Multi-Service Business Gateways

VoIP Media Gateways

SIP Protocol

Technical Note

Generating a Certificate Signing Request (CSR) using OpenSSL

February 2011

Document # LTRT-30900

Table of Contents

1 Introduction 7
2 Generating the Private Key 9

List of Figures

Figure 1-1: Generated CSR by AudioCodes Device 7
Figure 2-1: OpenSSL CSR Generation Script 9
Figure 2-2: Open SSL Generated CSR Ouput 10
Figure 2-3: Loading Private Key to the Gateway 10

Notice

This document describes the procedure for Generating a Certificate Signing Request (CSR) using OpenSSL.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee the accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents as well as software files can be viewed by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

Date Published: February-22-2011

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and service are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@audiocodes.com.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Reader's Notes

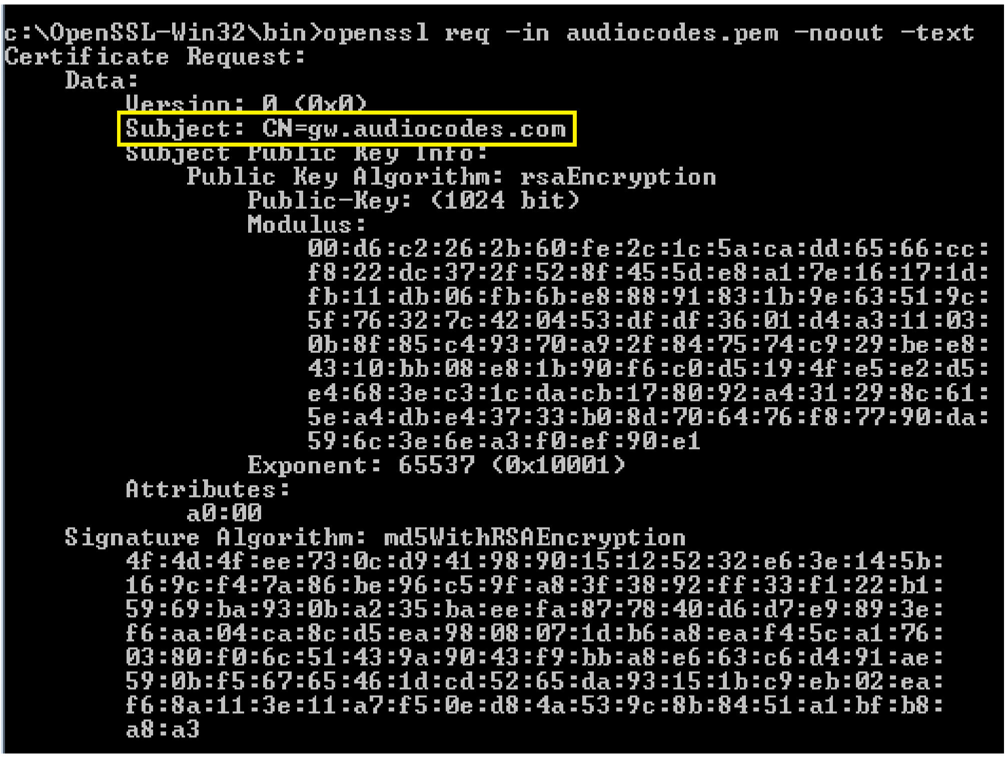
1 Introduction

The objective of this document is to describe how to generate a certificate signing request (CSR) and Private Key, using OpenSSL.

The procedure for generating a CSR for creating a server certificate as described in the relevant AudioCodes gateway (hereafter referred to as *device*) *User's Manual* is in most cases, sufficient. Typically, companies use their internal certificate server (e.g., Microsoft ‘certsrv’) to sign and generate a CSR.

In scenarios where the user decides to use a third-party CA to sign and create the certificate, the CSR generated by AudioCodes device alone may contain insufficient information to warrant a “valid” certificate. AudioCodes device generates only a CSR containing the “Common Name” attribute, as shown in the figure below.

