Vista de alto nivel de certificados y autoridades en CUCM

Contenido

Introducción

Este documento describe los aspectos básicos de los certificados y las autoridades de certificados. Complementa a otros documentos de Cisco que hacen referencia a cualquier función de cifrado o autenticación de Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

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). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Objetivo de los certificados

Los certificados se utilizan entre terminales para generar confianza/autenticación y cifrado de datos. Esto confirma que los terminales se comunican con el dispositivo deseado y tienen la opción de cifrar los datos entre los dos terminales.

Nota: Para comprender el impacto de cada certificado, consulte Proceso de regeneración de certificados para el impacto de Cisco Unified Communications Manager en el almacén de certificados

---

Definir la confianza desde el punto de vista de un certificado

La parte más importante de los certificados es la definición de los extremos en los que el terminal puede confiar. Este documento le ayuda a conocer y definir cómo se cifran y comparten sus datos con el sitio web, el teléfono, el servidor FTP, etc.

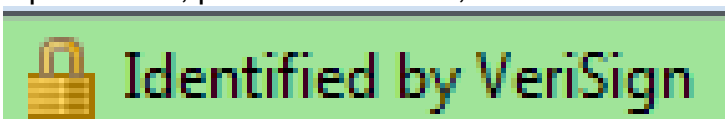
Cuando el sistema confía en un certificado, esto significa que hay uno o varios certificados preinstalados en el sistema que indican que está 100% seguro de que comparte información con el terminal correcto. De lo contrario, finaliza la comunicación entre estos extremos.

Un ejemplo no técnico de esto es su licencia de conducir. Usted utiliza esta licencia (certificado de servidor/servicio) para probar que es quien dice ser; obtuvo su licencia de su sucursal local de la División de Vehículos Motorizados (certificado intermedio) que ha recibido permiso de la División de Vehículos Motorizados (DMV) de su Estado (Autoridad de Certificación). Cuando necesita mostrar su licencia (certificado de servidor/servicio) a un oficial, el oficial sabe que puede confiar en la rama DMV (certificado intermedio) y la División de Vehículos Motorizados (autoridad de certificación), y pueden verificar que esta licencia fue emitida por ellos (autoridad de certificación). Tu identidad es verificada por el oficial y ahora confían en que eres quien dices ser. De lo contrario, si proporciona una licencia falsa (certificado de servidor/servicio) que no estaba firmada por el DMV (certificado intermedio), no confiarán en quién dice ser. El resto de este documento proporciona una explicación técnica detallada de la jerarquía de certificados.

Cómo utilizan los navegadores los certificados

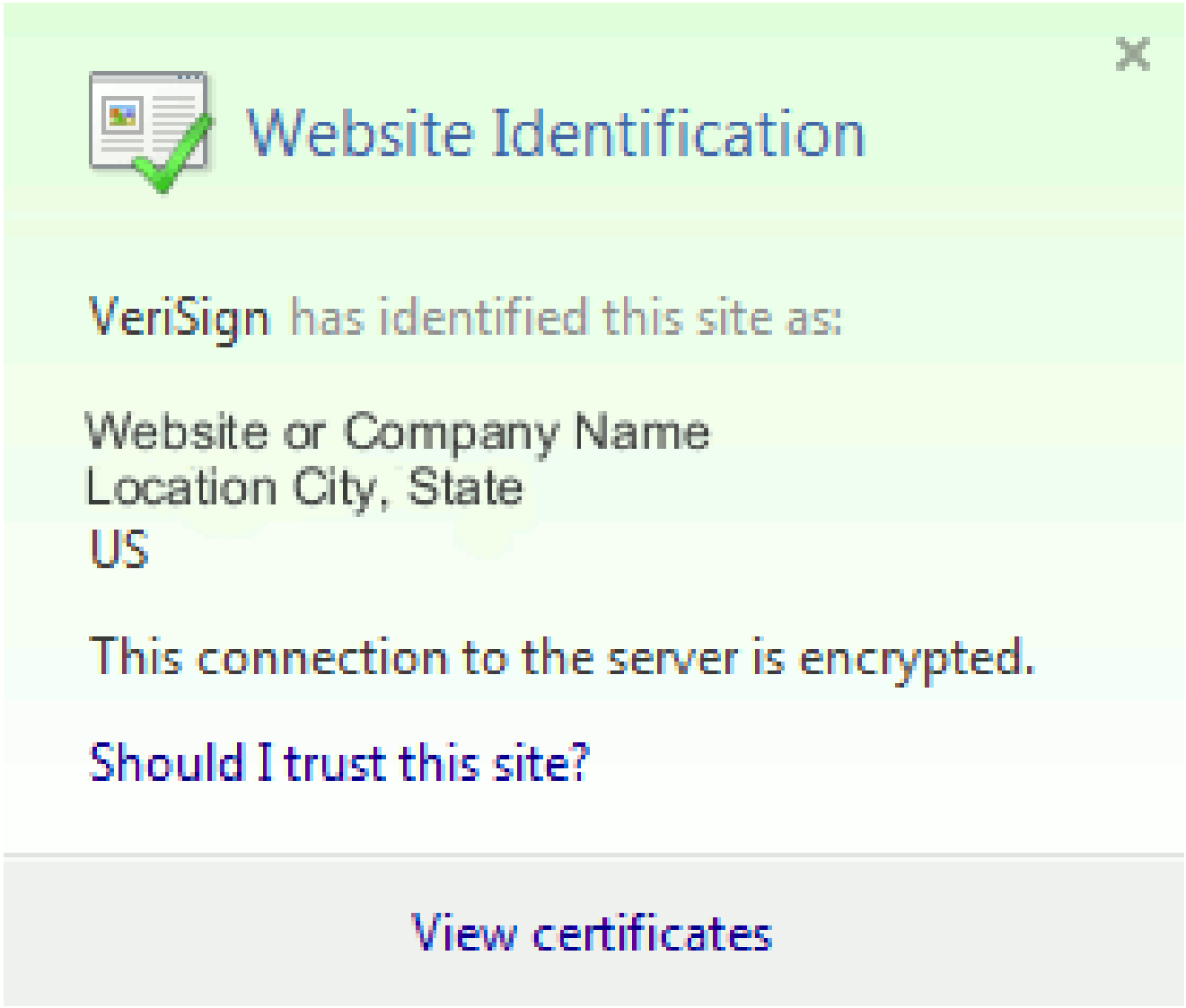
1. Cuando visite un sitio web, introduzca la URL, como http://www.cisco.com.
2. El DNS encuentra la dirección IP del servidor que aloja ese sitio.
3. El explorador se desplaza a ese sitio.

