Configurazione di CSR per CMS con OpenSSL per la crittografia

Sommario

Introduzione

In questo documento viene descritto come creare certificati per Cisco Meeting Server (CMS) con Open Secure Sockets Layer (OpenSSL).

Contributo di Moises Martinez, Cisco TAC Engineer.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Aprire SSL.
- configurazione CMS.

Componenti usati

Le informazioni fornite in questo documento si basano sui seguenti software:

- OpenSSL Light 1.1

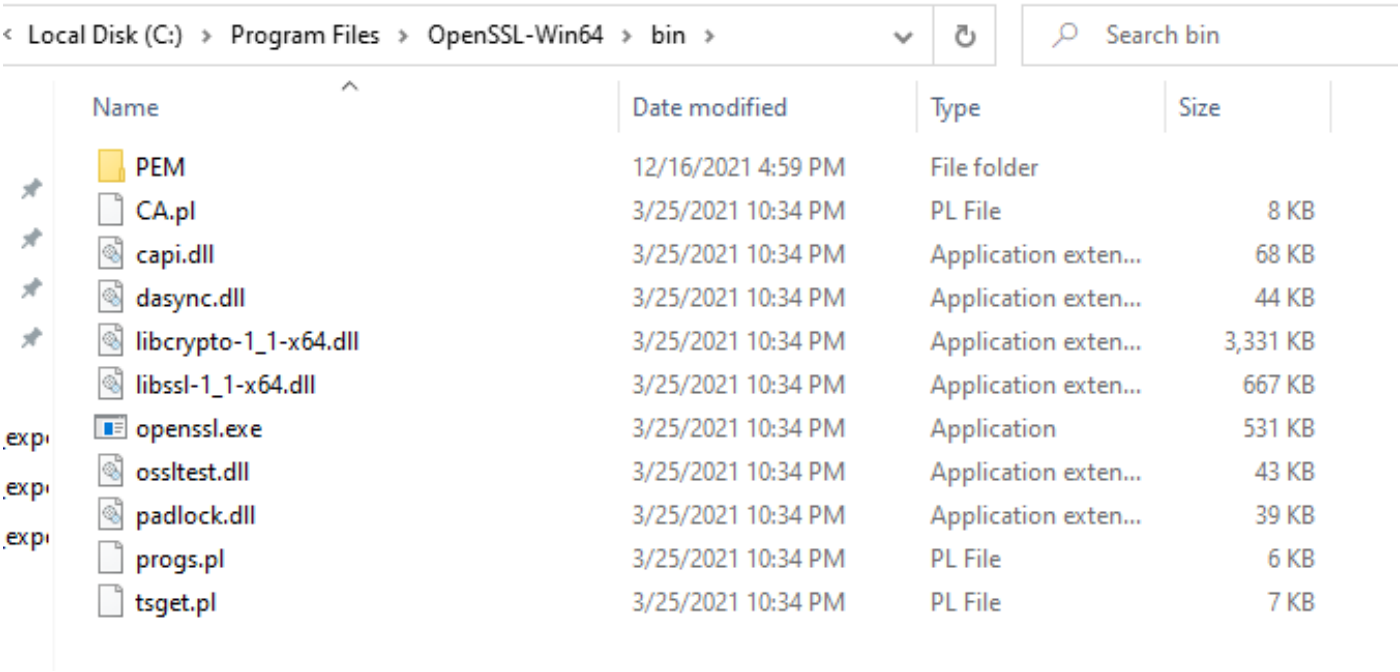
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Passaggio 1. Scaricare OpenSSL Light 1.1.

Passaggio 2. Installare OpenSSL nel computer.

