Konfigurieren des SIP-TLS-Trunks im Communications Manager mit einem von der Zertifizierungsstelle signierten Zertifikat

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Konfigurieren
Schritt 1: Verwenden Sie die öffentliche CA oder die Einrichtungs-CA auf Windows Server 2003.
Schritt 2: Hostname und Einstellungen überprüfen
Schritt 3: Erstellen und Herunterladen der Zertifikatsanforderung (Certificate Signing Request, CSR)
Schritt 4: Signieren Sie den CSR mit der Microsoft Windows 2003-Zertifizierungsstelle.
Schritt 5: Abruf des Root-Zertifikats von der CA
Schritt 6: CA-Stammzertifikat als CallManager Trust hochladen
Schritt 7: Laden Sie das CallManager CSR-Zertifikat für das CA-Zeichen als CallManager-Zertifikat hoch.
Schritt 8: Erstellen von SIP-Trunk-Sicherheitsprofilen
Schritt 9: SIP-Trunks erstellen
Schritt 10: Erstellen von Routenmustern
Überprüfen
Fehlerbehebung
Paketerfassung auf CUCM erfassen
Erfassung von CUCM-Ablaufverfolgungen

Einführung

Dieses Dokument beschreibt einen Schritt-für-Schritt-Prozess zur Konfiguration des SIP-Trunks (Session Initiation Protocol) Transport Layer Security (TLS) auf Communications Manager mit einem Zertifikat der Zertifizierungsstelle (Certificate Authority, CA).

Nach Befolgen dieses Dokuments werden SIP-Nachrichten zwischen zwei Clustern mithilfe des TLS verschlüsselt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Communications Manager (CUCM)
- SIP

Verwendete Komponenten

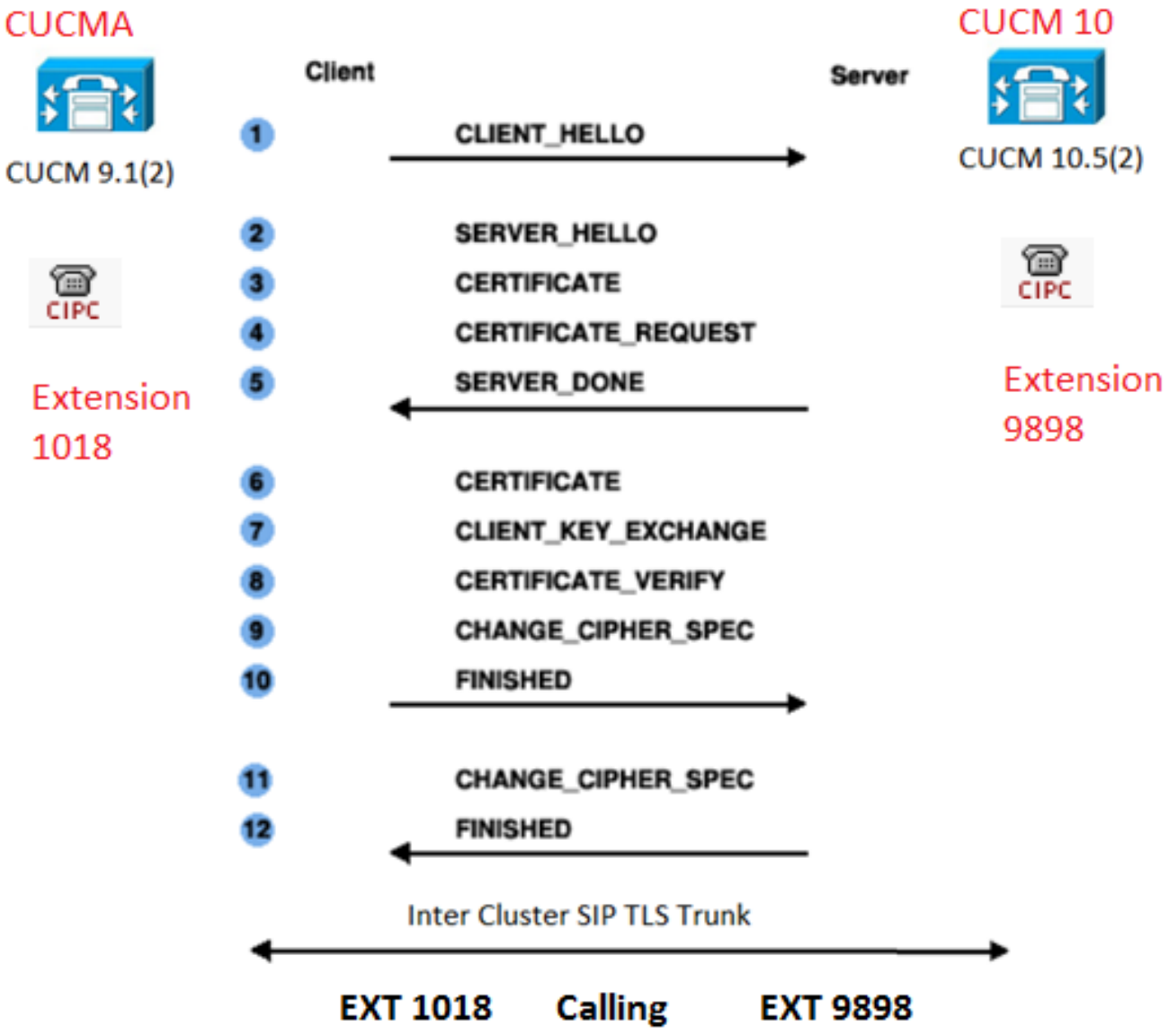
Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- CUCM-Version 9.1(2)
- CUCM-Version 10.5(2)
- Microsoft Windows Server 2003 als CA

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

Wie in diesem Bild gezeigt, SSL-Handshake mit Zertifikaten.



Konfigurieren

Schritt 1: Verwenden Sie die öffentliche CA oder die Einrichtungs-CA auf Windows Server 2003.

Weitere Informationen finden Sie unter: Einrichten der CA auf einem Windows 2003-Server

Schritt 2: Hostname und Einstellungen überprüfen

Zertifikate basieren auf Namen. Stellen Sie sicher, dass die Namen korrekt sind, bevor Sie beginnen.

```
From SSH CLI
admin:show cert own CallManager
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
```

Um den Hostnamen zu ändern, klicken Sie auf den folgenden Link: Ändern des Hostnamens in CUCM

Schritt 3: Erstellen und Herunterladen der Zertifikatsanforderung (Certificate Signing Request, CSR)

CUCM 9.1(2)

Um den CSR zu generieren, navigieren Sie zu **OS Admin > Security > Certificate Management > Generate CSR.**

Wählen Sie im Feld **Zertifikatsname die** Option **CallManager** aus der Dropdown-Liste aus.

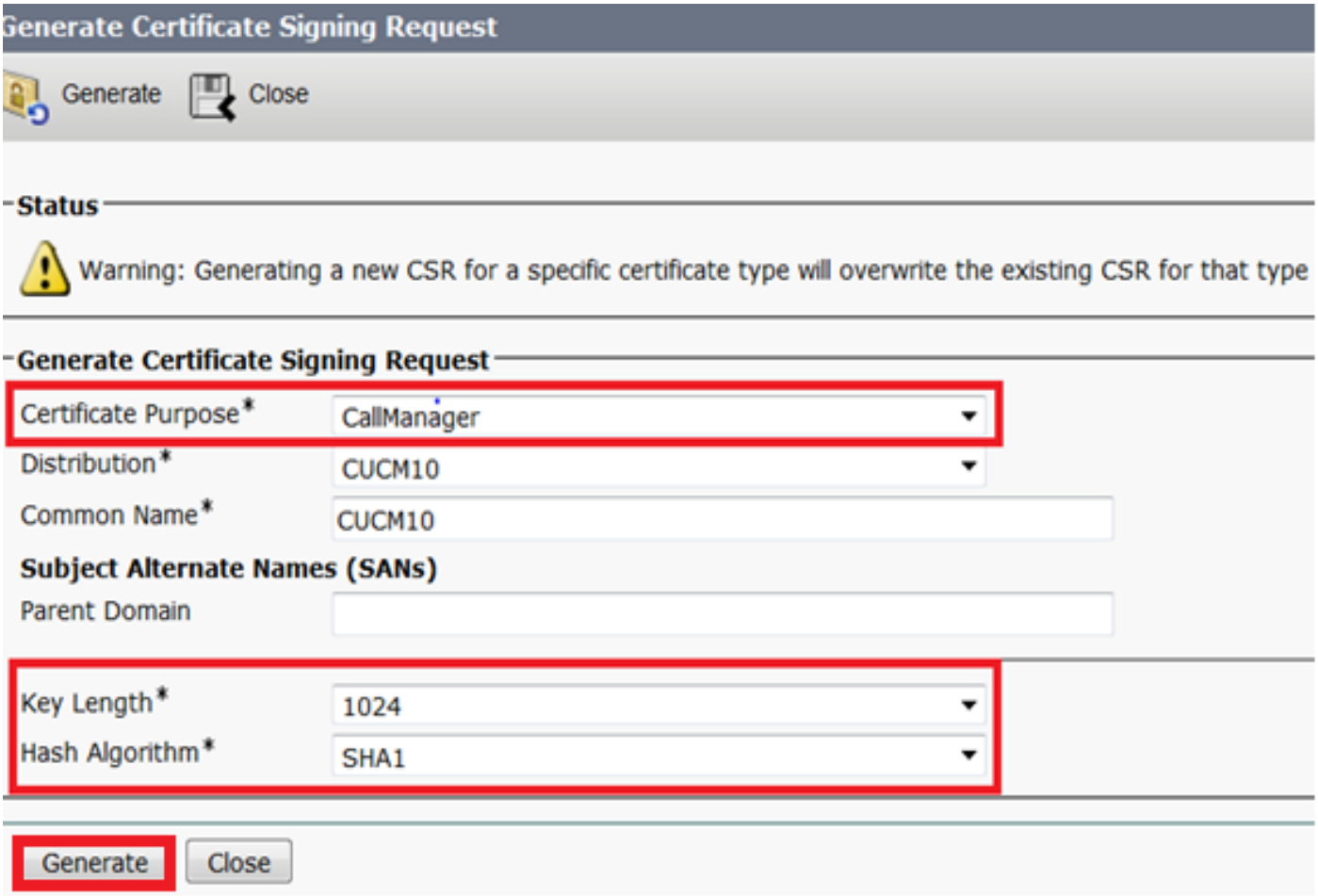
Um den CSR herunterzuladen, navigieren Sie zu **OS Admin > Security > Certificate Management > Download CSR (OS-Administrator > Sicherheit > Zertifikatsverwaltung > CSR herunterladen).**

Wählen Sie im Feld **Zertifikatsname** die Option **CallManager** aus der Dropdown-Liste aus.

