

# Enterprise CA (VCA)-certificaten van derden voor SIP-TLS en SRTP configureren en oplossen tussen CUCM, IP-telefoons en CUBE

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[CUBE configureren](#)

[CUCM configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

## Inleiding

Dit document beschrijft het configuratievoorbeeld van Session Initiation Protocol (SIP) Transport Layer Security (TLS) en Secure Real-time Transport Protocol (SRTP) tussen Cisco Unified Communications Manager (CUCM), IP-telefoon en Cisco Unified Border Element (CUBE) met het gebruik van Enterprise certificaatautoriteit (CA) (derde partij) Ondertekend certificaten en gebruikt gemeenschappelijk Enterprise CA om certificaten te ondertekenen voor alle netwerkcomponenten die Cisco-communicatieapparaten zoals IP, CUCM omvatten. gateways en CUBE's.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Enterprise CA-server is geconfigureerd
- CUCM Cluster is ingesteld in Gemengde modus en IP-telefoons worden geregistreerd in beveiligde modus (versleuteld)
- CUBE basisspraakservice VoIP en configuratie van dial-peers

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Windows 2008 server - certificeringsinstantie
- CUCM 10.5

- CUBE - 3925E met Cisco IOS® 15.3(3) M3
- CIPC

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Achtergrondinformatie

Secure-spraakcommunicatie via CUBE kan in twee delen worden verdeeld

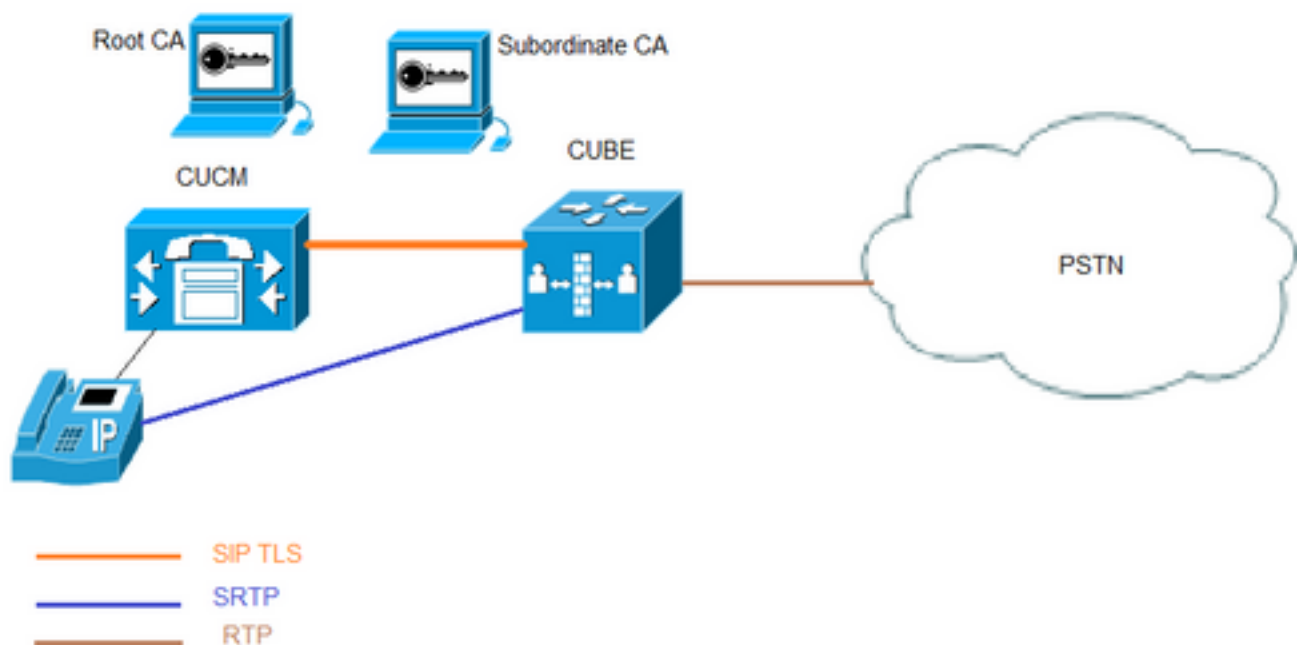
- Secure Signaling - CUBE-gebruik TLS om signaling via SIP en Internet Protocol Security (IPSec) te beveiligen met signaling via H.323
- Secure Media - Secure Real-time Transport Protocol (SRTP)

De functie CUCM Certificate Authority Proxy (CAPF) biedt een lokaal belangrijk certificaat (LSC) voor telefoons. Dus wanneer CAPF door externe CA wordt ondertekend, zou het als ondergeschikte CA voor de telefoons fungeren.

