Configuring Certificates

For AudioCodes MediaPack™ Series

This document describes how to configure certificates on the AudioCodes MediaPack Series VoIP Analog Gateways to enable secured management (HTTPS).

The procedure below describes how to exchange a certificate with the AudioCodes Certificate Authority (CA). The certificate is used by the MediaPack device to authenticate the connection in secured mode using HTTPS.

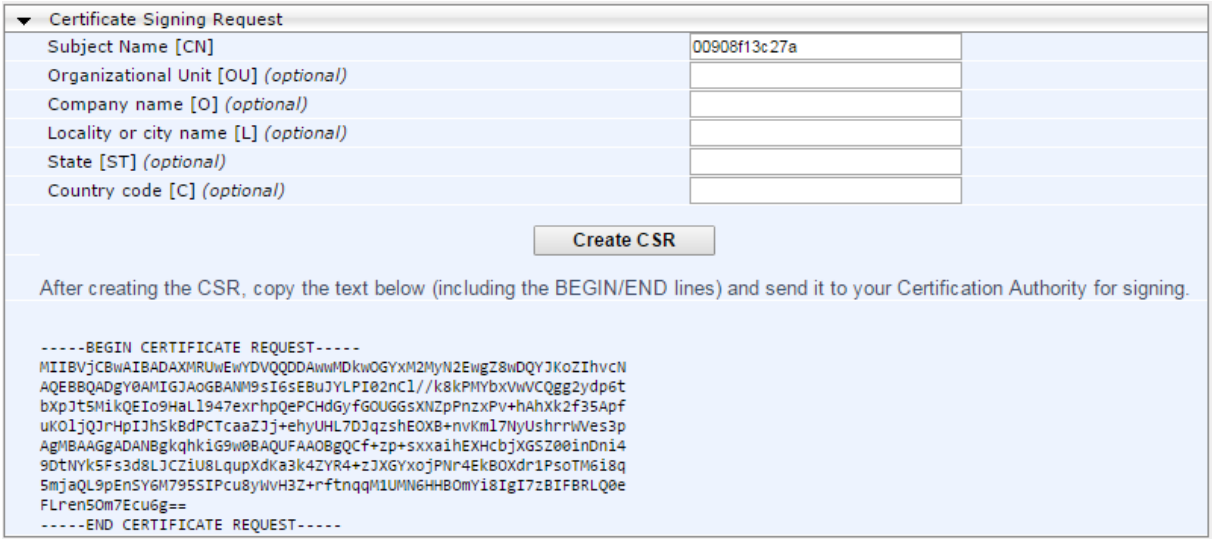
The procedure involves the following main steps:

1. Generating a Certificate Signing Request (CSR)
2. Requesting to sign Device Certificate by AudioCodes CA
3. Obtaining Trusted Root Certificate from AudioCodes CA
4. Deploying Device and Trusted Root Certificates on the MediaPack

To configure a certificate on <u>MP-1xx devices</u>:

1. Open the Certificates page (**Configuration** tab > **System** > **Certificates**).

Figure 1: Certificates Page - Creating CSR



2. In the 'Subject Name' field, enter the MediaPack's MAC address (e.g., **00908f13c27a**).
3. Click **Create CSR**; a certificate request is generated.

