# Signierte Zertifikate der Enterprise CA (Drittanbieter-CA) für SIP TLS und SRTP zwischen CUCM, IP-Telefonen und CUBE konfigurieren und Fehlerbehebung dafür durchführen

## Inhalt



## Einführung

Dieses Dokument beschreibt das Konfigurationsbeispiel für Session Initiation Protocol (SIP) Transport Layer Security (TLS) und Secure Real-time Transport Protocol (SRTP) zwischen Cisco Unified Communications Manager (CUCM), IP-Telefon und Cisco Unified Border Element (CUBE) unter Verwendung von signierten Zertifikaten der Enterprise Certificate Authority (CA) (Drittanbieter CA) und zur Verwendung einer gemeinsamen Enterprise CA zum Signieren von Zertifikaten für alle Netzwerkkomponenten, die Cisco Communications-Geräte wie IP-Telefone umfassen, CUCS, M, Gateways und CUBEs.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Der Enterprise CA-Server ist konfiguriert.
- Der CUCM-Cluster wird im gemischten Modus konfiguriert, und die IP-Telefone werden im sicheren Modus (verschlüsselt) registriert.
- Die grundlegende VoIP- und DFÜ-Peer-Konfiguration des CUBE-Sprachservice wird durchgeführt

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Windows 2008-Server - Zertifizierungsstelle
- CUCM 10,5
- CUBE - 3925E mit Cisco IOS® 15.3(3) M3
- CIPC

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Sichere Sprachkommunikation über CUBE kann in zwei Teile unterteilt werden

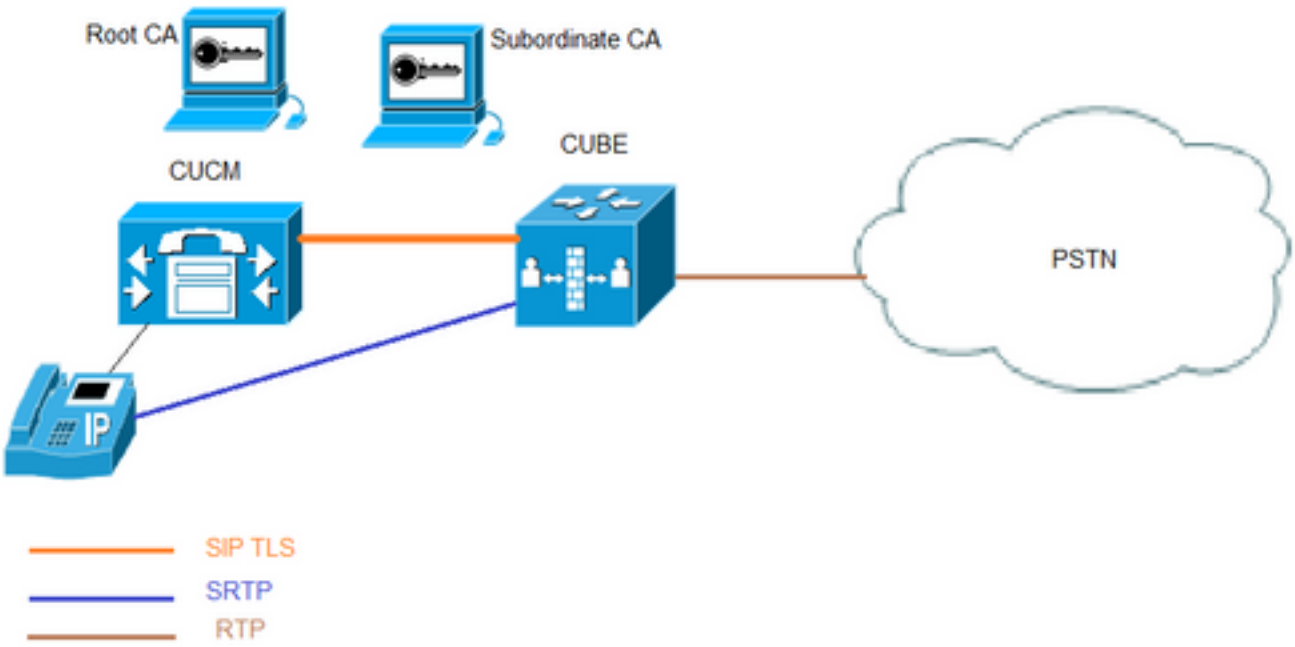
- Sichere Signalisierung - CUBE verwendet TLS zur Sicherung der Signalisierung über SIP und IPSec (Internet Protocol Security), um die Signalisierung über H.323 zu sichern.
- Secure Media - Secure Real-Time Transport Protocol (SRTP)

Die CUCM Certificate Authority Proxy Function (CAPF) stellt für Telefone ein LSC (Locally Significant Certificate) bereit. Wenn CAPF also von einer externen Zertifizierungsstelle signiert wird, fungiert es als untergeordnete Zertifizierungsstelle für die Telefone.

Informationen zum Abrufen von CA-signiertem CAPF finden Sie unter:

## Konfigurieren

### Netzwerkdiagramm



In dieser Konfiguration werden Root CA und eine untergeordnete CA verwendet. Alle CUCM- und CUBE-Zertifikate werden von der untergeordneten Zertifizierungsstelle signiert.

## Konfigurieren von CUBE

Generieren eines RSA-Keypair.

Dieser Schritt generiert private und öffentliche Schlüssel.

In diesem Beispiel ist CUBE nur ein Label, das kann alles sein.

```
CUBE-2(config)#crypto key generate rsa general-keys label CUBE modulus 2048
The name for the keys will be: CUBE

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 12 seconds)

CUBE-2(config)#
```

2. Erstellen Sie einen Vertrauenspunkt für die untergeordnete CA und die Stammzertifizierungsstelle. Der untergeordnete CA-Trustpoint wird für die SIP-TLS-Kommunikation verwendet.

In diesem Beispiel lautet der Trustpoint-Name für die untergeordnete CA SUBCA1 und für die Stammzertifizierungsstelle ROOT.

```
enrollment terminal pem allow manual cut-and-paste certificate enrollment. pem keyword is used
to issue certificate requests or receive issued certificates in PEM-formatted files through the
console terminal.
```

Der in diesem Schritt verwendete Betreffname muss mit dem X.509-Betreffnamen im CUCM-SIP-Trunk-Sicherheitsprofil übereinstimmen. Best Practice ist die Verwendung des Hostnamens mit dem Domänennamen (wenn der Domänenname aktiviert ist).

