Vista de alto nivel de certificados y autoridades en CUCM

Contenido

Introducción

El propósito de este documento es comprender los fundamentos de los certificados y las autoridades certificadoras. Este documento complementa 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.

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. 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.

Finalidad de los certificados

Los certificados se utilizan entre puntos finales para generar una 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.

Definir confianza desde el punto de vista de un certificado

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

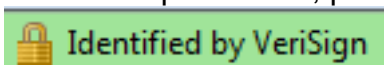
Cuando su sistema confía en un certificado, esto significa que hay un certificado preinstalado en su sistema que indica que está 100% seguro de que comparte información con el punto final correcto. De lo contrario, termina la comunicación entre estos terminales.

Un ejemplo no técnico de esto es su licencia de conducir. Utiliza esta licencia (certificado de servidor/servicio) para probar que es quien dice ser; ha obtenido su licencia de la sucursal local de la División de Vehículos de Motor (certificado intermedio) a la que ha concedido permiso la División de Vehículos de Motor (DMV) de su Estado (autoridad certificadora). Cuando necesita mostrar su licencia (certificado de servidor/servicio) a un oficial, el oficial sabe que pueden confiar en la sucursal DMV (certificado intermedio) y la División de Vehículos de Motor (autoridad certificadora), y pueden verificar que esta licencia fue emitida por ellos (autoridad certificadora). Su identidad se verifica para el oficial y ahora confían en que usted es quien dice ser. De lo contrario, si proporciona una licencia falsa (certificado de servidor/servicio) que no ha firmado el DMV (certificado intermedio), no confiarán en quién dice que es. El resto de este documento proporciona una explicación técnica detallada de la jerarquía de certificados.

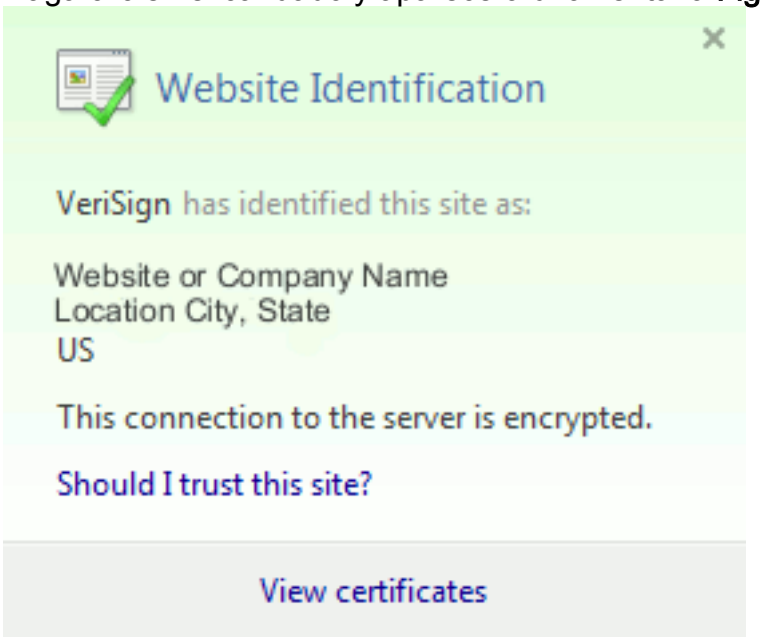
Cómo utilizan los exploradores los certificados

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.

