为CMS配置CSR，使用OpenSSL进行加密

目录

简介

本文档介绍如何为具有开放式安全套接字层(OpenSSL)的思科会议服务器(CMS)创建证书。

作者：思科TAC工程师Moises Martinez。

先决条件

Cisco 建议您了解以下主题：

- 打开SSL。
- CMS配置。

使用的组件

本文档中的信息基于以下软件：

- OpenSSL Light 1.1

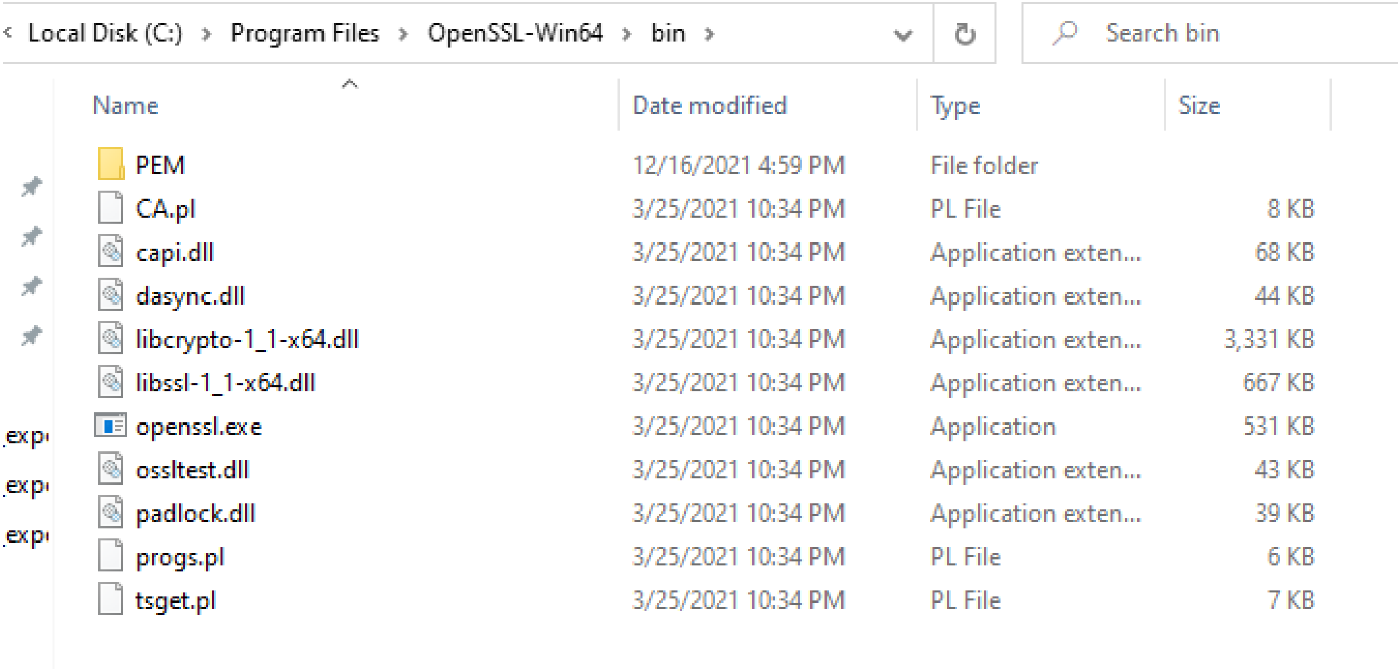
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