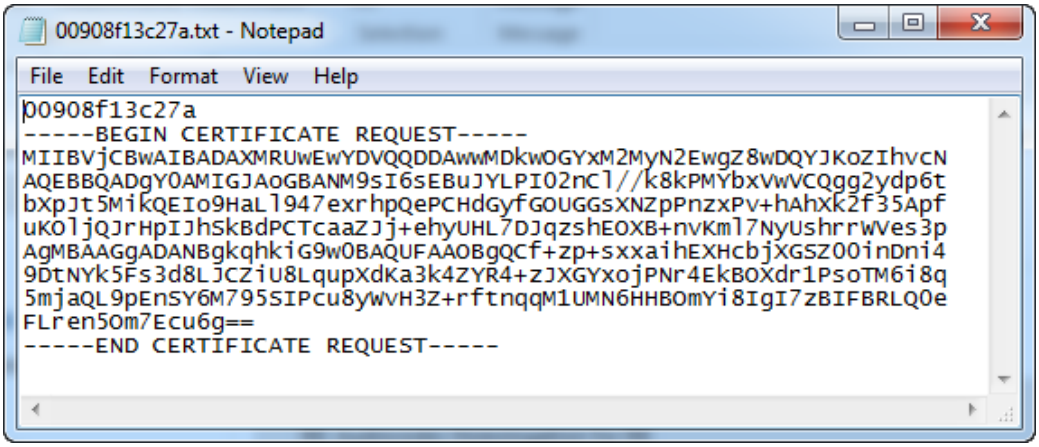
AudioCodes Inc.
200 Cottontail Lane, Suite A101E
Somerset, NJ 08873
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
1 Hayarden Street, Airport City, Lod 7019900
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

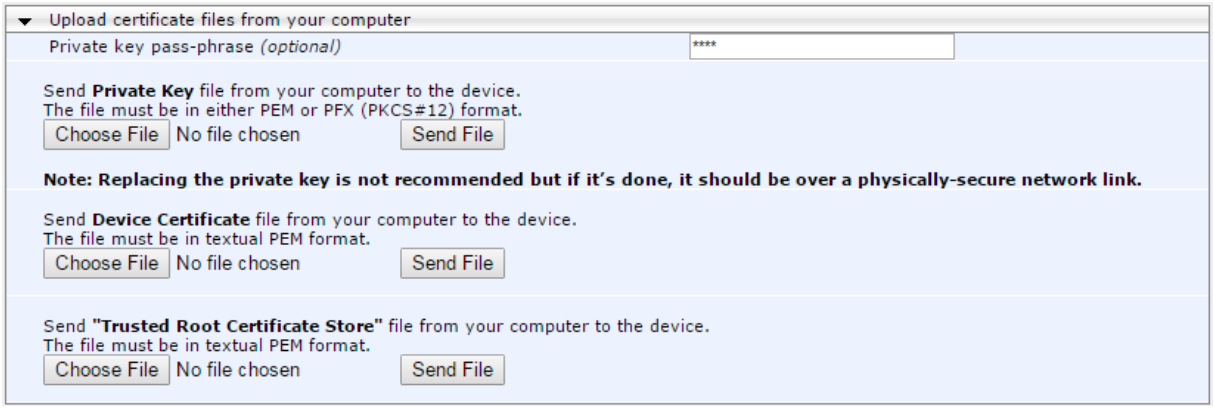
4. Copy the CSR from the line **"----BEGIN CERTIFICATE"** to **"----END CERTIFICATE REQUEST----"** to a text file (such as Notepad).
5. Enter the MediaPack's MAC address on the first line of the text file and then save the file to a folder on your computer with the file name <MediaPack MAC>.txt (e.g., *00908f13c27a.txt*).

