Flujo de llamada completo de la configuración UCCE 11.6 con SIP/TLS (CA firmó)

Contenido

Introducción

Este documento describe el proceso de configuración para desplegar el Session Initiation Protocol (SIP) sobre Transport Layer Security (TLS) en el flujo de llamada completo del Cisco Unified Contact Center Enterprise (UCCE) con los certificados firmados del Certificate Authority (CA).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- CUCCE
- Public Switched Telephone Network (PSTN)
- Protocolo SIP
- Public Key Infrastructure (PKI)
- TLS

Componentes Utilizados

Esta información en este documento se basa en estas versiones de software y hardware:

- Cisco 3945 Router
- Portal de la Voz de cliente de Cisco (CVP) 11.6
- Cisco virtualizó al buscador de voz (VVB) 11.6
- Cisco Intelligent Contact Management (ICM) 11.6

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Antecedentes

En este documento, utilizan al administrador de las Comunicaciones unificadas de Cisco (CUCM) al lado del simulatePSTN entre el PSTN y el gateway de ingreso. El SORBO sobre el Transmission Control Protocol (TCP) se utiliza entre el agente CUCM y el teléfono del IP del agente. El resto del SORBO del uso de las piernas del SORBO sobre TLS (CA firmado).

El flujo de llamada completo UCCE es el **Public Switched Telephone Network (PSTN) > gateway de ingreso > Cisco Unified Customer Voice Portal (CVP) > el Intelligent Contact Management (ICM) (escritura de la etiqueta de vuelta del agente) > CVP > el administrador de las Comunicaciones unificadas de Cisco (CUCM) > teléfono del IP del agente**.

SIP/TLS se introduce en la versión 11.6 UCCE. Después de la actualización al CVP 11.6, asegure la configuración manual del final de las propiedades unificadas del CVP.

UCCE 11.6 utiliza TLS 1.2, asegura los soportes TLS 1.2 del gateway de ingreso.

El IOS 15.6(1) T y el IOS XE 3.17S soportan TLS 1.2. Soportes anteriores TLS1.0 de las versiones de IOS solamente.

Las habitaciones siguientes de la cifra se introducen para el Cisco IOS 15.6(1)T de la versión:

- del TLS_DHE_RSA_WITH_AES_128_CBC_SHA1

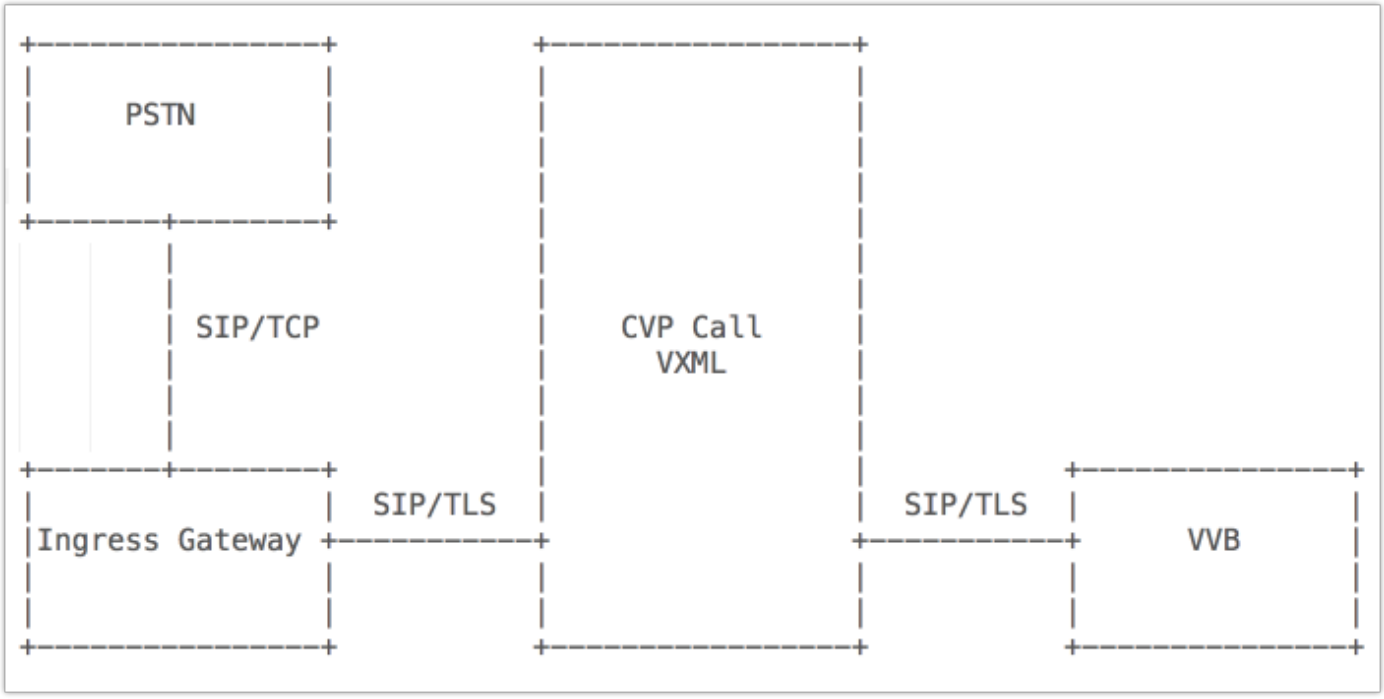
- del TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

