

# 用SIP/TLS (签字的CA配置UCCE 11.6全面的呼叫流)

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[背景信息](#)

[配置](#)

[Network Diagram](#)

[部分A. 入口网关TLS配置](#)

[配置 workflow](#)

[配置细节](#)

[部分B. CVP TLS配置](#)

[配置 workflow](#)

[配置细节](#)

[部分C. VVB Configuration](#)

[配置细节](#)

[部分D. CUCM Configuration](#)

[配置细节](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

本文描述配置流程配置在传输层安全(TLS)的会话初始化协议(SIP)在与Certificate Authority (CA)签名的证书的Cisco Unified Contact Center Enterprise (UCCE)全面的呼叫流。

## Prerequisites

## Requirements

Cisco 建议您了解以下主题：

- CUCCE
- 公共交换电话网(PSTN)
- SIP协议
- 公共密钥基础设施(PKI)
- TLS

## Components Used

此本文的信息根据这些软件和硬件版本：

- Cisco 3945 Router
- Cisco用户语音门户(CVP) 11.6
- Cisco虚拟化语音浏览器(VVB) 11.6
- Cisco智能联络管理(ICM) 11.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. 如果您的网络实际，请保证您了解所有命令的潜在影响。

## 背景信息

在本文中，Cisco Unified通信管理器(CUCM)用于在PSTN和入口网关之间的simulatePSTN边。在传输控制协议(TCP)的SIP使用在代理程序CUCM和代理程序IP电话之间。其他SIP段使用在TLS (签字的CA的SIP)。

UCCE全面的呼叫流是公共交换电话网(PSTN) > 入口Gateway>思科统一客户语音门户(CVP) > 智能联络管理(ICM) (回归代理程序标签) > CVP > Cisco Unified通信管理器(CUCM) > 代理程序IP电话。

SIP/TLS在UCCE版本11.6介绍。在对CVP 11.6的升级以后，请保证完成统一的CVP属性的手动配置。

UCCE 11.6使用TLS 1.2，保证入口网关技术支持TLS 1.2。

IOS 15.6(1) T和IOS XE 3.17S支持TLS 1.2。早先IOS版本技术支持TLS 1.0仅。

以下密码套件为版本Cisco IOS 15.6(1)T介绍：

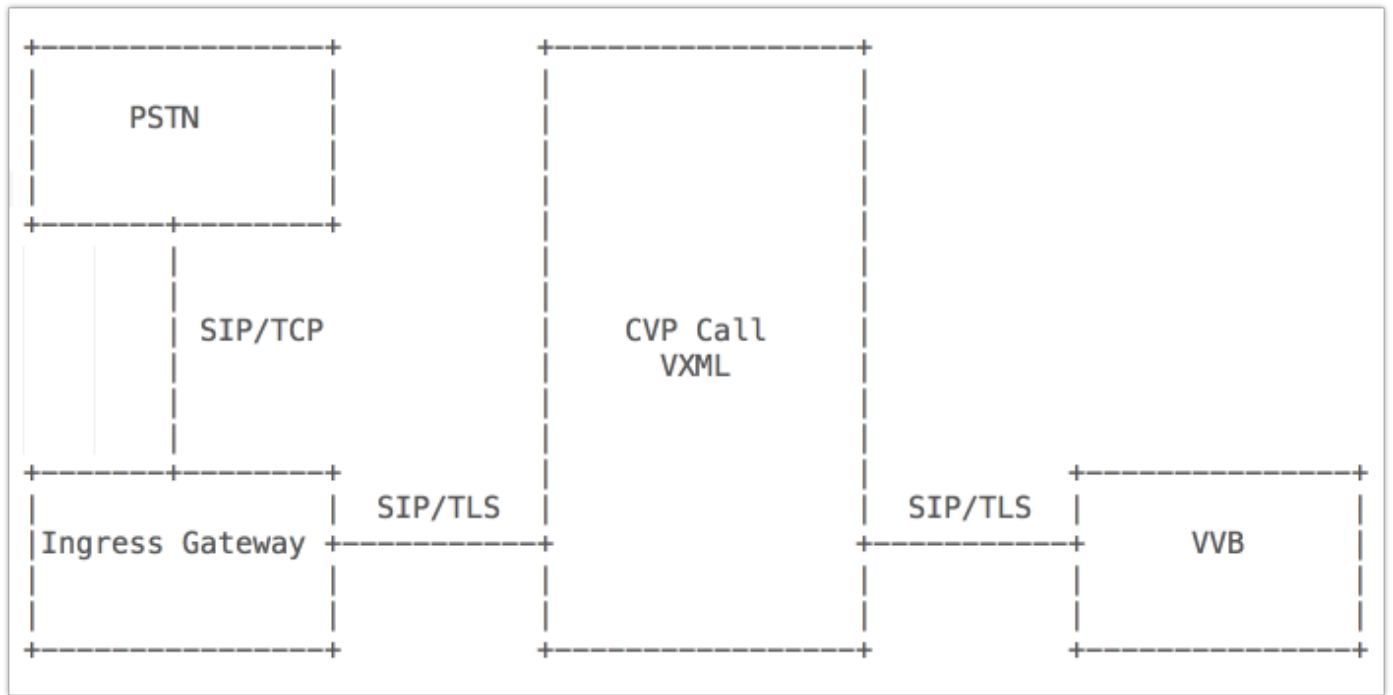
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA1
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Securityk9在入口网关必须启用许可证功能。

