

CSR generieren und Zertifikate auf CMS anwenden

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[CSR erstellen](#)

[Schritt 1: Syntaxstruktur.](#)

[Schritt 2: Generieren Sie callbridge, xmpp, webadmin und webbridge CSR.](#)

[Schritt 3: Generieren Sie den Datenbank-Cluster-CSR, und verwenden Sie die integrierte Zertifizierungsstelle, um sie zu signieren.](#)

[Schritt 4: Überprüfen der signierten Zertifikate](#)

[Schritt 5: Signierte Zertifikate auf Komponenten auf CMS-Servern anwenden.](#)

[Zertifikatvertrauenskettens und Pakete](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine Zertifikatsanforderung (Certificate Signing Request, CSR) generieren und signierte Zertifikate in Cisco Meeting Server (CMS) hochladen.

Voraussetzungen

Anforderungen

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

- Grundkenntnisse des CMS-Servers

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Putty oder ähnliche Software
- CMS 2.9 oder spätere Version

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 möglichen Auswirkungen aller Befehle kennen.

CSR erstellen

Es gibt zwei Möglichkeiten, CSR zu generieren. Eine Möglichkeit besteht darin, den CSR direkt auf dem CMS-Server über die Befehlszeilenschnittstelle (CLI) mit Administratorzugriff zu generieren. Die andere besteht darin, dies mit einer externen Zertifizierungsstelle eines Drittanbieters (Certificate Authority, CA) wie Open SSL zu tun.

In beiden Fällen muss der CSR mit der richtigen Syntax generiert werden, damit die CMS-Dienste ordnungsgemäß funktionieren.

Schritt 1: Syntaxstruktur.

```
pkc csr <key/cert basename> <CN:value> [OU:<value>] [O:<value>] [ST:<-value>] [C:<value>] [subjectAltName:<value>]
```

- <key/cert basename> ist eine Zeichenfolge, die den neuen Schlüssel und den CSR-Namen identifiziert. Es kann alphanumerische Zeichen, Bindestriche oder Unterstriche enthalten. Dies ist ein Pflichtfeld.
- <CN:value> ist der gebräuchliche Name. Hierbei handelt es sich um den vollqualifizierten Domännennamen (FQDN), der den genauen Standort des Servers im Domain Name System (DNS) angibt. Dies ist ein Pflichtfeld.
- [OU:<Wert>] ist der Name der Organisationseinheit oder Abteilung. Beispiele: Support, IT, Techniker, Finanzen. Dies ist ein optionales Feld.
- [O:<Wert>] ist der Name der Organisation oder des Unternehmens. In der Regel der gesetzlich eingetragene Name einer Firma. Dies ist ein optionales Feld.
- [ST:<Wert>] ist die Provinz, Region, Region oder das Bundesland. Zum Beispiel Buckinghamshire California. Dies ist ein optionales Feld.
- [C:<Wert>] ist das Land. Der zweistellige ISO-Code (International Organization for Standardization) für das Land, in dem Ihre Organisation ansässig ist. Beispiel: USA, GB, FR. Dies ist ein optionales Feld.
- [subjectAltName:<Wert>] ist der alternative Name (SAN) des Antragstellers. Ab X509 Version 3 (RFC 2459) ist es SSL-Zertifikaten (Secure Socket Layers) gestattet, mehrere Namen anzugeben, mit denen das Zertifikat übereinstimmen muss. In diesem Feld kann das generierte Zertifikat mehrere Domänen abdecken. Er kann IP-Adressen, Domännennamen, E-Mail-Adressen, reguläre DNS-Hostnamen usw. enthalten, die durch Kommas getrennt sind. Wenn es angegeben ist, müssen Sie auch den CN in diese Liste aufnehmen. Obwohl es sich um ein optionales Feld handelt, muss das SAN-Feld ausgefüllt werden, damit XMPP-Clients (Extensible Messaging and Presence Protocol) ein Zertifikat akzeptieren können. Andernfalls zeigen die XMPP-Clients einen Zertifikatfehler an.