Figure 1-1: Generated CSR by AudioCodes Device



```
c:\OpenSSL-Win32\bin>openssl req -in audiocodes.pem -noout -text
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: CN=gw.audiocodes.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:d6:c2:26:2b:60:fe:2c:1c:5a:ca:dd:65:66:cc:
                    f8:22:dc:37:2f:52:8f:45:5d:e8:a1:7e:16:17:1d:
                    fb:11:db:06:fb:6b:e8:88:91:83:1b:9e:63:51:9c:
                    5f:76:32:7c:42:04:53:df:df:36:01:d4:a3:11:03:
                    0b:8f:85:c4:93:70:a9:2f:84:75:74:c9:29:be:e8:
                    43:10:bb:08:e8:1b:90:f6:c0:d5:19:4f:e5:e2:d5:
                    e4:68:3e:c3:1c:da:cb:17:80:92:a4:31:29:8c:61:
                    5e:a4:db:e4:37:33:b0:8d:70:64:76:f8:77:90:da:
                    59:6c:3e:6e:a3:f0:ef:90:e1
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: md5WithRSAEncryption
        4f:4d:4f:ee:73:0c:d9:41:98:90:15:12:52:32:e6:3e:14:5b:
        16:9c:f4:7a:86:be:96:c5:9f:a8:3f:38:92:ff:33:f1:22:b1:
        59:69:ba:93:0b:a2:35:ba:ee:fa:87:78:40:d6:d7:e9:89:3e:
        f6:aa:04:ca:8c:d5:ea:98:08:07:1d:b6:a8:ea:f4:5c:a1:76:
        03:80:f0:6c:51:43:9a:90:43:f9:bb:a8:e6:63:c6:d4:91:ae:
        59:0b:f5:67:65:46:1d:cd:52:65:da:93:15:1b:c9:eb:02:ea:
        f6:8a:11:3e:11:a7:f5:0e:d8:4a:53:9c:8b:84:51:a1:bf:b8:
        a8:a3
```

Therefore, in such cases, you can use the freely available software, OpenSSL (http://www.openssl.org/) to generate a new private key and CSR. The generated private key and CSR contains additional details that are suitable for third-party verification.

Reader's Notes

2 Generating the Private Key

To generate the private key using OpenSSL, follow the procedure below.

➢ To generate a new private key and CSR, using OpenSSL:

1. Specify the following command to create a new private key and CSR at the same time:

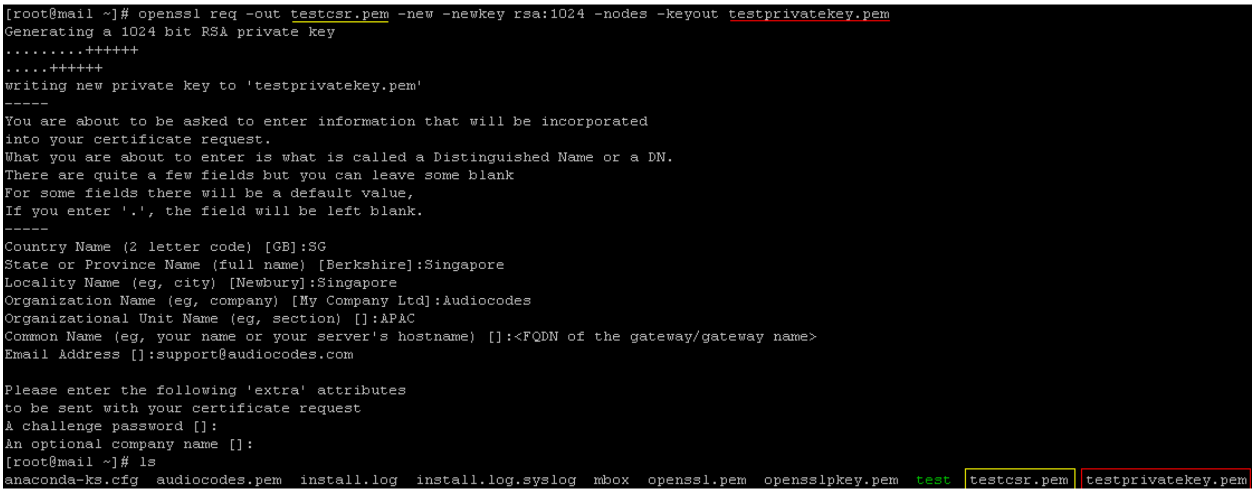
```
openssl req -out <csr filename> -new -newkey rsa:1024 -nodes -
keyout <private key filename>
```

where:

- *<csr filename>* contains the CSR data for certificate generation
- *<private key filename>* is the private key that later needs to be loaded to the device (see Figure 2-3).