Zuordnen - RSA-Schlüsselpaar erstellt in Schritt 1.

```
crypto pki trustpoint SUBCA1
enrollment terminal pem
serial-number none
ip-address none
subject-name CN=CUBE-2
revocation-check none
rsakeypair CUBE

crypto pki trustpoint ROOT
enrollment terminal
revocation-check none
```

3. Erstellen einer CUBE-Zertifikatsanforderung (Certificate Signing Request, CSR)

Der Befehl **crypto pki enroll** erstellt die CSR, die der Enterprise CA bereitgestellt wird, um das signierte Zertifikat zu erhalten.

```
CUBE-2(config)#crypto pki enroll SUBCA1
% Start certificate enrollment ..

% The subject name in the certificate will include: CN=CUBE-2
% The subject name in the certificate will include: CUBE-2
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIICjjCCAXYCAQAwKDEPMA0GA1UEAxMGQ1VCRS0yMRUwEwYJKoZIhvcNAQkCFgZD
VUJFLTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDAmVvufevAg1ip
Kn8FhWjFlNNUFMqkgh2Cr1IMV+ovR2HyPTFwgr0XDhZHMSsnBw67Ttze3Ebxxoau
cBQcIASZ4hdTSIgjxG+9YQacLm9MXpfxHp5kcICzSfSllrTexArTQglW8+rErYpk
2THN1S0PC4cRlBwoUCgB/+KCDkjJkUy8eCX+Gmd+6ehRKEQ5HdFHEfUr5hc/7/pB
liHietNKSxYEOr9TVZPiRJrtpUPMRMZElRUm7GoxBrCWIXVdvEAGC0Xqd1ZVLlTz
z2sQQDqvJ9fMN6fngKv2ePr+f5qejWVzGO0DFVQs0y5x+Yl+pHbsdV1hSSnPpJk6
TaaBmX83AgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB/wQEAwIFoDAN
BgkqhkiG9w0BAQUFAAOCAQEArWMJbdhlU8VfaF1cMJIbr569BZT+tIjQOz3OqNGQ
QpzHwclLoaKuC5pc/u0hw14MGS6Z440Iw4zK2/5bb/KL47r8H3d7T7PYMfK6lAzK
sU9Kf96zTvHNWl9wXImB5blJfRLXnFWXNsVEF4FjU74plxJL7siaa5e86eNy9deN
20iKjvP8o4MgWewILrD01YZMDMDS1Uy82kWI6hvXG5+xBT5A1lo2xCj1S9y6/D4d
f0ilDZvaQk+7jjBCzLv5hET+1neoQBw52e7RWU8s2biQw+7TEAdO8NytF3q/mA/x
bUKw5wT4pgGUJcDAWej3ZLqP91g5yyd9MiCdCRY+3mLccQ==
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
CUBE-2(config)#
```

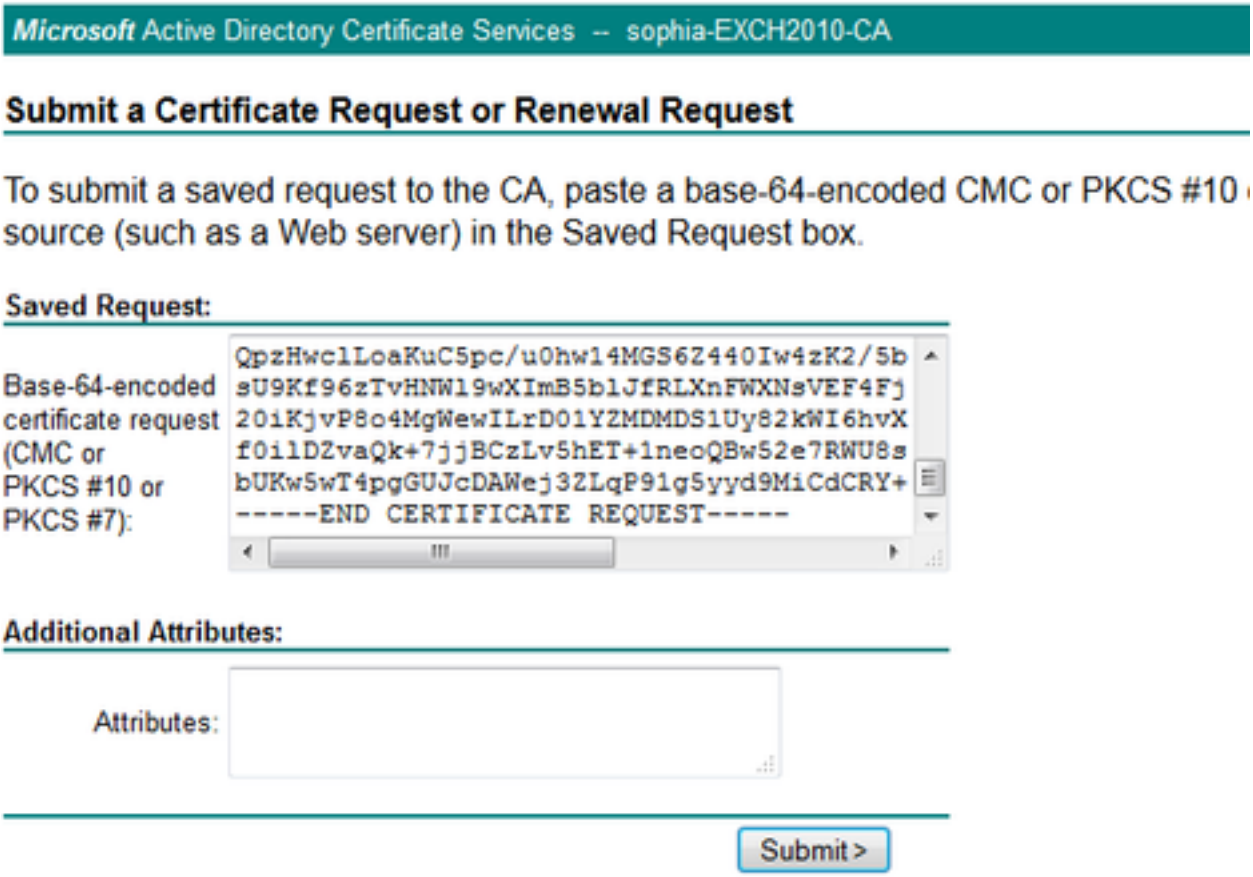
Kopieren Sie die Ausgabe zwischen BEGIN CERTIFICATE REQUEST (BEGINN-ZERTIFIZIERUNGSANTRAG), um die ENDZERTIFIZIERUNGSANFRAGE zu erstellen, und speichern Sie sie in der Notizblock-Datei.

CUBE CSR verfügt über folgende Schlüsselattribute:

```
 Attributes:
Requested Extensions:
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
```

4. CA-Zertifikat Root CA, dann CA-Zertifikat und signiertes CUBE-Zertifikat von untergeordneter CA.

Um ein signiertes CUBE-Zertifikat zu erhalten, verwenden Sie die in Schritt 3 generierte CSR-Nummer. Das Image stammt von einem Microsoft CA-Webserver.