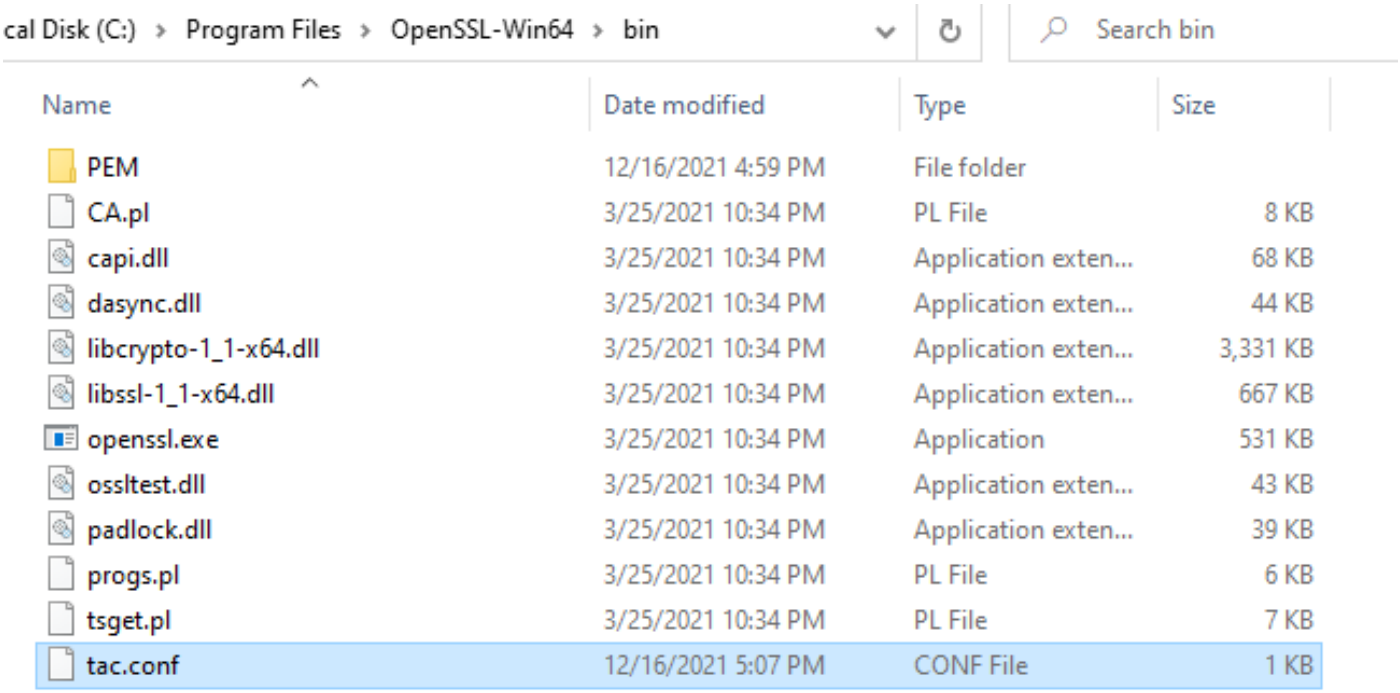
Passaggio 3. Passare alla cartella in cui è stato installato SSL. In genere è installato su **C:\Program Files\OpenSSL-Win64\bin**.



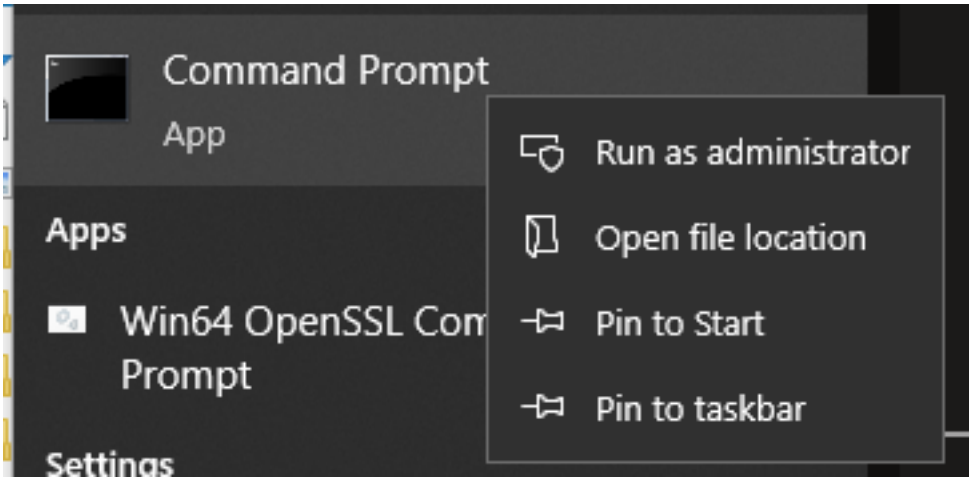
Passaggio 4. Aprire il **Blocco note** e immettere le informazioni necessarie per la richiesta di firma del certificato (CSR), come illustrato nell'esempio seguente:

```
[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
```

Passaggio 5. Dopo aver immesso le informazioni per il CSR, il file viene salvato come **tac.conf** nel percorso successivo: **C:\Program Files\OpenSSL-Win64\bin**.