Om te begrijpen hoe CA-Signed CAPF te krijgen, raadpleegt u:

## Configureren

### Netwerkdigram



In deze instelling worden Root CA en één ondergeschikte CA gebruikt. Alle CUCM- en CUBE-certificaten worden ondertekend door subordinair CA.

### CUBE configureren

Genereert een RSA-trapezium.

Deze stap genereert particuliere en openbare sleutels.

In dit voorbeeld is CUBE slechts een Label, dit kan alles zijn.

```
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. Maak een betrouwbaar punt voor subordinair CA en Root CA. Subordinaat CA trustpoint wordt gebruikt voor SIP TLS communicatie.

In dit voorbeeld is de naam van de trustpunten voor ondergeschikte CA SUBCA1 en voor Root CA het 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.

De Onderwerp naam die in deze stap wordt gebruikt moet op X.509 Onderwerp Naam op het veiligheidsprofiel van CUCM SIP Trunk overeenkomen. Best practice is host-name met domeinnaam te gebruiken (als domeinnaam is ingeschakeld).

Associate RSA Key pair die is gemaakt in Stap 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. CUBE-aanvraag voor certificaatsignalering genereren (CSR).

De opdracht voor het inschrijven van crypto-pki produceert de CSR die aan de Enterprise CA wordt verstrekt om het ondertekende certificaat te verkrijgen.

```
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-----
```

```
MIICjCCAXYCAQAwKDEPMA0GA1UEAxMGQ1VCRS0yMRUwEwYJKoZIhvcNAQkCFgZD
VUJFLTIwggEiMA0GCsqGSIB3DQEBAQUAA4IBDwAwggEKAoIBAQDAmVvufevAg1ip
Kn8FhWjF1NNUFMqkgh2Cr1IMV+ovR2HyPTFwgr0XDhZHMSSnBw67Ttze3Ebxxoau
cBQcIASZ4hdTSIgjxG+9YQacLm9MXpfxHp5kcICzSfS1lrTexArTQglW8+rErYpk
2THN1S0PC4cRlBwoUCgB/+KCDkjJkUy8eCX+Gmd+6ehRKEQ5HdFHEfUr5hc/7/pB
liHietNKSxYEOr9TVZPiRjRtpUPMRMZE1RUM7GoxBrCWIXVdvEAGC0Xqd1ZVL1Tz
z2sQQDqvJ9fMN6fngKv2ePr+f5qeJwVzGO0DFVQs0y5x+Yl+pHbsdV1hSSnPPjK6
TaaBmX83AgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQM4GA1UdDwEB/wQEAwIFoDAN
BgkqhkiG9w0BAQUFAAOCAQEArWMJbdhlU8VfaF1cMJIbr569BZT+tIjQOz3OqNGQ
QpzHwclLoaKuC5pc/u0hw14MGS6Z440Iw4zK2/5bb/KL47r8H3d7T7PYMfK61AzK
sU9Kf96zTvHNWl9wXImB5blJfRLXnFWXNsVEF4FjU74plxJL7siasa5e86eNy9deN
20iKjvP8o4MgWewILrD01YZMDMDS1Uy82kWI6hvXG5+xBT5A1lo2xCj1S9y6/D4d
f0ilDZvaQk+7jjBCzLv5hET+1neoQBw52e7RWU8s2biQw+7TEAd08NytF3q/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) #

**Kopieer de uitvoer tussen HET BEGIN-CERTIFICAATVERZOEK naar EINDE-CERTIFICAATVERZOEK en slaat deze op in een notebookbestand.**

**CUBE CSR zou deze sleuteleigenschappen hebben:**

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

**4. Ontvang CA-certificaatwortel, dan CA-certificaat en ondertekend CUBE-certificaat van Achteraf CA.**

**Gebruik CSR die in Stap 3 gegenereerd is, om een ondertekend CUBE-certificaat te verkrijgen. De afbeelding is gemaakt van de Microsoft CA-webserver.**

## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 source (such as a Web server) in the Saved Request box.

### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
QpzHwclLoaKuC5pc/u0hw14MGS6Z440Iw4zK2/5b
sU9Kf96zTvHnWl9wXIb5b1JfRLXnFWXNsVEF4Fj
20iKjvP8o4MgWewILrD01YZMDMDS1Uy82kWI6hvX
f0i1DZvaQk+7jjBCzLv5hET+1neoQBw52e7RWU8s
bUKw5wT4pgGUJcDAWej3ZLqP91g5yyd9MiCdCRY+
-----END CERTIFICATE REQUEST-----
```

### Additional Attributes:

Attributes:

Submit >

## 5. Importeer CA-certificaat van wortel CA en subordinaat CA.

Open certificaataanvraag voor het EINDE-CERTIFICAAT in notatieblok en kopieer- en deeginhoud van het BEGIN-CERTIFICAATVERZOEK.

```
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-----
```

```
MIIFhDCCBGygAwIBAgIKYZVFyQAAAAAFjANBgkqhkiG9w0BAQUFAADBQMRIwEAYK
CZImiZPyLQBGGRYCbGkxYjAUBGoJKiaJk/IsZAEZFgZzb3BoaWExIjAgBgNVBAMT
GXNvcGhpYS1XSU4tM1MxOEpmDM0xNMkEtQ0EwHhcNMTQwOTI1MDAwNzU2WhcNMTYw
OTI1MDAxNzU2WjBjMjRlIwEAYKZCZImiZPyLQBGGRYCbGkxYjAUBGoJKiaJk/IsZAEZ
FgZzb3BoaWExGzAZBgNVBAMTEhNvcGhpYS1FWENIMjAxc1Q0TCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBBAJK+Nmz4rieYfr9gH3ISTuYz3TWpafpjdJ7l
7kIwwwC28TvJF15vrKEiaPyFzXL5TEHaWQ9YAo/WmdtuyF7aB+pLJ1soKcZxtrGv
gTmtuphcJ5Fpd43681R8ZXJiAT/Dz+Nsh4PC9GUUKQeycyRDeOBz08vL5pLj/W99
b8UMU1VQBu4e1zwxWPMFxB7zOeYsCfXmNGFUlp3HFdWZczgK3ldNO9I0X+p70UP
R0CQPMEQxuheqv9kazI1JKfNH8NqO8IH176Y32vUzLg3uvZgqWG6hGch/gjm4L/
1KmdZTNSH8H7Kf6vG6PNWrxXwWLnkhrWaYERYHelIshEj7ZUeB8sCAwEAAAOCAmUw
ggJhMBIGCSsGAQQBgjcvAQQFAgMBAEEwIwYJKwYBBAGCNxUCBByEFlnnd8HnCFKE
isPgI580og/LqwVSMBOGA1UdDgQWBBSsdYJZIU9IXyGm9aL67+8uDhM/EzAZBgkr
BgEEAYI3FAIEDB4KAFMADQBiAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/
BAUwAwEB/zAfBgNVHSMGDAWgBTvo1P6OP4LXm9RDv5MbIMk8jnofDCB3QYDVR0f
BIHVMIHSMIHPOIHM0IHJhoHGGRhcDovLy9DTj1zb3BoaWETV01OLTNTMThkQzNM
TTJBLUNBLENOPvdJTi0zUzE4SkMzTE0yQSxDtj1DRFAsQ049UHVibGljJTIwS2V5
JTIwU2Vydm1jZXMzQ049U2Vydm1jZXMzQ049Q29uZmlndXJhdGlvbixEQz1zb3Bo
aWESREM9bGk/Y2VygG1maWNhdGVsZXZyY2F0aW9uTG1zdD9iYXNlP29iamVjdENS
YXNzPWNSTERpc3RyaWJ1dGlvb1BvaW50MIHJBBggrBgEFBQcBAQSBvDCBuTCBtgYI
KwYBBQUHMAKGgalsZGFWoi8vL0NOPXNvcGhpYS1XSU4tM1MxOEpmDM0xNMkEtQ0Es
```