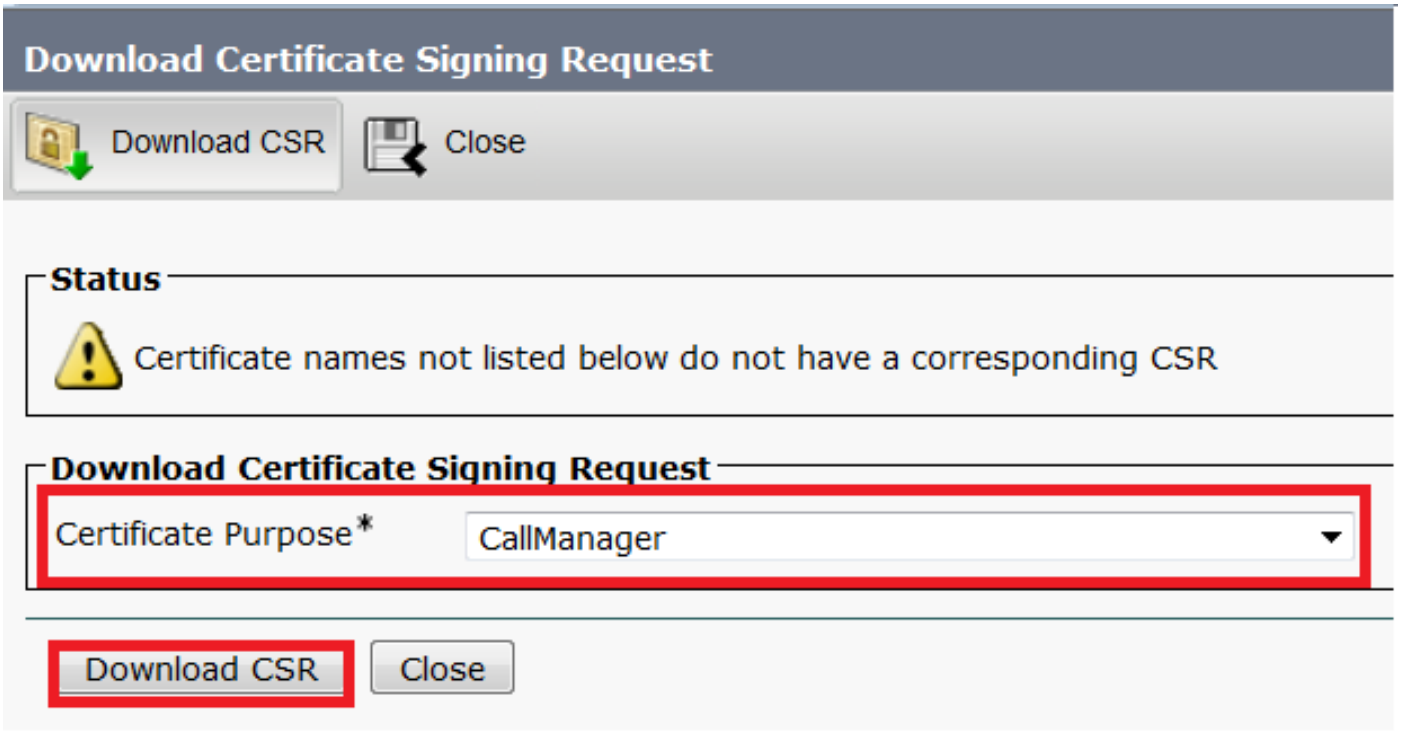
CUCM 10.5(2)

Um den CSR zu generieren, wählen Sie **OS Admin > Security > Certificate Management > Generate CSR (Betriebssystemadministrator > Sicherheit > Zertifikatsverwaltung > CSR erstellen)** aus.

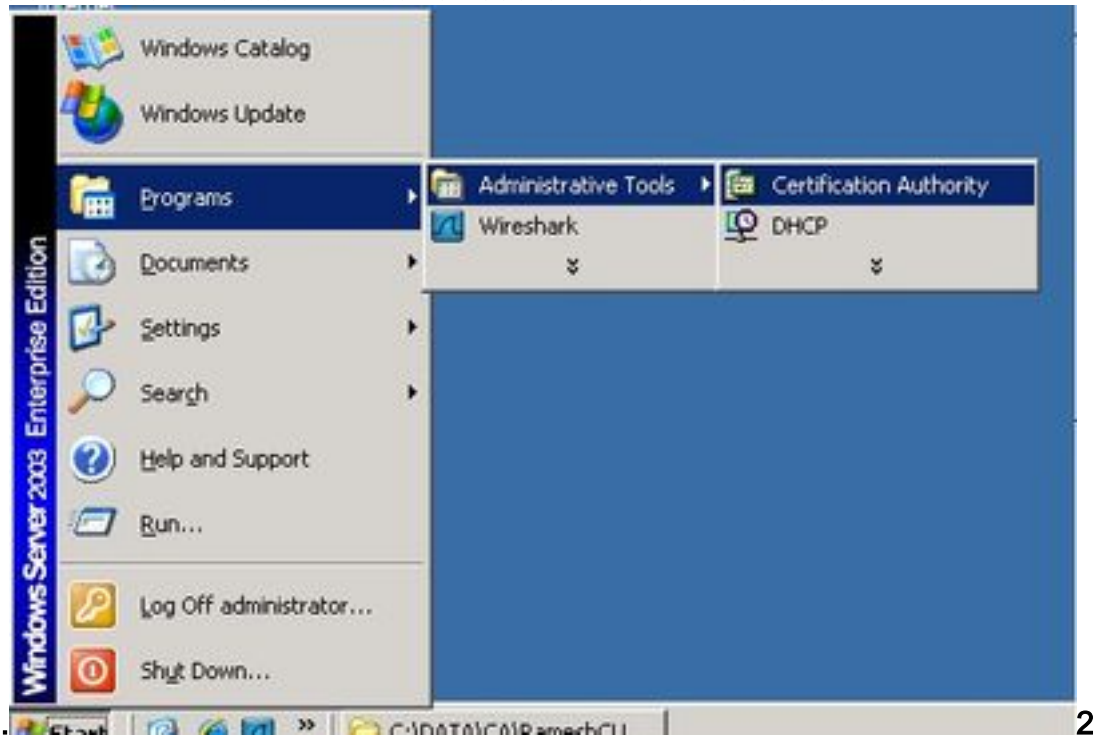
1. Wählen Sie im Feld Certificate Purpose (Zweck des Zertifikats) in der Dropdown-Liste CallManager aus.
2. Wählen Sie im Feld Schlüssellänge die Option 1024 aus der Dropdown-Liste aus..
3. Wählen Sie im Feld Hash Algorithm die Option SHA1 aus der Dropdown-Liste aus.



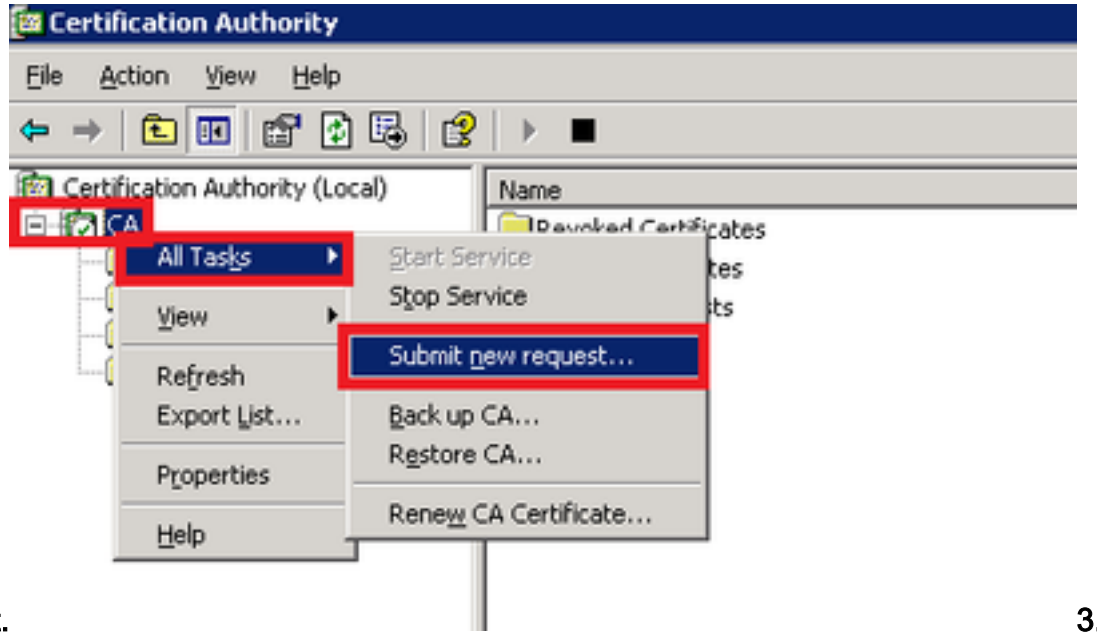
Um den CSR herunterzuladen, navigieren Sie zu OS Admin > Security > Certificate Management > Download CSR (OS-Administrator > Sicherheit > Zertifikatsverwaltung > CSR herunterladen).Wählen Sie im Feld Zertifikatzweck die Option CallManager aus der Dropdown-Liste aus.



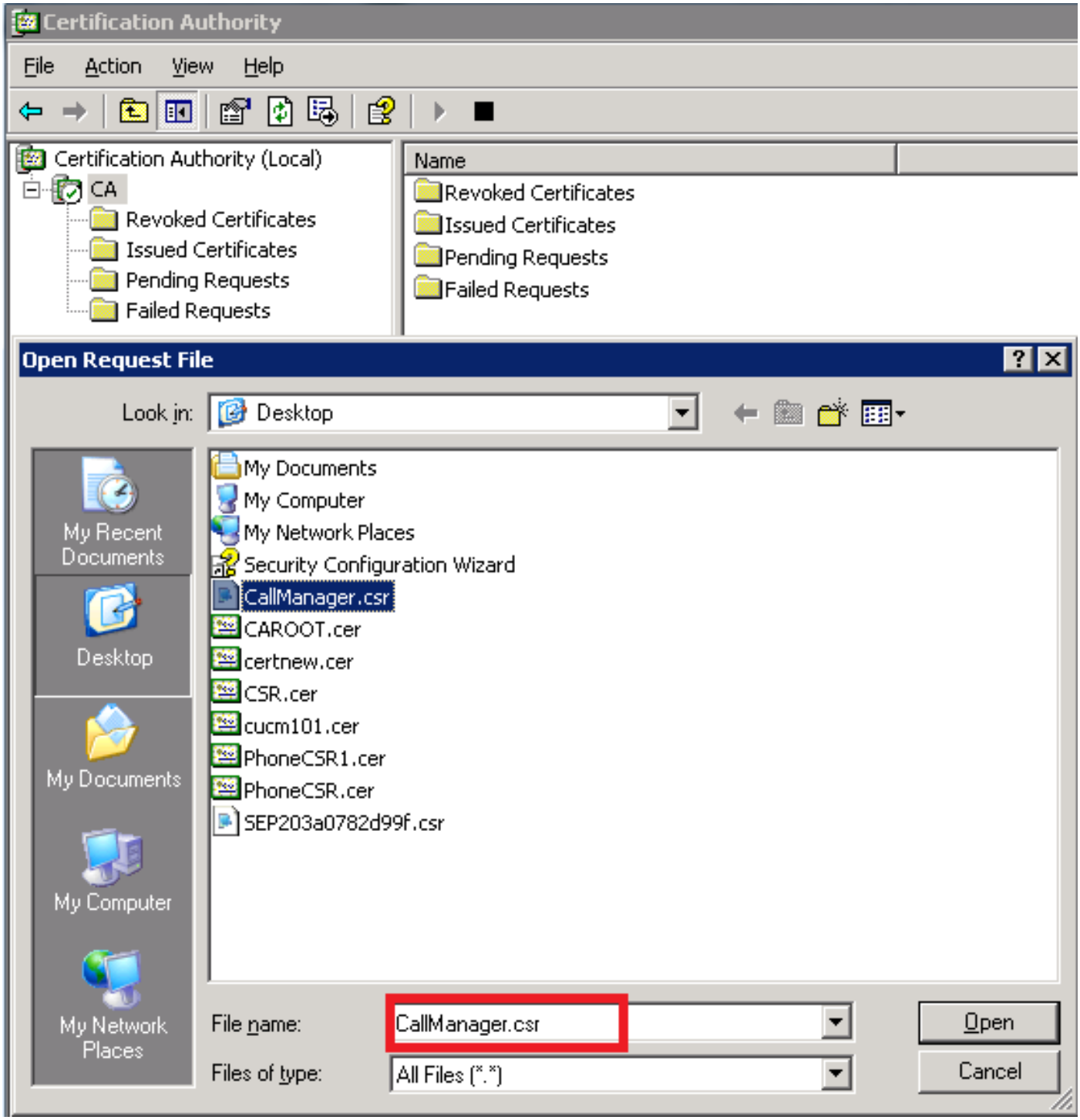
Hinweis: Der CallManager-CSR wird mit den 1024-Bit-RSA-Schlüsseln (Rivest-Shamir-Addleman) generiert.Schritt 4: Signieren Sie den CSR mit der Microsoft Windows 2003-Zertifizierungsstelle.Dies ist eine optionale Information zum Signieren des CSR mit der Microsoft Windows 2003 CA.1. Öffnen Sie die