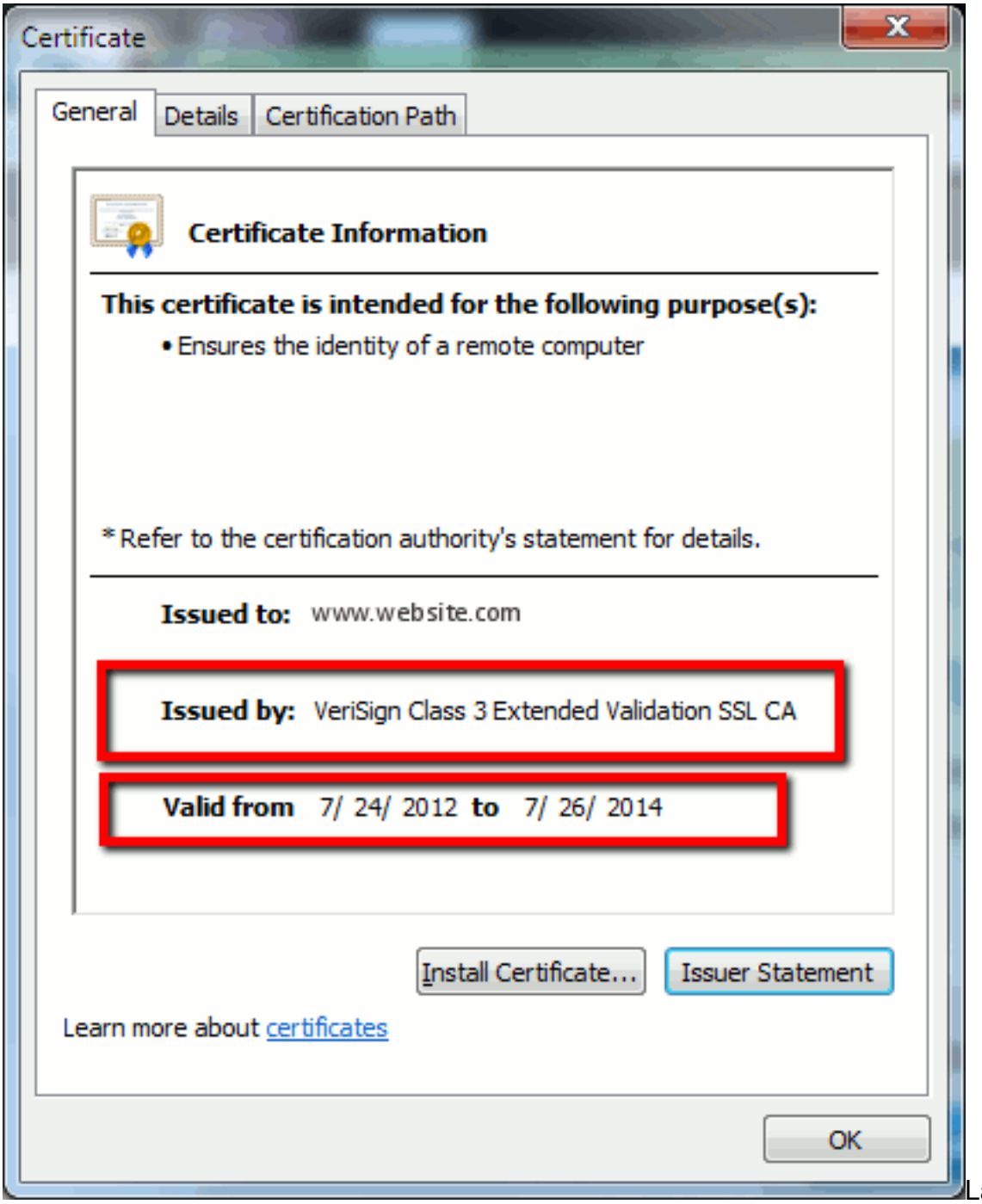
Sin certificados, es imposible saber si se utilizó un servidor DNS no autorizado o si se le enrutó a otro servidor. Los certificados garantizan que se le dirige de forma correcta y segura al sitio web deseado, como el sitio web del banco, donde la información personal o confidencial que introduzca es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

Todos los exploradores tienen iconos diferentes 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.**Emitida por** es la Empresa o Autoridad de Certificación (CA) en la que su sistema ya confía.**Válido de/a** es el rango de fechas que se puede utilizar este certificado. (A veces ve un certificado en el que sabe que confía en la CA, pero ve que el certificado no es válido. Compruebe siempre la fecha para saber si ha caducado o no.)**Consejo:** Una práctica recomendada es crear un recordatorio en su calendario para renovar el certificado antes de que caduque. Esto evita futuros problemas.