```
Q049QU1BLENOPVB1YmXpYyUyMETleSUyMFNlcnZpY2VzLENOPVn1cnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9c29waGhhLERDPWxpP2NBQ2VydGhmaWNhdGU/YmFz
ZT9vYmp1Y3RDbGFzc21jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MA0GCSqGSIb3DQEB
BQUAA4IBAQBj/+rX+9NjISZq1YwQXkLq6+LUh7OkCoeCHHfBGUaS+gvyYQ5OVwJI
TlPTj4YNh62A6pUXplo8mdxKxOmZeRLTYgf9Q/SiOY+qoxJ5zNliSqiRU4E02sRz
wrzfaQpLggyHXsyK1ABOGRGgqQWqZ7oXoKMRNmO+eu3NzBs4AVAAfL8UhFCv4IVx
/t6qIHY6YkNMVByjZ3MdFmohepN5CHZUHIvrOv9eAiv6+VaAn2nTeynyy7WnEv7P
+5L2kEFOSfnL4Zt2tEMqC5WyX6yJxDWmII0DTSyRshmxAoYl03EJHwW+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
MRIwEAYKCZImiZPyLQBGRYCbGkxFjAUBgoJkiaJk/IsZAEZFgZzb3BoaWExIjAg
BgNVBAMTGXNvcGhpYS1XSU4tM1MxOEpmDM0xNMkEtQ0EwHhcNMTQwOTEzMTZlMzQ1
WhcNMTEwOTEzMTZlMzQ1WjBQMRIwEAYKCZImiZPyLQBGRYCbGkxFjAUBgoJkiaJ
k/IsZAEZFgZzb3BoaWExIjAgBgNVBAMTGXNvcGhpYS1XSU4tM1MxOEpmDM0xNMkEt
Q0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC4aywr1oOpTdTrM8Ya
R3RkcahbbhR3q7P1l1uTDUDNM5Pi6P8z3MckfjB/yy6SWr1QnddhvMG6IGNtVxJ4
eyw0c7jBArXWOemGLOt454A0mCfcbwMhjQBycg9SM1r1Umzad7kOCzj/rD6hMbC4
jXpg6uU8g7eB3LzN1XF93DHjxYCBKMIeG45pqmsOc3mUj1CbCtnYXgno+mfhNzhR
HStH0z24XlGm99v46j/PqGjNRq4WKcWdc45SG3QjJDqDxnRJPkTRdNva66UJfDJp
4YMXQxOSkKMTDEDH/Eic7CrJ3EywUpMZAmqh4bmQ7Vo2pnRTbYdaAv/+yr8sMj
+FU3AgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1Ud
DgQWBBTvo1P6OP4LXm9RDv5MbIMk8jnOfDAQBgkrBgEEAYI3FQEEAwIBADANBgkq
hkiG9w0BAQUFAAOCAQEAmD7hJ2EEUmuMZrc/qtSJ2231oJlpKEPMVi7CrodtWSgu
5mNt1XsgxijYMqD5gJe1oq5dmv7efYvOvI2WTCXfwOBJ0on8tgLFwp1+SUJWs95m
OXTyoS9krsI2G2kQkQWniMqPdNxpj3C4WvQLPLwtEOSRZRBvsKy6lczrgrV2mZ
kx12n5YGrGcXSblPPUddlJep1l8U+AQC8wkSzfJu0yHJwoH+lrIfgqKUee4x7z6s
SCaGddCYr3OK/3Wzs/WjSO2UETvNL3NEtWHDC2t4Y7mmIMSDvGjHZUGZotwc9kt
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. Een CUBE-onderkend certificaat importeren.