Schritt 2: Generieren Sie callbridge, xmpp, webadmin und webbridge CSR.

1. Rufen Sie die CMS-CLI über Putty auf, und melden Sie sich mit dem Admin-Konto an.
2. Führen Sie die nächsten Befehle aus, um CSR für jeden auf CMS benötigten Dienst zu erstellen. Es ist auch möglich, ein einzelnes Zertifikat zu erstellen, das über einen Platzhalter (*.com) verfügt oder den Cluster-FQDN als CN, FQDNs jedes CMS-Servers und bei Bedarf eine Join-URL aufweist.

Service	Befehl
Webadmin	pkc csr <cert name> CN:<server FQDN>
Webbridge	pkc csr <cert name> CN:<Server FQDN> subjectAltName:<Join Url>,<XMPP domain>
Callbridge UMDREHEN Load Balancer	pkc csr <cert name> CN:<Server FQDN's>

3. Wenn das CMS geclustert ist, führen Sie die nächsten Befehle aus.

Service	Command
Callbridge UMDREHEN Load Balancer	pkc csr <cert name> CN:<cluster FQDN> subjectAltName:<Peer FQDN's>
XMPP	pkc csr <cert name> CN:<Cluster FQDN> subjectAltName:<XMPP Domain>,<Peer FQDN's>

Schritt 3: Generieren Sie den Datenbank-Cluster-CSR, und verwenden Sie die integrierte Zertifizierungsstelle, um sie zu signieren.

Seit CMS 2.7 benötigen Sie Zertifikate für Ihr Datenbank-Cluster. In Version 2.7 wurde eine integrierte Zertifizierungsstelle hinzugefügt, mit der die Datenbankzertifikate signiert werden können.

1. Führen Sie auf allen Kernen `database cluster remove` aus.

- Führen Sie auf dem Primary (Primär) den Befehl `pki selfsigned dbca CN:tplab.local` aus. Beispiel: **Pki selfsigned dbca CN:tplab.local**
- Führen Sie auf der primären `pki csr dbserver CN:cmscore1.example.com subjectAltName` die aus. Beispiel: `cmscore2.example.com,cmscore3.example.com`
- Erstellen Sie auf der primären ein Zertifikat für den Datenbankclient `pki csr dbclient CN:postgres` .
- Verwenden Sie auf dem Primary `dbca`, um das `dbserver`-Zertifikat **`pki sign dbserver dbca`** zu signieren.
- Verwenden Sie auf dem Primary `dbca`, um das `dbclient`-Zertifikat zu signieren `pki sign dbclient dbca`.
- Kopieren Sie die `dbclient.crt` auf alle Server, die eine Verbindung zu einem Datenbankknoten benötigen.
- Kopieren Sie die Datei `dbserver.crt` auf alle Server, die der Datenbank hinzugefügt wurden (Knoten, die den Datenbankcluster bilden).
- Kopieren Sie die Datei `dbca.crt` auf alle Server.
- Führen Sie auf dem primären DB-Server `database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt` aus. Hierbei wird der `dbca.crt` als `root ca-cert` verwendet.
- Führen Sie auf dem primären DB-Server den Befehl `database cluster localnode a` aus.
- Führen Sie auf dem primären DB-Server den Befehl `database cluster initialize` aus.
- Führen Sie auf dem primären DB-Server den Befehl `database cluster status` aus. Muss Knotenpunkte sehen: (me): Connected Primary.
- Führen Sie auf allen anderen Cores, die mit dem Datenbankcluster verbunden sind, den Befehl `database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt` aus.
- Führen Sie auf allen Kernen, die mit dem Datenbank-Cluster verbunden sind (nicht am selben Standort wie eine Datenbank), Folgendes aus: **`database cluster certs dbclient.key dbclient.crt dbca.crt`** .
- Bei verbundenen Kernen (am gleichen Standort wie eine Datenbank):
 - ausgeführt. `database cluster localnode a`
 - ausgeführt. `database cluster join`
- ON-Cores, die verbunden sind (nicht am selben Standort wie eine Datenbank):
 - ru n `database cluster localnode a` .
 - ausgeführt. `database cluster connect`