Figure 2: Certificate Request (CSR) Text File



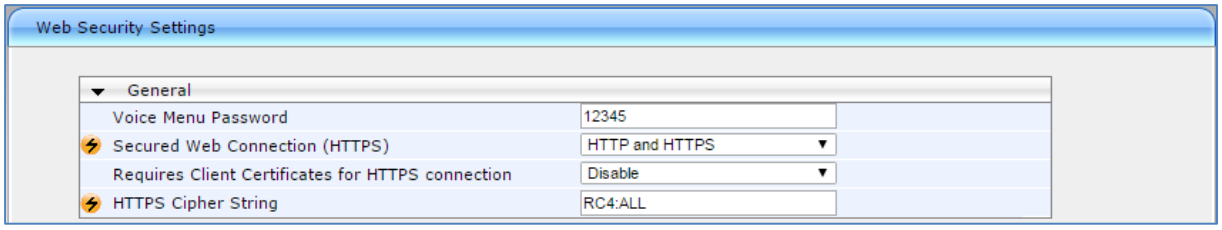
6. Send the saved CSR (*00908f13c27a.txt* file) to the AudioCodes Certificate Authority (CA) Administrator for signing.
7. You will receive a zip file from the AudioCodes Certificate Authority Administrator, containing two files: the signed certificate (in our example, *00908f13c27a.crt*) and the root certificate (*trust.pem*). Save these files to a folder on your computer.
8. In the MediaPack's Web interface, return to the Certificates page (see Step 1), scroll down to the 'Upload certificate files from your computer' group, and then do the following:
   a. In the 'Send Device Certificate file...' field, click **Choose File**, and then select the *00908f13c27a.crt* certificate file that you saved on your computer in Step 7.
   b. Click **Send File** to upload the certificate to the MediaPack.
   c. Confirm that the file was successfully loaded to the device.
   d. In the 'Send Trusted Root Certificate Store file…' field, click **Choose File**, and then select the *trust.pem* certificate file that you saved on your computer in Step 7.
   e. Click **Send File** to upload the certificate to the MediaPack.
   f. Confirm that the file was successfully loaded to the device.

Figure 3: Certificates Page (Uploading Certificate)



9. To avoid connectivity issues of the different browsers, it is recommended to change the default value of the 'HTTPS Cipher String' parameter to **RC4:ALL**:
   a. Open the Web Security Settings page (**Configuration** tab > **System** > **Management** > **WEB Security Settings**).
   b. Change the value of the 'HTTPS Cipher String' parameter to **RC4:ALL**.

Figure 4: HTTPS Cipher String

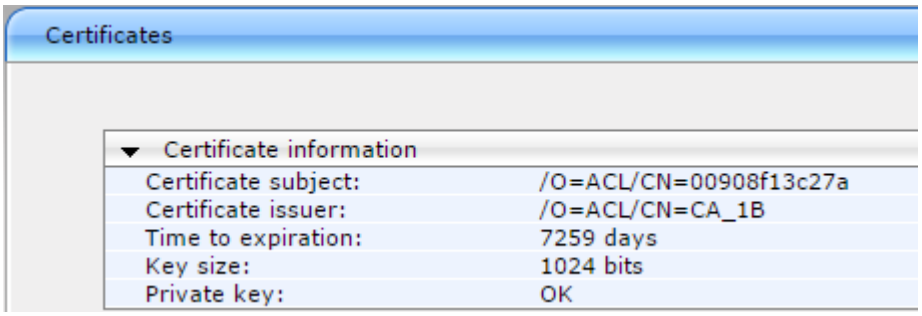


10. Reset the MediaPack device with a burn to flash for your settings to take effect.

To verify that an MP-1xx device has the correct signed certificate:

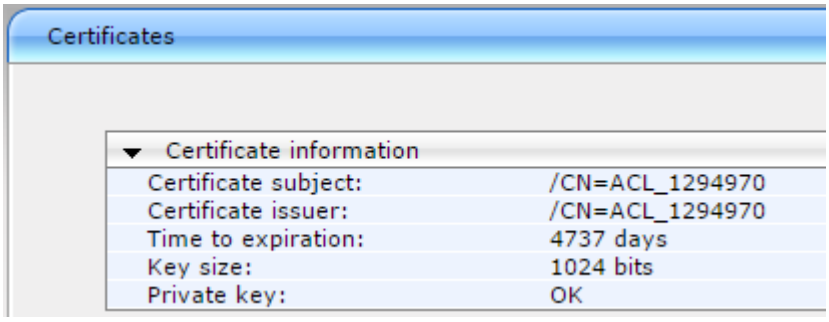
1. Open the Certificates page (**Configuration** tab > **System** > **Certificates**).
2. In the 'Certificate information' group, check that the certificate values are correct:
   - 'Certificate subject' should be equal to the device's MAC address **only**
   - 'Certificate issuer' should be different than the Certificate subject
   - 'Time to expiration' and 'Key size' values are per requirements
   - 'Private key' status value is **OK**