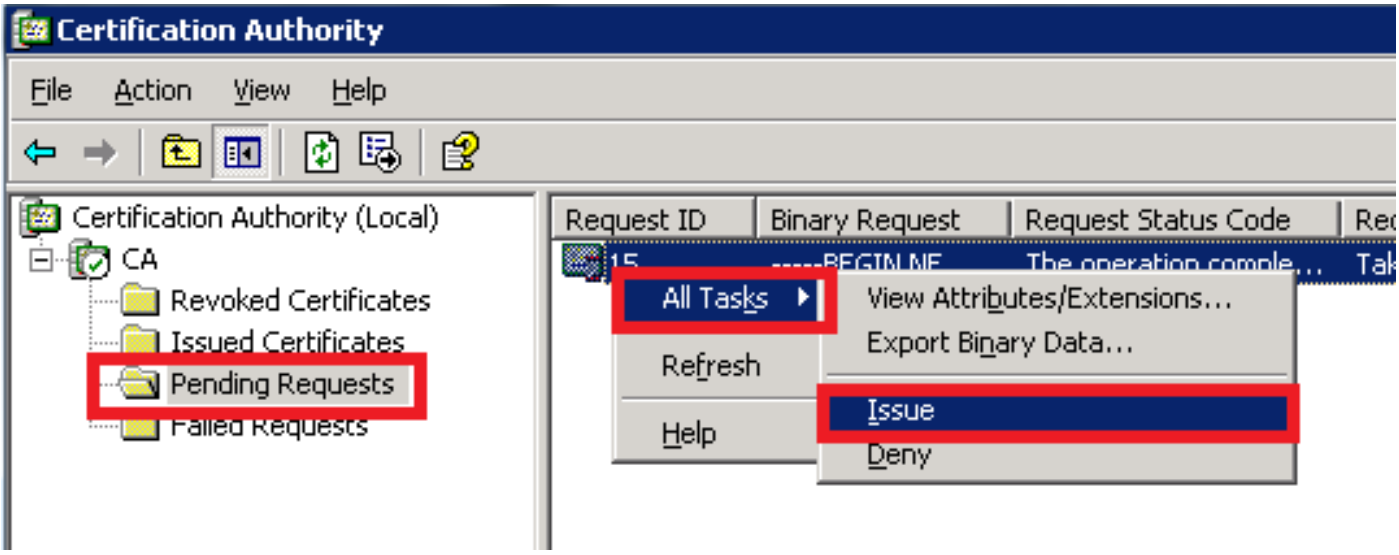
Zertifizierungsstelle. 2. Klicken Sie mit der rechten Maustaste auf das CA-Symbol, und navigieren Sie zu All Tasks >



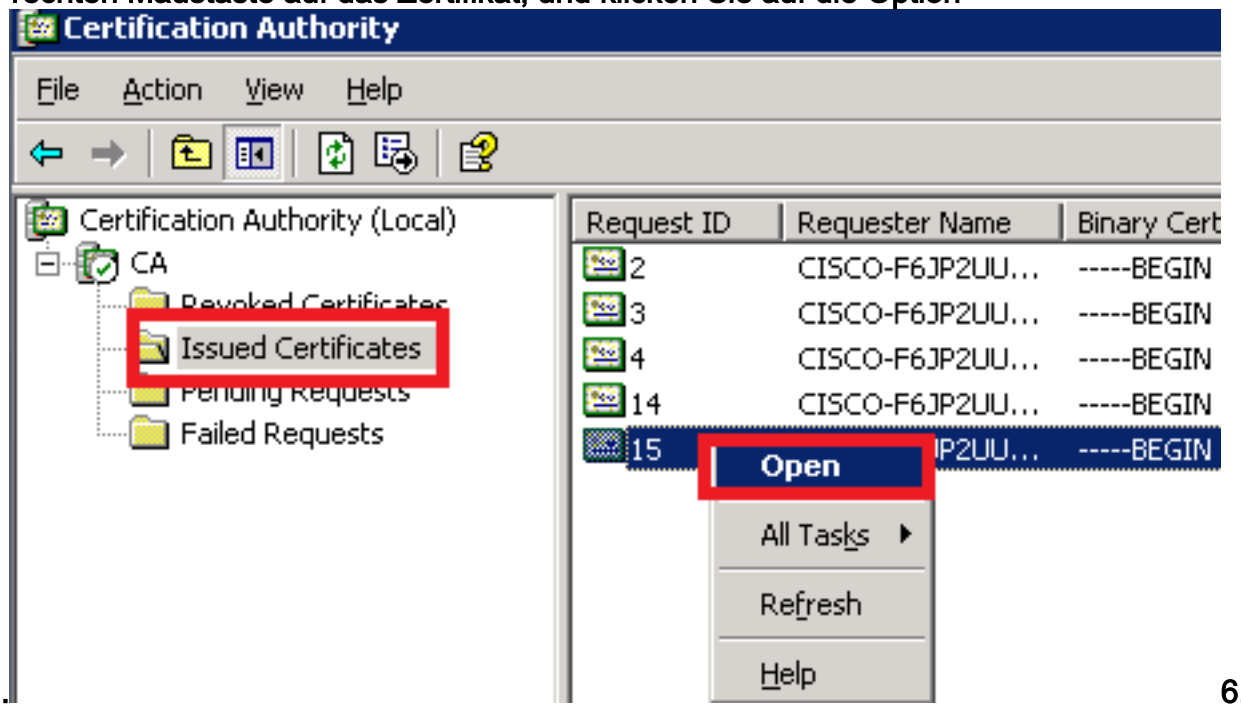
Submit new request. 3. Wählen Sie den CSR aus, und klicken Sie auf die Option Öffnen (gilt sowohl für die CSRs (CUCM 9.1(2) und CUCM
10.5(2))).



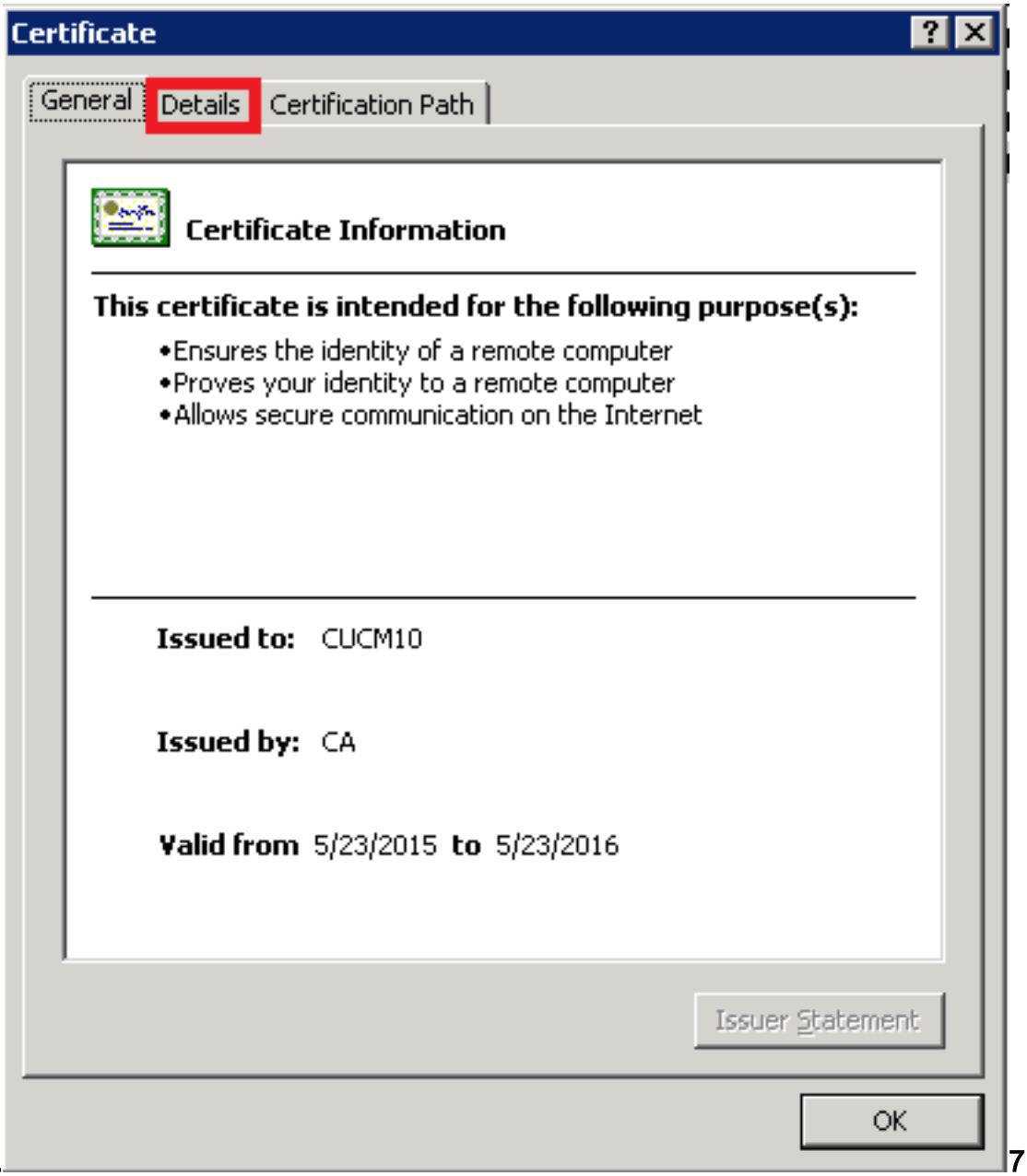
4. Alle geöffneten CSRs werden im Ordner Ausstehende Anfragen angezeigt. Klicken Sie mit der rechten Maustaste auf jeden CSR, und navigieren Sie zu Alle Aufgaben > Ausstellen, um die Zertifikate auszustellen. (Gilt sowohl für CSR (CUCM 9.1(2) und CUCM 10.5(2)))



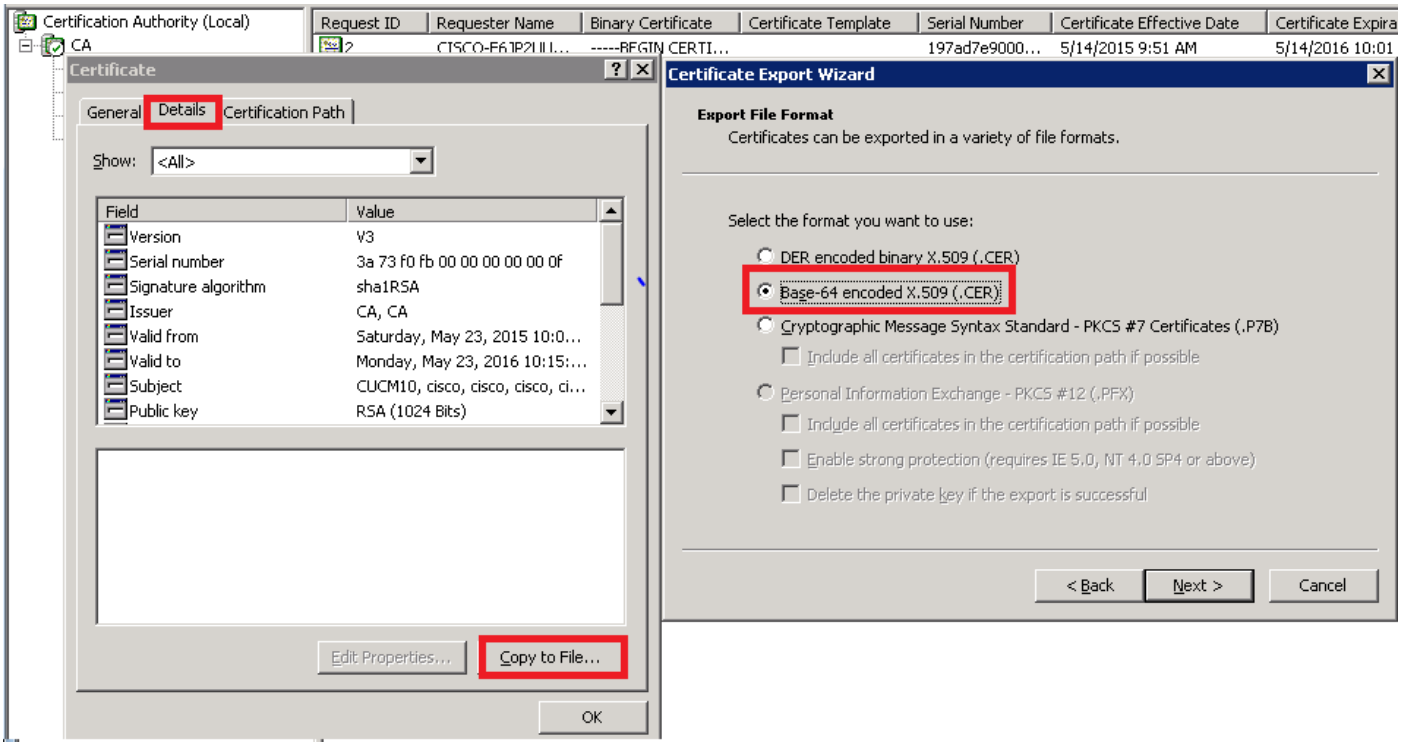
5. Um das Zertifikat herunterzuladen, wählen Sie den Ordner Ausgestellte Zertifikate.Klicken Sie mit der rechten Maustaste auf das Zertifikat, und klicken Sie auf die Option