Schritt 4: Überprüfen der signierten Zertifikate

- Die Gültigkeit des Zertifikats (Ablaufdatum) kann mit einer Zertifikatsüberprüfung überprüft werden. Führen Sie den Befehl **pki inspect <filename>** aus.
- Sie können überprüfen, ob ein Zertifikat mit einem privaten Schlüssel übereinstimmt. Führen Sie dazu den Befehl **pki match <keyfile> <certificate file>** aus.
- Führen Sie den Befehl **pki verify <cert> <certificate bundle/Root CA>** aus, um zu überprüfen, ob ein Zertifikat von der Zertifizierungsstelle signiert wurde und ob es mit dem Zertifikatpaket bestätigt werden kann.

Schritt 5: Signierte Zertifikate auf Komponenten auf CMS-Servern anwenden.

1. Führen Sie die folgenden Befehle aus, um Zertifikate auf Webadmin anzuwenden:

```
webadmin disable  
webadmin certs <keyfile> <certificate file> <certificate bundle/Root CA>  
webadmin enable
```

2. Führen Sie die folgenden Befehle aus, um Zertifikate auf Callbridge anzuwenden:

```
callbridge certs <keyfile> <certificate file> <certificate bundle/Root CA>
```

callbridge restart

3. Führen Sie zum Anwenden von Zertifikaten auf Webbridge die folgenden Befehle aus:

```
webbridge disable
webbridge certs <keyfile> <certificate file> <certificate bundle/Root CA>
webbridge enable
```

4. Führen Sie zum Anwenden von Zertifikaten auf XMPP die folgenden Befehle aus:

```
xmpp disable
xmpp certs <keyfile> <certificate file> <certificate bundle/Root CA>
xmpp enable
```

5. Führen Sie die folgenden Befehle aus, um Zertifikate auf die Datenbank anzuwenden oder abgelaufene Zertifikate im aktuellen DB-Cluster zu ersetzen:

```
database cluster remove (on all servers, noting who was primary before beginning)
database cluster certs <server_key> <server_certificate> <client_key> <client_certificate> <Root ca_certificate>
database cluster initialize (only on primary node)
database cluster join <FQDN or IP of primary> (only on slave node)
database cluster connect <FQDN or IP of primary> (only on nodes that are not part of the database cluster)
```