Figure 5: Certificates Page – Example of the Correct Signed Certificate Information



If the values of the Certificate subject and Certificate issuer are identical and the format is ACL_<Serial Number> (which indicates that the device is loaded with the default, self-signed certificate), the device does **not** include a signed certificate by AudioCodes.

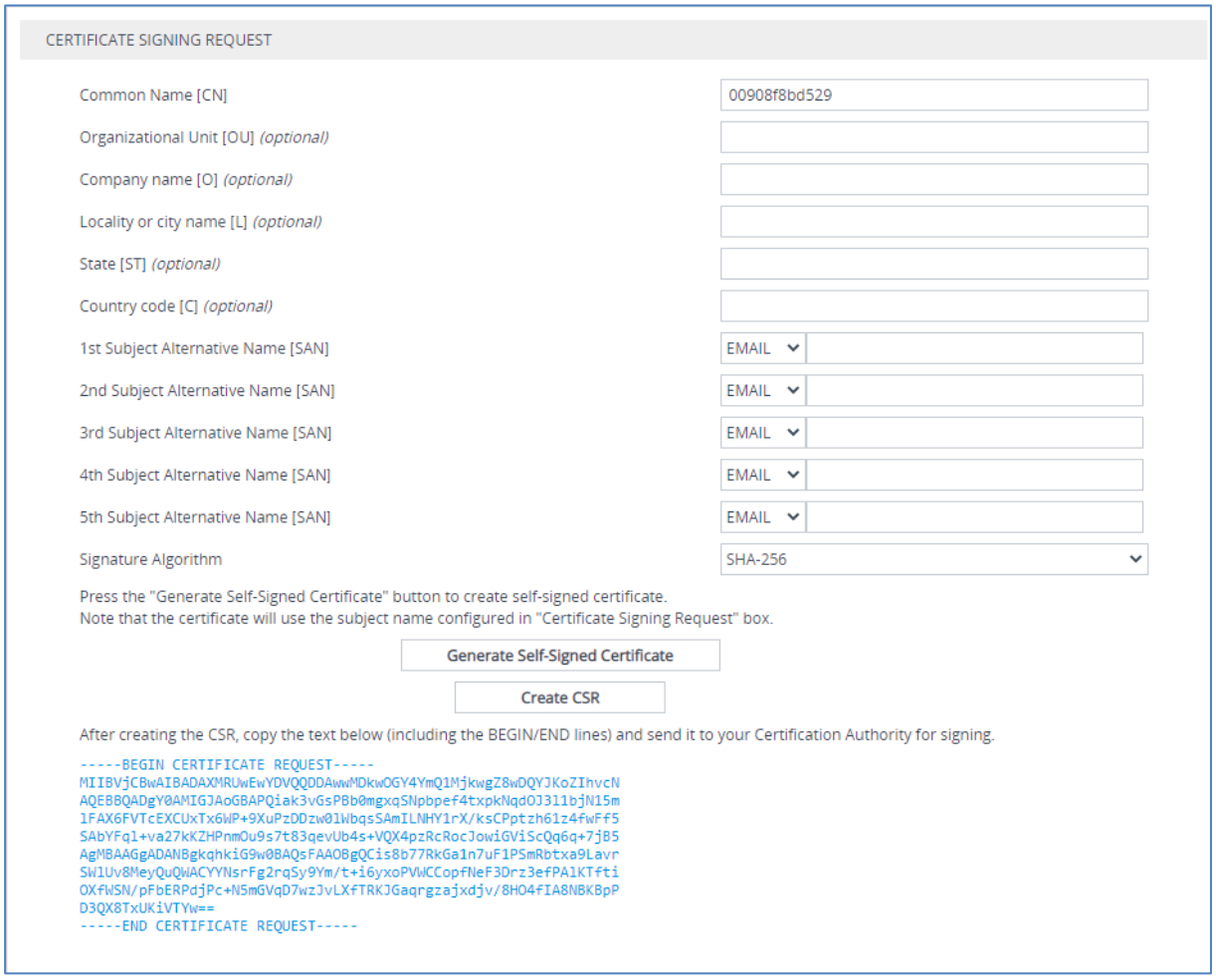
Figure 6: Certificates Page – Example of the Default Certificate Information