VVB需要被升级到11.6。

## 配置

### Network Diagram



配置包括四部分。

部分A.入口网关TLS配置

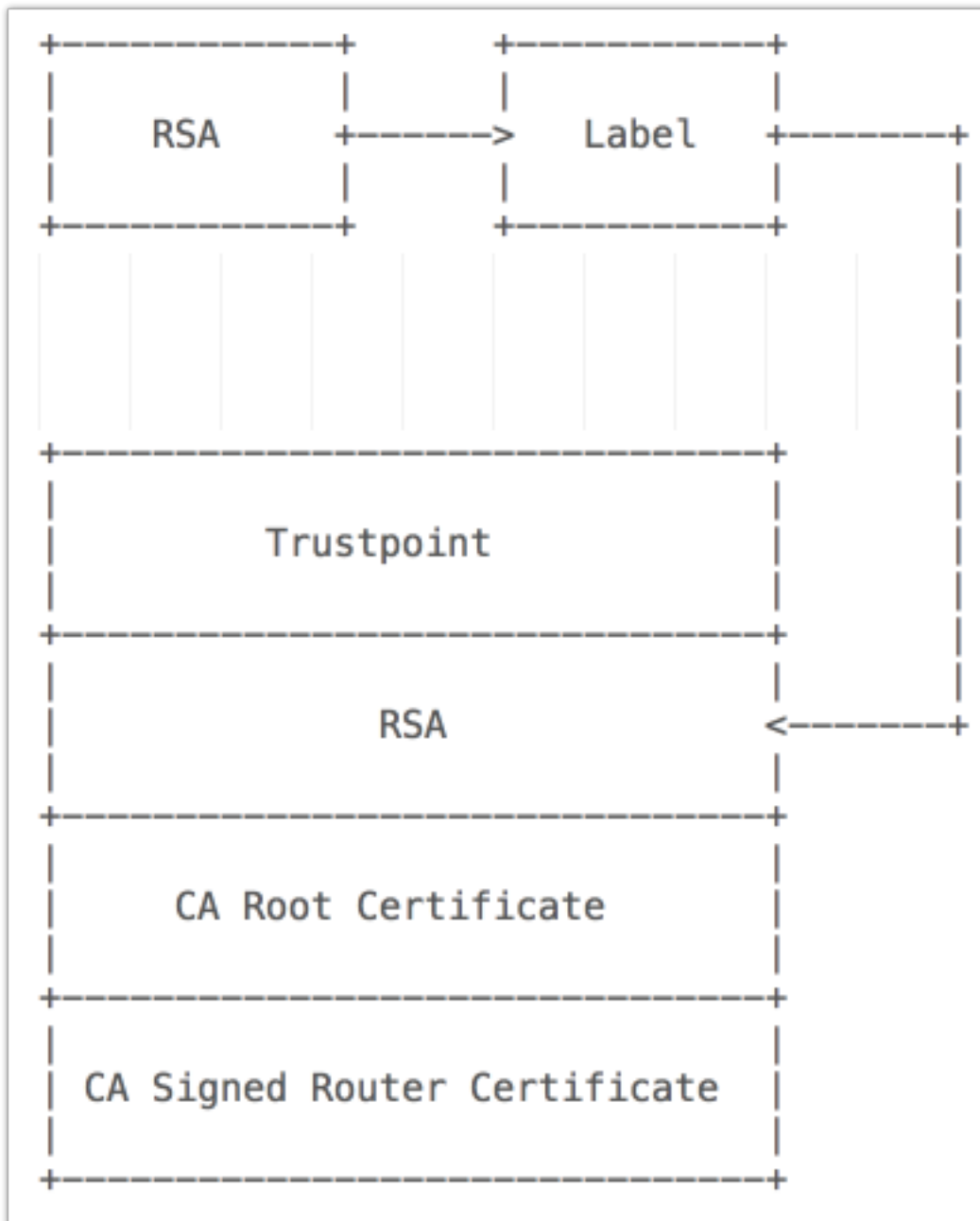
部分B. CVP TLS配置

部分C. VVB Configuration

部分D. CUCM Configuration

**部分A.入口网关TLS配置**

**配置 workflow**



## 配置细节

步骤1.生成RSA密钥在路由器(1024位RSA密钥)。

```
crypto key generate rsa modulus 1024 label INGW
```

步骤2.创建一信任点(信任点表示委托的CA)。

```
crypto pki trustpoint col115ca
revocation-check none
serial-number none
ip-address none
fqdn none
rsa keypair INGW
subject-name cn=INGRESSGW, ou=TAC, o=CISCO
```

```
crypto pki trustpoint col115ca
```

```
enrollment terminal
```

步骤3.创建将被发送到CA的证书请求(CSR)。

```
crypto ski enroll col115ca
```

步骤4. CA签名的证书(base64位CA CERT)。