La característica de la licencia Securityk9 se debe habilitar en el gateway de ingreso.

VVB necesita ser actualizado a 11.6.

Configuración

Diagrama de la red



La configuración incluye cuatro porciones.

Configuración de TLS del gateway de ingreso de la parte A.

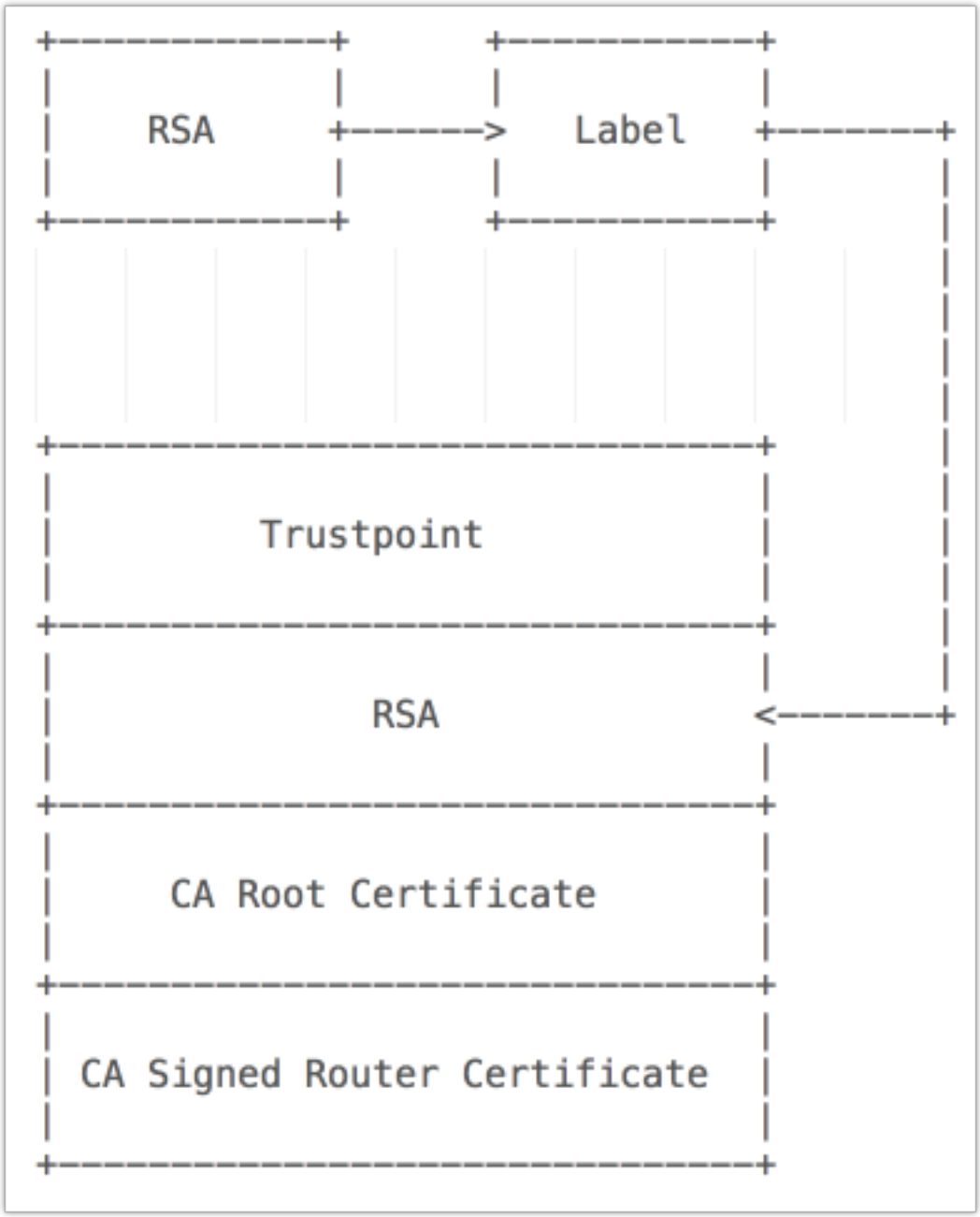
Configuración de B. CVP TLS de la parte

Parte C. VVB Configuration

Parte D. CUCM Configuration

Configuración de TLS del gateway de ingreso de la parte A.

Flujo de trabajo de la configuración



Detalles de la configuración

Paso 1. Genere la clave RSA en el router (clave 1024-bit RSA).

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

Paso 2. Cree un trustpoint (un trustpoint representa CA de confianza).

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

crypto pki trustpoint col115ca
```

```
enrollment terminal
```

Paso 3. Cree un pedido de certificado (CSR) que sea enviado a CA.

```
crypto ski enroll col115ca
```

Paso 4. Certificado firmado de CA (bit CA CERT del base 64).

Paso 5. Instale el certificado raíz.

```
crypto pki authenticate col115ca
```

Paso 6. Instale el certificado firmado de CA (CERT del base 64).

```
crypto pki import col115ca certificate
```

Paso 7. Verifique los Certificados han estado instalados.

```
show crypto pki certificates
```

Paso 8. TLS versión de la configuración en el gateway.

```
sip-ua
transport tcp tls v1.2
```

Paso 9. Especifique el según destino usado trustpoint.

```
sip-ua

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

Paso 10. Ajuste el dial-peer que señalan al CVP para utilizar TLS.