5. CA-Zertifikat von Root CA und untergeordneter CA importieren.

Öffnen Sie das Zertifikat in Ihrem Notizblock, und kopieren Sie den Inhalt von BEGIN CERTIFICATE REQUEST to END CERTIFICATE REQUEST.

```
CUBE-2(config)#crypto pki authenticate SUBCA1

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFhDCCBGygAwIBAgIKYZVFyQAAAAAAFjANBgkqhkiG9w0BAQUFADBQMRIwEAYK
CZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJk/IsZAEZFgZzb3BoaWExIjAgBgNVBAMT
GXNvcGhpYS1XSU4tM1MxOEpDM0xNMkEtQ0EwHhcNMTQwOTI1MDAwNzU2WhcNMTYw
OTI1MDAxNzU2WjBJMRIwEAYKCZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJk/IsZAEZ
FgZzb3BoaWExGzAZBgNVBAMTEnNvcGhpYS1FWENIMjAxMC1DQTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAJK+Nmz4rieYfr9gH3ISTuYz3TWpafpjDJ7l
7kIwwwC28TvjFl5vrKEiaPyFzxL5TEHaWQ9YAo/WMdtuyF7aB+pLJ1soKcZxtrGv
gTMtuphcJ5Fpd4368lR8ZXJiAT/Dz+Nsh4PC9GUUKQeycyRDeOBz08vL5pLj/W99
b8UMUlVOqBu4e1ZwxWPMFxB7zOeYsCfXMnGFUlp3HFdWZczgK3ldNO9I0X+p70UP
R0CQpMEQxuheqv9kazIIJKfNH8N0qO8IHl76Y32vUzLg3uvZgqWG6hGch/gjm4L/
1KmdZTNSH8H7Kf6vG6PNWrXWwLNkhrWaYEryHelIshEj7ZUeB8sCAwEAAaOCAmUw
ggJhMBIGCSsGAQQBgjcVAQQFAgMBAAEwIwYJKwYBBAGCNxUCBBYEFLnnd8HnCfKE
isPgI58Oog/LqwVSMB0GA1UdDgQWBBSsdYJZIU9IXyGm9aL67+8uDhM/EzAZBgkr
BgEEAYI3FAIEDB4KAFMAdQBiAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/
BAUwAwEB/zAfBgNVHSMEGDAWgBTvo1P6OP4LXm9RDv5MbIMk8jnOfDCB3QYDVR0f
BIHVMIHSMIHPoIHMoIHJhoHGbGRhcDovLy9DTj1zb3BoaWEtV0lOLTNTMThKQzNM
TTJBLUNBLENOPVdJTi0zUzE4SkMzTE0yQSxDTj1DRFAsQ049UHVibGljJTIwS2V5
JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1zb3Bo
aWEsREM9bGk/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENs
YXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBAQSBvDCBuTCBtgYI
KwYBBQUHMAKGgalsZGFwOi8vL0NOPXNvcGhpYS1XSU4tM1MxOEpDM0xNMkEtQ0Es
```

```
Q049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9c29waGlhLERDPWxpP2NBQ2VydGlmaWNhdGU/YmFz
ZT9vYmplY3RDbGFzcz1jZXJ0aW9uQXV0aG9yaXR5MA0GCSqGSIb3DQEB
BQUAA4IBAQBj/+rX+9NJiSZq1YwQXkLq6+LUh7OkCoeCHHfBGUaS+gvbYQ5OVwJI
TlPTj4YNh62A6pUXplo8mdxKxOmZeRLTYgf9Q/SiOY+qoxJ5zNliSqlRU4E02sRz
wrzfaQpLGgyHXsyK1ABOGRgGqqWqZ7oXoKMRNmO+eu3NzBs4AVAAfL8UhFCv4IVx
/t6qIHY6YkNMVByjZ3MdFmohepN5CHZUHIvrOv9eAiv6+Vaan2nTeynyy7WnEv7P
+5L2kEFOSfnL4Zt2tEMqc5WyX6yjxDWmII0DTSyRshmxAoYlo3EJHwW+fIocdmIS
hgWDzioZ70SM9mJqNReHMC1jL3FD2nge
-----END CERTIFICATE-----

Trustpoint 'SUBCA1' is a subordinate CA and holds a non self signed cert
Certificate has the following attributes:
Fingerprint MD5: C420B7BB 88A2545F E26B0875 37D9EB45
Fingerprint SHA1: 110AF87E 53E6D1C2 19404BA5 0149C5CA 2CF2BE1C

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

CUBE-2(config)#
CUBE-2(config)#crypto pki authenticate ROOT

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgIQMVF/OWq+ELxFC2IdUGvd2jANBgkqhkiG9w0BAQUFADBQ
MRIwEAYKCZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJk/IsZAEZFgZzb3BoaWExIjAg
BgNVBAMTGXNvcGhpYS1XSU4tM1MxOEpDM0xNMkEtQ0EwHhcNMTQwOTEzMjMzODA2
WhcNMTkwOTEzMjM0ODA1WjBQMRIwEAYKCZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJ
k/IsZAEZFgZzb3BoaWExIjAgBgNVBAMTGXNvcGhpYS1XSU4tM1MxOEpDM0xNMkEt
Q0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC4aywr1oOpTdTrM8Ya
R3RkcahbbhR3q7P1luTDUDNM5Pi6P8z3MckfjB/yy6SWr1Qnddhyv MG6IGNtVxJ4
eyw0c7jbArXWOemGLOt454A0mCfcbwMhjQBycg9SM1r1Umzad7kOCzj/rD6hMbC4
jXpg6uU8g7eB3LzN1XF93DHjxYCBKMIeG45pqmsOc3mUj1CbCtnYXgno+mfhNzhR
HSth02z4XlGm99v46j/PqGjNRq4WKCwDc45SG3QjJDqDxnRJPKtRdNva66UJfDJp
4YMXQxOSkKMtDEDhH/Eic7CrJ3EywpUpMZAmqh4bmQ7Vo2pnRTbYdaAv/+yr8sMj
+FU3AgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1Ud
DgQWBBTvo1P6OP4LXm9RDv5MbIMk8jnOfDAQBgkrBgEEAYI3FQEEAwIBADANBgkq
hkiG9w0BAQUFAAOCAQEAmd7hJ2EEUmuMZrc/qtSJ223loJlpKEPMVi7CrodtWSgu
5mNt1XsgxijYMqD5gJe1oq5dmv7efYvOvI2WTCXfwOBJ0on8tgLFwp1+SUJWs95m
OXTyoS9krsI2G2kQkjQWniMqPdNxpmJ3C4WvQLPLwtEOSRZRBvsKy6lczrgrV2mZ
kx12n5YGrGcXSblPPUddlJep1l8U+AQC8wkSzfJu0yHJwoH+lrIfgqKUee4x7z6s
SCaGddCYr3OK/3Wzs/WjSO2UETvNL3NEtWHDc2t4Y7mmIMSDvGjHZUgGZotwc9kt
9f2dZA0rtgBq4IDtpxkR3CQaauB7wUCpzemHzf+z9Q==
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 511E1008 6D315E03 4B748601 7EE1A0E5
Fingerprint SHA1: 8C35D9FA 8F7A00AC 0AA2FCA8 AAC22D5F D08790BB

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

CUBE-2(config)#
```

6. CUBE-signiertes Zertifikat importieren.

Öffnen Sie das Zertifikat in Ihrem Notizblock, und kopieren Sie den Inhalt von BEGIN CERTIFICATE REQUEST to END CERTIFICATE REQUEST.

```
CUBE-2(config)#crypto pki import SUBCA1 certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIEAjCCAuqgAwIBAgIKQZZrHQABAAAAEzANBgkqhkiG9w0BAQUFADBJMRIwEAYK
CZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJk/IsZAEZFgZzb3BoaWExGzAZBgNVBAMT
EnNvcGhpYS1FWENIMjAxMC1DQTAeFw0xNTA0MDEwMDEzNDFaFw0xNjA0MDEwMDIz
NDFaMBExDzANBgNVBAMTBkNVQkUtMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMCZW+5968CDWKkqfwWFaMWU01QUyqSCHYKvUgxX6i9HYfI9MXCCvRcO
FkcxKycHDrtO3N7cRvHGhq5wFBwgBJniF1NIiCPEb71hBpwub0xel/EenmRwgLNJ
9KWWtN7ECtNCCVbz6sStimTZMc3VLQ8LhxGUHChQKAH/4oIOSMmRTLx4Jf4aZ37p
6FEoRDkd0UcR9SvmFz/v+kGWIeJ600pLFgQ6v1NVk+JEmu2lQ8xExkSVFSbsajEG
sJYhdV28QAYLRep3VlUuVPPPaxBAOq8n18w3p+eAq/Z4+v5/mp6NZXMY7QMVVCzT
LnH5iX6kdux1XWFJKc+kmTpNpoGZfzcCAwEAAaOCASIwggEeMA4GA1UdDwEB/wQE
AwIFoDAdBgNVHQ4EFgQU9PbHMHSkYrjJ2+/+hSSMEoma0QIwHwYDVR0jBBgwFoAU
rHWCWSFPSF8hpvWi+u/vLg4TPxMwTwYDVR0fBEgwRjBEoEKgQIY+ZmlsZTovL0VY
Q0gyMDEwLnNvcGhpYS5saS9DZXJ0RW5yb2xsL3NvcGhpYS1FWENIMjAxMC1DQSgx
KS5jcmwwbQYIKwYBBQUHAQEEYTBfMF0GCCsGAQUFBzAChlFmaWxlOi8vRVhDSDIw
MTAuc29waGlhLmxpL0NlcnRfbnJvbGwvRVhDSDIwMTAuc29waGlhLmxpX3NvcGhp
YS1FWENIMjAxMC1DQSgxKS5jcnQwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQUF
AAOCAQEAe7EAoXKIAij4vxZuxROOFOfsmjcojU31ac5nrLCbq/FyW7eNblphL0NI
Dt/DlfZ5WK2q3Di+/UL1lDt3KYt9NZ1dLpmccnipbbNZ5LXLoHDkLNqt3qtLfKjv
J6GnnWCxLM18lxm1DzZT8VQtiQk5XZ8SC78hbTFtPxGZvfX70v22hekkOL1Dqw4h
/3mtaqxfnslB/J3Fgps1och45BndGiMAWavzRjjOKQaVLgVRvVrPIy3ZKDBaUleR
gsy5uODVSrhwMo3z84r+f03k4QarecgwZE+KfXoTpTAfhiCbLKw0ZyRMXXzWqNfl
iotEQbs52neCwXNwV24aOCChQMw2xw==
-----END CERTIFICATE-----

% Router Certificate successfully imported

CUBE-2(config)#
```