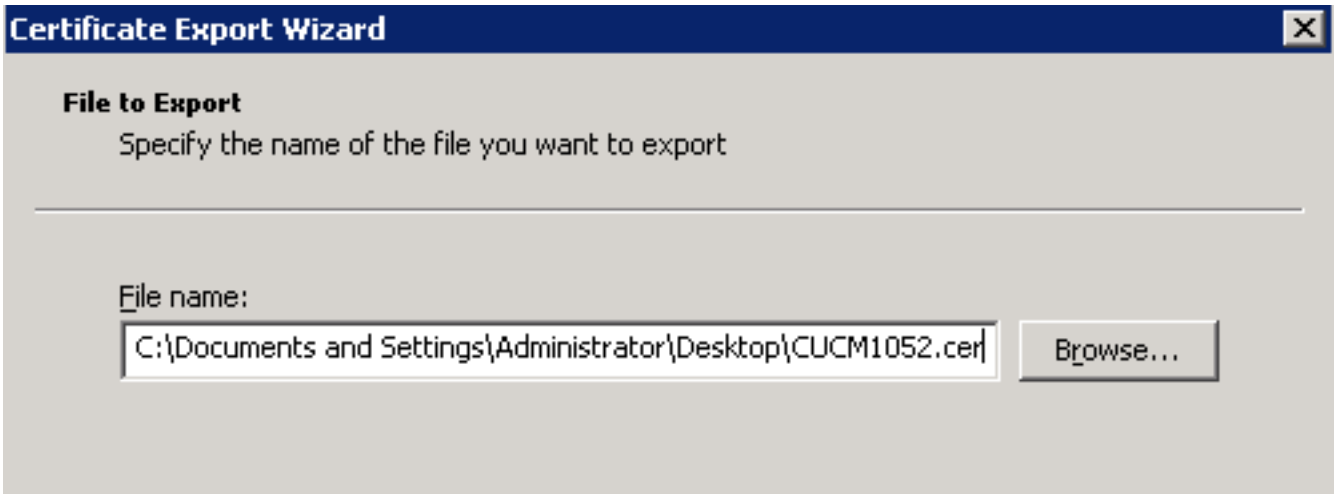
Öffnen. 6. Die Zertifikatdetails werden angezeigt. Um das Zertifikat herunterzuladen, wählen Sie die Registerkarte Details aus und klicken auf die Schaltfläche In Datei



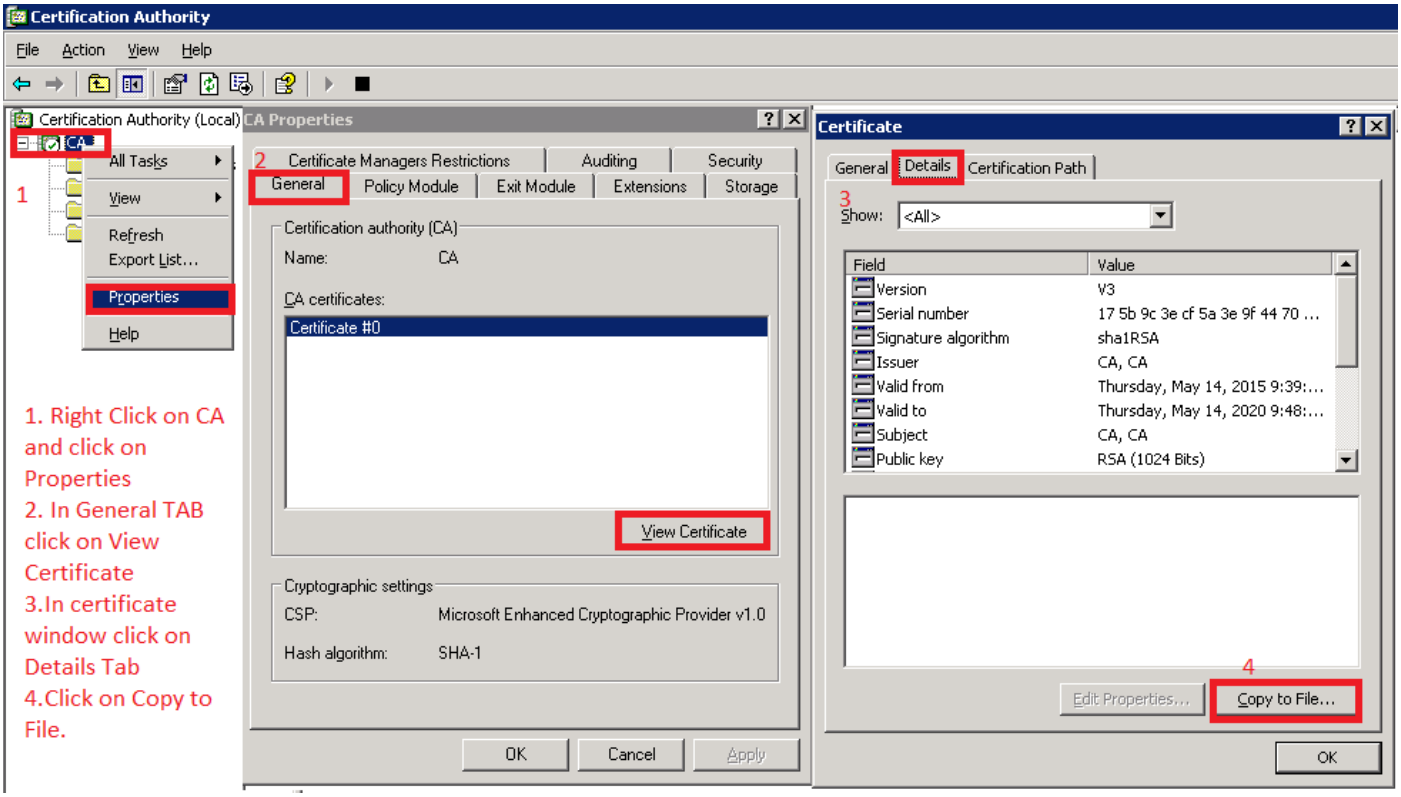
kopieren...7. Klicken Sie im Fenster Certificate Export Wizard (Assistent für den Zertifikatsexport) auf das Optionsfeld Base-64-codierte
X.509(.CER).



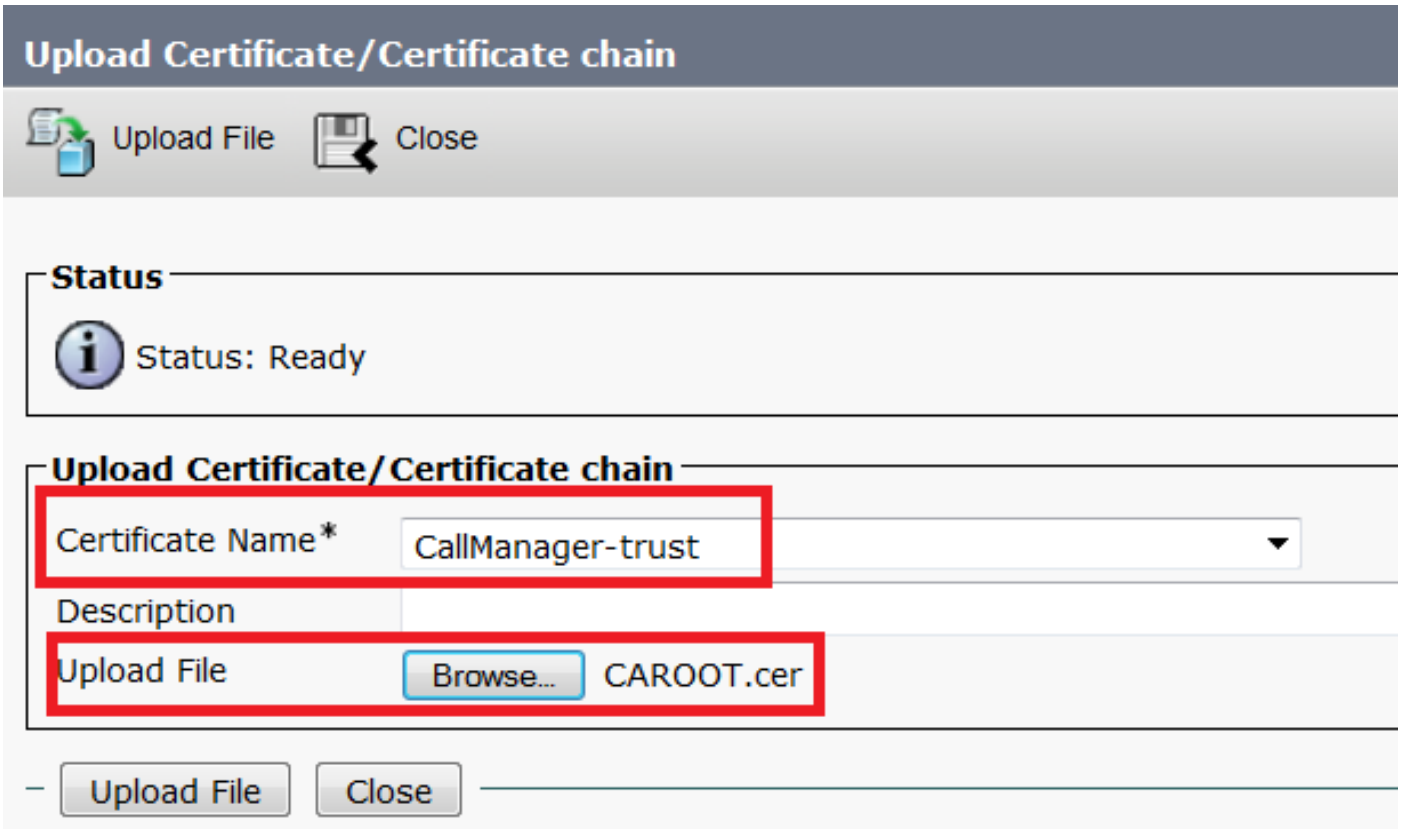
8. Geben Sie der Datei einen korrekten Namen. In diesem Beispiel wird das Format CUCM1052.cer
verwendet.