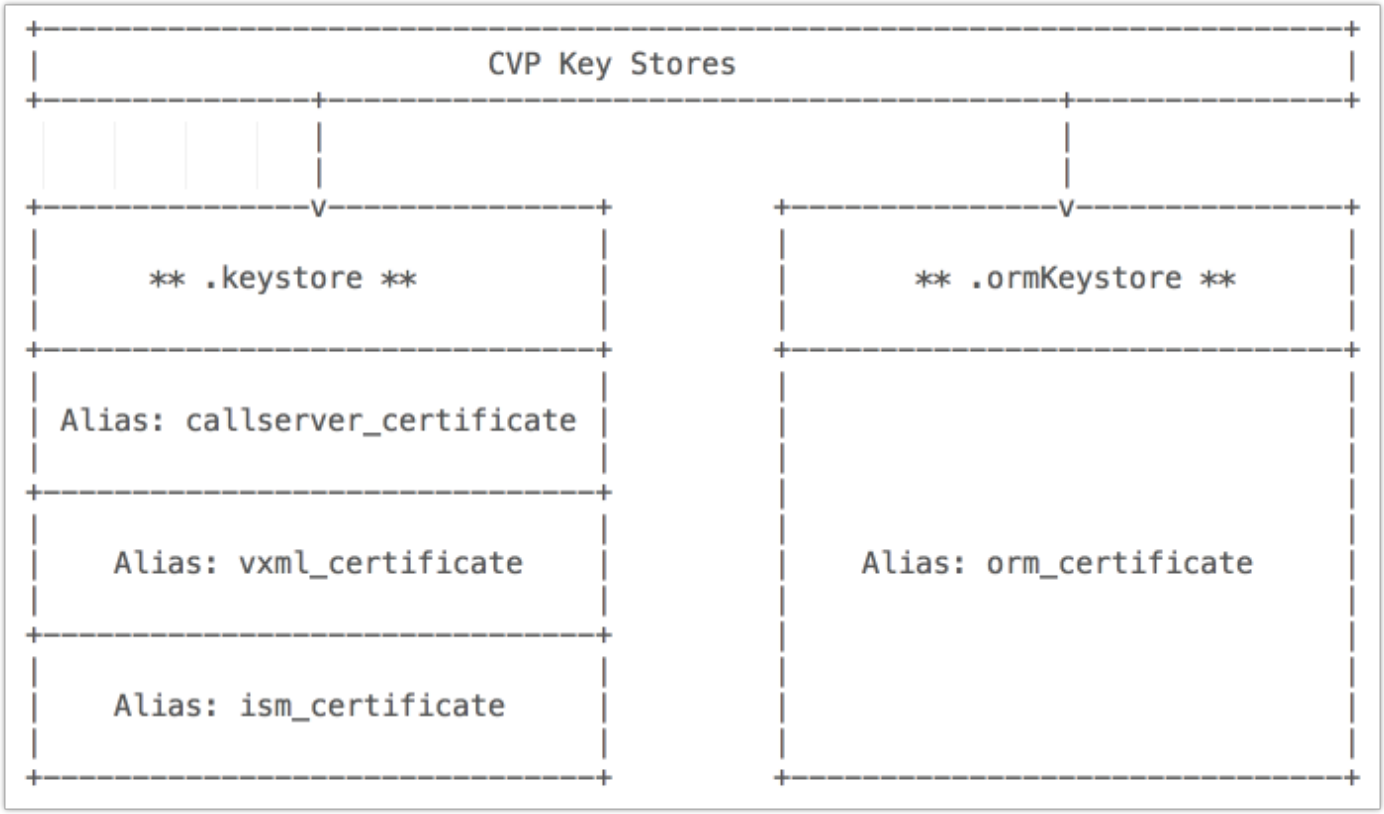
```
dial-peer voice 7205 voip
  description to CVP
  destination-pattern 700.$
  session protocol sipv2
  session target ipv4:10.66.75.49
  session transport tcp tls
  dtmf-relay rtp-nte
  codec g711ulaw
```

Pieza la configuración de B. CVP TLS

Flujo de trabajo de la configuración

El CVP tiene dos almacenes dominantes, situados en **c:\Cisco\CVP\conf\security**.

Tal y como se muestra en de la imagen, estos dos almacenes dominantes sostienen diversos Certificados.



Detalles de la configuración

Paso 1. Navegue al servidor de la llamada del CVP de **c:\Cisco\CVP\conf\security.propertiesin** para encontrar esta contraseña. Este archivo contiene la contraseña para el almacén dominante, se requiere que al actuar el almacén dominante.

Paso 2. Valor predeterminado del sistema Callserver_certificate de la cancelación.

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

Paso 3. Genere el keypair.

```
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
```

Paso 4. Cree un CSR y sálvelo en el C: conduzca la carpeta raíz (**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
```

Paso 5. Firme la petición y someta la petición a CA (cuando usted descarga el CERT, elige el base 64 codificado).

Paso 6. Instale el certificado raíz (CERT salvado en **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
```

