. In the side menu, click on ***ini* Parameters,** a new page opens.

- In the **Parameter Name** textbox, type **HTTPSCipherString**.
- In the **Enter Value** textbox, type **ALL**.

Click the **Apply New Value** button (highlighted) when ready.

The new values are applied to the AudioCodes, the **Output Window** shows the new value.

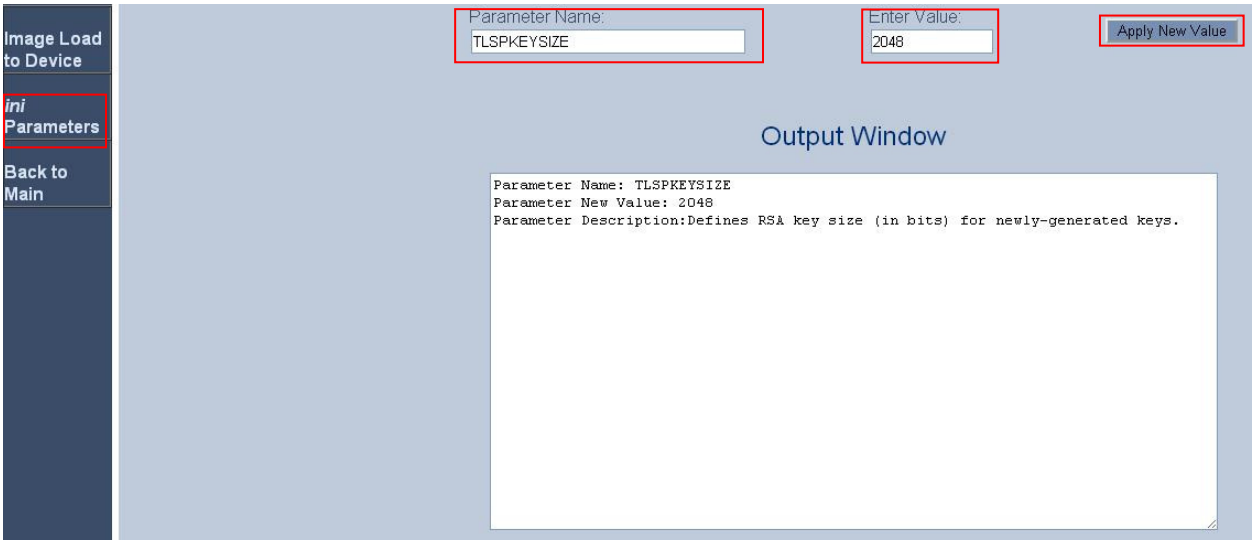


Click on ***ini* Parameters** again to clear the page.

- In the **Parameter Name** textbox, type **TLSPKEYSIZE**.
- In the **Enter Value** textbox, type **2048**.

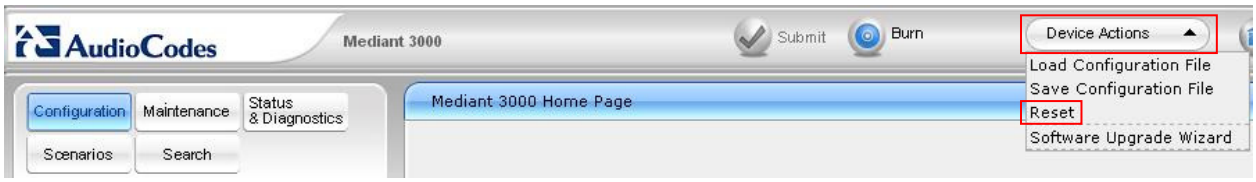
Click the **Apply New Value** button (highlighted) when ready.

The new values are applied to the AudioCodes, the **Output Window** shows the new value.

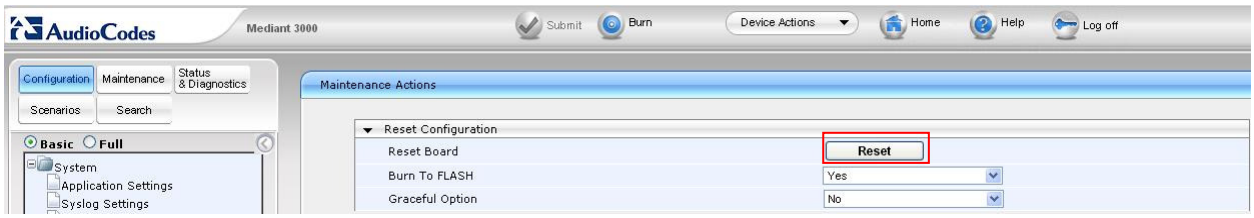


Click **Back to Main** from the side menu to navigate to AudioCodes main configuration screens.