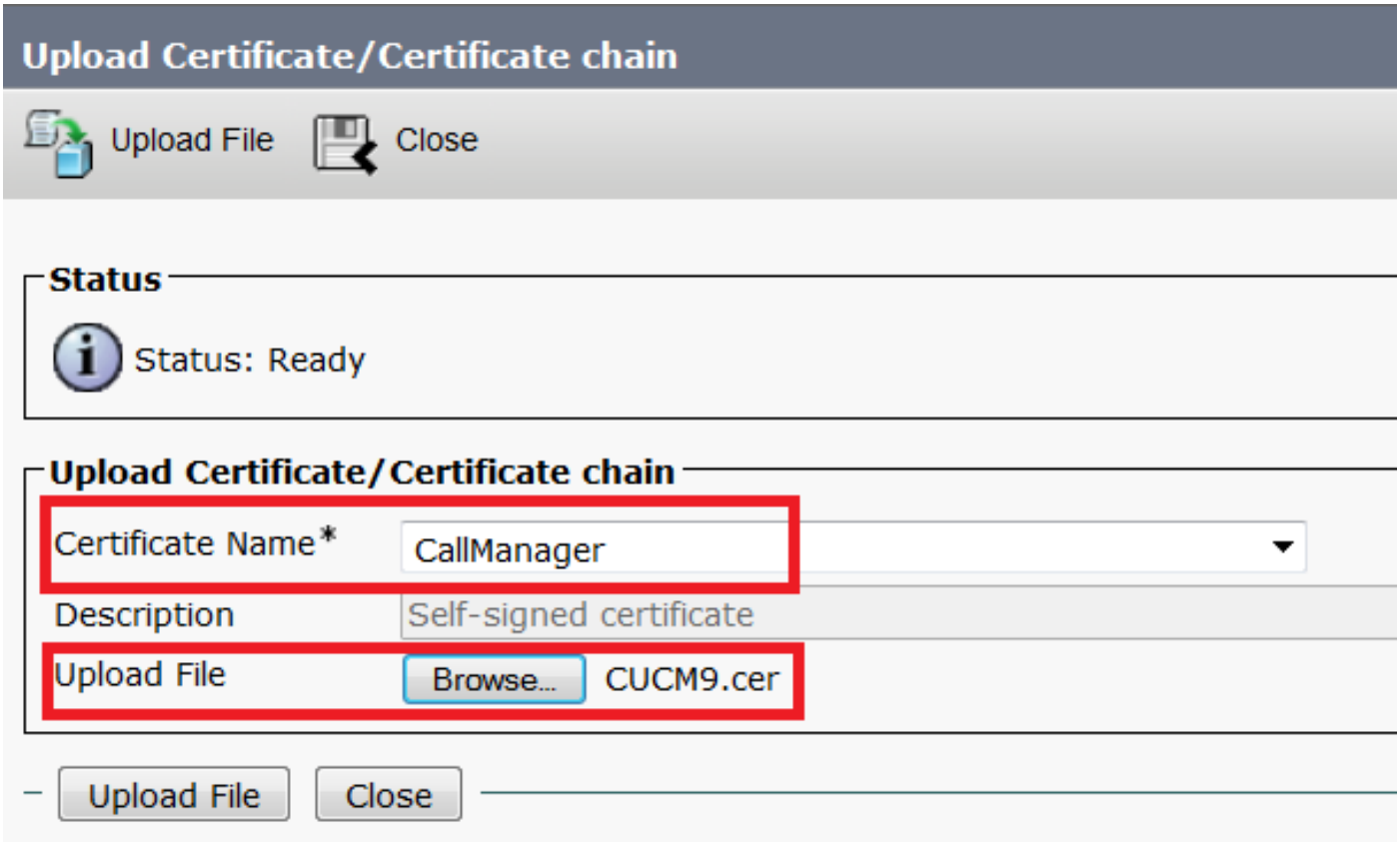
Für CUCM 9.1(2) ist das gleiche Verfahren anzuwenden.Schritt 5: Abruf des Root-Zertifikats von der CAÖffnen Sie das Fenster Zertifizierungsstelle. So laden Sie die Root-CA herunter1. Klicken Sie mit der rechten Maustaste auf das CA-Symbol, und klicken Sie auf die Option Eigenschaften.2. Klicken Sie in der Regel auf Zertifikat anzeigen.3. Klicken Sie im Fenster Zertifikat auf die TAB mit den Details.4. Klicken Sie auf In Datei
kopieren...



Schritt 6: CA-Stammzertifikat als CallManager Trust hochladenMelden Sie sich zum Hochladen des CA-Stammzertifikats bei OS Admin > Security > Certificate Management > Upload Certificate/Certificate Chain an.

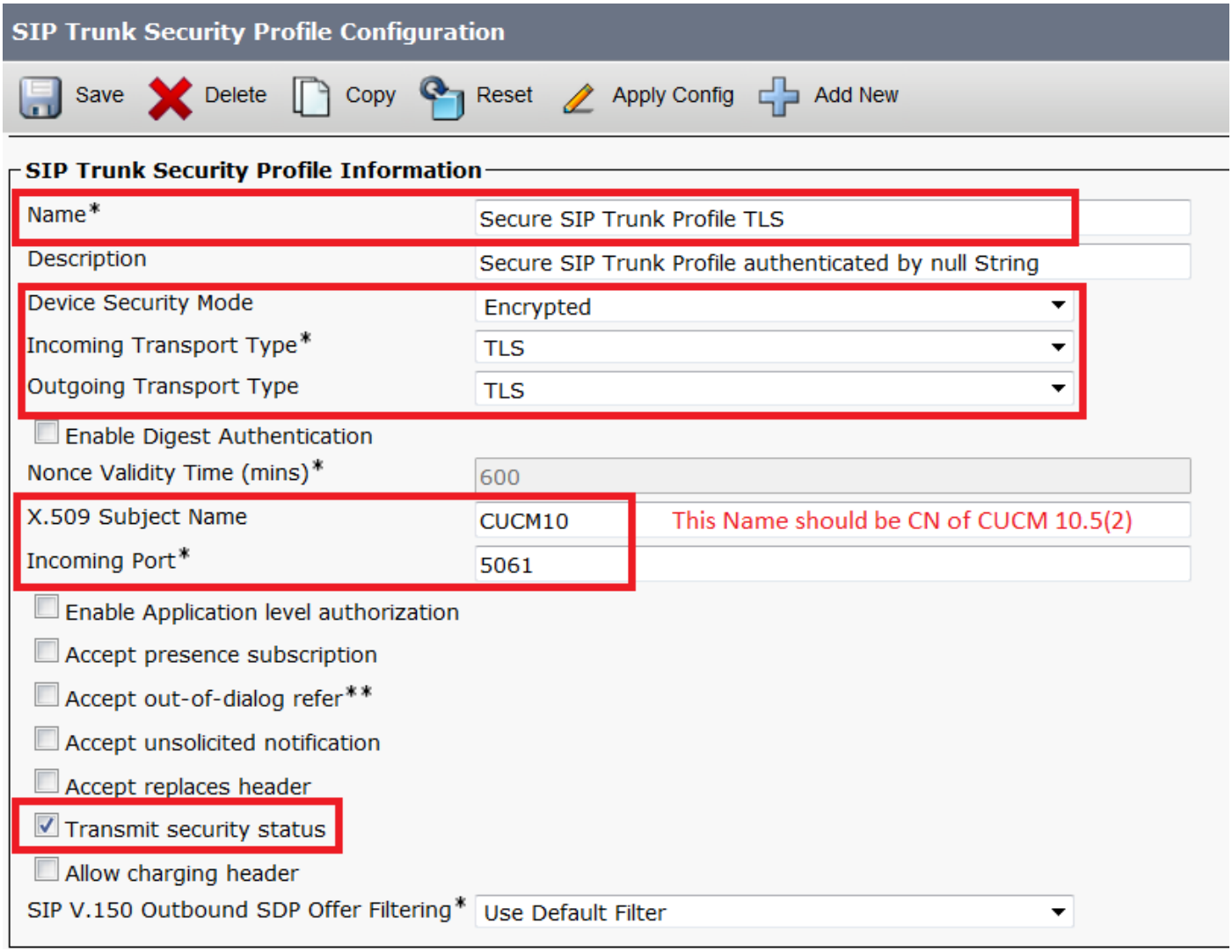


Hinweis: Führen Sie diese Schritte für die CUCMs (CUCM 9.1(2) und CUCM 10.5(2)) aus.Schritt 7: Laden Sie das CallManager CSR-Zertifikat für das CA-Zeichen als CallManager-Zertifikat hoch.Melden Sie sich für das Hochladen des CA-Zeichens CallManager CSR an bei OS Admin > Security > Certificate Management > Upload Certificate/Certificate
Chain.



Hinweis: Führen Sie diese Schritte für die CUCMs (CUCM 9.1(2) und CUCM 10.5(2)) aus.Schritt 8: Erstellen von SIP-Trunk-SicherheitsprofilenCUCM 9.1(2)

Um das SIP-Trunk-Sicherheitsprofil zu erstellen, navigieren Sie zu System > Security > SIP Trunk Security Profile.Kopieren Sie das vorhandene nicht sichere SIP-Trunk-Profil, und geben Sie ihm einen neuen Namen. Im Beispiel wurde das nicht sichere SIP-Trunk-Profil in das sichere SIP-Trunk-Profil TLS
umbenannt.



In X.509 Subject Name verwenden Sie den Common Name (CN) des CUCM 10.5(2) (Zertifizierungsstellen-signiertes Zertifikat), wie in diesem Bild gezeigt.

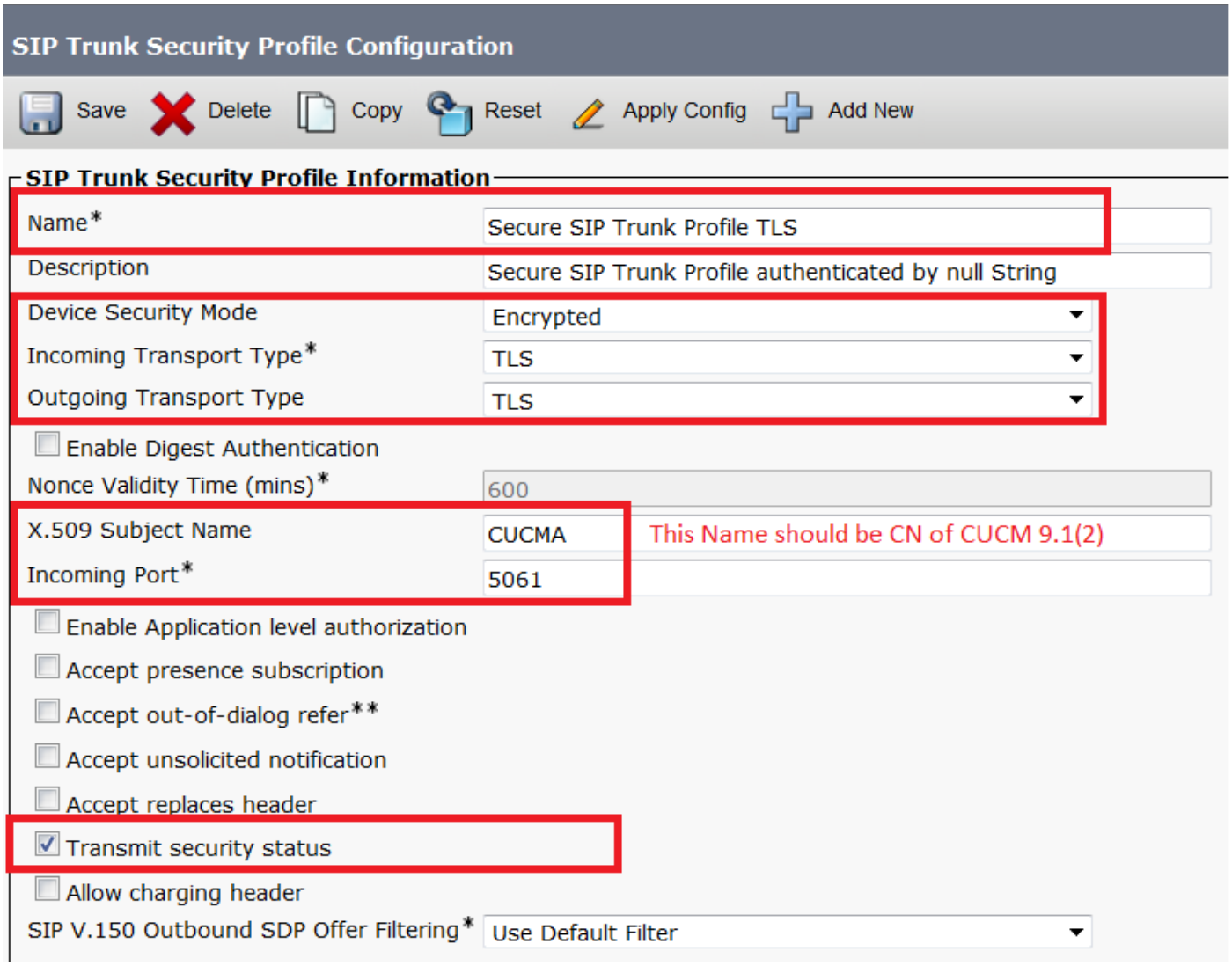
Certificate Settings

Locally Uploaded	23/05/15
File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Certificate Signed by CA