Sin certificados, es imposible saber si se ha utilizado un servidor DNS no autorizado o si se ha enrutado a otro servidor. Los certificados garantizan que se le dirige de forma correcta y segura al sitio web deseado, como el sitio web de su banco, donde la información personal o confidencial que introduce es segura.

Todos los navegadores tienen diferentes iconos que utilizan, pero normalmente, se ve un candado en la barra de direcciones como este: 

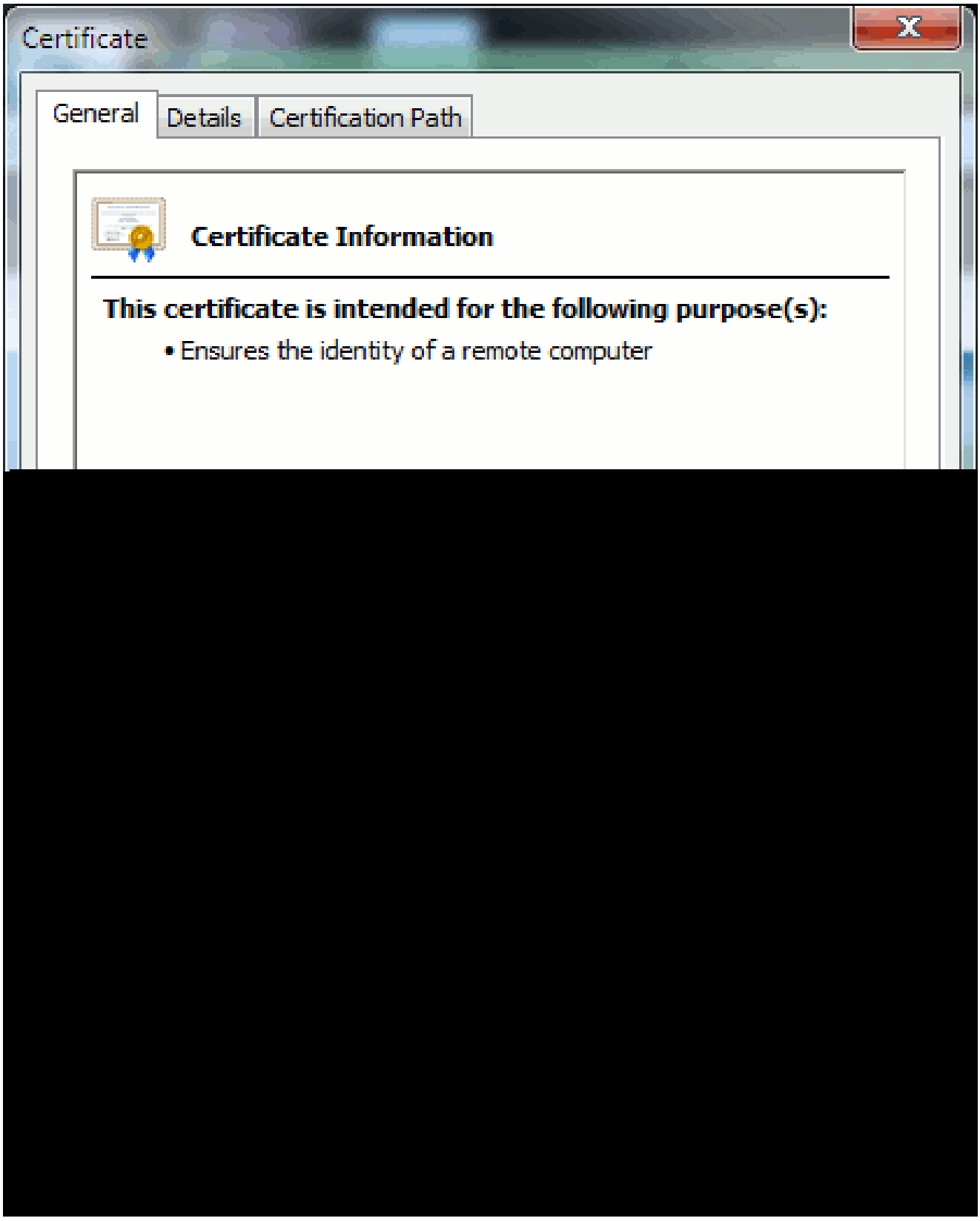
1. Haga clic en el candado y aparecerá una ventana:

Figura 1: Identificación del sitio web



2. Haga clic en Ver certificados para ver el certificado del sitio como se muestra en este ejemplo:

Figura 2: Información del certificado, ficha General



La información resaltada es importante.

- Emitido por es la Empresa o Autoridad de certificación (CA) en la que ya confía su sistema.
- Válido de/a es el rango de fechas en el que se puede utilizar este certificado. (A veces, aparece un certificado en el que se sabe que se confía en la CA, pero se ve que el certificado no es válido. Compruebe siempre la fecha para saber si ha caducado o no.)

Sugerencia: una práctica recomendada es crear un aviso en el calendario para renovar el certificado antes de que caduque. Esto evita futuros problemas.

Diferencias entre los certificados PEM y DER

PEM es ASCII; DER es binario. La figura 3 muestra el formato del certificado PEM.

Figura 3: Ejemplo de certificado PEM

PEM Certificate

```
-----BEGIN CERTIFICATE-----
MIID2DCCAsCgAwIBAgIIDY2I6UJvckUwDQYJKoZIhvcNAQEFBQAwaTEXMBUGA1UE
AwwOODUxUHViLmtqbC5jb20xDDAKBgNVBAsMA1RBQzERMA8GA1UECgwIQ1VDTV9M
YWIxEzARBgNVBAcMCkJveGJvcm91Z2gxCzAJBgNVBAgMAk1BMQswCQYDVQQGEwJV
UzAeFw0xMjA2MDgxNDA0MzdaFw0xNzA2MDgxNDA0MzdaMGkxFzAVBgNVBAMMDjg1
MVB1Yi5ramwuY29tMQwwCgYDVQQLDANUQUMxETAPBgNVBAoMCENVQ01fTGFiMRMw
EQYDVQQHDApCb3hib3JvdWdoMQswCQYDVQQIDAJNQTELMAkGA1UEBhMCVVMwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC261nIdUNKiaMqFH29vClz4iC/
E/4A8zAiqsAupLw0FpDpQnUCkquw6Tntk0nxo2SbUQdtjyheaHa9YphkECsynDwa
aIEfcoMdTpWaWRjvJ7VCQPg8dGettLoklbSNe08tv8D/HYdKGG+zhF1i4kzvwYJy
ipthHlZB0+MnMglM/R7RcZ18oAUF3IMIhv6p3sm6o51J0HhvVJm9JDA7zyz7iCvg
WHolJa9ck338/R9rd0KUhioDIahQBqOiUAN8pYdgxcPxtE5REx7/3CMoDCBKeC5W
wGMJyHpAeGW8zaTqpXLXDM/7hJwIWWVXomUU7Qwvm/DceGnc4e6uaZ/a9B3zAgMB
AAGjgYMwgYAwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMBBggrBgEF
BQcDAgYIKwYBBQUHAwUwKQYDVR0RBCIwIIIOODUxUHViLmtqbC5jb22CDnBob251
cy5ramwuY29tMB0GA1UdDgQWBBTbWvEUfpl7hvrsTJpQfmcoNpB4LzANBgkqhkiG
9w0BAQUFAAOCAQEArZWeqarg4tagW0O0rQEl2j6UJ9S8ZAcp9XDT4Iz1QwRaaiBr
EBhfulaMjmtMKXFV5eCU9QcPbPG8XmiRZiEg9Q8Wtn0OZpuPGlkwxmFYRz40aY4T
5lw+d0wVb9sPChNQEGccjjqwtstElYWDo/A4RoqdH0ALceP8a4bovK/CpmRGdb5C
+hqP4zIJs4P+YKmzrJeq7H8xCCqqkYXcRLkmG6mif78txFQ5lr8rJEoU1VlL8znc
fJvSfEsCfwnSqPaGcQTnxMOZOIyM0OjXvvhWIezrpk8cyj3vSTgXSTwO53flZX4L
tu28d5H3AHo8U6cfHRIJ1f6Yv2ClGBShXwFp6Q==
-----END CERTIFICATE-----
```

La figura 4 muestra el certificado DER.