7. Konfigurieren von TCP TLS als Transportprotokoll

Dies kann entweder auf globaler Ebene oder auf DFÜ-Peer-Ebene erfolgen.

```
 voice service voip
sip
session transport tcp tls
```

8. Wenn Trustpoint für sip-ua zugewiesen wird, wird dieser Trustpoint für die gesamte SIP-Signalisierung zwischen CUBE und CUCM verwendet:

```
 sip-ua
crypto signaling remote-addr <cucm pub ip address> 255.255.255.255 trustpoint SUBCA1
crypto signaling remote-addr <cucm sub ip address> 255.255.255.255 trustpoint SUBCA1
```

oder, der Standard-Trustpoint kann für alle SIP-Signalisierungen vom Würfel konfiguriert werden:

```
 sip-ua
crypto signaling default trustpoint SUBCA1
```

9. Aktivieren Sie SRTP.

Dies kann entweder auf globaler Ebene oder auf DFÜ-Peer-Ebene erfolgen.

```
Voice service voip
srtp fallback
```

10. Für das SRTP- und Real-Time Transport Protocol (RTP)-Internetworking ist ein sicherer Transcoder erforderlich.

Wenn die Cisco IOS® Version 15.2.2T (CUBE 9.0) oder höher ist, kann der LTI-Transcoder (Local Transcoding Interface) konfiguriert werden, um die Konfiguration zu minimieren.

Der LTI-Transcoder benötigt für SRTP-RTP-Anrufe keine PKI-Konfiguration (Public Key Infrastructure).

```
 dspfarm profile 1 transcode universal security
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
maximum sessions 10
associate application CUBE
```

Wenn Cisco IOS® unter 15.2.2T liegt, konfigurieren Sie den SCCP-Transcoder.

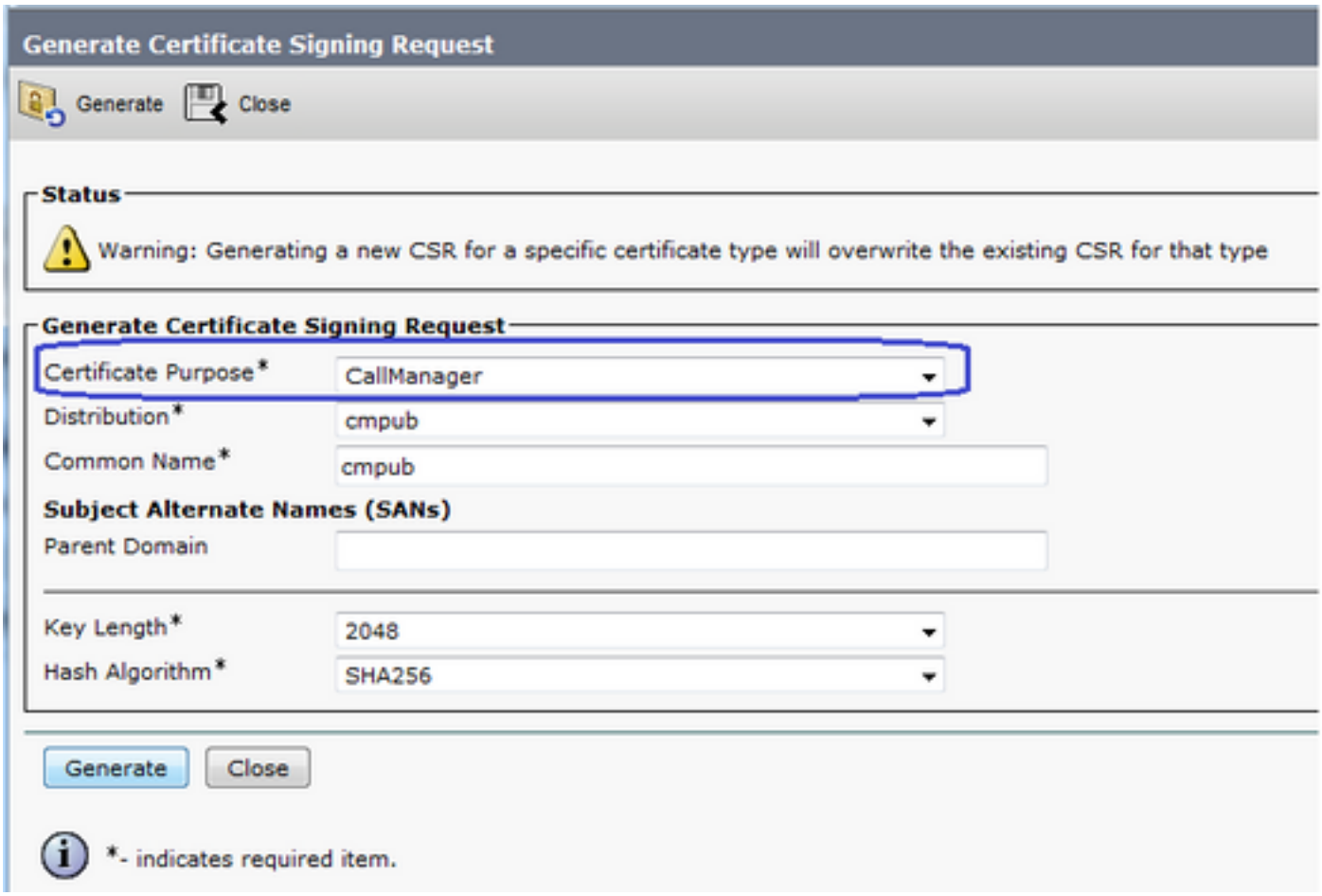
Der SCCP-Transcoder benötigt für die Signalisierung einen Vertrauenspunkt. Wenn jedoch derselbe Router zum Hosten des Transcoders verwendet wird, kann derselbe Vertrauenspunkt (SUBCA1) für CUBE sowie für Transcoder verwendet werden.

```
sccp local GigabitEthernet0/2
sccp ccm 10.106.95.153 identifier 1 priority 1 version 7.0
sccp
!
sccp ccm group 1
bind interface GigabitEthernet0/0
associate ccm 1 priority 1
associate profile 2 register secxcode
!
dspfarm profile 2 transcode universal security
trustpoint SUBCA1
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
maximum sessions 10
associate application SCCP

telephony-service
secure-signaling trustpoint SUBCA1
sdspfarm units 1
sdspfarm transcode sessions 10
sdspfarm tag 1 secxcode
max-ephones 1
max-dn 1
ip source-address 10.106.95.153 port 2000
max-conferences 8 gain -6
transfer-system full-consult
```

## Konfigurieren von CUCM

1. Erstellen Sie den CallManager-CSR für alle CUCM-Knoten.

Navigieren Sie zu **CM OS Administration > Security > Certificate Management > Generate Certificate Signing Request** wie im Bild gezeigt.