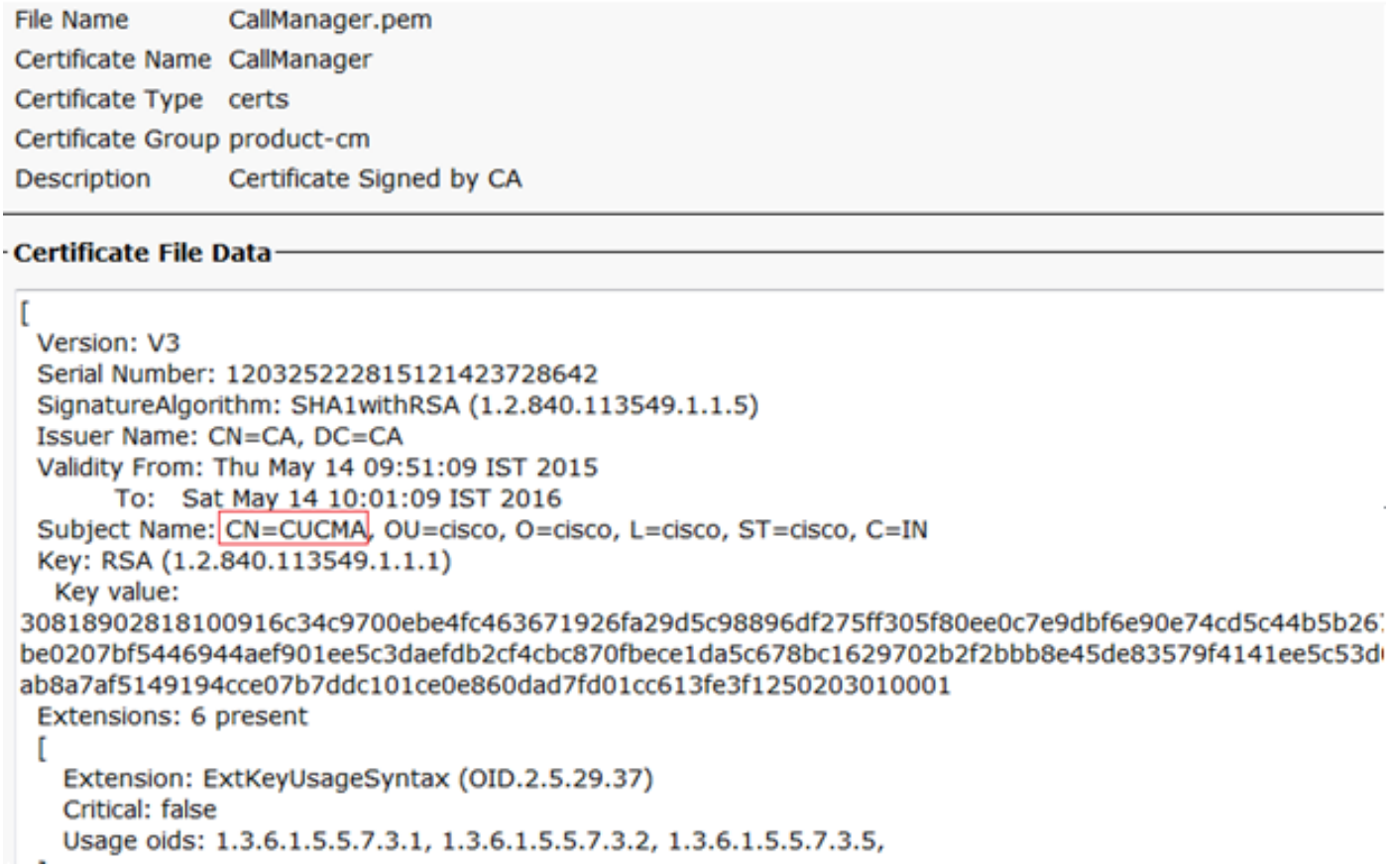
Certificate File Data

```
[
  Version: V3
  Serial Number: 398B1DA600000000000E
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=CA, DC=CA
  Validity From: Sat May 23 17:50:42 IST 2015
         To:   Mon May 23 18:00:42 IST 2016
  Subject Name: CN=CUCM10, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
  Key: RSA (1.2.840.113549.1.1.1)
    Key value:
30818902818100bcf093aa206190fe76abe13e3bd3ec45cc8b2afeee86e8393f568e1c9aa0c5fdf3f044eebc
f2d999ed8ac3592220fef3f9dcf2d2e7e939a4b26896152ebb250e407cb65d9e04bf71e8c345633786041e
5c806405160ac42a7133d7d644294226b850810fffd001e5bf2b39829b1fb27f126624e5011f151f0ef07c7
eccb734710203010001
  Extensions: 6 present
  [
```

CUCM 10.5(2)Navigieren Sie zu System > Security > SIP Trunk Security Profile.Kopieren Sie das vorhandene nicht sichere SIP-Trunk-Profil, und geben Sie ihm einen neuen Namen. Im Beispiel wurde das nicht sichere SIP-Trunk-Profil in das sichere SIP-Trunk-Profil TLS umbenannt.



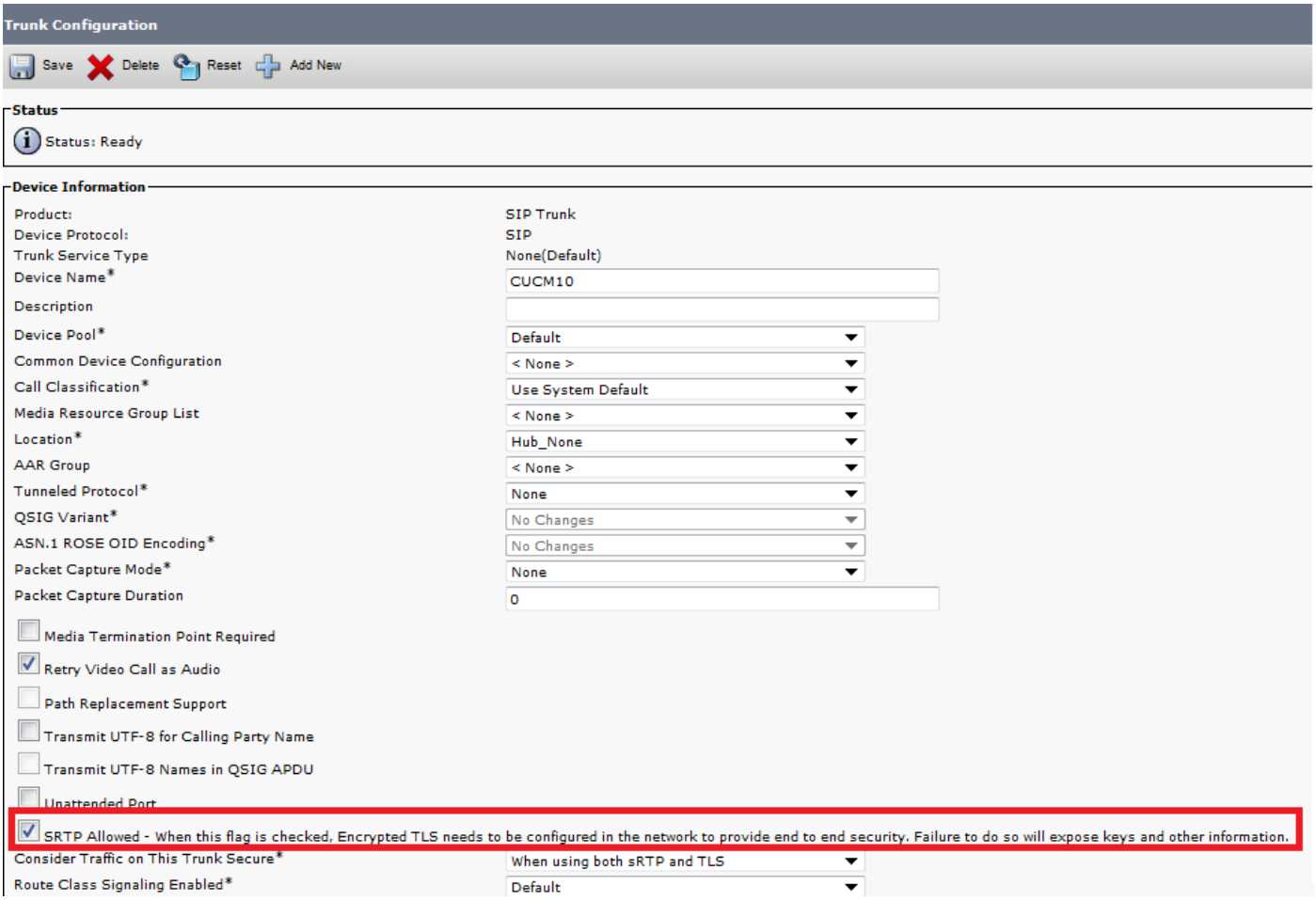
In X.509 Subject Name verwenden Sie den CN von CUCM 9.1(2) (Zertifizierungsstellen-signiertes Zertifikat), wie
hervorgehoben:



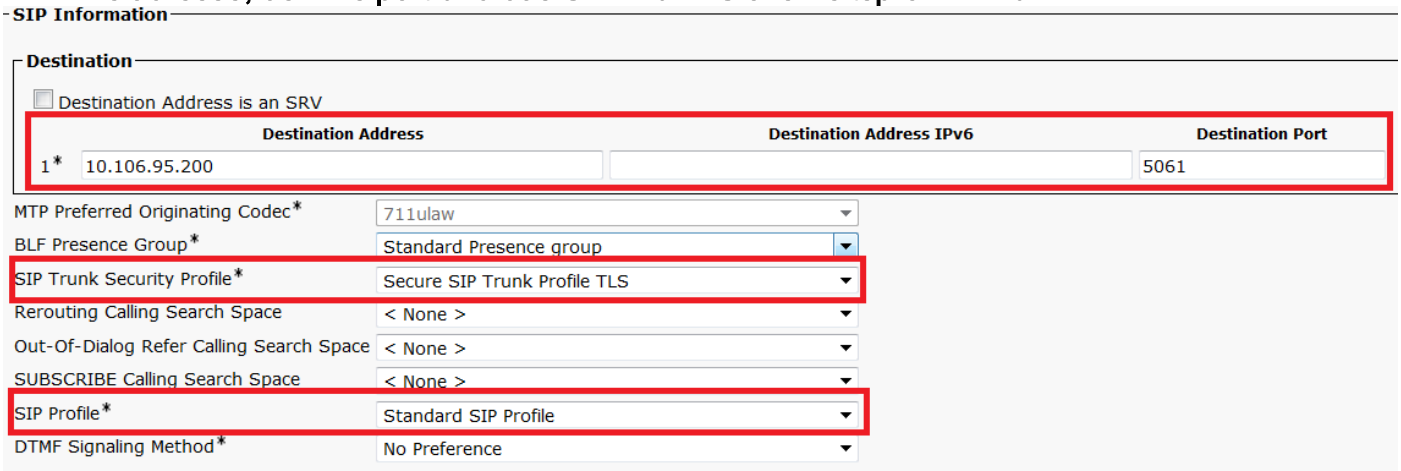
Beide SIP-Trunk-Sicherheitsprofile legen den eingehenden Port 5061 fest, bei dem jeder Cluster den TCP-Port 5061 für die neuen eingehenden SIP-TLS-Anrufe abhört.Schritt 9: SIP-Trunks erstellenErstellen Sie nach der Erstellung der Sicherheitsprofile die SIP-Trunks, und nehmen Sie die Änderungen für die unten stehenden Konfigurationsparameter im SIP-Trunk vor.CUCM 9.1(2)

1. Aktivieren Sie im Fenster "SIP Trunk Configuration" das Kontrollkästchen configuration parameter SRTP Allowed.

Dadurch wird das Real-Time Transport Protocol (RTP) für die Anrufe über diesen Trunk gesichert. Dieses Kontrollkästchen darf nur bei Verwendung von SIP TLS aktiviert werden, da die Schlüssel für Secure Real-Time Transport Protocol (SRTP) im Hauptteil der SIP-Nachricht ausgetauscht werden. Die SIP-Signalisierung muss durch TLS gesichert werden. Andernfalls kann jeder Benutzer mit der nicht sicheren SIP-Signalisierung den entsprechenden SRTP-Stream über den Trunk
entschlüsseln.