Open certificaataanvraag voor het EINDE-CERTIFICAAT in notitieblok en kopieer- en deeginhoud van het BEGIN-CERTIFICAATVERZOEK.

```
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-----
```

```
MIIEAjCCAuqgAwIBAgIKQZZrHQABAAAAEzANBgkqhkiG9w0BAQUFADBjMREwEAYK
CZImiZPyLgQBGRYCbGkxJfjAUBgoJkiaJk/IsZAEZFgZzb3BoaWExGzAZBgNVBAMT
EnNvcGhpYS1FWENIMjAxMCI1DQTAeFw0xNTA0MDEwMDEzNDFAFw0xNjA0MDEwMDIz
NDFAmBExDzANBgNVBAMTBkNVQkUtMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMCZw+5968CDWkKqfWwFAMWU01QUYqSCHYKvUgxX6i9HYfI9MXCCvRcO
FkcxKycHDrT03N7cRvHGhq5wFBwgBJniF1NIiCPEb71hBpwub0xel/EenmRwgLNJ
9KWWtN7ECTnCCVbz6sStimTZMc3VLQ8LhxGUHChQKAH/4oIOSMmRTLx4Jf4aZ37p
6FEoRdKd0UcR9SvmFz/v+kGWIeJ600pLFgQ6v1NVk+JEmu2lQ8xExkSVFSbsajEG
sJYhdV28QAYLRep3VlUuVPPPaxBAOq8n18w3p+eAq/Z4+v5/mp6NZXMY7QMVCzT
LnH5iX6kdux1XWFJKc+kmTpNpogZfzcCAwEAAaOCASiWggEeMA4GA1UdDwEB/wQE
AwIFoDAdBgNVHQ4EFgQU9PbHMHSkYrjJ2+/+hSMEoma0QIwHwYDVR0jBBgwFoAU
rHWCWSFSPSf8hpvWi+u/vLg4TPxMwTwYDVR0fBEGwRjBEoEKgQIY+ZmlsZTovL0VY
Q0gyMDEwLnNvcGhpYS5saS9DZXJ0RW5yb2xsL3NvcGhpYS1FWENIMjAxMCI1DQSGx
KS5jcmwwbQYIKwYBBQUHAQEETBfMF0GCCsGAQUFBzACHlFmaWx1Oi8vRVhDSDIw
MTAuc29waG1hLmXpL0N1cnRfbnJvbGwvRVhDSDIwMTAuc29waG1hLmXpX3NvcGhp
YS1FWENIMjAxMCI1DQSGxKS5jcnQwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQUF
AAOCAQEAE7EAoXKIAij4vxZuxROOFofsmjcojU31ac5nrLCbq/FyW7eNblphL0NI
Dt/DlFZ5WK2q3Di+/UL1ldt3KYt9NZ1dLpmccnipbbNZ5LXLoHDkLNqt3qtLfKjv
J6GnnWCxLM18lxmlDzZT8VQtIQk5XZ8SC78hbTFtPxGZvfX70v22hekkOL1Dqw4h
/3mtaqxfnslB/J3Fgps1och45BndGiMAWavzRjjOKQaVLgVRvRvPIy3ZKDBaUleR
gsy5uODVSRhwMo3z84r+f03k4QarecgwZE+KfXoTpTAFhiCbLkKw0ZyRMXXzWqNfl
iotEQbs52neCwXNwV24aOCChQMw2xw==
```

```
-----END CERTIFICATE-----
```

```
% Router Certificate successfully imported
```

```
CUBE-2(config)#
```

## 7. Configuratie van TCP-TLS als transportprotocol.

Dit kan op mondiaal of op dial-peers niveau worden gedaan.

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

## 8. Aan sip-ua toegewezen trustpoint wordt dit trustpoint gebruikt voor alle signaling tussen CUBE en CUCM:

```
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
```

of, standaard trustpoint kan worden ingesteld voor alle sip signaling vanuit kubus:

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

## 9. Schakel SRTP in.

Dit kan op mondiaal of op dial-peers niveau worden gedaan.

```
Voice service voip
srtp fallback
```

10. Voor SRTP en Real-time Transport Protocol (RTP) is een beveiligde transcoder vereist.

Als de versie van Cisco IOS® 15.2.2T (CUBE 9.0) of hoger is, kan de lokale transcoder (LTI) worden geconfigureerd om de configuratie tot een minimum te beperken.

LTI-transcoder heeft geen PKI (Public Key Infrastructure)-betrouwbaarheidsconfiguratie nodig voor SRTP-RTP-oproepen.

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

Als Cisco IOS® lager is dan 15.2.2T, moet u de SCCP-transcoder configureren.

SCCP-transcoder zou echter een betrouwbaar punt voor signalering nodig hebben, wanneer dezelfde router wordt gebruikt om de transcoder te ontvangen, dan kan hetzelfde trustpunt (SUBCA1) worden gebruikt voor CUBE en transcoder.

```
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
```

## CUCM configureren

1. Generate CallManager CSR op alle CUCM-knooppunten.



Navigeer naar **CM OS-beheer > Beveiliging > certificaatbeheer > Aanvraag tot signalering** genereren zoals in de afbeelding.