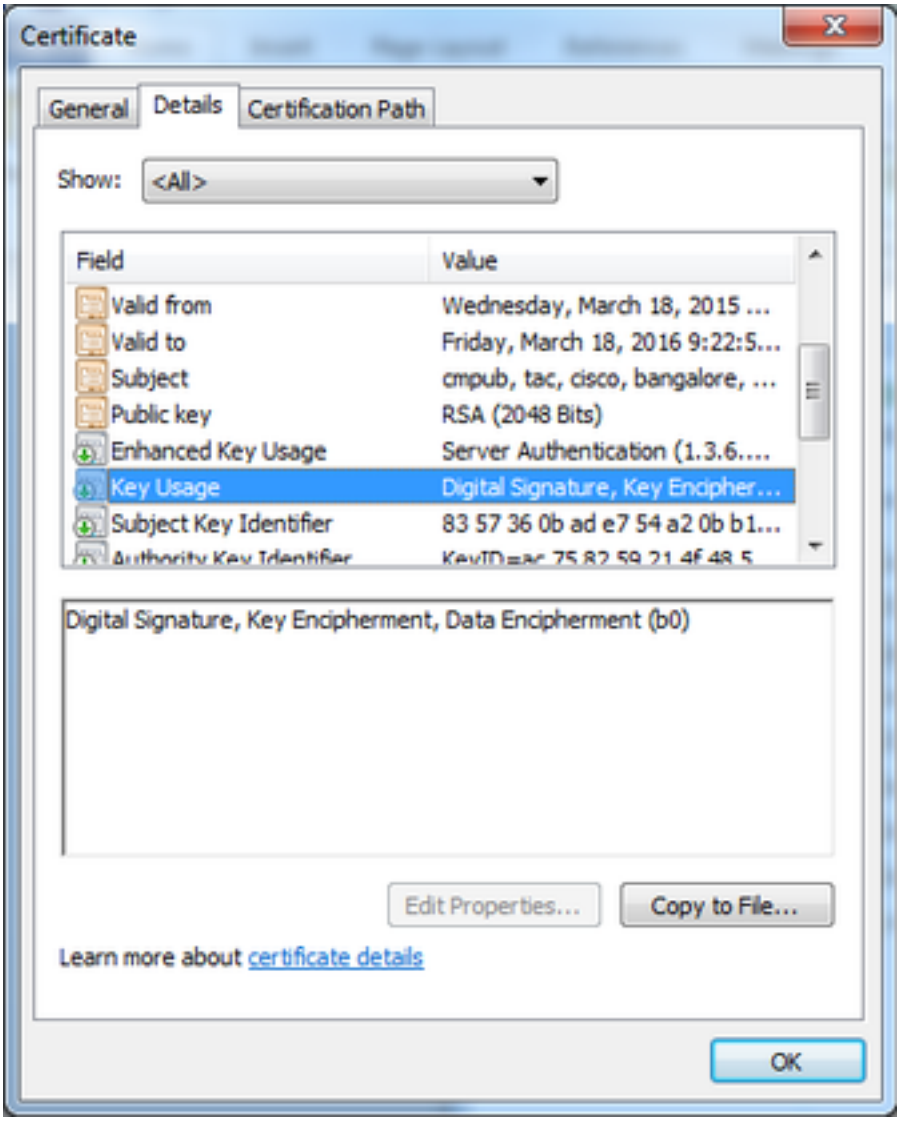



CallManager CSR verfügt über folgende Schlüsselattribute:

```
Requested Extensions:
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

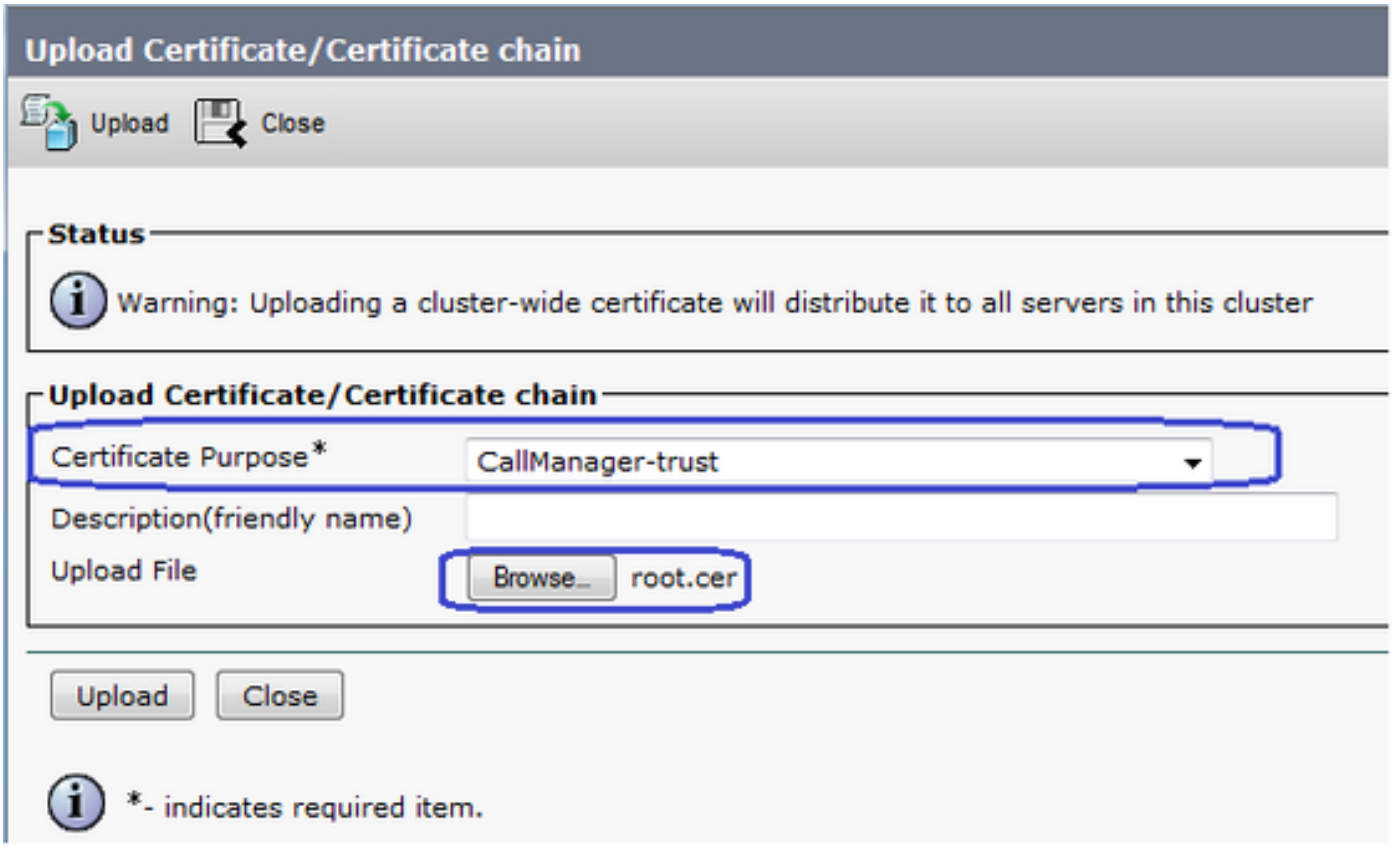
2. Rufen Sie das CallManager-Zertifikat für alle CM-Knoten ab, die von der untergeordneten CA signiert wurden.

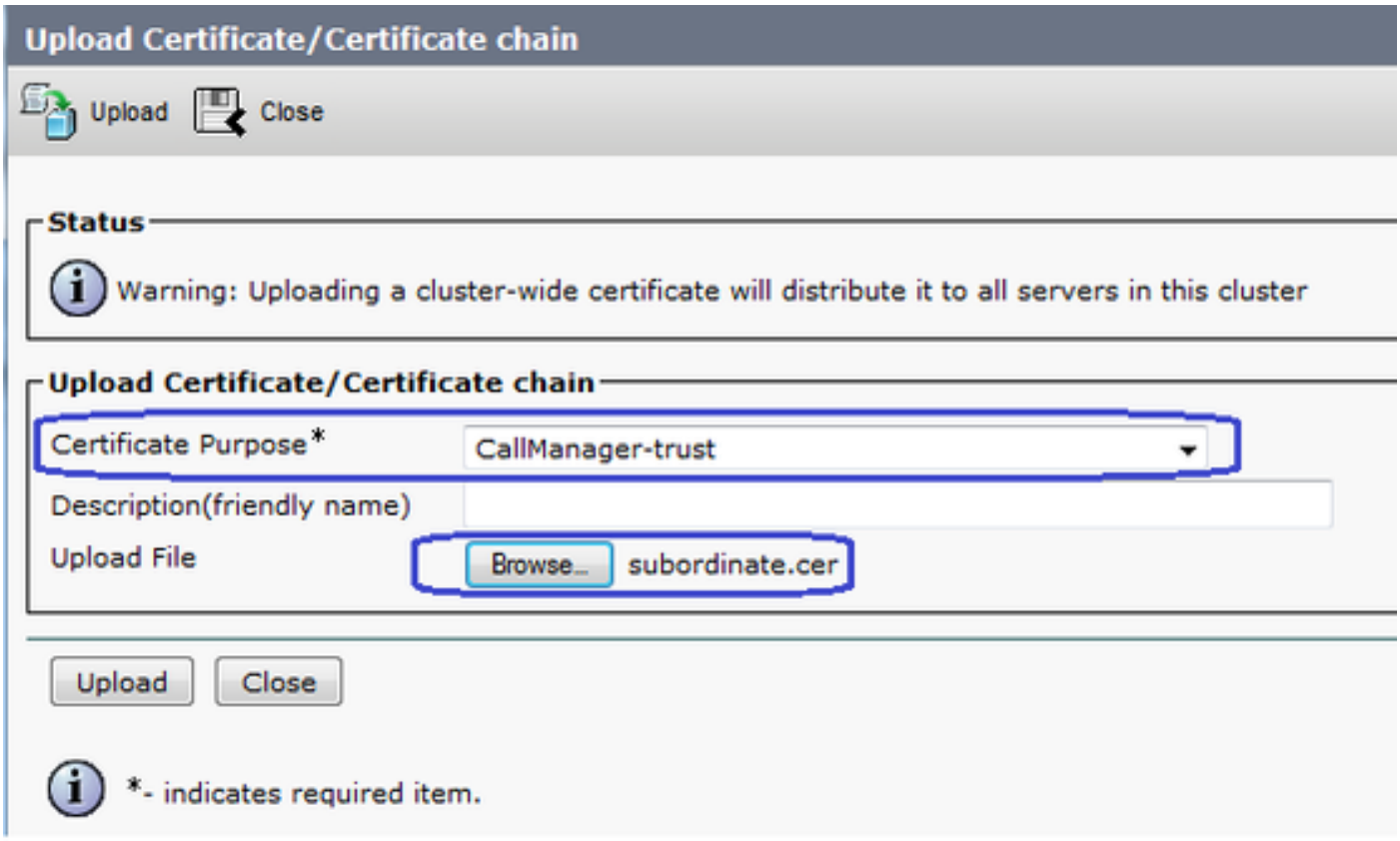
Verwenden Sie in Schritt 1 generierten CSR. Jede Webserver-Zertifikatsvorlage würde funktionieren. Stellen Sie sicher, dass das signierte Zertifikat mindestens über die folgenden Attribute für Schlüsselverwendungen verfügt: **Digitale Signatur, Schlüsselverschlüsselung, Datenerfassung** wie im Bild gezeigt.



