# Vista de alto nivel de los Certificados y de las autoridades en CUCM

## Contenido


Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Propósito de los Certificados
Defina la confianza de Point of View de un certificado
Cómo los navegadores utilizan los Certificados
Las diferencias entre el PEM contra los Certificados DER
Jerarquía del certificado
Certificados autofirmados contra los Certificados de tercera persona
Nombres comunes y nombres alternativos sujetos
Certificados de la placa comodín
Identifique los Certificados
CSR y su propósito
Uso de los Certificados entre el proceso del punto extremo y del apretón de manos SSL/TLS
Cómo CUCM utiliza los Certificados
La diferencia entre el tomcat y la Tomcat-confianza
Conclusión
Información Relacionada


## Introducción

El propósito de este documento es entender los fundamentos de los Certificados y de las autoridades de certificación. Este documento felicita otros documentos de Cisco que refieran a cualquier cifrado o característica de autenticación en el administrador de las Comunicaciones unificadas de Cisco (CUCM).

## prerrequisitos

### Requisitos

No hay requisitos específicos para este documento.

### Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

### Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

## Propósito de los Certificados

Los Certificados se utilizan entre los puntos extremos para construir una confianza/una autenticación y una encripción de datos. Esto confirma que los puntos finales comunican con el dispositivo previsto y tienen la opción para cifrar los datos entre los dos puntos finales.

### Defina la confianza de Point of View de un certificado

La mayoría de la parte importante de los Certificados es la definición cuyo los puntos extremos se pueden confiar en por su punto extremo. Este documento le ayuda a saber y a definir sus datos se cifran y se comparten con el sitio web previsto, teléfono, servidor FTP, y así sucesivamente.

Cuando su sistema confía en un certificado, éste significa que hay certificados instalados previamente en su sistema que lo estado sea el 100 por ciento de confiado que comparte la información con el punto extremo correcto. Si no, termina la comunicación entre estos puntos extremos.

Un ejemplo no técnico de esto es su licencia de driver. Usted utiliza esta licencia (servidor/certificado del servicio) de probar que usted es quién usted le dice es; usted obtuvo su licencia de su división local de bifurcación de los vehículos de motor (certificado intermedio) que ha sido dada el permiso por la división de los vehículos de motor (DMV) de su estado (Certificate Authority). Cuando usted necesita mostrar su licencia (servidor/certificado del servicio) a un oficial, el oficial sabe que pueden confiar en la bifurcación DMV (certificado intermedio) y la división de vehículos de motor (Certificate Authority), y pueden verificar que esta licencia fuera publicada por ellos (Certificate Authority). Su identidad se verifica al oficial y ahora confían en que usted es quién usted le dice es. Si no, si usted da una licencia falsa (servidor/certificado del servicio) que no fue firmada por el DMV (certificado intermedio), después no confiarán en que quién usted dice usted es. El recordatorio de este documento proporciona una explicación profundizada, técnica de la jerarquía del certificado.

### Cómo los navegadores utilizan los Certificados

1. Cuando usted visita un Web site, ingrese el URL, tal como http://www.cisco.com.
2. El DNS encuentra la dirección IP del servidor que host ese sitio.
3. El navegador navega a ese sitio.

Sin los Certificados, es imposible saber si utilizaron a un servidor DNS rogue, o si le rutearon a otro servidor. Los Certificados se aseguran de que le ruteen correctamente y con seguridad al

Web site previsto, tal como su Web site del banco, donde está segura el personal o la información vulnerable que usted ingresa.

Todos los navegadores tienen diversos iconos que utilizan, pero normalmente, usted ve un candado en la barra de dirección como esto:

1. Haga clic en las visualizaciones del candado y de una ventana:**Figura 1: Identificación del sitio web**
2. Haga clic en los **Certificados de la visión** para ver el certificado del sitio tal y como se muestra en de este ejemplo:**Figura 2: Información del certificado, ficha general** La información resaltada es importante.**Por publican la** compañía o el Certificate Authority (CA) confianzas de ese sus sistema ya.**Válido desde/hasta** es el rango de la fecha que este certificado es usable. (Usted ve a veces un certificado donde usted conoce le confianza CA, pero le ve que el certificado es inválido. Marque siempre la fecha así que usted sabe independientemente de si ha expirado.)**CONSEJO:** Una mejor práctica es crear un recordatorio en su calendario para renovar el certificado antes de que expire. Esto previene los problemas futuros.

## Las diferencias entre el PEM contra los Certificados DER

El PEM es ASCII; El DER es binario. El cuadro 3 muestra el formato del certificado PEM.

**Figura 3: Ejemplo del certificado PEM**
El cuadro 4 muestra el certificado DER.

**Figura 4: Ejemplo del certificado DER**
La mayoría de las compañías de CA como formato del uso PEM de Verisign o de Thawt para enviar los Certificados a los clientes, porque es correo electrónico-cómodo. El cliente debe copiar la cadena entera e incluirla **-----COMIENCE EL CERTIFICADO-----** y **-----CERTIFICADO DEL EXTREMO-----**, pegúelo en un archivo de texto, y sálvelo con el .PEM de la extensión o el .CER.