When the above command is run, a series of prompts are displayed requesting you to input the appropriate values for the CSR. The values can be arbitrarily chosen, except for the “Common Name”, which is the FQDN of AudioCodes device or the configured AudioCodes gateway name. The RSA encryption used by AudioCodes device by default is ‘1024’ bits; however, using the OpenSSL utility, you can specify ‘2048’ bits. An example script generation is shown in the figure below.

Figure 2-1: OpenSSL CSR Generation Script

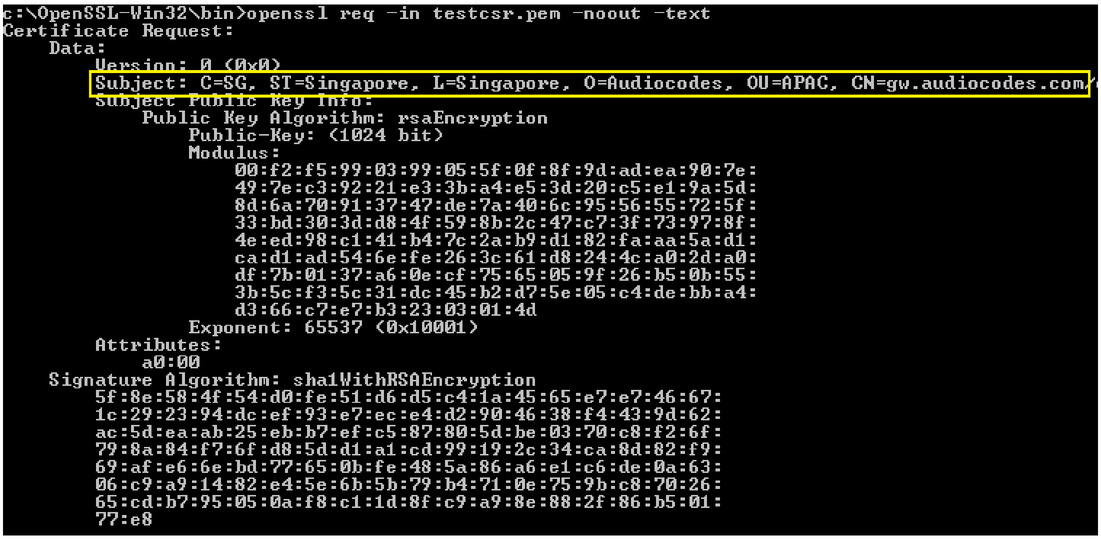


```
[root@mail ~]# openssl req -out testcsr.pem -new -newkey rsa:1024 -nodes -keyout testprivatekey.pem
Generating a 1024 bit RSA private key
.........++++++
.....++++++
writing new private key to 'testprivatekey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:SG
State or Province Name (full name) [Berkshire]:Singapore
Locality Name (eg, city) [Newbury]:Singapore
Organization Name (eg, company) [My Company Ltd]:Audiocodes
Organizational Unit Name (eg, section) []:APAC
Common Name (eg, your name or your server's hostname) []:<FQDN of the gateway/gateway name>
Email Address []:support@audiocodes.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@mail ~]# ls
anaconda-ks.cfg  audiocodes.pem  install.log  install.log.syslog  mbox  openssl.pem  opensslpkey.pem  test  testcsr.pem  testprivatekey.pem
```

The generated CSR using the OpenSSL utility includes additional information such as country, location, organization, etc., as shown in the figure below.