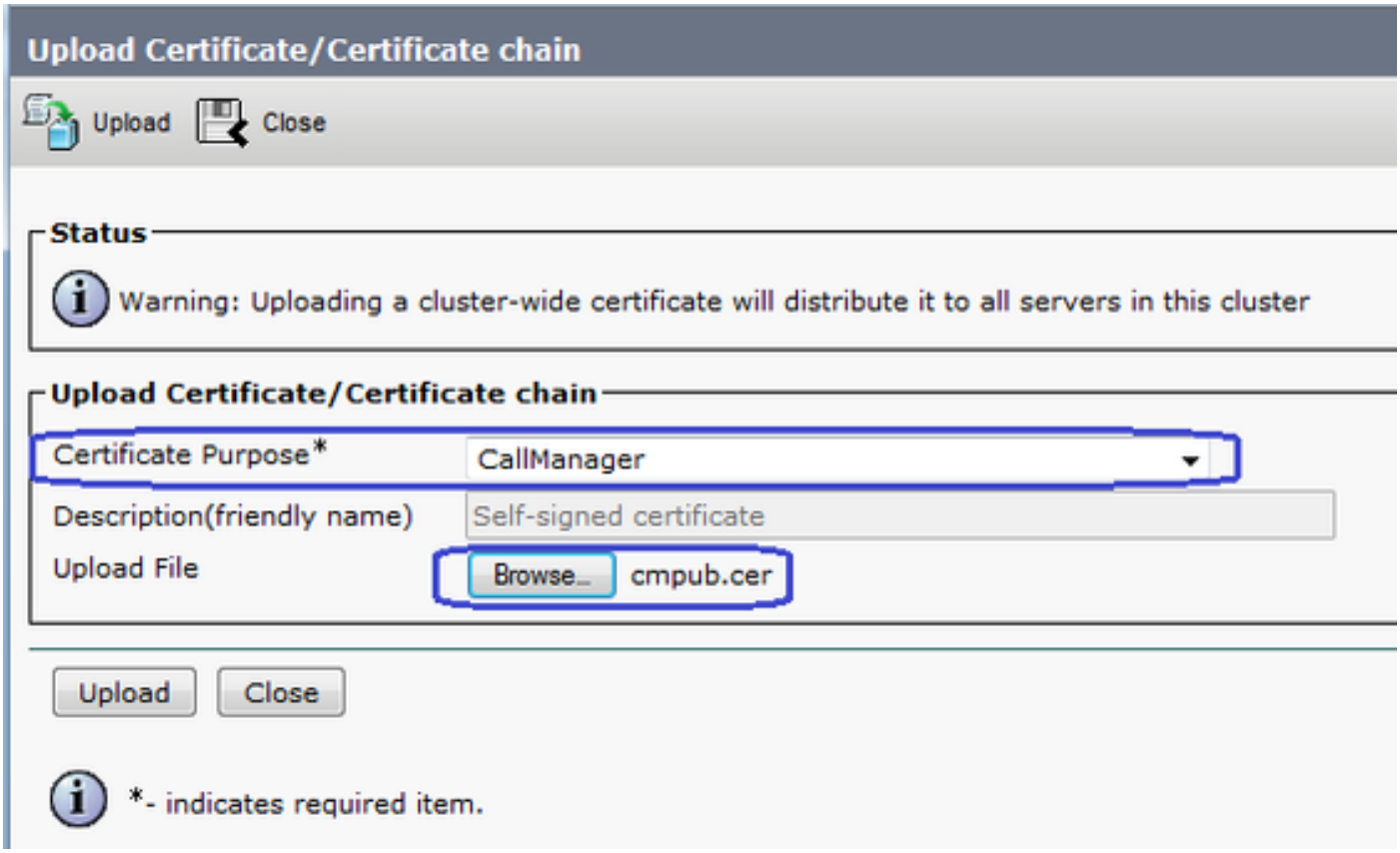

3. Laden Sie das CA-Zertifikat von der Root-CA und der untergeordneten CA als CallManager-Trust hoch.

Navigieren Sie zu **CM OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain (CM Betriebssystemverwaltung > Sicherheit > Zertifikatsverwaltung > Zertifikat-Management hochladen/Zertifikat**, wie in den Bildern gezeigt.




4. Laden Sie das signierte CallManager-Zertifikat als **CallManager** hoch, wie im Bild gezeigt.




5. Aktualisieren der CTL-Datei (Certificate Trust List) auf Publisher (über CLI)

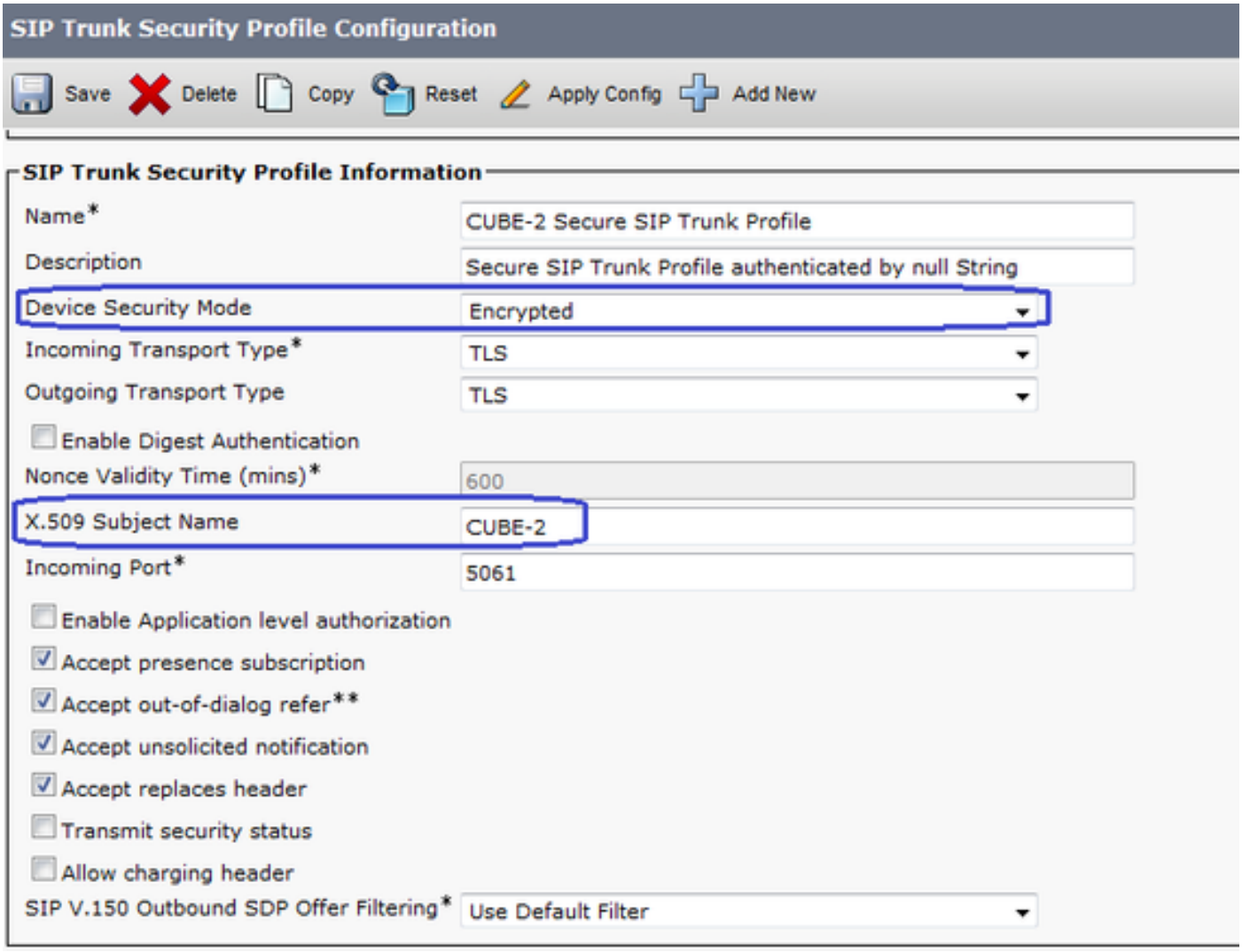
```
admin:utils ctl update CTLFile
This operation will update the CTLFile. Do you want to continue? (y/n):