Click **Device Actions** (top of page) and select **Reset** from the drop down list.



In the new page, click the **Reset** button (highlighted). AudioCodes will restart, please allow up to two minutes before logging in.



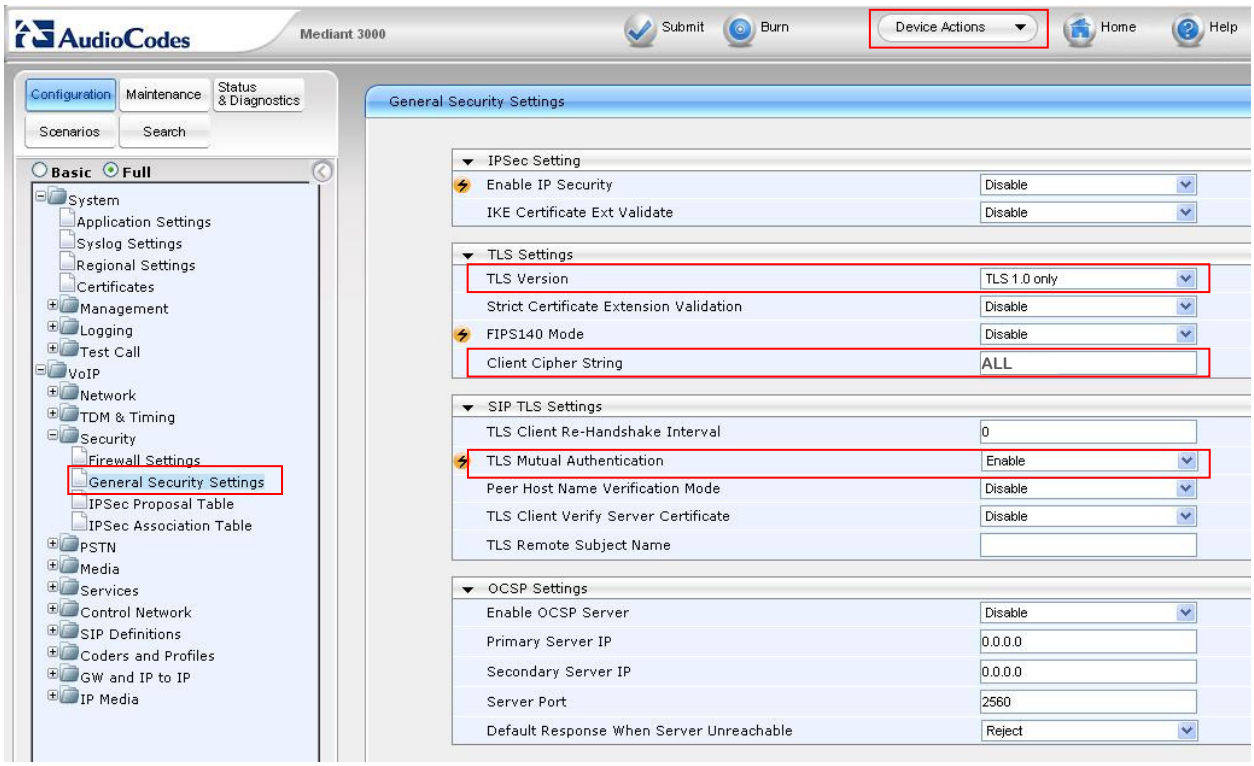
8.2. Configure General Security Settings

On the main AudioCodes page, click the **Full** radio button, expand the **VoIP** side menu, and then expand the **Security** menu. Click on **General Security Settings** (highlighted), a new page opens.

- For **TLS Version**, select **TLS 1.0** only from the drop down list.
- Ensure **Client Cipher String** is **ALL**.
- **TLS Mutual Authentication** should be set to **Enable**.

Click the **Submit** button (not shown) at the bottom right side of the page to save the settings.