Figura 4: Ejemplo de certificado DER

La mayoría de las empresas de CA como VeriSign o Thawt utilizan el formato PEM para enviar los certificados a los clientes, ya que es compatible con el correo electrónico. El cliente debe

copiar la cadena completa e incluir -----BEGIN CERTIFICATE— y -----END CERTIFICATE—, pegarla en un archivo de texto y guardarla con la extensión .PEM o .CER.

Windows puede leer los formatos DER y CER con su propio subprograma de administración de certificados y muestra el certificado como se muestra en la figura 5.

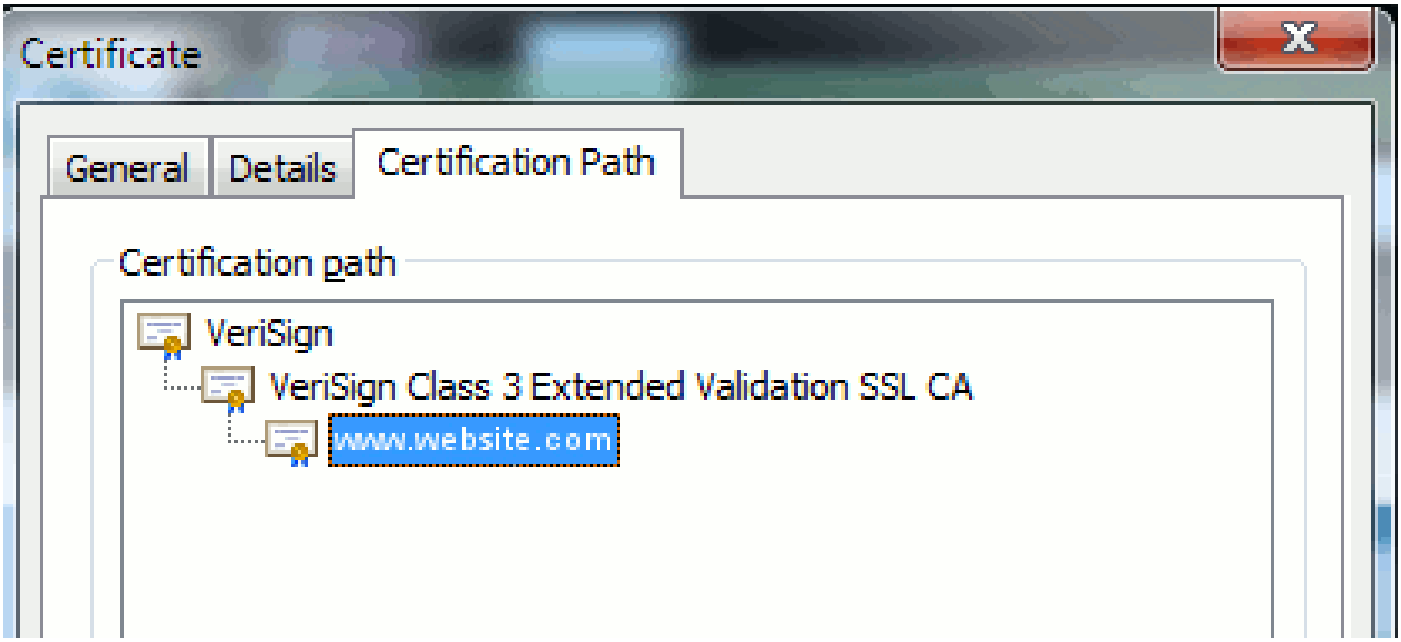
Figura 5: Información del certificado

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

Jerarquía de certificados

Para confiar en un certificado de un extremo, debe haber una confianza ya establecida con una CA de terceros. Por ejemplo, en la figura 6 se muestra una jerarquía de tres certificados.

Figura 6: Jerarquía de certificados



- Verisign es una CA.
- Verisign Class 3 Extended Validation SSL CA es un certificado de servidor intermedio o de firma (un servidor autorizado por CA para emitir certificados en su nombre).
- www.website.com es un certificado de servidor o servicio.

Su punto final necesita saber que puede confiar en la CA y en los certificados intermedios antes de saber que puede confiar en el certificado de servidor presentado por el protocolo de enlace SSL (detalles a continuación). Para entender mejor cómo funciona esta confianza, consulte la sección de este documento: Definir "Confianza" desde el punto de vista de un certificado.