步骤5.安装根证明。

```
crypto pki authenticate col115ca
```

步骤6.安装CA签名的证书(base64 cert)。

```
crypto pki import col115ca certificate
```

步骤7.验证安装了证书。

```
show crypto pki certificates
```

步骤8.配置在网关的TLS版本。

```
sip-ua
```

```
transport tcp tls v1.2
```

步骤9.指定信任点使用的根据终点站。

```
sip-ua
```

```
crypto signaling remote-addr 10.66.75.49 255.255.255.255 trustpoint col115ca
```

步骤10.调整指向CVP使用TLS的拨号点。

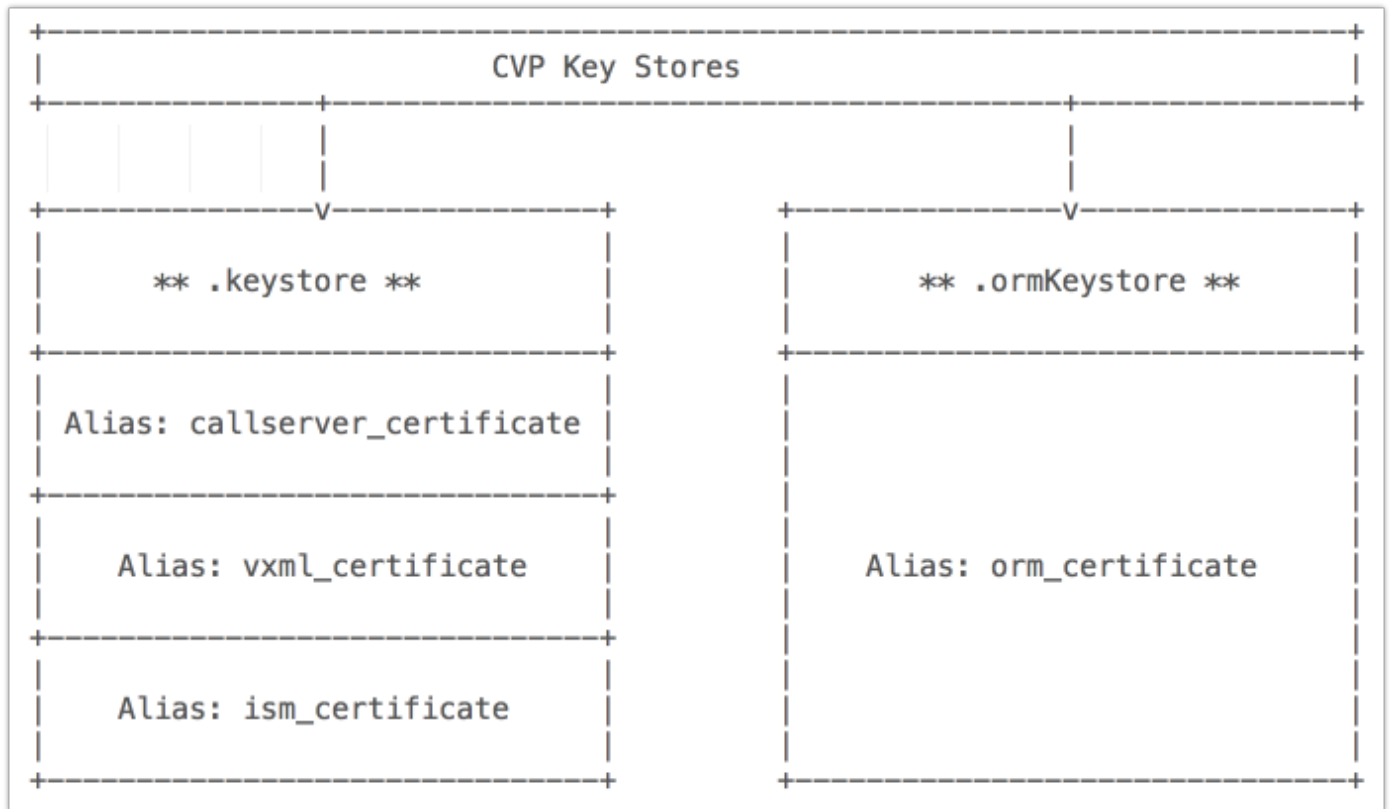
```
dial-peer voice 7205 voip
  description to CVP
  destination-pattern 700.$
  session protocol sipv2
  session target ipv4:10.66.75.49
  session transport tcp tls
  dtmf-relay rtp-nte
  codec g711ulaw
```