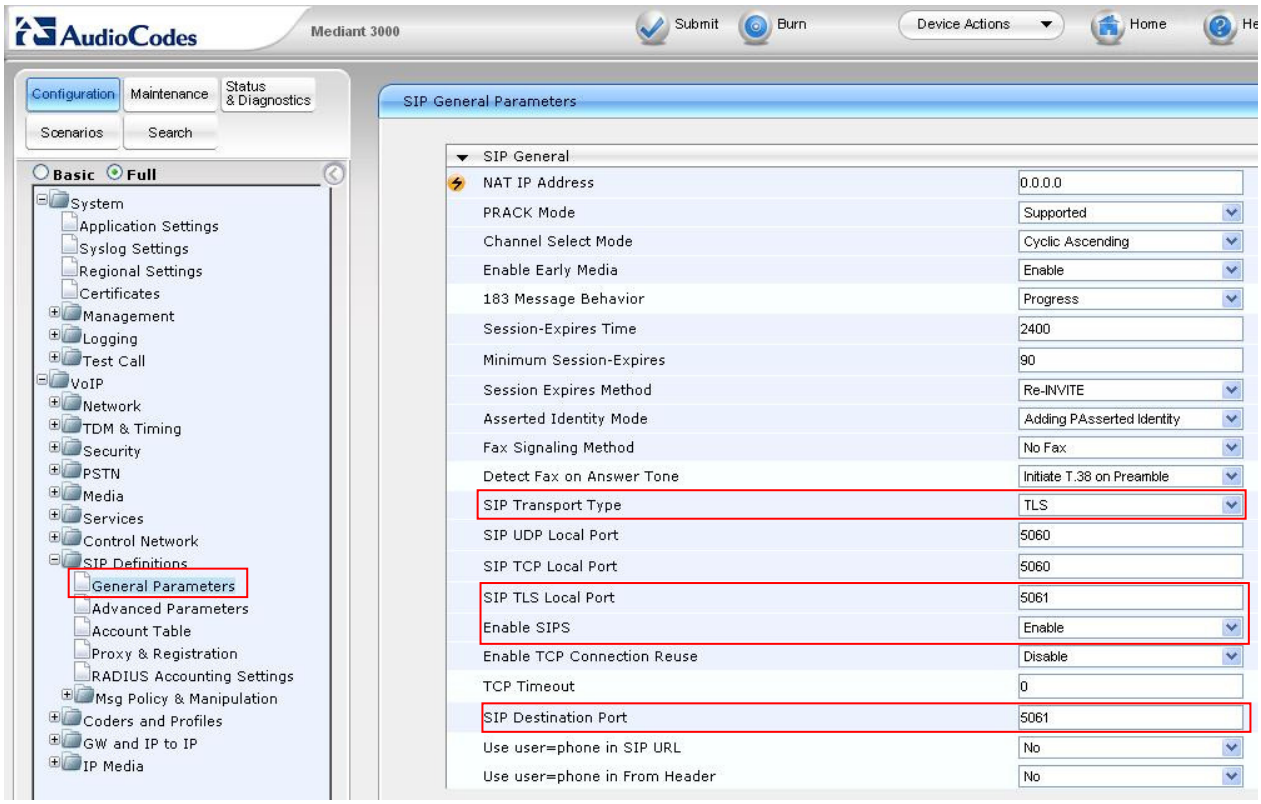
Note: settings with a small lightening symbol in a yellow circle require the AudioCodes is reset before these are activated. This can be done now by selecting **Reset** from **Device Options** at the top of the page or it can be done later in the configuration steps.



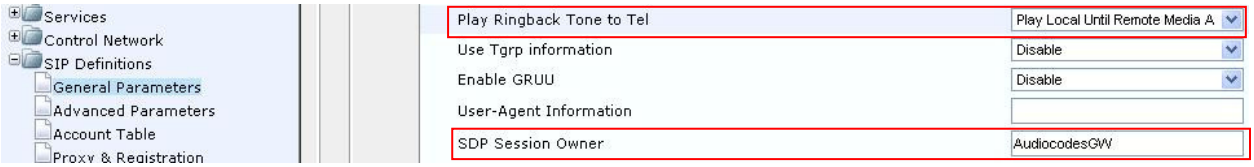
8.3. Enable TLS and select ports

On **Configuration** tab, expand **VoIP→SIP Definitions→General Parameters**.