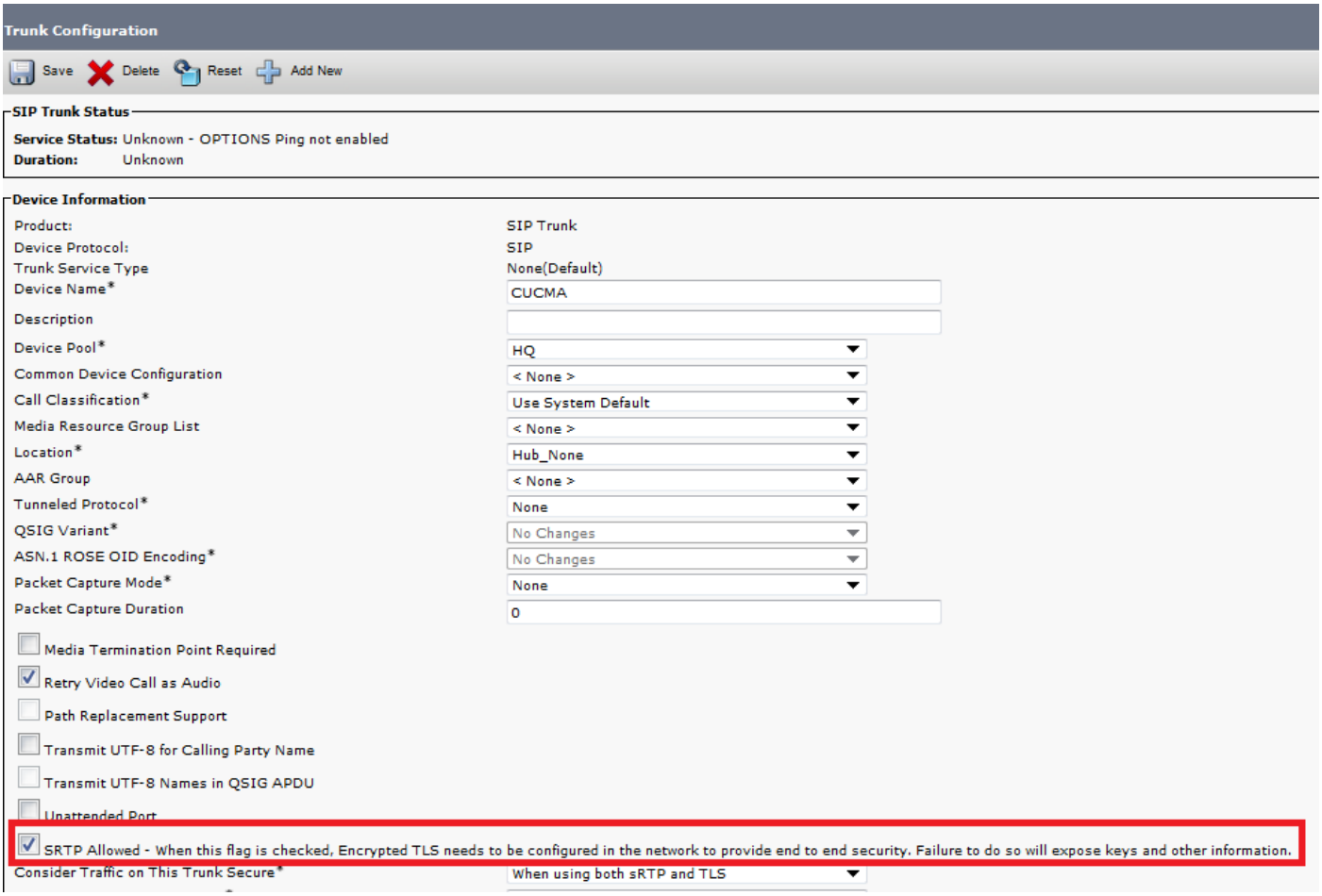
2. Fügen Sie im Abschnitt SIP-Informationen des Fensters "SIP-Trunk-Konfiguration" die Zieladresse, den Zielport und das SIP-Trunk-Sicherheitsprofil hinzu.



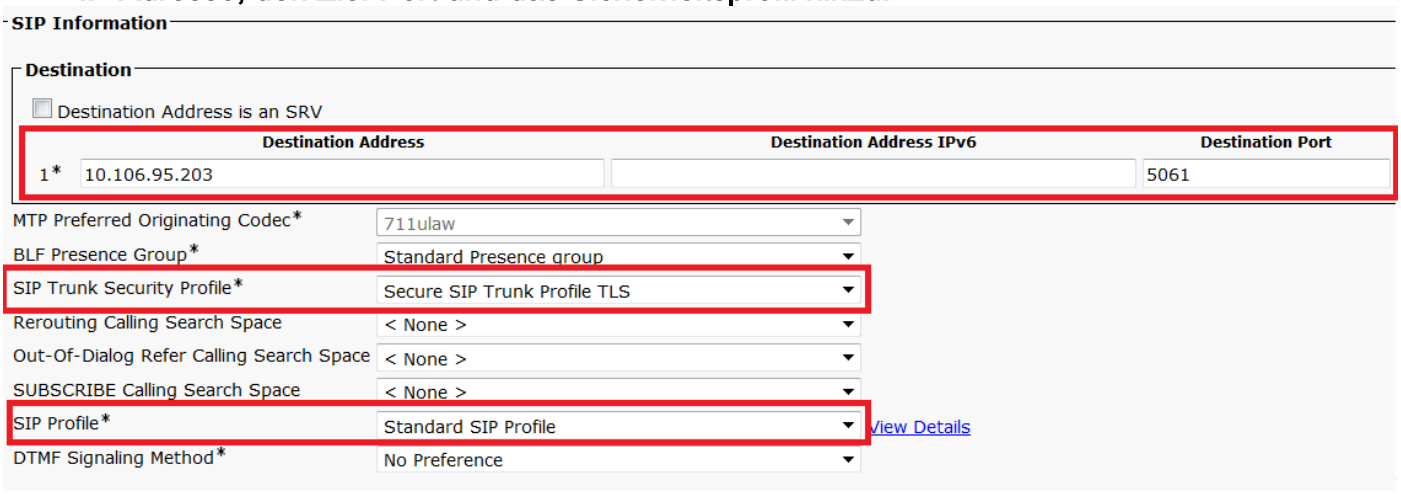
CUCM 10.5(2)

1. Aktivieren Sie im Fenster "SIP Trunk Configuration" das Kontrollkästchen configuration parameter SRTP Allowed.

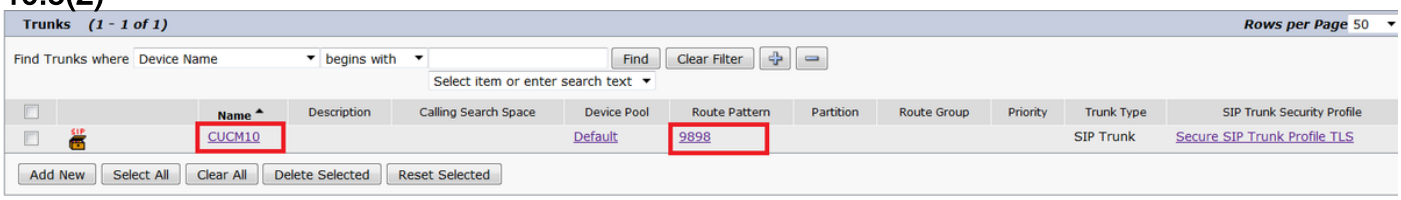
Auf diese Weise kann SRTP für Anrufe über diesen Trunk verwendet werden. Dieses Kontrollkästchen darf nur bei Verwendung von SIP TLS aktiviert werden, da die SRTP-Schlüssel im Hauptteil der SIP-Nachricht ausgetauscht werden. Die SIP-Signalisierung muss durch das TLS gesichert werden, da jeder mit einer nicht sicheren SIP-Signalisierung den entsprechenden sicheren RTP-Stream über den Trunk entschlüsseln
kann.



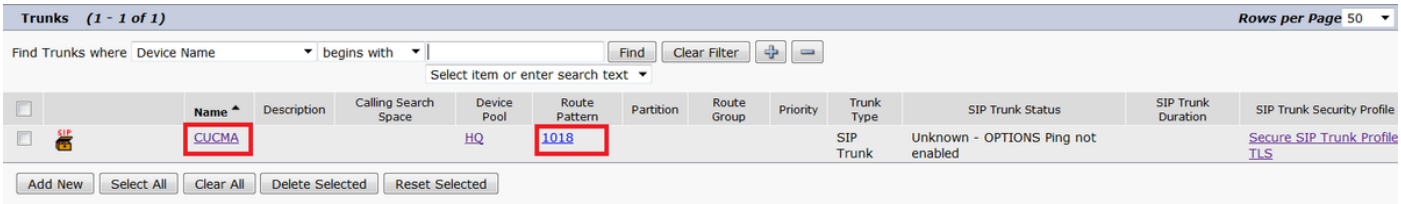
2. Fügen Sie im Abschnitt SIP-Informationen des Fensters "SIP-Trunk-Konfiguration" die Ziel-IP-Adresse, den Ziel-Port und das Sicherheitsprofil hinzu.



Schritt 10: Erstellen von RoutenmusternDie einfachste Methode besteht in der Erstellung eines Routenmusters für jeden Cluster, der direkt auf den SIP-Trunk verweist. Routengruppen und Routenlisten können ebenfalls verwendet werden.CUCM 9.1(2) verweist auf das Routenmuster 9898 über den TLS-SIP-Trunk zum CUCM
10.5(2)



Der CUCM 10.5(2) verweist auf das Routenmuster 1018 über den TLS-SIP-Trunk zum CUCM 9.1(2).



ÜberprüfenFür diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.Fehlerbehebung

Der SIP-TLS-Anruf kann mit diesen Schritten gedebuggt werden.

Paketerfassung auf CUCM erfassen

Um die Verbindung zwischen dem CUCM 9.1(2) und dem CUCM 10.5(2) zu überprüfen, führen Sie eine Paketerfassung auf den CUCM-Servern durch, und achten Sie auf den SIP-TLS-Datenverkehr.Der SIP-TLS-Datenverkehr wird über den TCP-Port 5061 übertragen, der als "sip-tls" angesehen wird.Im folgenden Beispiel wird eine SSH-CLI-Sitzung für CUCM 9.1(2) eingerichtet.1. CLI-Paketerfassung auf dem BildschirmDiese CLI druckt die Ausgabe für den SIP-TLS-Datenverkehr auf dem Bildschirm.

```
admin:utils network capture host ip 10.106.95.200
Executing command with options:
interface=eth0
ip=10.106.95.200
19:04:13.410944 IP CUCMA.42387 > 10.106.95.200.sip-tls: P 790302485:790303631(1146) ack
3661485150 win 182 <nop,nop,timestamp 2864697196 5629758>
19:04:13.450507 IP 10.106.95.200.sip-tls > CUCMA.42387: . ack 1146 win 249 <nop,nop,timestamp
6072188 2864697196>
19:04:13.465388 IP 10.106.95.200.sip-tls > CUCMA.42387: P 1:427(426) ack 1146 win 249
<nop,nop,timestamp 6072201 2864697196>
```