## 部分B. CVP TLS配置

### 配置 workflow

CVP有两关键存储，位于c:\Cisco\CVP\conf\security。

如镜像所显示，这两关键存储有另外证书。



## 配置细节

步骤1.连接到c:\Cisco\CVP\conf\security.propertiesin CVP呼叫服务器为了查找此密码。此文件包含关键存储的密码，需要，当运行关键存储时。

步骤2.删除系统默认Callserver\_certificate。

```
C:\Cisco\CVP\jre\bin>keytool.exe -delete -alias orm_certificate -storetype JCEKS -keystore
c:\Cisco\CVP\conf\security\.keystore
```

步骤3.生成密钥对。

```
C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -alias callserver_certificate -v -k eysize 1024 -
keyalg RSA -storetype JCEKS -keystore c:\Cisco\CVP\conf\security\.keystore
```

步骤4.创建CSR并且保存它在硬盘根文件夹(c:\callcsr.csr)。

```
C:\Cisco\CVP\jre\bin>keytool.exe -certreq -alias callserver_certificate -file c:\callcsr.csr -
storetype JCEKS
-keystore c:\Cisco\CVP\conf\security\.keystore
```

步骤5.请签署请求并且提交请求给CA (当您下载cert时，选择编码的Base64)。

步骤6.安装根证明(cert存储在C:\DC - Root.cer)。

```
C:\Cisco\CVP\jre\bin>keytool.exe -import -v -trustcacerts -alias root -file C:\ DC-Root.cer -
storetype JCEKS -keystore C:\Cisco\CVP\conf\security\.Keystore
```

步骤7.安装CA签名的证书(cert存储在c:\95callserver.cer)。

```
C:\Cisco\CVP\jre\bin>keytool.exe -import -v -trustcacerts -alias callserver_certificate -file c:\95callserver.cer -sto retype JCEKS -keystore c:\Cisco\CVP\conf\security\keystore
```

步骤8.在关键存储验证证书详细信息。

```
C:\Cisco\CVP\jre\bin>keytool.exe -list -v -storetype JCEKS -keystore c:\Cisco\CVP\conf\security\keystore
```

## 部分C. VVB Configuration

### 配置细节

步骤1.从系统参数的Enable (event) TLS

此示例使用RTP，因此在VVB的SRTP不是启用的。

The screenshot displays the 'System Parameters Configuration' window. It features a menu bar with 'System', 'Applications', 'Subsystems', 'Tools', and 'Help'. Below the menu, there are 'Update' and 'Clear' buttons. The 'Status' section shows 'Status : Ready'. The main configuration area is divided into three sections:

- Generic System Parameter**: A table with two columns: 'Parameter Name' and 'Parameter Value'. The entry is 'System Time Zone' with the value 'Australian Eastern Standard Time (New South Wales)'.
- Media Parameters**: A table with two columns: 'Parameter Name' and 'Parameter Value'. The entries are: 'Codec' (G711U), 'MRCP Version' (MRCPv2), and 'User Prompts override System Prompts' (radio buttons for 'Disable' and 'Enable', with 'Disable' selected).
- Security Parameters**: A table with two columns: 'Parameter Name' and 'Parameter Value'. The entries are: 'TLS(SIP)' (radio buttons for 'Disable' and 'Enable', with 'Enable' selected), 'Supported TLS(SIP) Versions' (TLSv1.2), and 'SRTP' (radio buttons for 'Disable' and 'Enable', with 'Disable' selected). Below the SRTP entry, there is a checkbox for 'Allow RTP (Mixed mode)' which is unchecked.