- Set **SIP Transport Type** to **TLS**.
- Ensure **TLS Local Port** is **5061**
- To enable secure SIP sessions, **Enable SIPS** should be set to **Enable**.
- **SIP Destination Port** should be **5061**.



Scroll down the page and ensure **Play Ringback Tone to Tel** is set to **Play Local Until Remote Media Arrives** and **SDP Session Owner** is set to **AudiocodesGW**.



Click on the **Submit** button (not shown) to save the settings.

8.4. Enable Secure Media

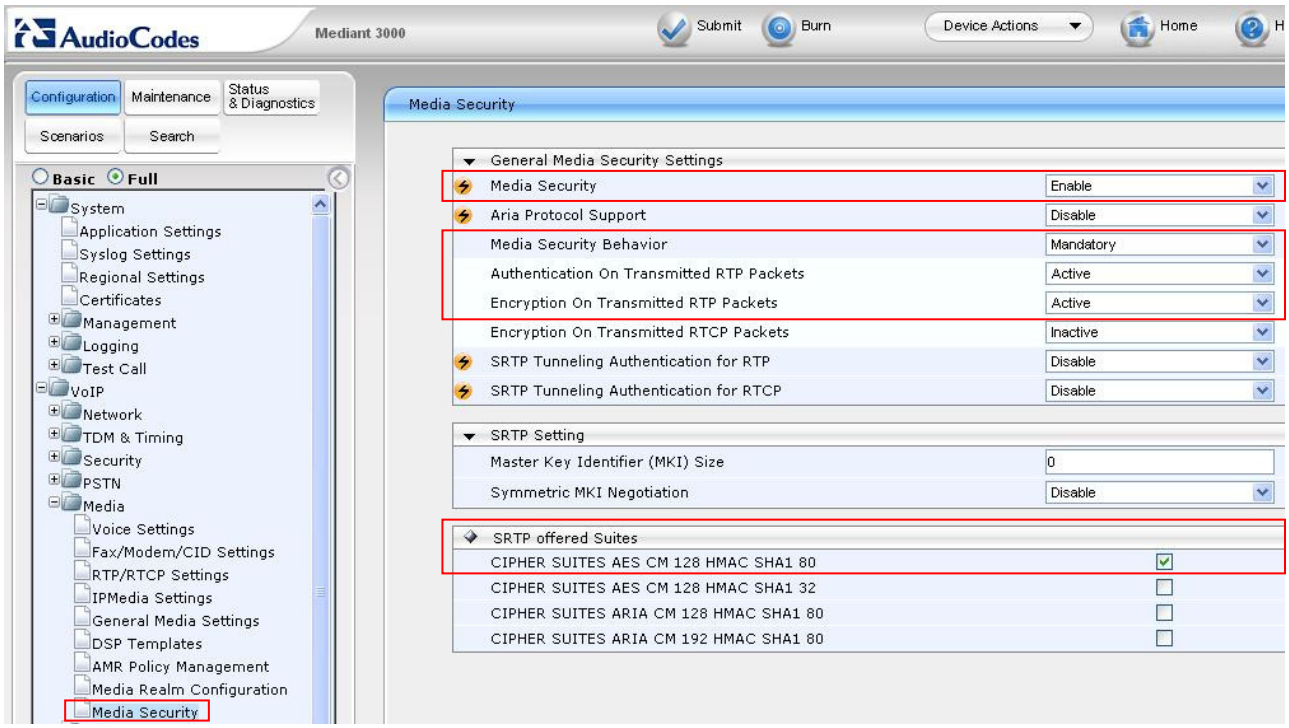
On **Configuration** tab, expand **VoIP→Media→Media Security** (highlighted)**.**

Media Security must be set to **Enable**.

To ensure all calls are protected, **Media Security Behavior** is set to **Mandatory**. **Authentication On Transmitted RTP Packets** and **Encryption On Transmitted RTP Packets** should both be set to **Active**.

Click on the radio button beside **SRTP offered Suites** to expand the list.
Click the checkbox beside the same cipher suite as chosen for Communication Manager media encryption (see **Section 5.2**).