To configure a certificate on MP-1288 devices:

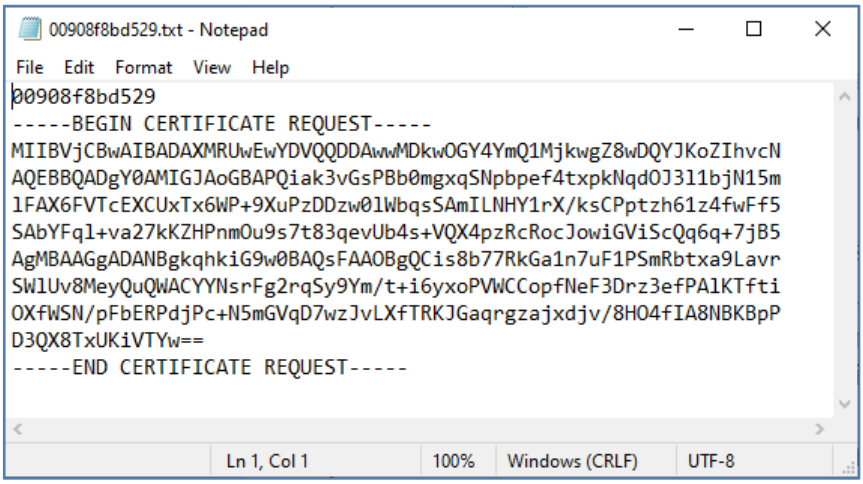
1. Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. On the TLS Contexts page, select the default TLS Context index (0) row, and click the **Change Certificate** link located below the table; the Context Certificates page appears.

Figure 7: Certificates Page - Creating CSR



3. In the 'Common Name' field, enter the MP-1288's MAC address (e.g., **00908f8bd529**).
4. Click **Create CSR**; a certificate request is generated.
5. Copy the CSR text (from **"----BEGIN CERTIFICATE"** to **"----END CERTIFICATE REQUEST-----"** to a text file (such as Notepad).
6. Enter the MP-1288's MAC address on the first line of the text file, and then save the file to a folder on your computer with the file name <MediaPack MAC>.txt (e.g., *00908f8bd529.txt*).