Paso 7. Instale el certificado firmado de CA (CERT salvado en 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
```

Paso 8. Verifique a los detalles del certificado en el almacén dominante.

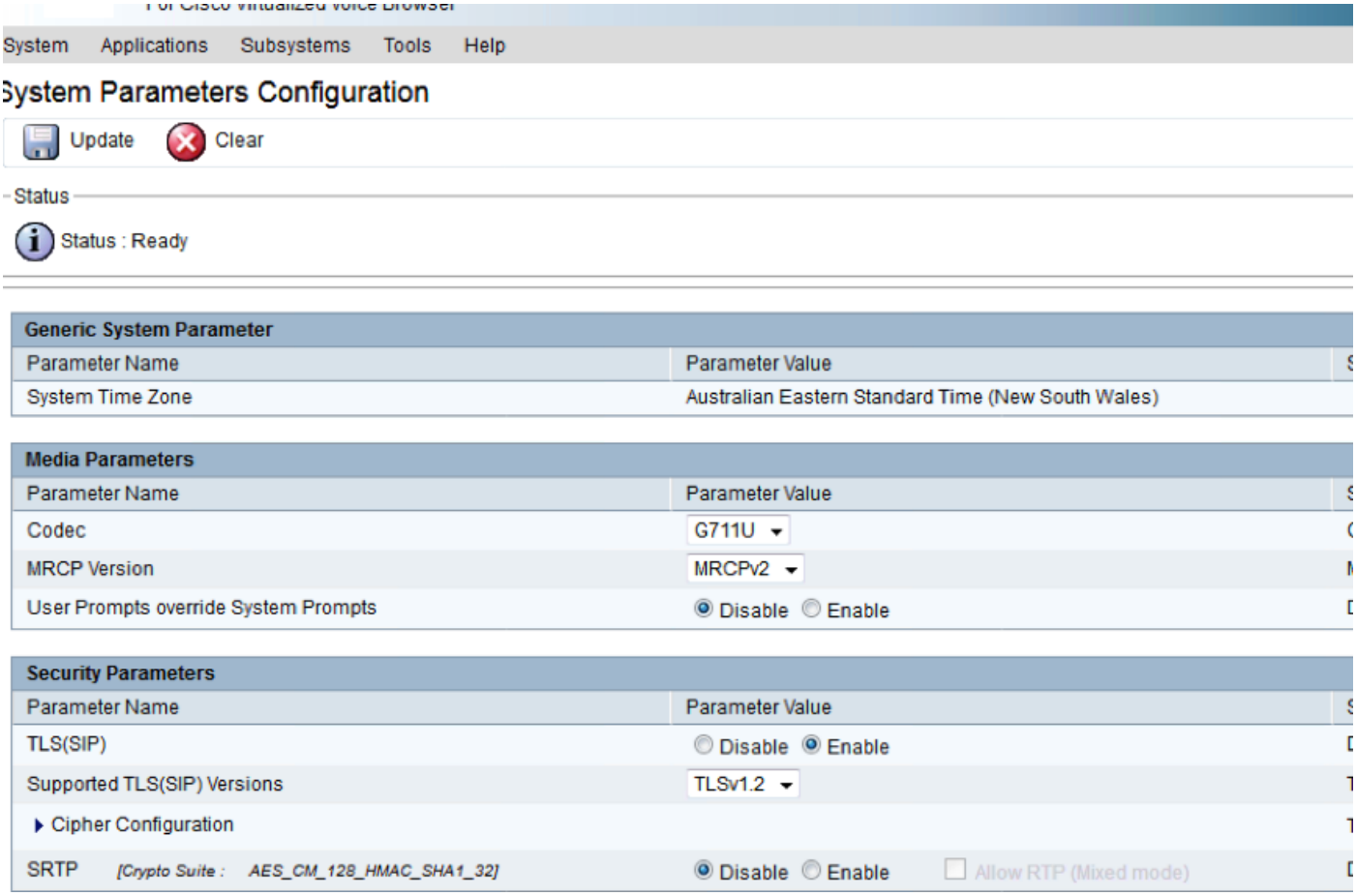
```
C:\Cisco\CVP\jre\bin>keytool.exe -list -v -storetype JCEKS -keystore c:\Cisco\CV
P\conf\security\.keystore
```

Pieza a C. VVB Configuration

Detalles de la configuración

Paso 1. Permiso TLS del parámetro del sistema

Este ejemplo utiliza el RTP, así que el SRTP en VVB no se habilita.



Paso 2. Genere e importe el certificado firmado de CA para VVB, esta parte es lo mismo que certificado del tomcat CUCM

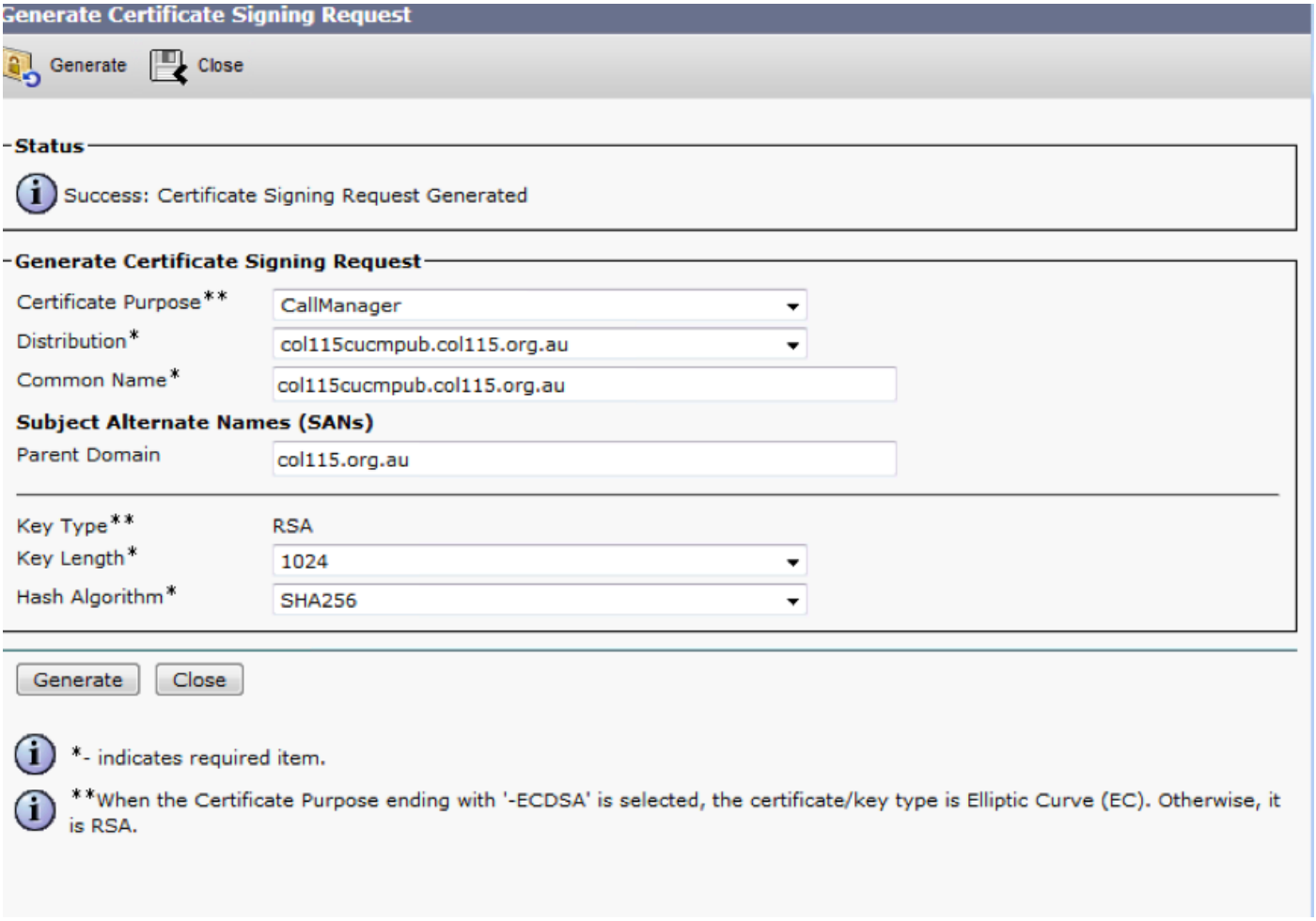