Windows puede leer el DER y el CER formata con su propio applet de la administración de certificados y muestra el certificado tal y como se muestra en del cuadro 5.

**Figura 5: Información del certificado**
En algunos casos, un dispositivo requiere un formato específico (ASCII o binario). Para cambiar esto, descargue el certificado de CA en el formato necesario o utilice una herramienta del convertidor SSL, tal como https://www.sslshopper.com/ssl-converter.html.

## Certifique la jerarquía

Para confiar en un certificado de un punto extremo, debe haber una confianza establecida ya con otro vendedor CA por ejemplo, cuadro 6 demostraciones allí es una jerarquía de tres Certificados.

**Figura 6: Jerarquía del certificado**
- **Verisign** es CA.
- **La validación ampliada SSL CA de la clase 3 de Verisign** es un intermedio o un certificado de servidor de firma (un servidor autorizado por CA para publicar los Certificados en su nombre).
- **www.website.com** es un servidor o un certificado del servicio.

Su punto extremo necesita saber que pueda confiar en CA y los Certificados del intermedio primero antes de que sepa que puede confiar en el certificado de servidor presentado por el contacto SSL (detalles abajo). Para entender mejor cómo esta confianza trabaja, refiera a la sección en este documento: **Defina la "confianza" de Point of View de un certificado**.

## Certificados autofirmados contra los Certificados de tercera persona

Las diferencias principales entre los Certificados uno mismo-firmados y de tercera persona son quién firmada el certificado, si usted los confía en.

Un certificado autofirmado es un certificado firmado por el servidor que lo presenta; por lo tanto, el servidor/el certificado del servicio y el certificado de CA son lo mismo.

CA de tercera persona es un servicio proporcionado por o CA público (como Verisign, confía, Digicert) o un servidor (como Windows 2003, Linux, Unix, IOS) ese controla la validez del servidor/del certificado del servicio.

Cada uno puede ser un CA independientemente de si su sistema confía en ese CA, es qué importa más.

# Nombres comunes y nombres alternativos sujetos

Los nombres comunes (CN) y los nombres alternativos sujetos (SAN) son referencias a la dirección IP o al nombre de dominio completo (FQDN) del direccionamiento se pide que. Por ejemplo, si usted ingresa https://www.cisco.com, después el CN o el SAN debe tener www.cisco.com en la encabezado.

En el ejemplo mostrado en el cuadro 7, el certificado tiene el CN como www.cisco.com. La petición URL para www.cisco.com del navegador marca el URL FQDN contra la información que el certificado presenta. En este caso, hacen juego, y muestra que el contacto SSL es acertado. Este sitio web se ha verificado para ser el sitio web correcto y las comunicaciones ahora se cifran entre el escritorio y el sitio web.

**Figura 7: Verificación del sitio web**

En el mismo certificado, hay una encabezado SAN para tres direccionamientos FQDN/DNS:

**Figura 8: Encabezado SAN**

Este certificado puede autenticar/verifica www.cisco.com (también definido en el CN), cisco.com, y cisco-images.cisco.com. Esto significa que usted puede también teclear cisco.com, y este mismo certificado se puede utilizar para autenticar y para cifrar este sitio web.

CUCM puede crear las encabezados SAN. Refiera al documento de la quemadura de Jason, CUCM que carga los Certificados de la red GUI del ccmadmin en la comunidad del soporte para más información sobre las encabezados SAN.

## Certificados de la placa comodín

Los Certificados del comodín son los Certificados que utilizan un asterisco (*) para representar cualquier cadena en una sección de un URL. Por ejemplo, para tener un certificado para www.cisco.com, ftp.cisco.com, ssh.cisco.com, y así sucesivamente, un administrador necesitaría solamente crear un certificado para *.cisco.com. Para salvar el dinero, las necesidades del

administrador solamente de comprar un solo certificado y no necesitan comprar los certificados múltiples.

Esta característica no es soportada actualmente por el administrador de las Comunicaciones unificadas de Cisco (CUCM). Sin embargo, usted puede no perder de vista esta mejora: CSCta14114: Pedido el soporte del certificado del comodín en CUCM y la importación de la clave privada.

## Identifique los Certificados

Cuando los Certificados tienen la misma información en ellos, usted puede ver si es el mismo certificado. Todos los Certificados tienen un número de serie único. Usted puede utilizar esto para comparar si los Certificados son los mismos Certificados, regenerado, o falsificación. El cuadro 9 proporciona un ejemplo:

**Figura 9: Número de serie del certificado**

## CSR y su propósito

Pedido de firma de certificado de la significa CSR. Si usted quiere crear un certificado de tercera persona para un servidor CUCM, usted necesita un CSR presentar a CA. Este CSR parece mucho un certificado PEM (ASCII).

**Nota:** Esto no es un certificado y no se puede utilizar como uno.

CUCM crea los CSR automáticamente vía la red GUI: **Cisco unificó el** Certificate Management (Administración de certificados) del **>** Security (Seguridad) de la **administración del sistema operativo > genera CSR >** elige el servicio que usted quiere crear el certificado **>** entonces **genera el CSR**. Cada vez que se utiliza esta opción, se genera una nuevos clave privada y CSR.