Figure 8: Certificate Request (CSR) Text File

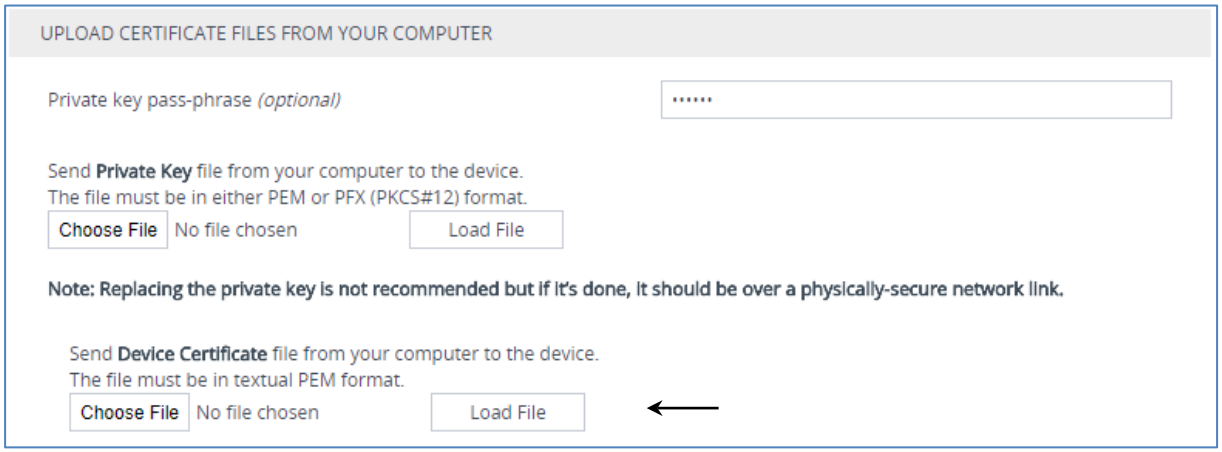


7. Send the saved CSR (*00908f8bd529.txt* file) to the AudioCodes Certificate Authority (CA) Administrator for signing.

   You will receive a zip file from the AudioCodes Certificate Authority Administrator, containing two files: the signed certificate (in our example, *00908f8bd529.crt*) and the root certificate (*trust.pem*).

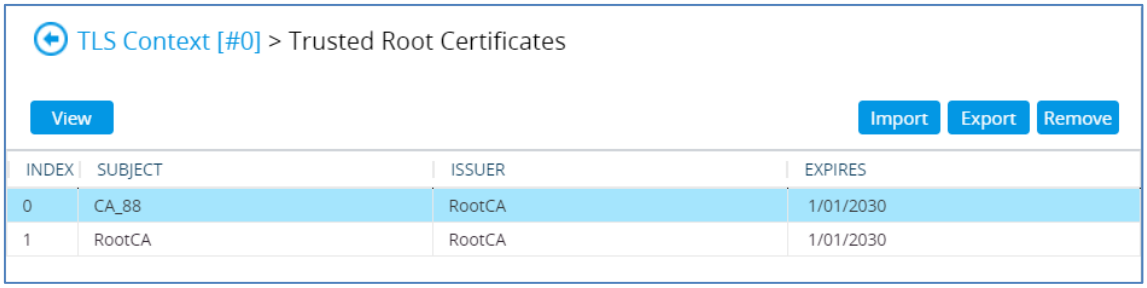
8. Unzip and save the two files to a folder on your computer.
9. On the MP-1288's Web interface, return to the **TLS Contexts** page (see Step 1) and do the following:
   a. In the TLS Contexts page, select the default TLS Context index (0) row and click the **Change Certificate** link located below the table; the Context Certificates page appears.
   b. Scroll down to the Upload certificates files from your computer group.
   c. Click the **Choose File** button corresponding to the '**Send Device Certificate...**' field.
   d. Navigate to the certificate file obtained from the CA (in our example, *00908f8bd529.crt*) and saved on your computer in Step 8 and click **Load File** to upload the certificate to the MP-1288 device.

Figure 9: Uploading the Certificate Obtained from the Certification Authority



10. Confirm that the certificate was uploaded correctly. A message indicating that the certificate was uploaded successfully is displayed in blue in the lower part of the page.
11. On the MP-1288's Web interface, return to the **TLS Contexts** page.
    a. On the TLS Contexts page, select the default TLS Context index (0) row, and click the Trusted Root **Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
    b. Click the **Import** button, and then select the *trust.pem* certificate file saved on your computer in Step 8.
12. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store:

Figure 10: Example of Configured Trusted Root Certificates



To check that the MP-1288 device has the correct signed certificate:

1. Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the default TLS Context index (0) row, and then click the **Certificate Information** link located at the bottom of the TLS.
3. Validate the certificate **Status** and **Common Name**:

Figure 11: Certificate Information Example