Updating CTL file
CTL file Updated
Please Restart the TFTP and Cisco CallManager services on all nodes in the cluster that run
these services
admin:
```

6. Starten Sie den CallManager- und den TFTP-Dienst auf allen Knoten neu, und starten Sie den CAPF-Dienst auf Publisher.

7. Erstellen Sie ein neues SIP-Trunk-Sicherheitsprofil.

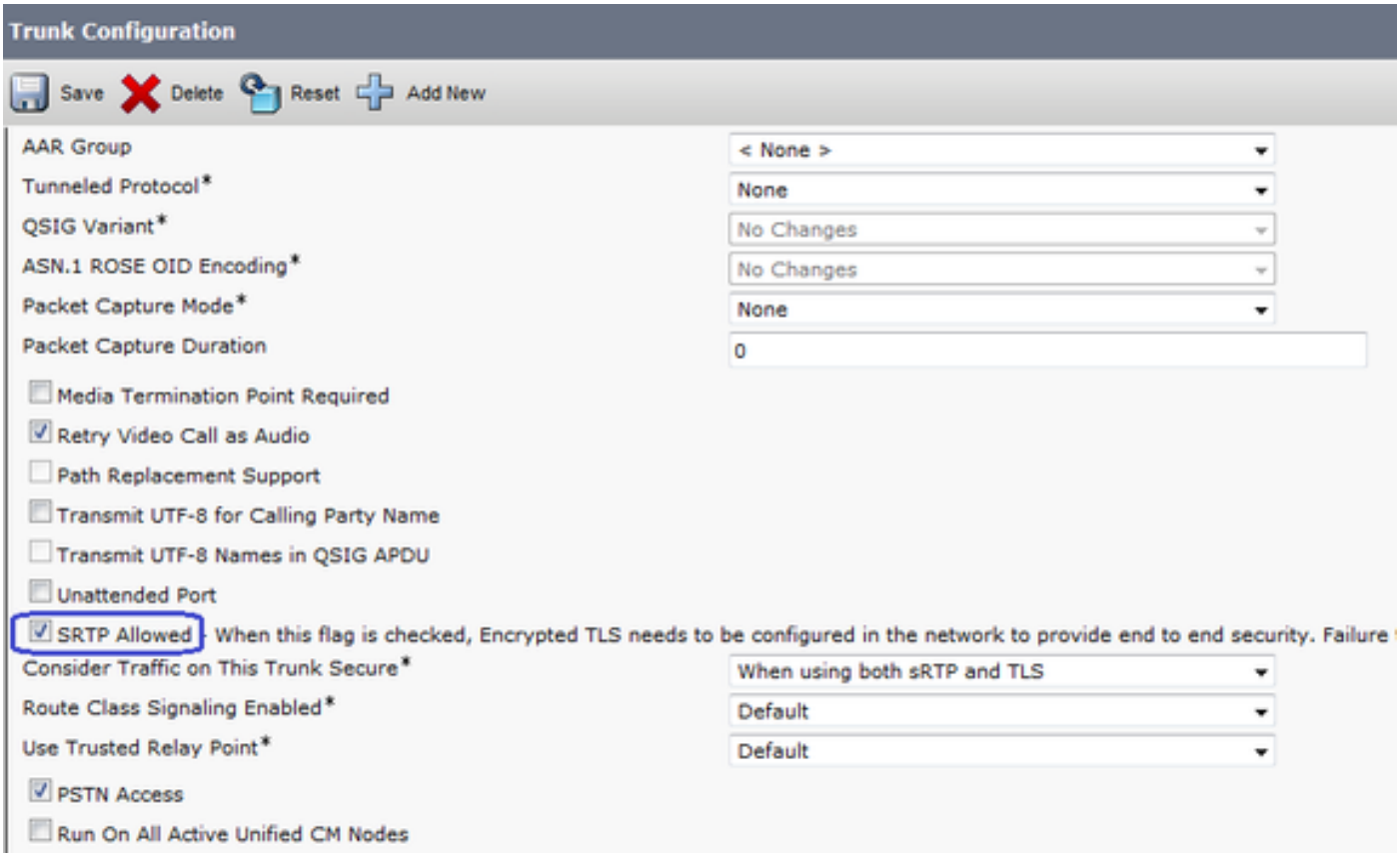
Navigieren Sie unter CM-Verwaltung zu **System > Security > SIP Trunk Security Profiles > Find**.

Kopieren Sie ein vorhandenes nicht sicheres SIP-Trunk-Profil, um ein neues sicheres Profil zu erstellen, wie in diesem Bild gezeigt.

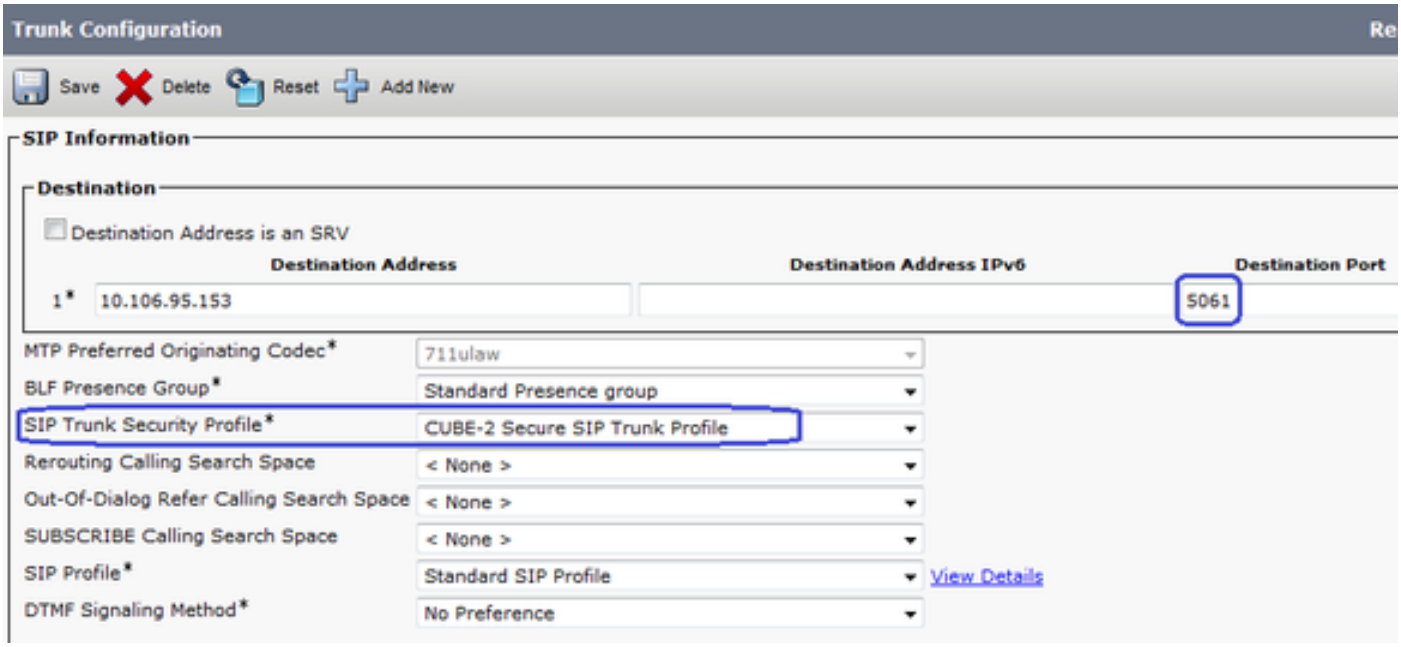



8. Erstellen Sie einen SIP-Trunk zum CUBE.

Aktivieren Sie **SRTP, das** auf einem SIP-Trunk **zulässig** ist, wie im Bild gezeigt.




Konfigurieren Sie den Ziel-Port 5061 (TLS), und wenden Sie ein neues sicheres SIP-Trunk-Sicherheitsprofil auf den SIP-Trunk an, wie im Bild gezeigt.




# Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