**Generate Certificate Signing Request**

Generate Close

**Status**

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

**Generate Certificate Signing Request**

Certificate Purpose\* CallManager

Distribution\* cmpub

Common Name\* cmpub

**Subject Alternate Names (SANs)**

Parent Domain

Key Length\* 2048

Hash Algorithm\* SHA256

Generate Close

i \*- indicates required item.

CallManager CSR zou deze belangrijke eigenschappen hebben:

Requested Extensions:

X509v3 Extended Key Usage:

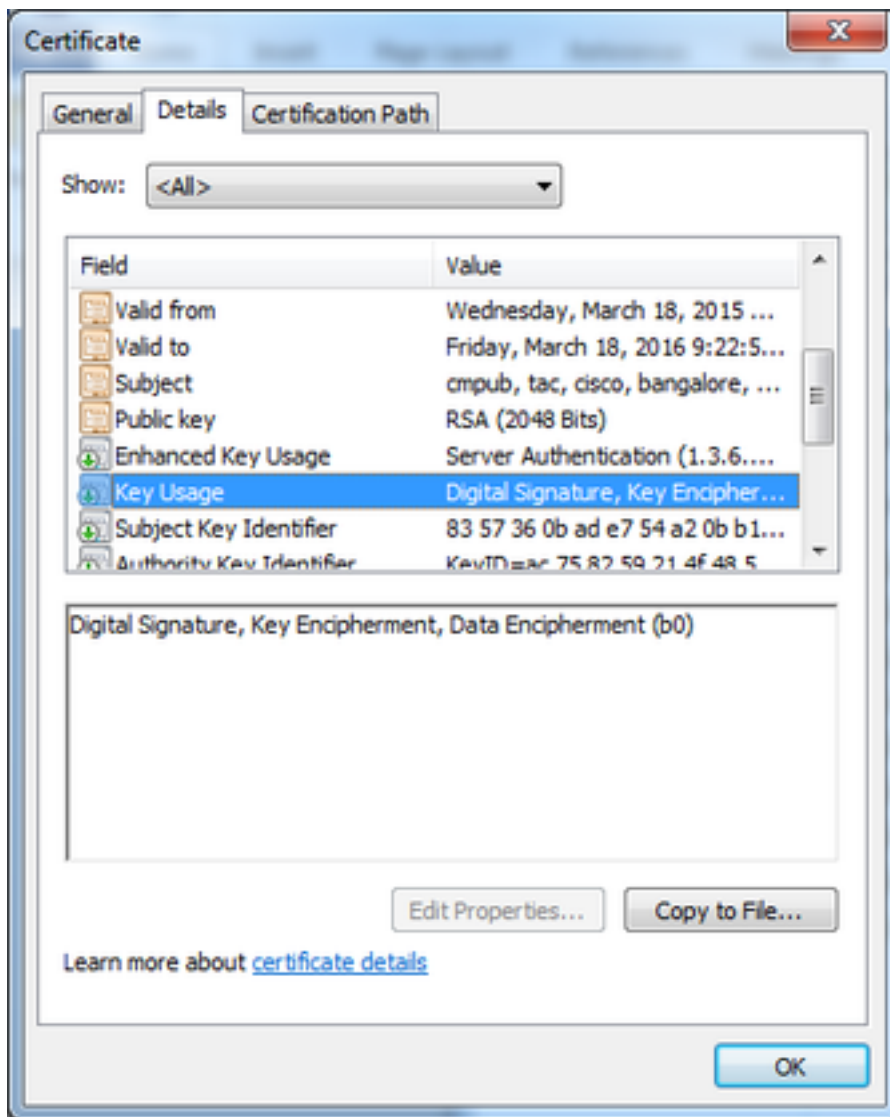
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System

X509v3 Key Usage:

Digital Signature, Key Encipherment, Data Encipherment, Key Agreement

2. Ontvang CallManager-certificaat voor alle CM-knooppunten die door ondergeschikte CA zijn ondertekend.



Gebruik CSR gegenereerd in Stap 1. Elk certificaatsjabloon van een webserver zou werken, zorg ervoor dat het ondertekende certificaat ten minste deze eigenschappen in gebruik heeft: **Digitale handtekeningen, toetsuitbreiding, gegevensversterking** zoals in de afbeelding.




