

CSR für CMS mit OpenSSL für Verschlüsselung konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Zertifikate für Cisco Meeting Server (CMS) mit Open Secure Sockets Layer (OpenSSL) erstellt werden.

Mitwirkend von Moises Martinez, Cisco TAC Engineer.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Öffnen Sie SSL.
- CMS-Konfiguration.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der folgenden Software:

- OpenSSL Light 1.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Schritt 1: Laden Sie OpenSSL Light 1.1 herunter.

Schritt 2: Installieren Sie OpenSSL auf Ihrem Computer.

Schritt 3: Navigieren Sie zu dem Ordner, in dem SSL installiert wurde. Normalerweise wird es auf `C:\Program Files\OpenSSL-Win64\bin` installiert.

< Local Disk (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

Schritt 4: Öffnen Sie den **Editor**, und geben Sie die für die Zertifikatsanforderung (Certificate Signing Request, CSR) erforderlichen Informationen ein, wie im folgenden Beispiel gezeigt:

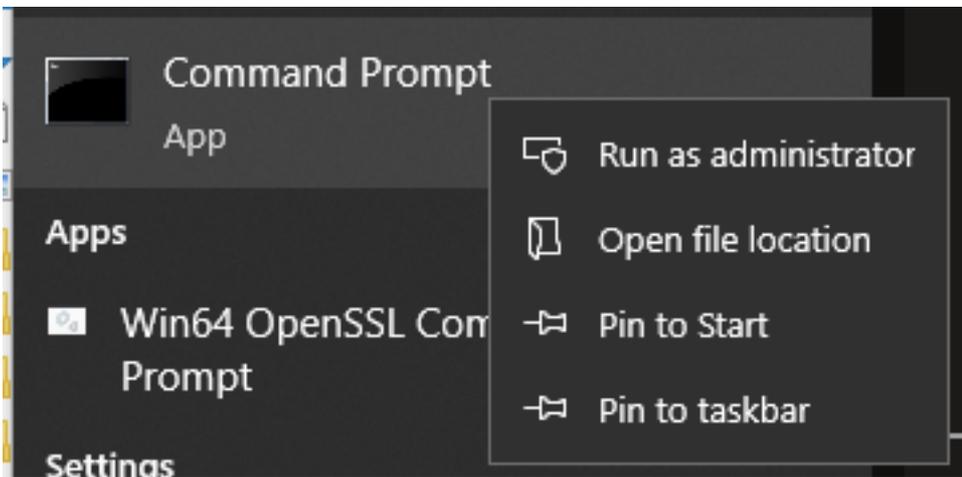
```
[req] distinguished_name = req_distinguished_name req_extensions = v3_req prompt = no
[req_distinguished_name] C = US ST = California L = San Jose O = TAC OU = IT CN =
cms.tac.cisco.com [v3_req] extendedKeyUsage = serverAuth, clientAuth subjectAltName = @alt_names
[alt_names] DNS.1 = webbridge3.tac.cisco.com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

Schritt 5: Sobald die Informationen für den CSR eingegeben wurden, wird diese Datei als **tac.conf** im nächsten Pfad gespeichert: **C:\Program Files\OpenSSL-Win64\bin**.

cal Disk (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

Schritt 6: Öffnen Sie die **Eingabeaufforderung** auf dem PC, und wählen Sie **Als Administrator ausführen** aus.



Schritt 7: Navigieren Sie zu dem Pfad, in dem die Datei über die Eingabeaufforderung gespeichert wird, geben Sie command **openssl.exe** ein, und wählen Sie Enter aus.

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

Schritt 8: Führen Sie den folgenden Befehl aus: **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'
-----
```

Überprüfung

Wenn keine Fehler angezeigt werden, werden zwei neue Dateien im gleichen Ordner generiert:

- cms.key
- 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

Diese neue Datei **cms.csr** kann von einer Zertifizierungsstelle (Certificate Authority, CA) signiert werden.