```
show sip-ua connections tcp tls detail
show call active voice brief
```

**e.g.**

```
Secure-CUBE#show sip-ua connections tcp tls detail
Total active connections : 2
No. of send failures : 0
No. of remote closures : 13
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition

Remote-Agent:10.106.95.151, Connections-Count:2
Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
=========== ======= =========== =========== ===========
5061 16 Established 0 10.106.95.153
57396 17 Established 0 10.106.95.153


-------------- SIP Transport Layer Listen Sockets ---------------
Conn-Id Local-Address
=========== ============================
2 [10.106.95.153]:5061
```

Die Ausgabe des Befehls **show call active voice brief** wird erfasst, wenn der LTI-Transcoder verwendet wird.

```
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00

1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```

Wenn zwischen dem Cisco IP-Telefon und CUBE oder Gateway ein verschlüsselter SRTP-Anruf getätigt wird, wird auf dem IP-Telefon ein Sperrsymbol angezeigt.

# Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Diese Debug-Tools sind hilfreich bei der Behebung von PKI/TLS/SIP/SRTP-Problemen.

```
debug crypto pki{ API | callbacks | messages | scep | server | transactions | validation }
debug ssl openssl { errors | ext | msg | states }
debug srtp {api | events }
debug ccsip {messages | error | events | states | all }
debug voip ccapi inout
```