Certificados autofirmados frente a certificados de terceros

Las principales diferencias entre los certificados autofirmados y los de terceros son quién firmó el certificado, independientemente de si confía en ellos.

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

Una CA de terceros es un servicio proporcionado por una CA pública (como Verisign, Entrust, Digicert) o un servidor (como Windows 2003, Linux, Unix, IOS) que controla la validez del certificado de servicio/servidor.

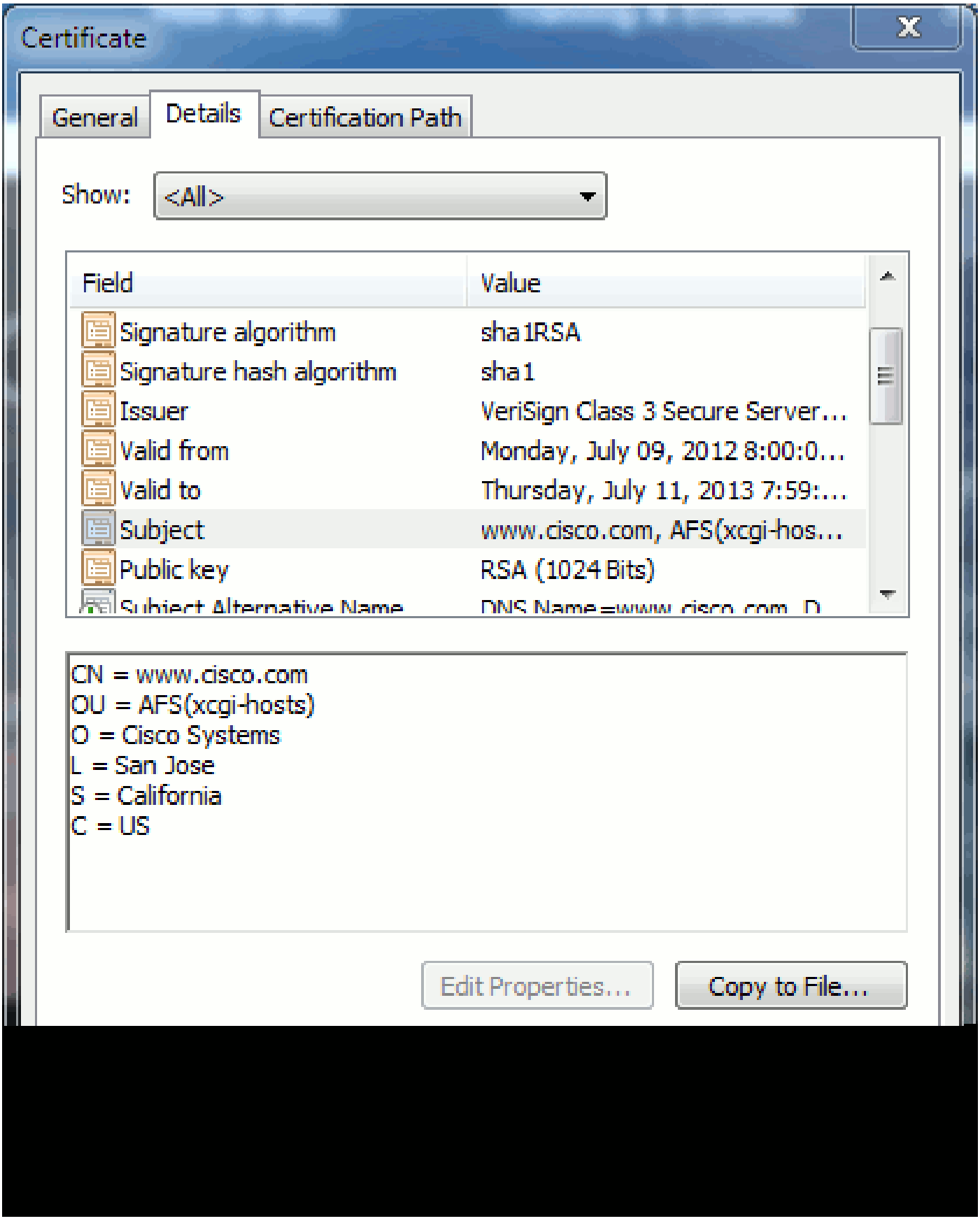
Cada una puede ser una CA. Si su sistema confía o no en esa CA, es lo que más importa.