3. Upload CA-certificaat van Root CA en subordineer CA als CallManager-Trust.

Navigeer in op **CM OS-beheer > Beveiliging > certificaatbeheer > Upload certificaatketting/certificaat** - zoals in de afbeeldingen wordt weergegeven.

### Upload Certificate/Certificate chain

 Upload  Close

**Status**


 Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

**Upload Certificate/Certificate chain**



Certificate Purpose\*

Description(friendly name)


Upload File  root.cer

 \*- indicates required item.

### Upload Certificate/Certificate chain

 Upload  Close

**Status**


 Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

**Upload Certificate/Certificate chain**

Certificate Purpose\*

Description(friendly name)

Upload File  subordinate.cer

 \*- indicates required item.

4. Het certificaat van Upload CallManager als **CallManager** ondertekend zoals in de afbeelding.

**Upload Certificate/Certificate chain**

Upload Close

**Status**

**i** Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

**Upload Certificate/Certificate chain**

Certificate Purpose\* CallManager

Description(friendly name) Self-signed certificate

Upload File Browse... cmpub.cer

Upload Close

**i** \*- indicates required item.

5. certificaatlijst (CTL) bijwerken met betrekking tot uitgever (via 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. Start CallManager en TFTP-service op alle knooppunten en de CAPF-service op uitgever.

7. Maak een nieuw SIP Trunk-beveiligingsprofiel.

Raadpleeg bij CM-beheer **stelsel > Security > SIP Trunk-beveiligingsprofielen > Zoeken**.

Kopieert bestaand niet-beveiligd SIP Trunk-profiel om een nieuw beveiligd profiel te maken zoals in deze afbeelding.

## SIP Trunk Security Profile Configuration

Save  Delete  Copy  Reset  Apply Config  Add New

### SIP Trunk Security Profile Information

Name*	CUBE-2 Secure SIP Trunk Profile
Description	Secure SIP Trunk Profile authenticated by null String
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	CUBE-2
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input checked="" type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

8. Maak SIP romp aan CUBE.

Schakel **SRTP** in op SIP-romp zoals in de afbeelding **toegestaan**.

**Trunk Configuration**

Save Delete Reset Add New

AAR Group: < None >

Tunneled Protocol\*: None

QSIG Variant\*: No Changes

ASN.1 ROSE OID Encoding\*: No Changes

Packet Capture Mode\*: None

Packet Capture Duration: 0

Media Termination Point Required

Retry Video Call as Audio

Path Replacement Support

Transmit UTF-8 for Calling Party Name

Transmit UTF-8 Names in QSIG APDU

Unattended Port

SRTP Allowed: When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure Consider Traffic on This Trunk Secure\*: When using both sRTP and TLS

Route Class Signaling Enabled\*: Default

Use Trusted Relay Point\*: Default

PSTN Access

Run On All Active Unified CM Nodes

Configureer de doelpoort 5061 (TLS) en pas het nieuwe beveiligde SIP-routerbeveiligingsprofiel op de SIP-romp toe zoals in de afbeelding.

**Trunk Configuration**

Save Delete Reset Add New

**SIP Information**

**Destination**

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.95.153		5061

MTP Preferred Originating Codec\*: 711ulaw

BLF Presence Group\*: Standard Presence group

**SIP Trunk Security Profile\*: CUBE-2 Secure SIP Trunk Profile**

Rerouting Calling Search Space: < None >

Out-Of-Dialog Refer Calling Search Space: < None >

SUBSCRIBE Calling Search Space: < None >

SIP Profile\*: Standard SIP Profile [View Details](#)

DTMF Signaling Method\*: No Preference

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

```
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
```

De output van **show roepen actieve stem korte** opdracht wordt opgenomen wanneer LTI transcoder wordt gebruikt.

```
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
```

Tevens wordt, wanneer SRTP een versleuteld gesprek tussen de Cisco IP-telefoon en CUBE of Gateway wordt uitgevoerd, een pictogram voor het slot op de IP-telefoon weergegeven.

# Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Deze ideeën kunnen helpen bij het oplossen van problemen met PKI/TLS/SIP/SRTP.

```
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
```