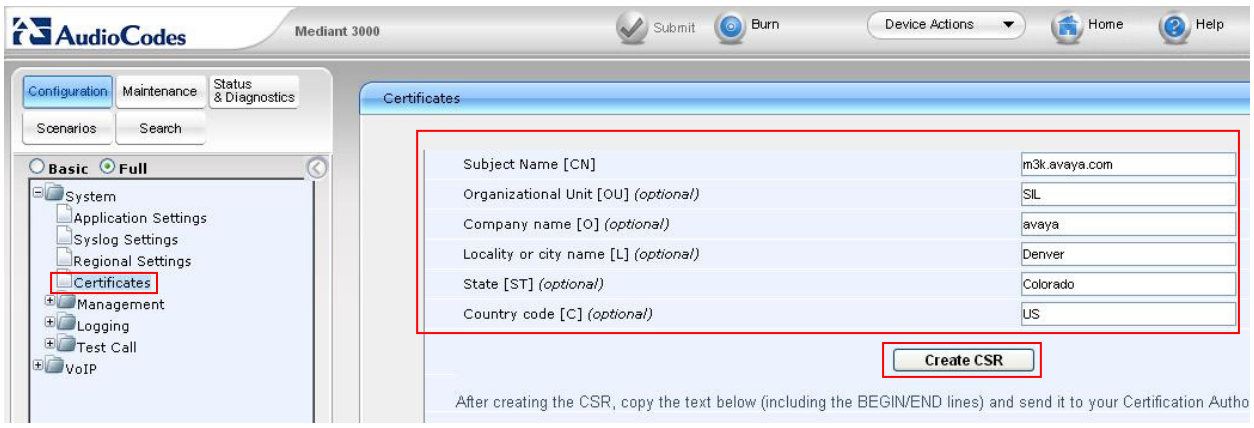
Click the **Submit** button (not shown).



8.5. Generate a new AudioCodes TLS identity certificate

Navigate to **Configuration→System→Certificates**. Expand the **Certificates** section and fill in the required information as in the example below.

Subject Name [CN] should be the AudioCodes fully qualified domain name.
When completed, click the **Create CSR** button.



The page refreshes and displays the CSR text. Copy all the text from **-----BEGIN CERTIFICATE REQUEST-----** up to and including **-----END CERTIFICATE REQUEST-----** and save this to a file.

Follow the procedure in **Section 6.3** to sign the AudioCodes CSR. Save the file (in PEM format) as **m3k.pem**.

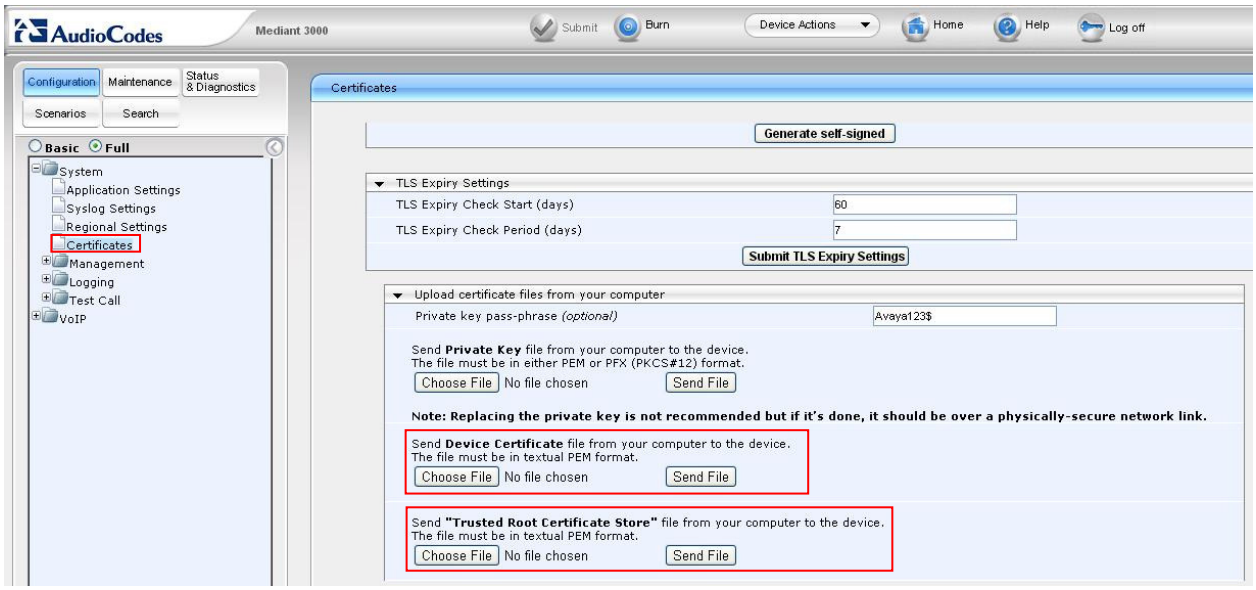
8.6. Import the Signed Certificate and root CA Certificate

The signed certificate obtained in **Section 8.5** can now be imported into AudioCodes along with the root CA certificate from **Section 6.1**. Using a web browser, navigate to **Configuration→System→Certificates**.