Nombres comunes y nombres alternativos del asunto

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

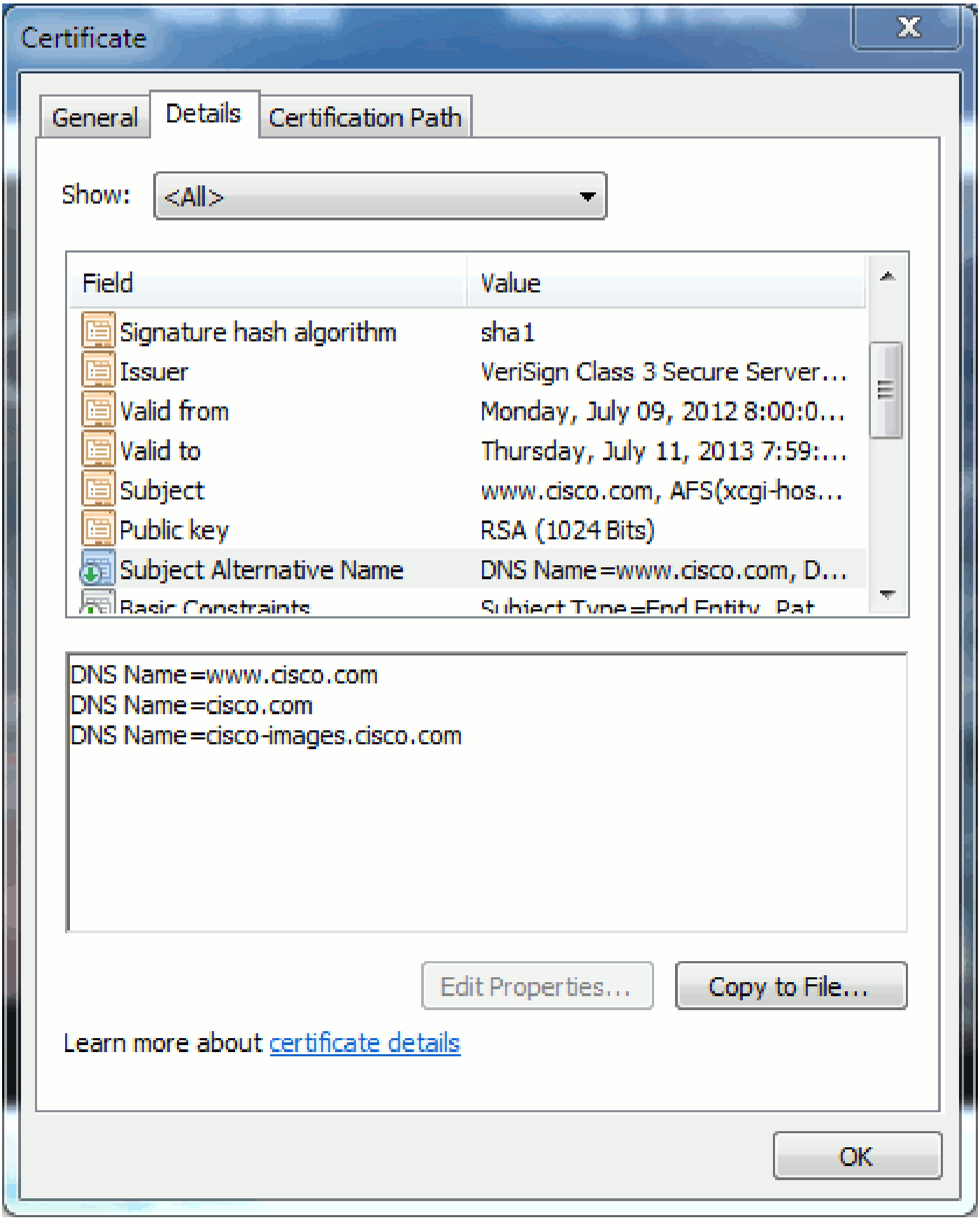
En el ejemplo de la figura 7, el certificado tiene el CN como www.cisco.com. La solicitud de URL para www.cisco.com desde el navegador verifica el FQDN de URL con la información que presenta el certificado. En este caso, coinciden y muestra que el intercambio de señales SSL es exitoso. Se ha comprobado que este sitio web es el correcto y las comunicaciones están cifradas entre el escritorio y el sitio web.

Figura 7: Verificación del sitio web



En el mismo certificado, hay un encabezado SAN para tres direcciones FQDN/DNS:

Figura 8: Encabezado de SAN



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

CUCM puede crear encabezados SAN. Consulte el documento de Jason Burn, CUCM Uploading

CCMAdmin Web GUI Certificates en la Support Community para obtener más información sobre los encabezados SAN.