步骤1.下载OpenSSL Light 1.1。

步骤2.在计算机中安装OpenSSL。

步骤3.导航至安装SSL的文件夹。通常安装在C:\Program Files\OpenSSL-Win64\bin上。

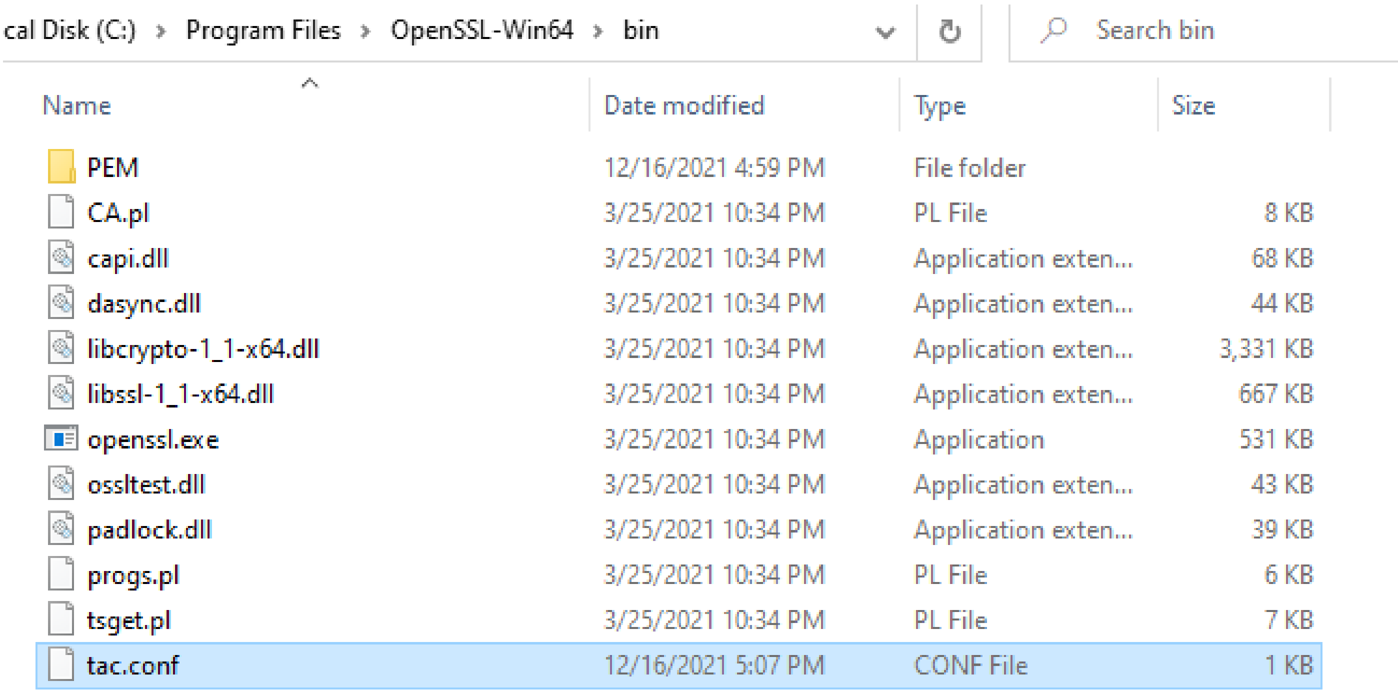


Name	Date modified	Type	Size
PEM	12/16/2021 4:59 PM	File folder	
CA.pl	3/25/2021 10:34 PM	PL File	8 KB
capi.dll	3/25/2021 10:34 PM	Application exten...	68 KB
dasync.dll	3/25/2021 10:34 PM	Application exten...	44 KB
libcrypto-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	3,331 KB
libssl-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	667 KB
openssl.exe	3/25/2021 10:34 PM	Application	531 KB
ossltest.dll	3/25/2021 10:34 PM	Application exten...	43 KB
padlock.dll	3/25/2021 10:34 PM	Application exten...	39 KB
progs.pl	3/25/2021 10:34 PM	PL File	6 KB
tsget.pl	3/25/2021 10:34 PM	PL File	7 KB

步骤4.打开记事**本**并输入证书签名请求(CSR)所需的信息，如下例所示：

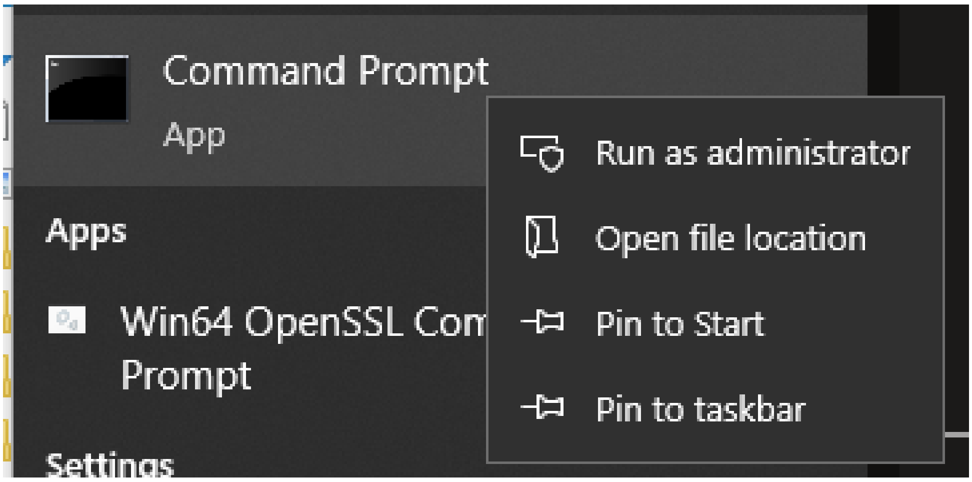
```
[req] distinguished_name = req_distinguished_name req_extensions = v3_req prompt = no
[req_distinguished_name] C = US ST = California L = San Jose O = TAC OU = IT CN =
cms.tac.cisco.com [v3_req] extendedKeyUsage = serverAuth, clientAuth subjectAltName = @alt_names
[alt_names] DNS.1 = webbridge3.tac.cisco.com DNS.2 = webadmin.tac.cisco.com DNS.3 =
xmpp.tac.cisco.com
```