**Nota:** Una clave privada es un archivo que es único a este servidor y servicio. ¡Esto se debe nunca dar a cualquier persona! Si usted proporciona una clave privada alguien, compromete la Seguridad que el certificado proporciona. También, no regenere un nuevo CSR para el mismo servicio si usted utiliza el CSR viejo para crear un certificado. CUCM borra el viejos CSR y clave privada y substituye ambos ellos, que hace el CSR viejo inútil.

Refiera a la documentación de la quemadura de Jason en la comunidad del soporte: CUCM que carga los Certificados de la red GUI del ccmadmin para la información sobre cómo crear los CSR.

# Uso de los Certificados entre el proceso del punto extremo y del apretón de manos SSL/TLS

El protocolo de entrada en contacto es una serie de mensajes ordenados que negocien los parámetros de seguridad de una sesión de la Transferencia de datos. Refiera al SSL/TLS detalladamente , que documenta la secuencia de mensaje en el protocolo de entrada en contacto. Éstos se pueden ver en una captura de paquetes (PCAP). Los detalles incluyen la inicial, subsiguiente, y los últimos mensajes enviados y recibidos entre el cliente y servidor.

# Cómo CUCM utiliza los Certificados

## La diferencia entre el tomcat y la Tomcat-confianza

Cuando los Certificados están cargados a CUCM, hay dos opciones para cada servicio vía **Cisco unificó el** Certificate Management (Administración de certificados) > el **hallazgo del** > Security (Seguridad) de la **administración del sistema operativo**.

Los cinco servicios que permiten que usted **maneje los** Certificados en CUCM son:

- tomcat
- IPSec
- callmanager
- capf
- TV (en la versión 8.0 CUCM y posterior)

Aquí están los servicios que permiten que usted **cargue los** Certificados a CUCM:

- tomcat
- Tomcat-confianza
- IPSec
- IPSec-confianza
- callmanager
- CallManager-confianza
- capf
- CAPF-confianza

Éstos son los servicios disponibles en la versión 8.0 CUCM y posterior:

- TV
- TV-confianza
- teléfono-confianza
- teléfono-VPN-confianza
- teléfono-sast-confianza
- teléfono-CTL-confianza

Refiera a las guías de la Seguridad CUCM por la versión para más detalles en estos tipos de Certificados. Esta sección explica solamente la diferencia entre un certificado del servicio y un certificado de confianza.

Por ejemplo, con el **tomcat**, las Tomcat-**confianzas** cargan CA y los Certificados intermedios de modo que este nodo CUCM lo conozca pueden confiar en cualquier certificado firmado por CA y el servidor intermedio. El certificado del tomcat es el certificado que es presentado por el servicio del tomcat en este servidor, si un punto extremo hace un pedido de HTTP a este servidor. Para permitir la presentación de los Certificados de tercera persona por el tomcat, el nodo CUCM necesita saber que pueda confiar en CA y el servidor intermedio. Por lo tanto, es un requisito cargar CA y los Certificados intermedios antes de que el certificado del tomcat (servicio) esté cargado.

Refiera al CUCM de la quemadura de Jason que carga los Certificados de la red GUI del ccmadmin en la comunidad del soporte para la información que le ayudará a entender cómo cargar los Certificados a CUCM.

Cada servicio tiene su propio certificado del servicio y Certificados de confianza. No trabajan de uno a. Es decir CA y un certificado intermedio cargados como servicio de la Tomcat-confianza no

se pueden utilizar por el servicio de CallManager.

**Nota:** Los Certificados en CUCM son a por nodo por. Por lo tanto, si usted necesita los Certificados cargados al editor, y usted necesite a los suscriptores tener los mismos Certificados, usted necesita cargar los a cada servidor individual y el nodo antes de la versión 8.5 CUCM. En la versión 8.5 CUCM y posterior, hay un servicio que replica los Certificados cargados al resto de los Nodos en el cluster.

**Nota:** Cada nodo tiene un diverso CN. Por lo tanto, un CSR se debe crear por cada nodo para que el servicio presente sus propios Certificados.

Si usted tiene preguntas específicas adicionales sobre las funciones de seguridad unas de los CUCM, refiera a la documentación de la Seguridad.

## Conclusión

Este documento ayuda y construye a un nivel elevado de conocimiento en los Certificados. Este tema puede importar puede llegar a ser más profundizado, pero este documento le familiariza bastante para trabajar con los Certificados. Si usted tiene preguntas sobre cualesquiera funciones de seguridad CUCM, refiera a las guías de la Seguridad CUCM por la versión para más información.

## Información Relacionada

- Guías del mantenimiento y de la Seguridad del Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- Comunidad del soporte de Cisco: CUCM que carga los Certificados de la red GUI del ccmadmin
- Bug CSCta14114: Pedido el soporte del certificado del comodín en CUCM y la importación de la clave privada
- Cisco Emergency Responder (CER) explicado
- Soporte Técnico y Documentación - Cisco Systems