Certificados de comodín

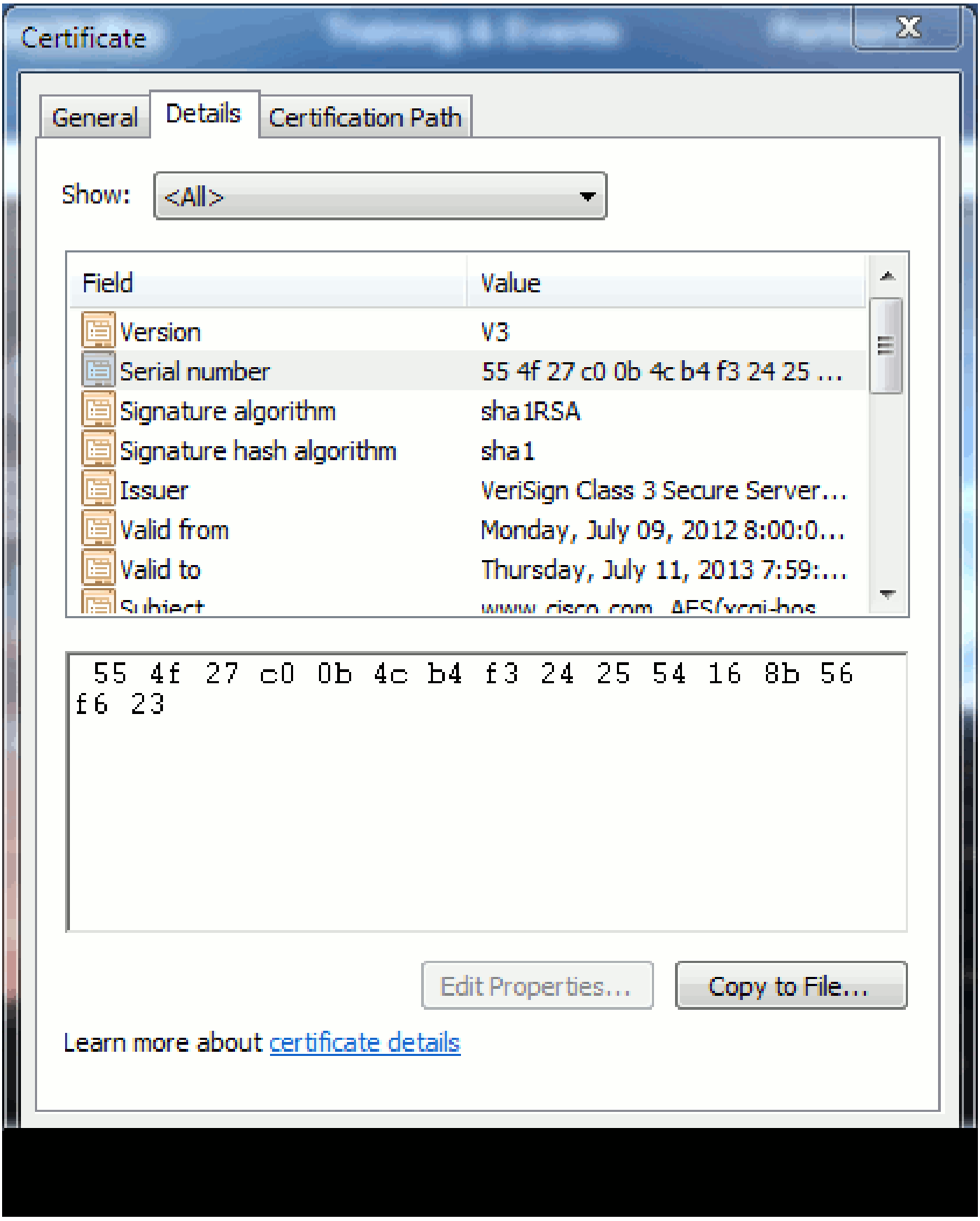
Los certificados comodín son certificados que utilizan un asterisco (*) para representar cualquier cadena de una sección de una dirección URL. Por ejemplo, para tener un certificado para www.cisco.com, ftp.cisco.com, ssh.cisco.com, etc., un administrador sólo tendría que crear un certificado para *.cisco.com. Para ahorrar dinero, el administrador solo necesita comprar un único certificado y no necesita comprar varios certificados.

Cisco Unified Communications Manager (CUCM) no admite actualmente esta función. Sin embargo, puede realizar un seguimiento de esta mejora: CSCta14114: Request for support of wildcard certificate in CUCM and private key import.

Identificar los certificados

Cuando los certificados contienen la misma información, puede ver si se trata del mismo certificado. Todos los certificados tienen un número de serie único. Puede utilizar esta opción para comparar si los certificados son los mismos certificados, regenerados o falsificados. La Figura 9 proporciona un ejemplo:

Figura 9: Número de serie del certificado



RSC y su propósito

CSR significa Solicitud de firma de certificado. Si desea crear un certificado de terceros para un servidor de CUCM, necesita un CSR para realizar la presentación a la CA. Este CSR se parece

mucho a un certificado PEM (ASCII).

Nota: no se trata de un certificado y no se puede utilizar como tal.