步骤2.生成并且导入VVB的CA签名的证书，这部分是同CUCM Tomcat认证一样

- 生成CSR和签字由CA。
- 导入Tomcat信任(CA根Cert)。
- 导入Tomcat (CA签字的Cert)。

## 部分D. CUCM Configuration

### 配置细节

步骤1.加载CA在CUCM服务器的签字的呼叫管理器认证。CUCM用途SIP/TLS的呼叫管理器认证。

步骤2.生成呼叫管理器认证的CSR，确定密钥长度是1024。

**Generate Certificate Signing Request**

Generate Close

**- Status -**

**i** Success: Certificate Signing Request Generated

**- Generate Certificate Signing Request -**

Certificate Purpose\*\* CallManager

Distribution\* col115cucmpub.col115.org.au

Common Name\* col115cucmpub.col115.org.au

**Subject Alternate Names (SANs)**

Parent Domain col115.org.au

Key Type\*\* RSA

Key Length\* 1024

Hash Algorithm\* SHA256

Generate Close

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

**i** \*\*When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

步骤3.提供CSR给CA并且检索呼叫管理器认证。

步骤4.导入根CA证书和最近签字的呼叫管理器认证。

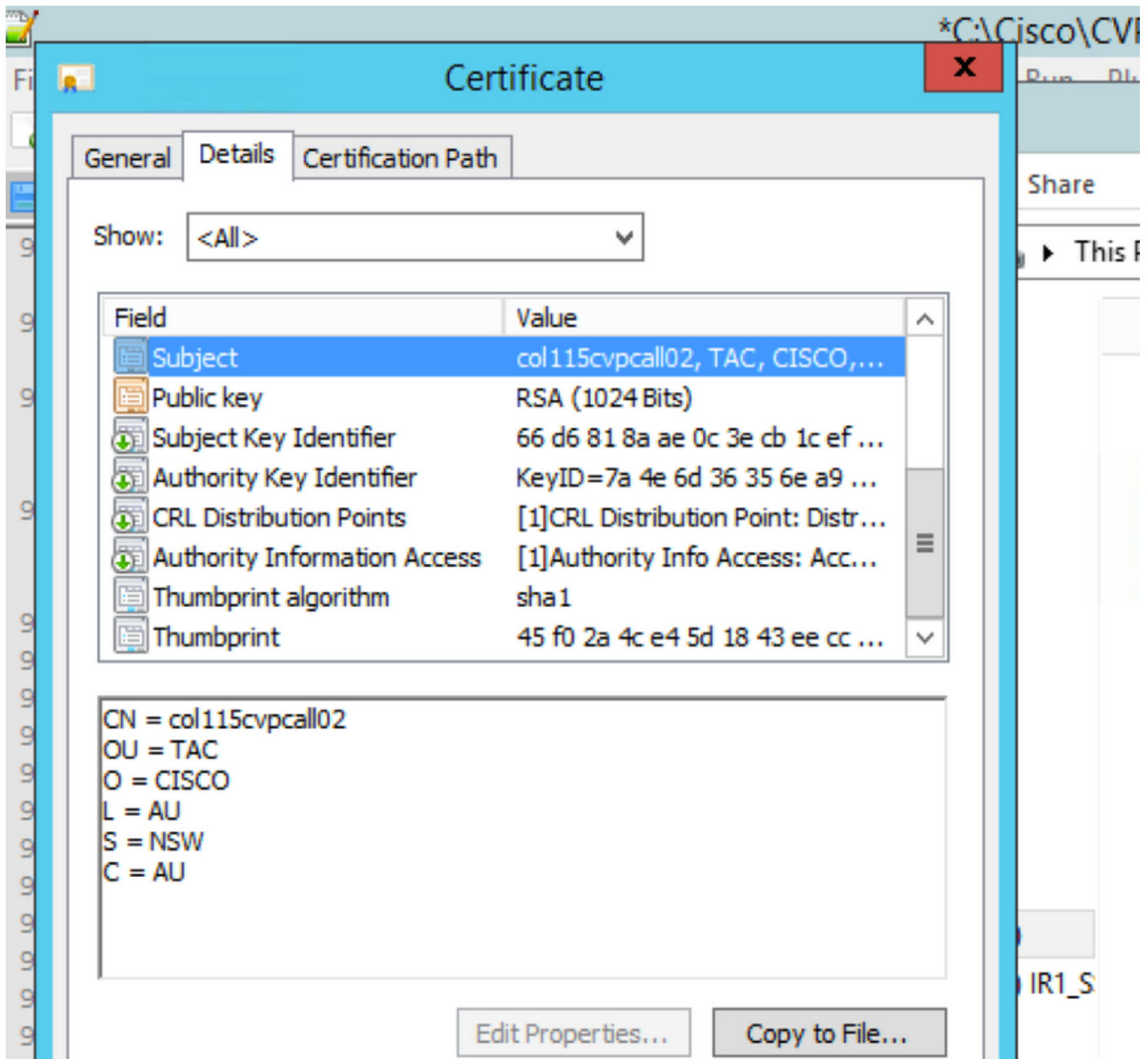
步骤5.重新启动呼叫管理器和TFTP服务。

步骤6.配置SIP Trunk安全配置文件。连接对系统> Security > SIP Trunk安全配置文件

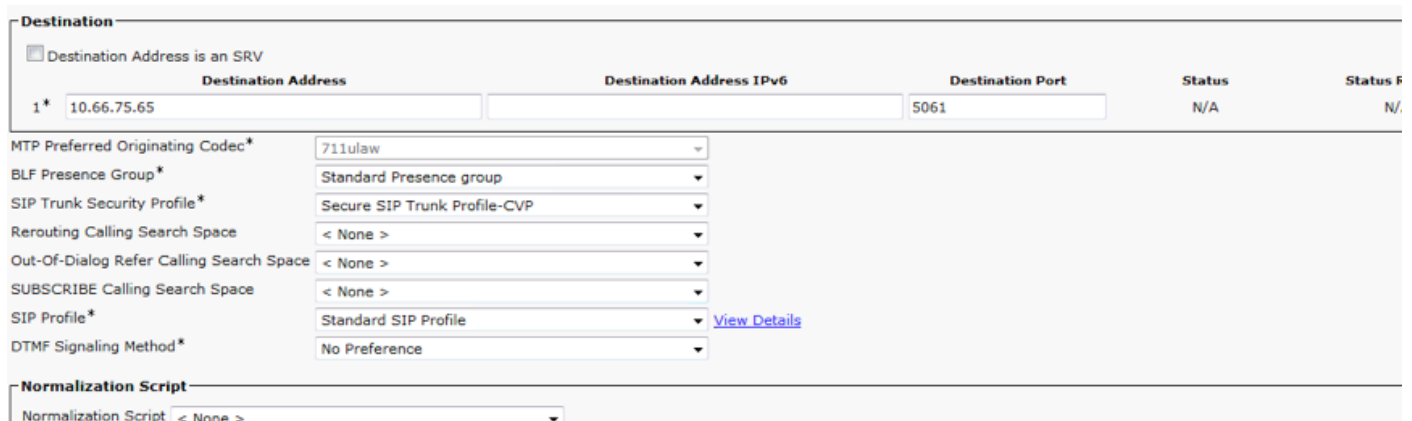
如镜像所显示，保证X.509主题名称同一样在CVP呼叫服务器证明使用的。



Name*	Secure SIP Trunk Profile-CVP
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	col115cvpcall02
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input checked="" type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	



步骤7.创建SIP Trunk并且分配它到安全配置文件。



## Verify

验证在入口网关上安装的证书。

```
show crypto pki certificates
```

在CVP键存储验证证书详细信息。

```
C:\Cisco\CVP\jre\bin>keytool.exe -list -v -storetype JCEKS -keystore c:\Cisco\CV  
P\conf\security\keystore
```

## Troubleshoot

调试指令与TLS有关。

```
debug ssl openssl errors
```

```
debug ssl openssl msg
```

```
debug ssl openssl states
```

## Related Information

- [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cust\\_contact/contact\\_center/customer\\_voice\\_portal/cvp11\\_6/configuration/guide/ccvp\\_b\\_configuration-guide-for-cisco-unified.pdf](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/cvp11_6/configuration/guide/ccvp_b_configuration-guide-for-cisco-unified.pdf)
- [Technical Support & Documentation - Cisco Systems](#)