- Genere el CSR y firmado por CA.
- Importe la confianza de Tomcat (CERT de la raíz de CA).
- Importe Tomcat (CERT firmado CA).

Pieza a D. CUCM Configuration

Detalles de la configuración

Paso 1. Cargue el certificado firmado CA del callmanager en el servidor CUCM. CUCM utiliza el certificado del callmanager para SIP/TLS.

Paso 2. Genere el CSR para el certificado del callmanager, aseegurese la longitud de clave es 1024.



Paso 3. Proporcione el CSR a CA y extraiga el certificado del callmanager.

Paso 4. Importación certificado raíz CA y el certificado recientemente firmado del callmanager.

Paso 5. Callmanager del reinicio y servicios TFTP.

Paso 6. Perfil de seguridad del trunk del SORBO de la configuración. Navegue al **> Security (Seguridad) del sistema > al perfil de seguridad del trunk del SORBO**

Asegúrese que el asunto X.509 sea lo mismo que se utiliza en el certificado de servidor de la llamada del CVP, tal y como se muestra en de las imágenes.

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

☐ Enable Digest Authentication

Nonce Validity Time (mins)*: 600

X.509 Subject Name: col115cvpcall02

Incoming Port*: 5061

☐ Enable Application level authorization

☐ Accept presence subscription

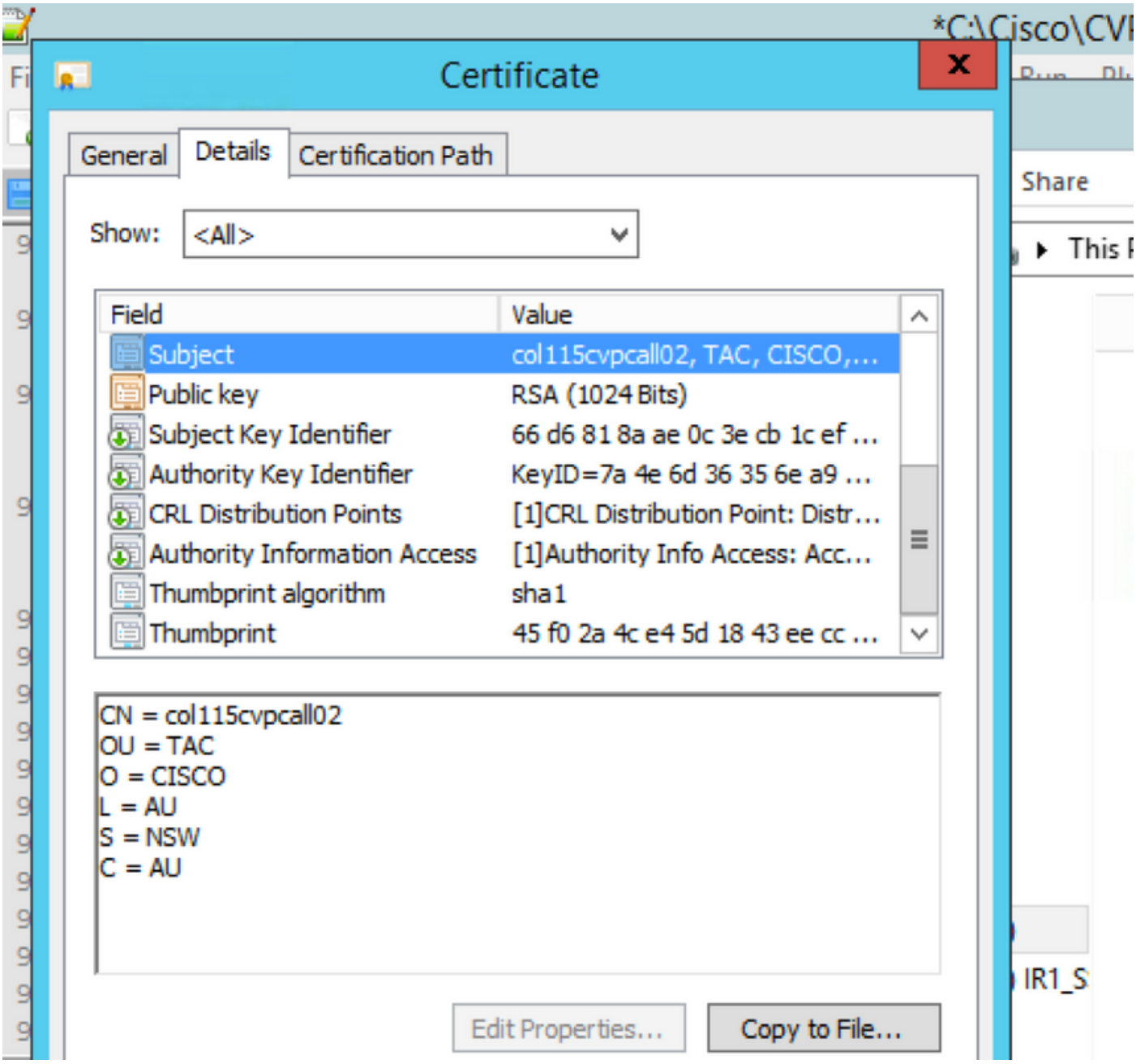
☐ Accept out-of-dialog refer**

☐ Accept unsolicited notification

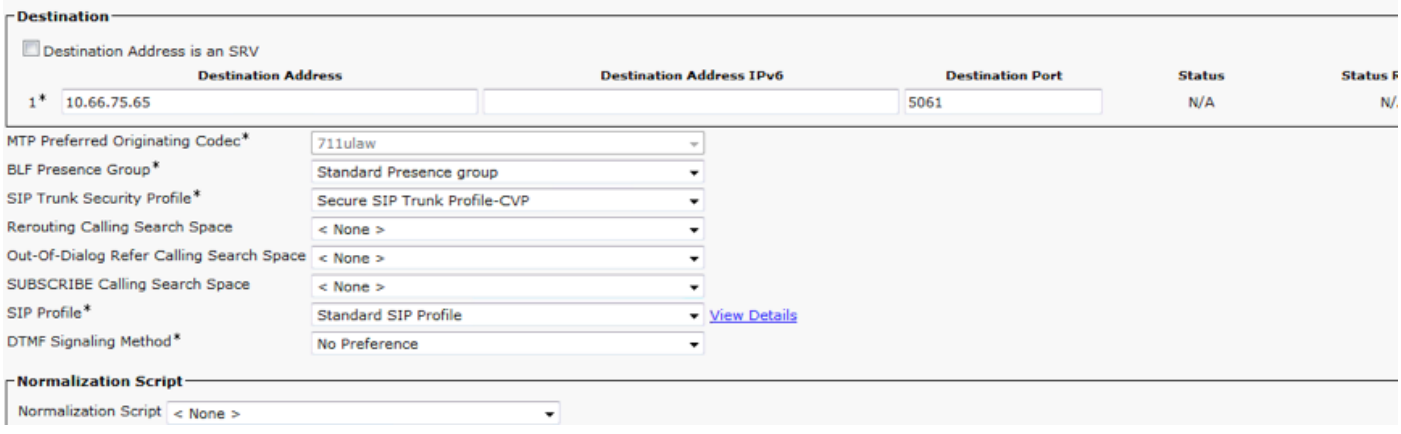
☐ Accept replaces header

☑ Transmit security status

☐ Allow charging header



Paso 7. Cree el trunk del SORBO y aféctelo un aparato a un perfil de seguridad.



Verificación

Verifique los Certificados instalados en el gateway de ingreso.

```
show crypto pki certificates
```

Verifique a los detalles del certificado en el almacén de la clave del CVP.

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

Troubleshooting

Comandos Debug relacionados con TLS.

```
debug ssl openssl errors

debug ssl openssl msg

debug ssl openssl states
```

Información Relacionada

- 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
- Soporte Técnico y Documentación - Cisco Systems