\

CUCM crea CSR automáticamente a través de la GUI web: Cisco Unified Operating System Administration > Security > Certificate Management > Generate CSR, seleccione el servicio que desea crear el certificado snf y, a continuación, Generate CSR. Cada vez que se utiliza esta opción, se genera una nueva clave privada y CSR.

Nota: Una clave privada es un archivo que es único para este servidor y servicio. ¡Esto nunca se le debe dar a nadie! Si proporciona una clave privada a alguien, pone en peligro la seguridad que proporciona el certificado. Además, no vuelva a generar una nueva CSR para el mismo servicio si utiliza la antigua CSR para crear un certificado. CUCM elimina la antigua CSR y la clave privada y reemplaza ambas, lo que hace que la antigua CSR sea inútil.

Consulte la documentación de Jason Burn sobre la Comunidad de soporte: CUCM Uploading CCMAdmin Web GUI Certificates para obtener información sobre cómo crear CSR.

Uso de certificados entre el punto final y el proceso de intercambio de señales SSL/TLS

El protocolo de enlace es una serie de mensajes en secuencia que negocian los parámetros de seguridad de una sesión de transferencia de datos. Consulte SSL/TLS en Detalle , que documenta la secuencia de mensajes en el protocolo de intercambio de señales. Esto se puede observar en la captura de paquetes (PCAP). Los detalles incluyen los mensajes inicial, subsiguiente y final enviados y recibidos entre el cliente y el servidor.

Cómo utiliza CUCM los certificados

La diferencia entre tomcat y tomcat-trust

Cuando los certificados se cargan en CUCM, hay dos opciones para cada servicio a través de Cisco Unified Operating System Administration > Security > Certificate Management > Find.

Los cinco servicios que le permiten administrar certificados en CUCM son:

- tomcat
- ipsec

- callmanager
- capf
- tvs (en CUCM versión 8.0 y posteriores)

Estos son los servicios que le permiten cargar certificados en CUCM:

- tomcat
- tomcat-trust
- ipsec
- ipsec-trust
- callmanager
- callmanager-trust
- capf
- capf-trust

Estos son los servicios disponibles en CUCM Release 8.0 y versiones posteriores:

- tvs
- tvs-trust
- phone-trust
- phone-vpn-trust
- phone-sast-trust
- phone-ctl-trust

Consulte las Guías de seguridad de CUCM por versión para obtener más detalles sobre estos tipos de certificados. Esta sección sólo explica la diferencia entre un certificado de servicio y un certificado de confianza.

Por ejemplo, con tomcat, tomcat-trusts carga la CA y los certificados intermedios para que este nodo de CUCM sepa que puede confiar en cualquier certificado firmado por la CA y el servidor intermedio. El certificado tomcat es el certificado que presenta el servicio tomcat en este servidor si un punto final realiza una solicitud HTTP a este servidor. Para permitir la presentación de certificados de terceros por parte de tomcat, el nodo de CUCM necesita saber que puede confiar en la CA y el servidor intermedio. Por lo tanto, es un requisito cargar la CA y los certificados intermedios antes de que se cargue el certificado (de servicio) tomcat.

Consulte Carga de certificados de GUI web de CUCM de Jason Burn en la Comunidad de soporte

para obtener información que le ayudará a comprender cómo cargar certificados en CUCM.

Cada servicio tiene su propio certificado de servicio y certificados de confianza. No funcionan el uno con el otro. En otras palabras, el servicio CallManager no puede utilizar una CA y un certificado intermedio cargados como servicio tomcat-trust.

Nota: los certificados de CUCM se basan en cada nodo. Por lo tanto, si necesita certificados cargados en el editor y necesita que los suscriptores tengan los mismos certificados, debe cargarlos en cada servidor y nodo individual antes de la versión 8.5 de CUCM. En CUCM Release 8.5 y versiones posteriores, existe un servicio que replica certificados cargados en el resto de los nodos del clúster.

Nota: Cada nodo tiene un CN diferente. Por lo tanto, cada nodo debe crear una CSR para que el servicio presente sus propios certificados.

Si tiene preguntas específicas adicionales sobre alguna de las funciones de seguridad de CUCM, consulte la documentación de seguridad.

Conclusión

Este documento ayuda y genera un alto nivel de conocimiento sobre los certificados. Este tema puede llegar a ser más detallado, pero este documento lo familiariza lo suficiente para trabajar con certificados. Si tiene alguna pregunta sobre las funciones de seguridad de CUCM, consulte las Guías de seguridad de CUCM por versión para obtener más información.

Información Relacionada

- Guías de mantenimiento y seguridad de Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- Comunidad de soporte de Cisco: CUCM carga de certificados GUI web de CCMAdmin
- Error CSCta14114: Solicitud de compatibilidad con certificado comodín en CUCM e importación de clave privada
- Explicación de Cisco Emergency Responder (CER)
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).