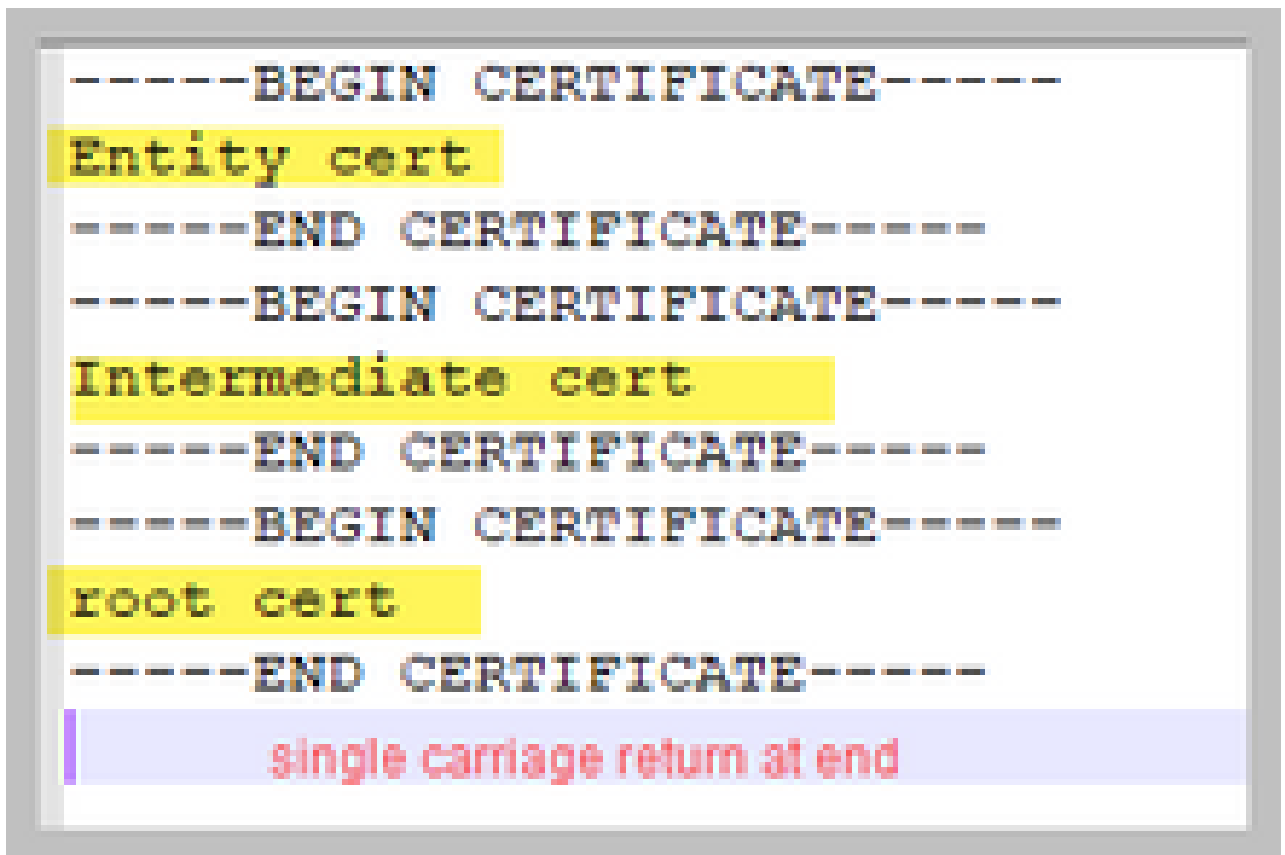
6. Führen Sie die folgenden Befehle aus, um Zertifikate auf TURN anzuwenden:

```
turn disable  
turn certs <keyfile> <certificate file> <certificate bundle/Root CA>  
turn enable
```

Zertifikatvertrauensketten und Pakete

Seit CMS 3.0 müssen Sie Certificate trust chains oder full chain trusts verwenden. Außerdem ist es für jeden Service wichtig, dass Sie wissen, wie Zertifikate erstellt werden sollen, wenn Sie Pakete erstellen.

Wenn Sie eine Zertifikatvertrauenskette erstellen, wie für Web Bridge 3 erforderlich, müssen Sie sie wie im Bild dargestellt erstellen, mit Entitätszertifikat oben, und dazwischen in der Mitte, und Stammzertifizierungsstelle unten, dann eine einzelne Wagenrückgabe.



```
-----BEGIN CERTIFICATE-----  
Entity cert  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
Intermediate cert  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
root cert  
-----END CERTIFICATE-----  
single carriage return at end
```

Jedes Mal, wenn Sie ein Paket erstellen, darf das Zertifikat nur einen Wagenrücklauf am Ende haben.