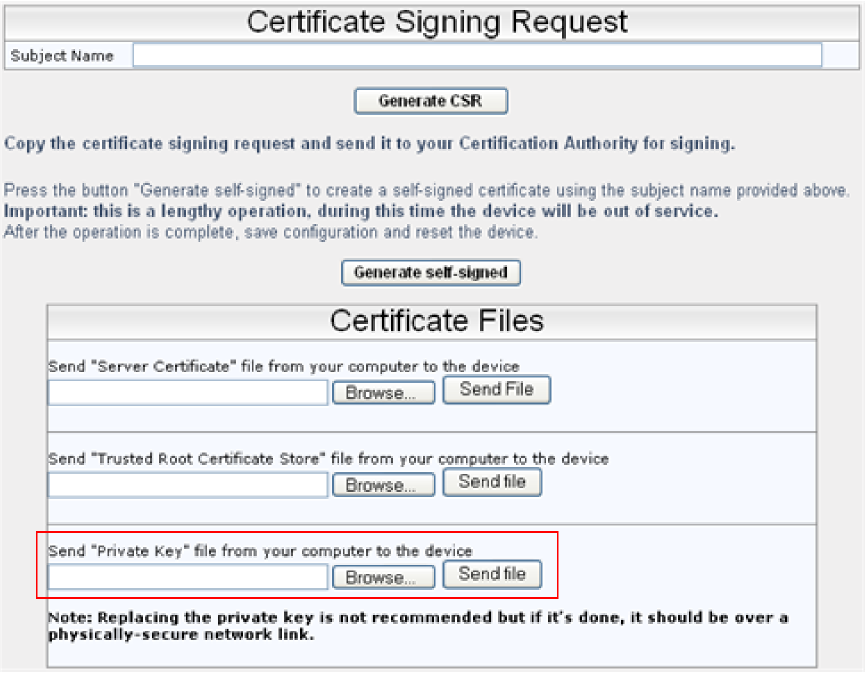
Figure 2-2: Open SSL Generated CSR Ouput



```
c:\OpenSSL-Win32\bin>openssl req -in testcsr.pem -noout -text
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=SG, ST=Singapore, L=Singapore, O=Audiocodes, OU=APAC, CN=gw.audiocodes.com/
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:f2:f5:99:03:99:05:5f:0f:8f:9d:ad:ea:90:7e:
                    49:7e:c3:92:21:e3:3b:a4:e5:3d:20:c5:e1:9a:5d:
                    8d:6a:70:91:37:47:de:7a:40:6c:95:56:55:72:5f:
                    33:bd:30:3d:d8:4f:59:8b:2c:47:c7:3f:73:97:8f:
                    4e:ed:98:c1:41:b4:7c:2a:b9:d1:82:fa:aa:5a:d1:
                    ca:d1:ad:54:6e:fe:26:3c:61:d8:24:4c:a0:2d:a0:
                    df:7b:01:37:a6:0e:cf:75:65:05:9f:26:b5:0b:55:
                    3b:5c:f3:5c:31:dc:45:b2:d7:5e:05:c4:de:bb:a4:
                    d3:66:c7:e7:b3:23:03:01:4d
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
        5f:8e:58:4f:54:d0:fe:51:d6:d5:c4:1a:45:65:e7:e7:46:67:
        1c:29:23:94:dc:ef:93:e7:ec:e4:d2:90:46:38:f4:43:9d:62:
        ac:5d:ea:ab:25:eb:b7:ef:c5:87:80:5d:be:03:70:c8:f2:6f:
        79:8a:84:f7:6f:d8:5d:d1:a1:cd:99:19:2c:34:ca:8d:82:f9:
        69:af:e6:6e:bd:77:65:0b:fe:48:5a:86:a6:e1:c6:de:0a:63:
        06:c9:a9:14:82:e4:5e:6b:5b:79:b4:71:0e:75:9b:c8:70:26:
        65:cd:b7:95:05:0a:f8:c1:1d:8f:c9:a9:8e:88:2f:86:b5:01:
        77:e8
```

2. Load the generated private key to AudioCodes device:
   a. Open the 'Certificates Signing Request' page (**Configuration** tab > **System** menu > **Certificates**).
   b. Under the 'Send Private Key File…' group, click the **Browse** button and navigate to select the file.
   c. Click **Send File** to load the private key.

Figure 2-3: Loading Private Key to the Gateway



Certificate Signing Request

Subject Name

Generate CSR

Copy the certificate signing request and send it to your Certification Authority for signing.

Press the button "Generate self-signed" to create a self-signed certificate using the subject name provided above.
Important: this is a lengthy operation, during this time the device will be out of service.
After the operation is complete, save configuration and reset the device.

Generate self-signed

Certificate Files

Send "Server Certificate" file from your computer to the device

Browse... Send File

Send "Trusted Root Certificate Store" file from your computer to the device

Browse... Send file

Send "Private Key" file from your computer to the device

Browse... Send file

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

3. Save your changes and restart AudioCodes device.

For more information, refer to the relevant product *User's Manual*.

Reader's Notes

Technical Note

www.audiocodes.com