步骤5.为CSR输入信息后，此文件将保存为**tac.conf**，位于下一路径：**C:\Program Files\OpenSSL-Win64\bin**。

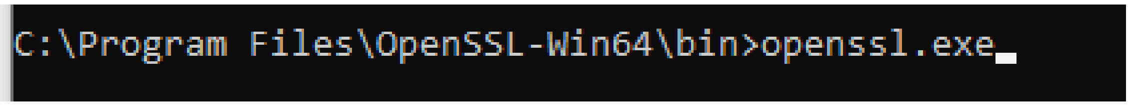


Name	Date modified	Type	Size
PEM	12/16/2021 4:59 PM	File folder	
CA.pl	3/25/2021 10:34 PM	PL File	8 KB
capi.dll	3/25/2021 10:34 PM	Application exten...	68 KB
dasync.dll	3/25/2021 10:34 PM	Application exten...	44 KB
libcrypto-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	3,331 KB
libssl-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	667 KB
openssl.exe	3/25/2021 10:34 PM	Application	531 KB
ossltest.dll	3/25/2021 10:34 PM	Application exten...	43 KB
padlock.dll	3/25/2021 10:34 PM	Application exten...	39 KB
progs.pl	3/25/2021 10:34 PM	PL File	6 KB
tsget.pl	3/25/2021 10:34 PM	PL File	7 KB
tac.conf	12/16/2021 5:07 PM	CONF File	1 KB

步骤6.在PC上打**开命令**项目，并选择以管理员**身份运行**。

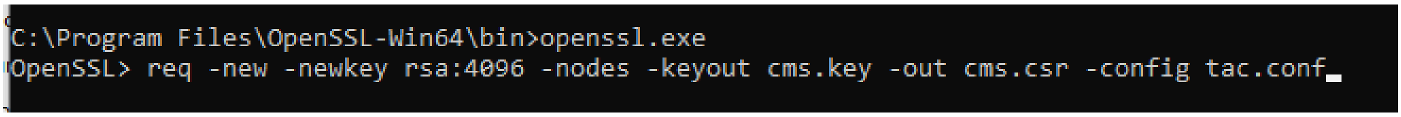


步骤7.导航至通过命令提示符存储文件的路径，输入命令**openssl.exe**并选择enter。

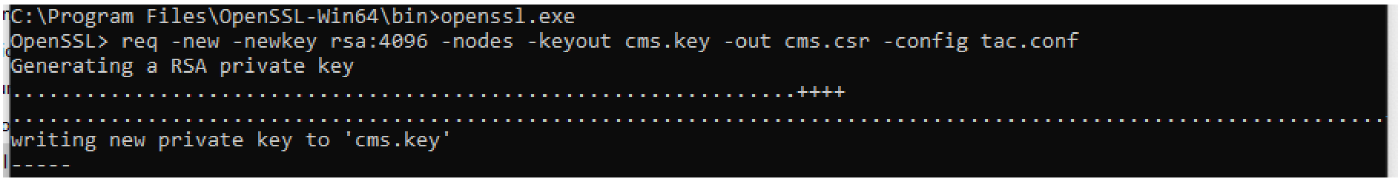


```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
```

步骤8.运行下一个命令：**req -new -newkey rsa:4096 - nodes -keyout cms.key -out cms.csr -config tac.conf**。



```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> req -new -newkey rsa:4096 -nodes -keyout cms.key -out cms.csr -config tac.conf
```