In the **Send Device Certificate file from your computer to the device** area, click on the **Choose File** button and navigate to where the AudioCodes signed certificate (m3k.pem) is located, select the file. Click on the **Send File** to upload the new device certificate.

In the **Send "Trusted Root Certificate Store" file from your computer to the device** area, click the **Choose File** button and navigate to where the root CA certificate (rootCA_cert.pem) is located, select the file. Click on the **Send File** to upload the new rootCA certificate.

Note: Since the CSR was generated on M3K using the existing private key, uploading a private key is not needed.



Navigate back to the main AudioCodes page to reset the device. Follow the reset procedure located at the end of **Section 8.1** to reset M3K.

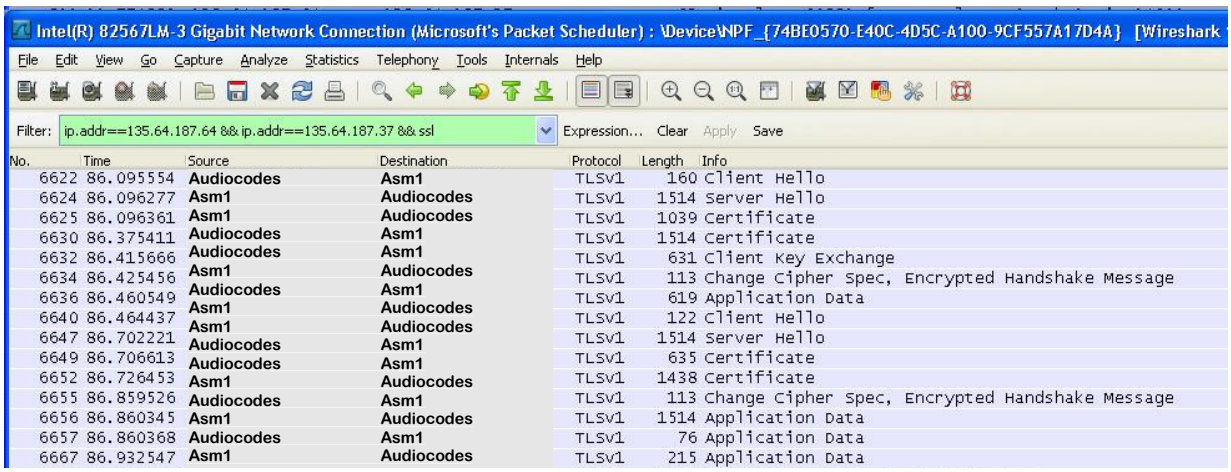
9. Verification Steps

To verify the configuration steps have been successfully completed, perform the following operational tests. It is assumed the AudioCodes Mediant 3000 R3 has been connected to PSTN trunks and that Communication Manager has been setup with endpoints that have PSTN calling capability.

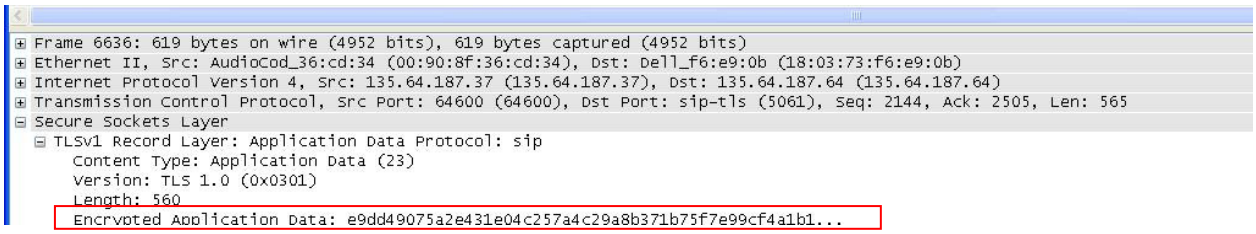
9.1. Confirm AudioCodes Mediant 3000 successfully completing a TLS Handshake

Using an Ethernet packet capture application (e.g., Wireshark or similar), monitor communications between AudioCodes and Session Manager by either using an Ethernet hub to insert a tap point or else using port mirroring on an Ethernet switch.