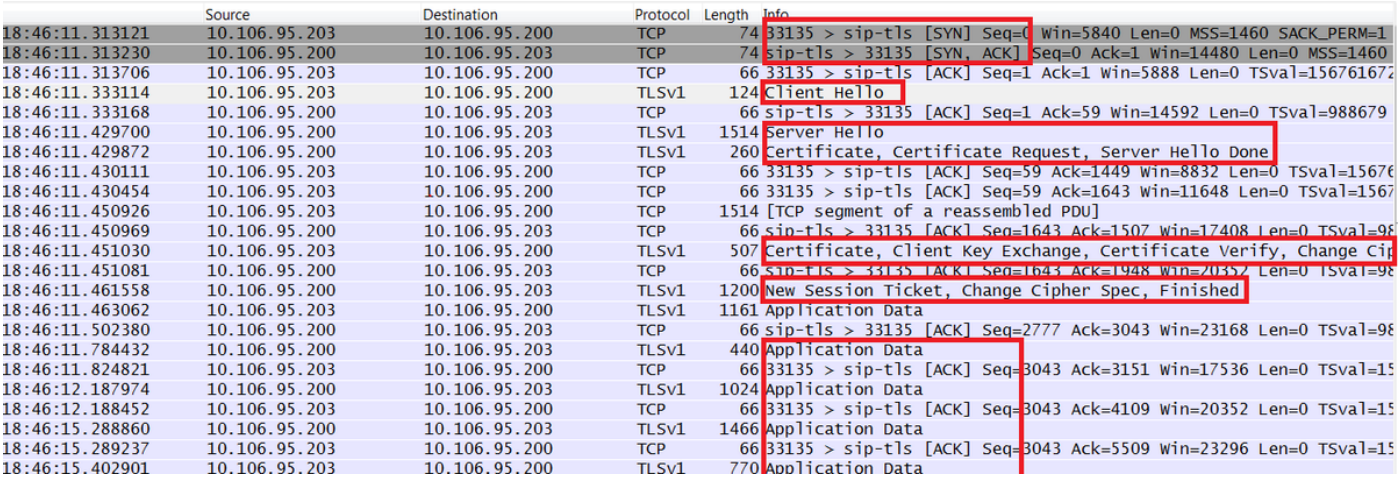
2. CLI-Erfassung in DateiDiese CLI erfasst die Pakete basierend auf dem Host und erstellt eine Datei mit dem Namen Packets.

```
admin:utils network capture eth0 file packets count 100000 size all host ip 10.106.95.200
```

Starten Sie den SIP-Trunk auf CUCM 9.1(2) neu, und tätigen Sie den Anruf von der Durchwahl 1018 (CUCM 9.1(2)) zur Durchwahl 9898 (CUCM 10.5(2)).Führen Sie den folgenden Befehl aus, um die Datei von der CLI herunterzuladen:

```
admin:file get activelog platform/cli/packets.cap
```

Die Erfassung erfolgt im Standard .cap-Format. In diesem Beispiel wird Wireshark verwendet, um die Datei "packages.cap" zu öffnen. Es kann jedoch jedes Anzeigetool für die Paketerfassung verwendet
werden.

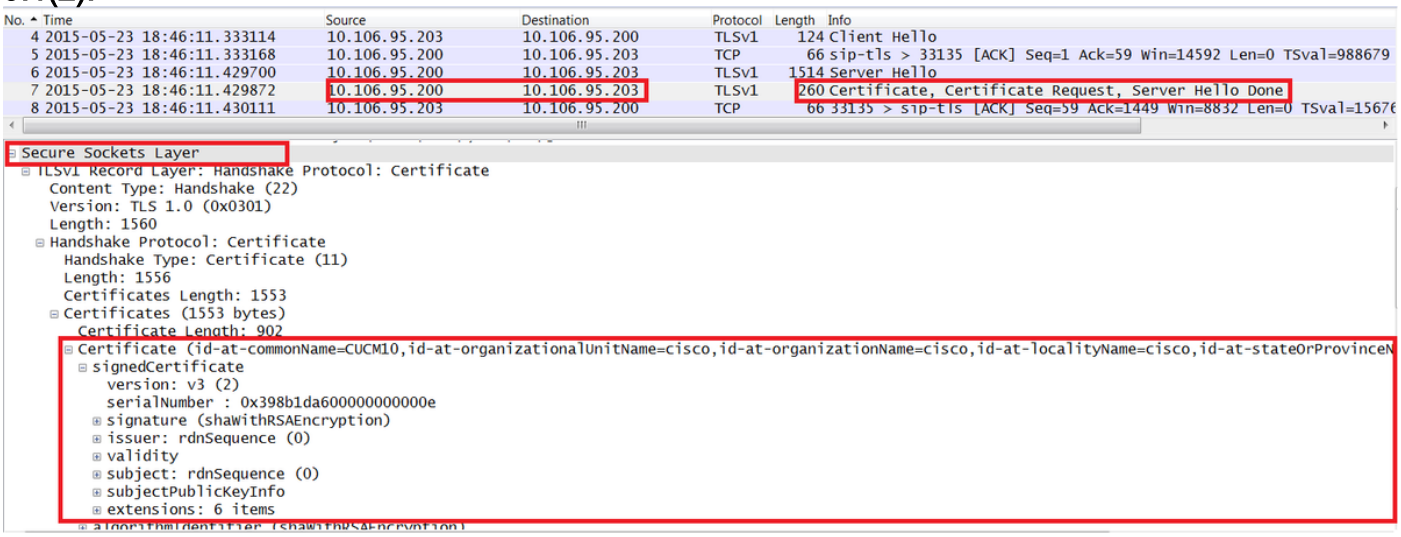


1. Das Transmission Control Protocol (TCP) Synchronize (SYN) dient zum Herstellen der TCP-Kommunikation zwischen dem CUCM 9.1(2)(Client) und dem CUCM 10.5(2)(Server).
2. Der CUCM 9.1(2) sendet den Client Hello, um die TLS-Sitzung zu starten.
3. Der CUCM 10.5(2) sendet The Server Hello, Server Certificate und Certificate Request, um den Zertifikataustauschprozess zu starten.
4. Das Zertifikat, das der Client CUCM 9.1(2) sendet, um den Zertifikataustausch

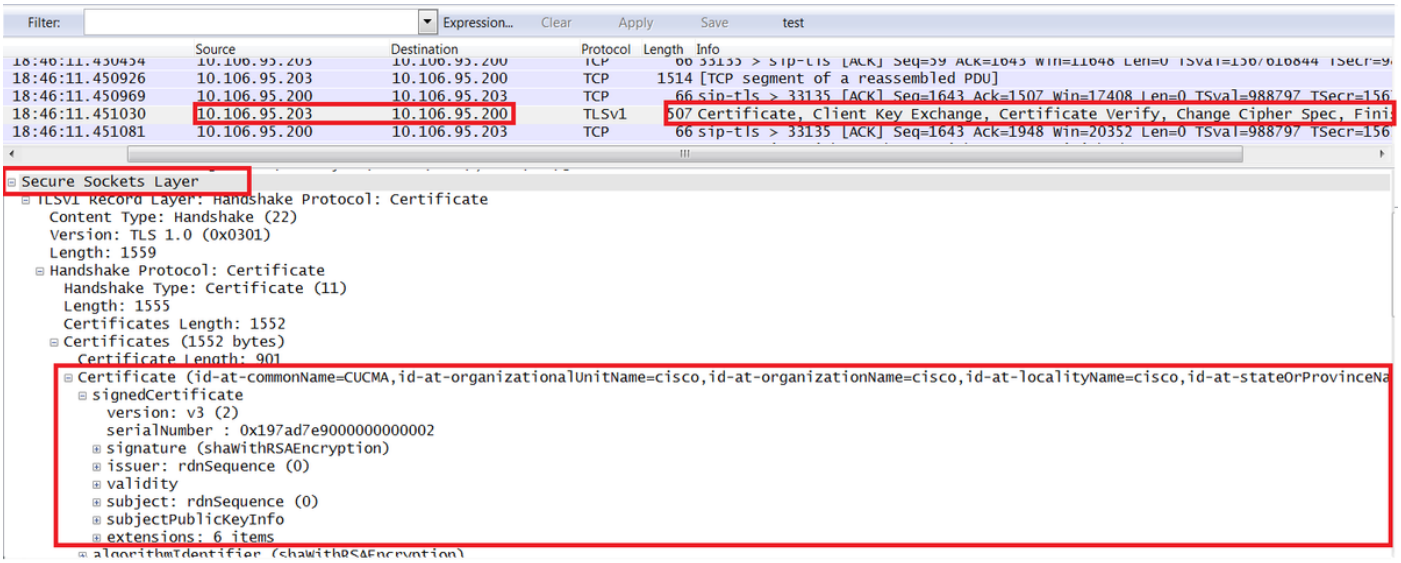
abzuschließen.

5. Die verschlüsselten Anwendungsdaten für die SIP-Signalisierung zeigen, dass die TLS-Sitzung eingerichtet wurde.

Überprüfen Sie noch einmal, ob die richtigen Zertifikate ausgetauscht werden. Nach dem ServerHello sendet der Server CUCM 10.5(2) sein Zertifikat an den Client CUCM 9.1(2).



Die Seriennummer und die Fachinformationen, die der Server CUCM 10.5(2) hat, werden dem Client CUCM 9.1(2) präsentiert.Seriennummer, Betreff, Aussteller und Gültigkeitsdatum werden mit den Informationen auf der Seite "OS Admin Certificate Management" (Verwaltung von Betriebssystemzertifikaten) verglichen.Der Server CUCM 10.5(2) stellt ein eigenes Zertifikat zur Überprüfung zur Verfügung, jetzt prüft er das Zertifikat des Clients CUCM 9.1(2). Die Überprüfung findet in beide Richtungen
statt.



Wenn eine Abweichung zwischen den Zertifikaten in der Paketerfassung und den Zertifikaten in der OS Admin-Webseite besteht, werden die richtigen Zertifikate nicht hochgeladen.Die richtigen Zertifikate müssen auf die Seite Betriebssystemadministratorzertifikate hochgeladen werden.Erfassung von CUCM-AblaufverfolgungenDie CUCM-Ablaufverfolgungen können auch hilfreich sein, um zu bestimmen, welche Nachrichten zwischen den CUCM 9.1(2)- und den CUCM 10.5(2)-Servern ausgetauscht werden und ob die SSL-Sitzung ordnungsgemäß eingerichtet wurde oder nicht.Im Beispiel wurden die Spuren aus CUCM 9.1(2) gesammelt.Anruffluss:Durchwahl 1018 > CUCM 9.1(2) > SIP TLS TRUNK > CUCM 10.5(2) > Ext 9898++ Ziffernanalyse

```
04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pi="2", fqcn="1018",
cn="1018",plv="5", pss="", TodFilteredPss="", dd="9898",dac="0")
04530161.010 |19:59:21.185 |AppInfo |Digit analysis: analysis results
04530161.011 |19:59:21.185 |AppInfo ||PretransformCallingPartyNumber=1018
```

```
|CallingPartyNumber=1018
|DialingPartition=
|DialingPattern=9898
|FullyQualifiedCalledPartyNumber=9898
```

++ SIP TLS wird für diesen Anruf auf dem Port 5061 verwendet.

```
04530191.034 |19:59:21.189 |AppInfo |//SIP/SIPHandler/ccbId=0/scbId=0/SIP_PROCESS_ENQUEUE:
createConnMsg tls_security=3
04530204.002 |19:59:21.224 |AppInfo
|//SIP/Stack/Transport/0x0/sipConnectionManagerProcessConnCreated: gConnTab=0xb444c150,
addr=10.106.95.200, port=5061, connid=12, transport=TLS Over TCP
04530208.001 |19:59:21.224 |AppInfo |SIPTcp - wait_SdlSPISignal: Outgoing SIP TCP message to
10.106.95.200 on port 5061 index 12
[131,NET]
INVITE sip:9898@10.106.95.200:5061 SIP/2.0
Via: SIP/2.0/TLS 10.106.95.203:5061;branch=z9hG4bK144f49a43a
From: <sip:1018@10.106.95.203>;tag=34~4bd244e4-0988-4929-9df2-2824063695f5-19024196
To: <sip:9898@10.106.95.200>
Call-ID: 94fffc00-57415541-7-cb5f6a0a@10.106.95.203
User-Agent: Cisco-CUCM9.1
```

++ Signal Distribution Layer (SDL)-Nachricht SIPCertificateInd enthält Details zu BetreffCN und Verbindungsinformationen.

```
04530218.000 |19:59:21.323 |SdlSig   |SIPCertificateInd                    |wait
                  |SIPHandler(1,100,72,1)           |SIPTcp(1,100,64,1)
|1,100,17,11.3^**^                        |[T:N-H:0,N:1,L:0,V:0,Z:0,D:0] connIdx= 12 --
remoteIP=10.106.95.200 --remotePort = 5061 --X509SubjectName
/C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --SubjectAltname =
04530219.000 |19:59:21.324 |SdlSig   |SIPCertificateInd
|restart0                       |SIPD(1,100,74,16)
|SIPHandler(1,100,72,1)           |1,100,17,11.3^**^                        |[R:N-
H:0,N:0,L:0,V:0,Z:0,D:0] connIdx= 12 --remoteIP=10.106.95.200 --remotePort = 5061 --
X509SubjectName /C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --
SubjectAltname =
```