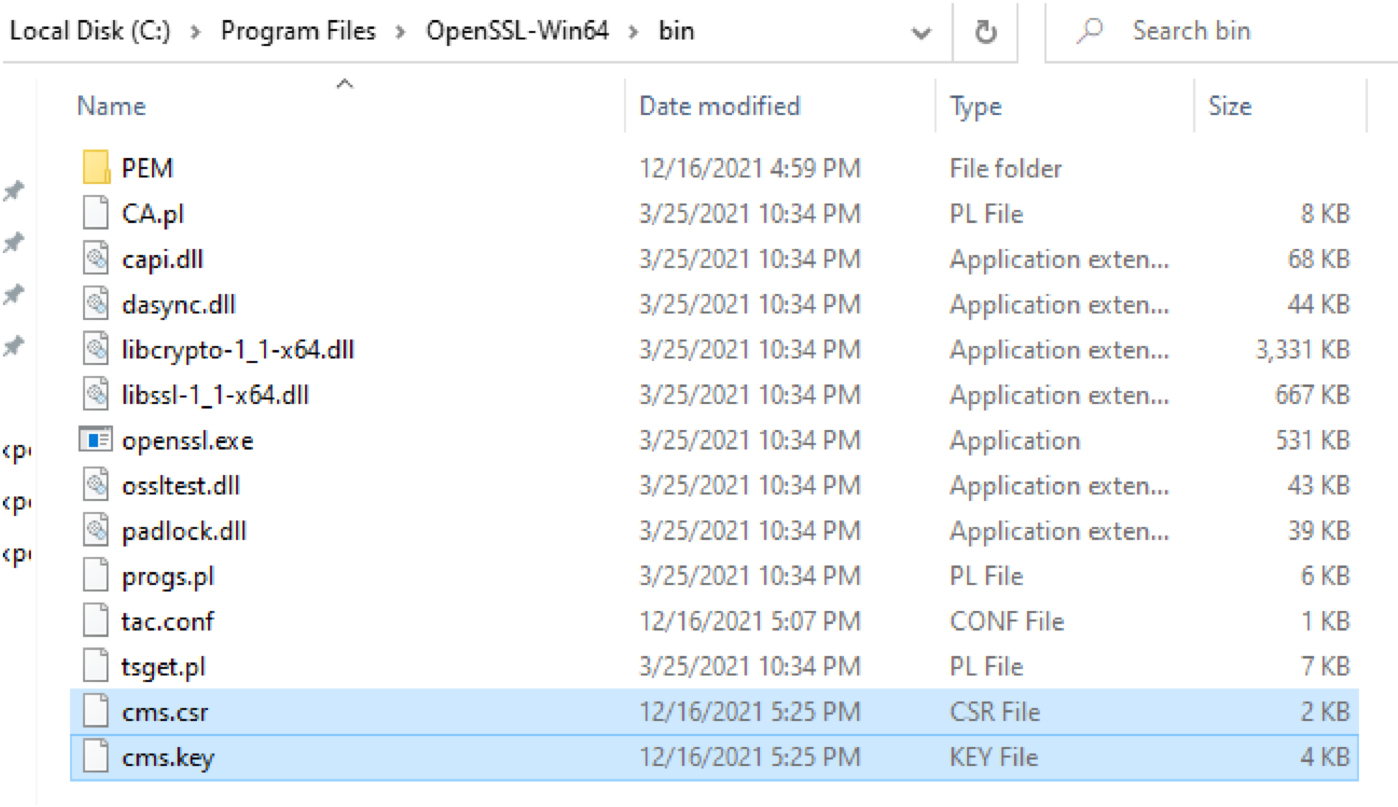


```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> req -new -newkey rsa:4096 -nodes -keyout cms.key -out cms.csr -config tac.conf
Generating a RSA private key
..................................................................++++
...................................................................................................................
writing new private key to 'cms.key'
-----
```

验证

如果未显示任何错误，则会在同一文件夹中生成两个新文件：

- **cms密钥**
- **cms.csr**



Name	Date modified	Type	Size
PEM	12/16/2021 4:59 PM	File folder	
CA.pl	3/25/2021 10:34 PM	PL File	8 KB
capi.dll	3/25/2021 10:34 PM	Application exten...	68 KB
dasync.dll	3/25/2021 10:34 PM	Application exten...	44 KB
libcrypto-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	3,331 KB
libssl-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	667 KB
openssl.exe	3/25/2021 10:34 PM	Application	531 KB
ossltest.dll	3/25/2021 10:34 PM	Application exten...	43 KB
padlock.dll	3/25/2021 10:34 PM	Application exten...	39 KB
progs.pl	3/25/2021 10:34 PM	PL File	6 KB
tac.conf	12/16/2021 5:07 PM	CONF File	1 KB
tsget.pl	3/25/2021 10:34 PM	PL File	7 KB
cms.csr	12/16/2021 5:25 PM	CSR File	2 KB
cms.key	12/16/2021 5:25 PM	KEY File	4 KB

此新文件**cms.csr**可由证书颁发机构(CA)签名。