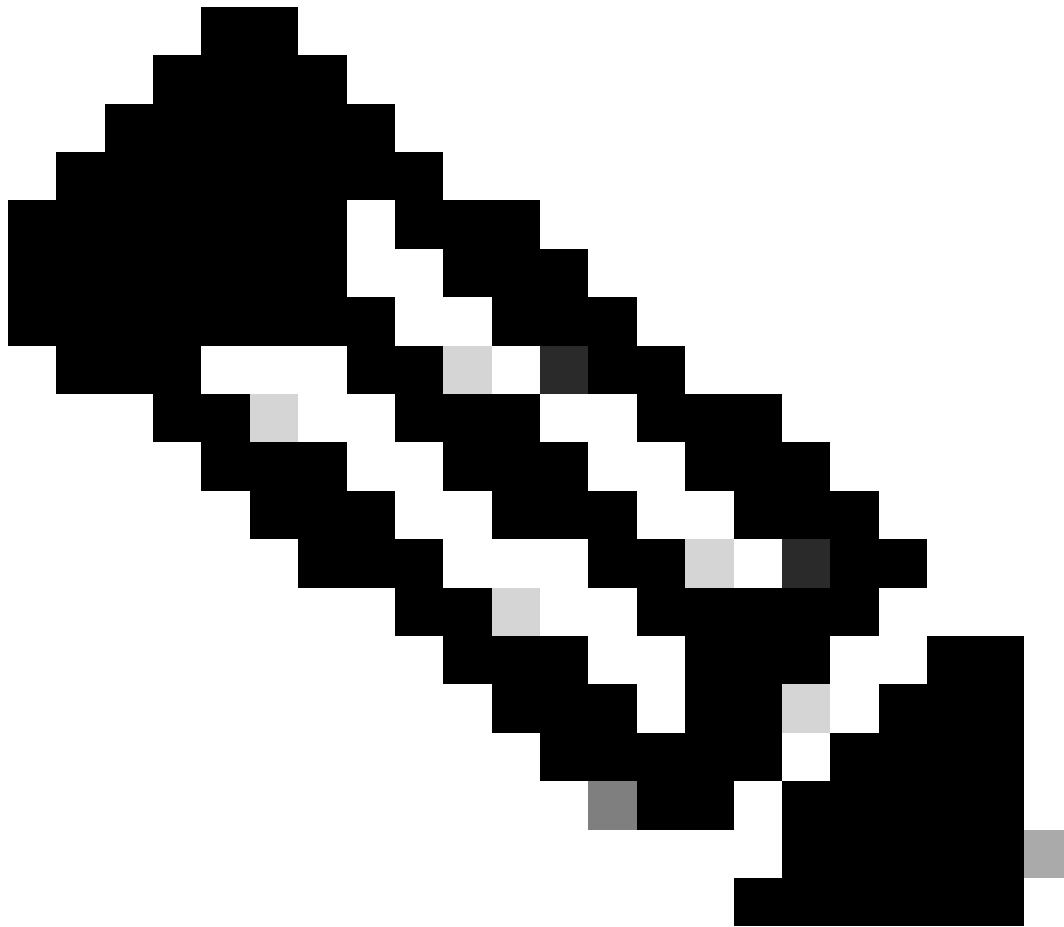
CA-Pakete wären die gleichen wie im Bild, es gäbe aber natürlich kein Entity-Zertifikat.

Fehlerbehebung

Wenn Sie ein abgelaufenes Zertifikat für alle Dienste mit Ausnahme von Datenbankzertifikaten ersetzen müssen, ist die einfachste Methode, neue Zertifikate mit dem GLEICHEN Namen wie die alten Zertifikate hochzuladen. In diesem Fall muss der Dienst nur neu gestartet werden, und Sie müssen den Dienst nicht neu konfigurieren.

Wenn Sie ausführen `pki csr ...` und dieser Zertifikatsname mit einem aktuellen Schlüssel übereinstimmt, wird der Dienst sofort unterbrochen. Wenn die Produktion live ist und Sie proaktiv einen neuen CSR und Key erstellen, verwenden Sie einen neuen Namen. Sie können den aktuell aktiven Namen umbenennen, bevor Sie das neue Zertifikat auf die Server hochladen.

Wenn die Datenbankzertifikate abgelaufen sind, müssen Sie überprüfen, **database cluster status** wer die primäre Datenbank ist, und auf allen Knoten führen Sie den Befehl `database cluster remove` aus. Anschließend können Sie die Anweisungen aus Schritt 3 verwenden. Generieren Sie den Datenbank-Cluster-CSR, und verwenden Sie die integrierte Zertifizierungsstelle, um ihn zu signieren.



Hinweis: Falls Sie die Cisco Meeting Manager (CMM)-Zertifikate erneuern müssen, lesen Sie das folgende Video: [Updating the Cisco Meeting Management SSL Certificate \(Aktualisierung des Cisco Meeting Management SSL-Zertifikats\)](#)

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.