Passaggio 6. Aprire il **prompt dei comandi** sul PC e selezionare **Esegui come amministratore**.



Passaggio 7. Passare al percorso in cui è memorizzato il file al prompt dei comandi, immettere il comando **openssl.exe** e selezionare invio.

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

Passaggio 8. Eseguire il comando successivo: **req -new -newkey rsa:4096 - nodes -keyout cms.key -out cms.csr -config tac.conf**.

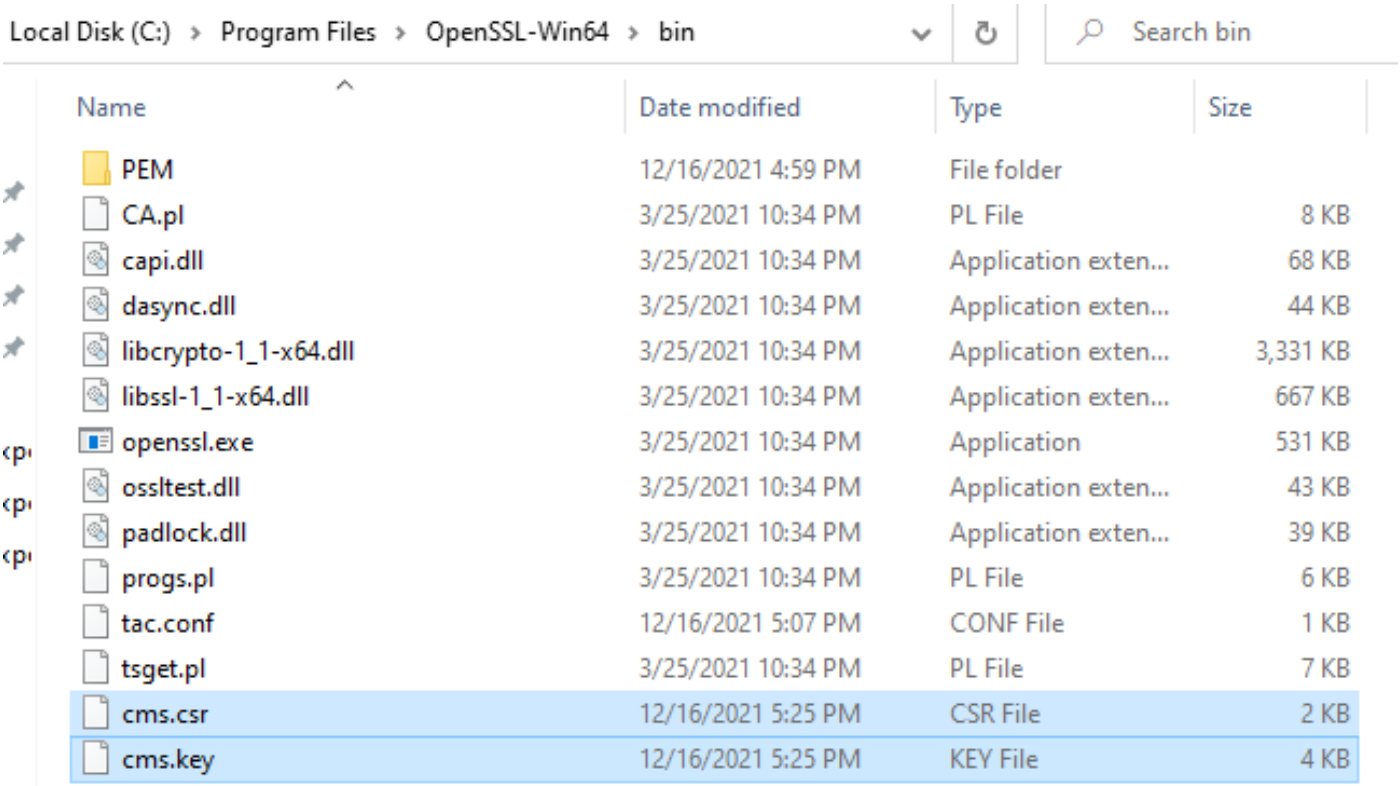
```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> req -new -newkey rsa:4096 -nodes -keyout cms.key -out cms.csr -config tac.conf
```

```
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'
-----
```

Verifica

Se non vengono visualizzati errori, nella stessa cartella vengono generati due nuovi file:

- **chiave.cms**
- **cms.csr**



Il nuovo file **cms.csr** può essere firmato da un'Autorità di certificazione (CA).