Activate packet capturing on Wireshark and then perform a reset on M3K using the procedure at the end of **Section 8.1**. On restart, M3K will negotiate TLS, the procedure can be observed by examining the packets sent between M3K and Session Manager.



Select a packet to view the contents. Confirm the payload is Encrypted Application Data.



9.2. Place a Telephone Call from the PSTN to a Avaya Aura® Communication Manager Station

Logon to Avaya Aura® Session Manager using a SSH client and the craft account. At the command line, enter the following command:

traceSM –uni –dt (hit the enter key)

Using a PSTN phone, place a call to a Communication Manager station from a PSTN phone. Observe the incoming call on the SIP trace. Confirm the call is using **SIPS** and the **SDP** contains information on cryptographic options.

Answer the call, confirm there is two-way speech.

Logon to Avaya Aura® Communication Manager using the SAT interface (craft account) and enter the following command:

status trunk x (where x is the SIP trunk between Communication Manager and Session Manager). Page through the screens until the active trunk member is located. In the example below, member **0002/032** is active.

```
status trunk 2                                                          Page   3

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0002/029 T00035   in-service/idle    no
0002/030 T00036   in-service/idle    no
0002/031 T00037   in-service/idle    no
0002/032 T00038   in-service/active  no   T00050
```

Issue the command **status trunk 0002/032** and scroll to **Page 3**. Observe the SRTP encryption scheme is use, it should be as configured in **Section 5.2**.

```
status trunk 0002/032                                          Page   3 of   3
                       SRC PORT TO DEST PORT TALKPATH
src port: T00038
T00038:TX:192.168.187.37:35010/g711u/20ms/1-srtp-aescm128-hmac80
T00050:RX: 192.168.187.120:37118/g711u/20ms/1-srtp-aescm128-hmac80
```

10. Conclusion

These Application Notes describe the configuration of AudioCodes Mediant 3000 Media Gateway 3.0 to use TLS and SRTP when communicating with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. The use of TLS significantly increases the signaling security and SRTP confirms the integrity of the voice channel. AudioCodes Mediant 3000 Media Gateway 3.0 provides bi-directional PSTN to SIP translation. One minor issue was found with AudioCodes private key generation, see description in **Section 2.2** for details.

11. Additional References

Avaya Product documentation relevant to these Application Notes is available at http://support.avaya.com.

[1] Administrating Avaya Aura® System Manager, Release 6.3, Issue 2, may 2013

[2] Administering Avaya Aura® Session Manager, Release 6.3 Issue 2, May 2013

[3] Avaya Aura® 6.2 Feature Pack 2 System Manager Release 6.3.2 Security Guide, Release 6.3.2, Issue 0.1, May, 2013

[4] Security Design in Avaya Aura® Session Manager, Release 6.3, October 2013

[5] Application Notes - Configuring Avaya Aura® System Manager 6.2 FP2 and Avaya Aura® Session Manager 6.2 FP2 to use Third-Party Security Certificates for Transport Layer Security

[6] Application Notes - Configuring SIP Trunks in a High Availability network configuration among Avaya Aura® Session Manager 6.2 FP2, AudioCodes Mediant 3000 Media Gateway 3.0 and Avaya Aura® Communication Manager 6.2 FP2

[7] Configuring Avaya Aura® Communication Manager 6.3 and Avaya Utility Services 6.3 using Third-Party Certificates

[8] Configuring Avaya Aura®Messaging 6.2 Service Pack 2 for Transport Layer Security (TLS) and Secure Real-Time Transport Protocol(SRTP) with Third-Party Certificates

[9] AudioCodes Mediant 3000 Interoperability Configuration Guides & Scenario Files on http://www.audiocodes.com

[10] Microsoft Technet on http://technet.microsoft.com

[11] RFC 5246 - The Transport Layer Security (TLS) Protocol
- available from http://www.ietf.org/

[12] RFC 3711 - The Secure Real-time Transport Protocol (SRTP)
- available from http://www.ietf.org/

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com