Las diferencias entre PEM y DER Certificados

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

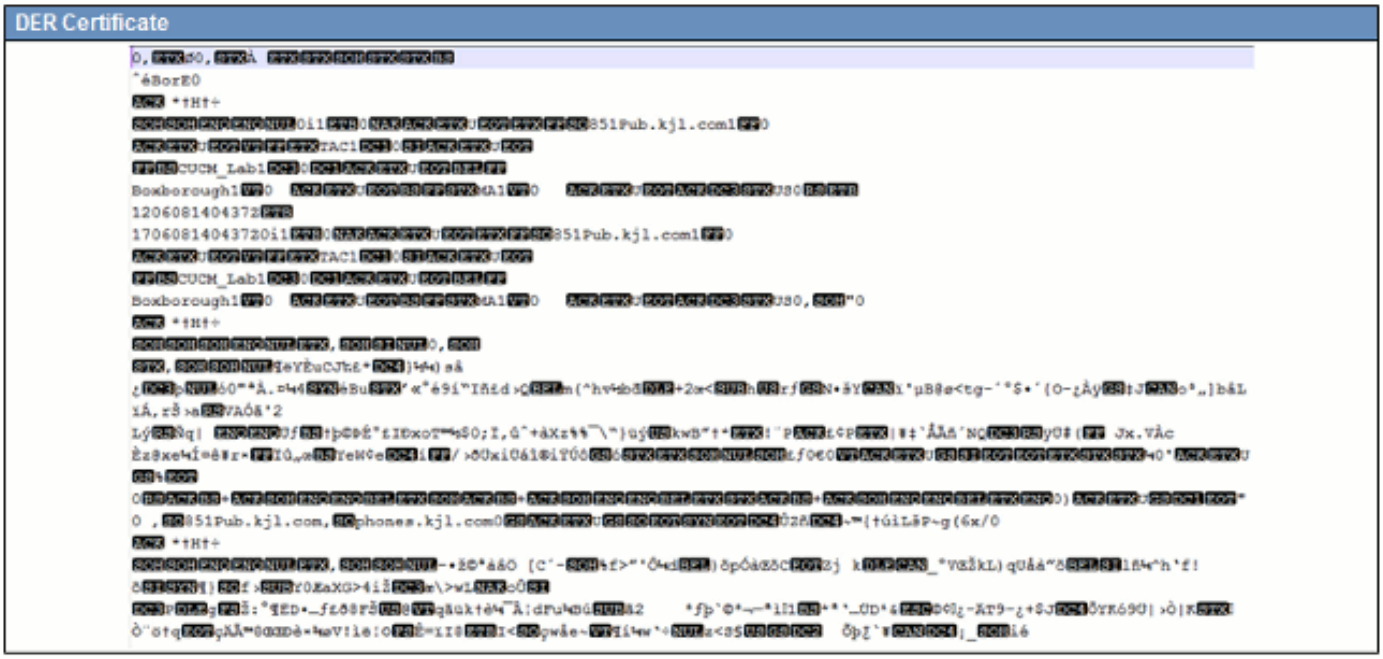
Figura 3: Ejemplo de certificado PEM

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
9w0BAQUFAAOCAQEArZWeqarg4tagW0O0rQElZj6UJ9S8ZAcp9XDT4Iz1QwRaaiBr
EBhfulaMjmtMKXFV5eCU9QcPbPG8XmiRZiEg9Q8Wtn0OZpuPGlkwxmFYRz40aY4T
5lw+d0wVb9sPChNQEGccjjqwtstElYWDo/A4RoqdH0ALceP8a4bovK/CpmRGdb5C
+hqP4zIJs4P+YKmzrJeq7H8xCCqqkYXcRLkmG6mif78txFQ5lr8rJEoU1VlL8znc
fJvSfEsCfwnSqPaGcQTnxMOZOIyM0OjXvvhWIezrpk8cyj3vSTgXSTwO53flZX4L
tu28d5H3AHo8U6cfHRIJ1f6Yv2ClGBShXwFp6Q==
-----END CERTIFICATE-----
```

La figura 4 muestra el certificado DER.

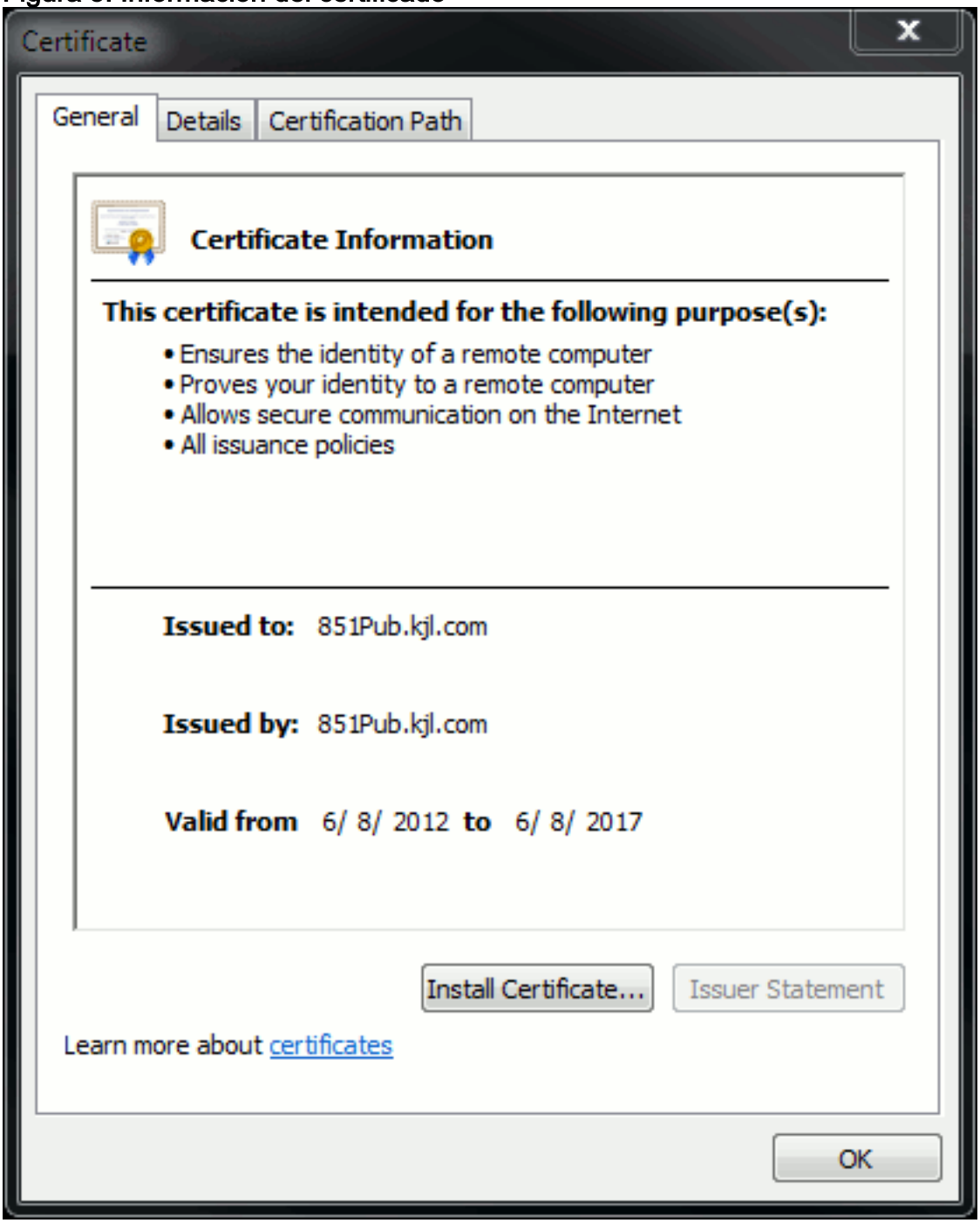
Figura 4: Ejemplo de certificado DER



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 fácil de enviar por 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 Applet de administración de certificados y muestra el certificado como se muestra en la figura 5.

Figura 5: Información del certificado

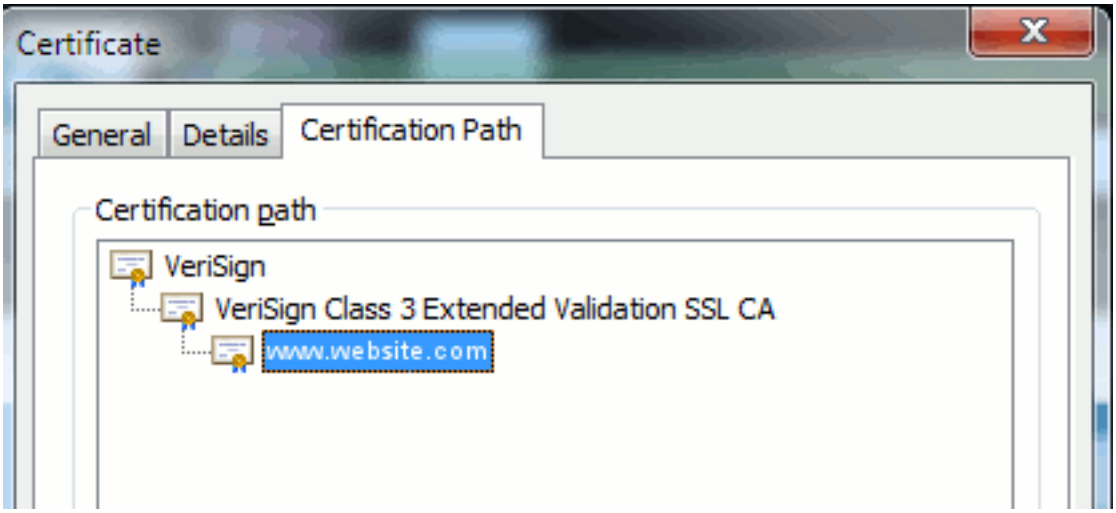


En algunos casos, un dispositivo requiere un formato específico (ASCII o binario). Para cambiar esto, descargue el certificado de la CA en el formato necesario o utilice una herramienta de convertidor SSL, como https://www.sslshopper.com/ssl-converter.html.

Jerarquía de certificados

Para confiar en un certificado desde un punto final, debe haber una confianza ya establecida con una CA de terceros. Por ejemplo, la figura 6 muestra que hay 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.

El terminal debe saber que puede confiar en los certificados CA e intermedios antes de que sepa que puede confiar en el certificado de servidor presentado por el intercambio de señales SSL (detalles a continuación). Para entender mejor cómo funciona esta confianza, consulte la sección de este documento: **Defina "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 certificados 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 servidor/servicio 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 servidor/servicio.

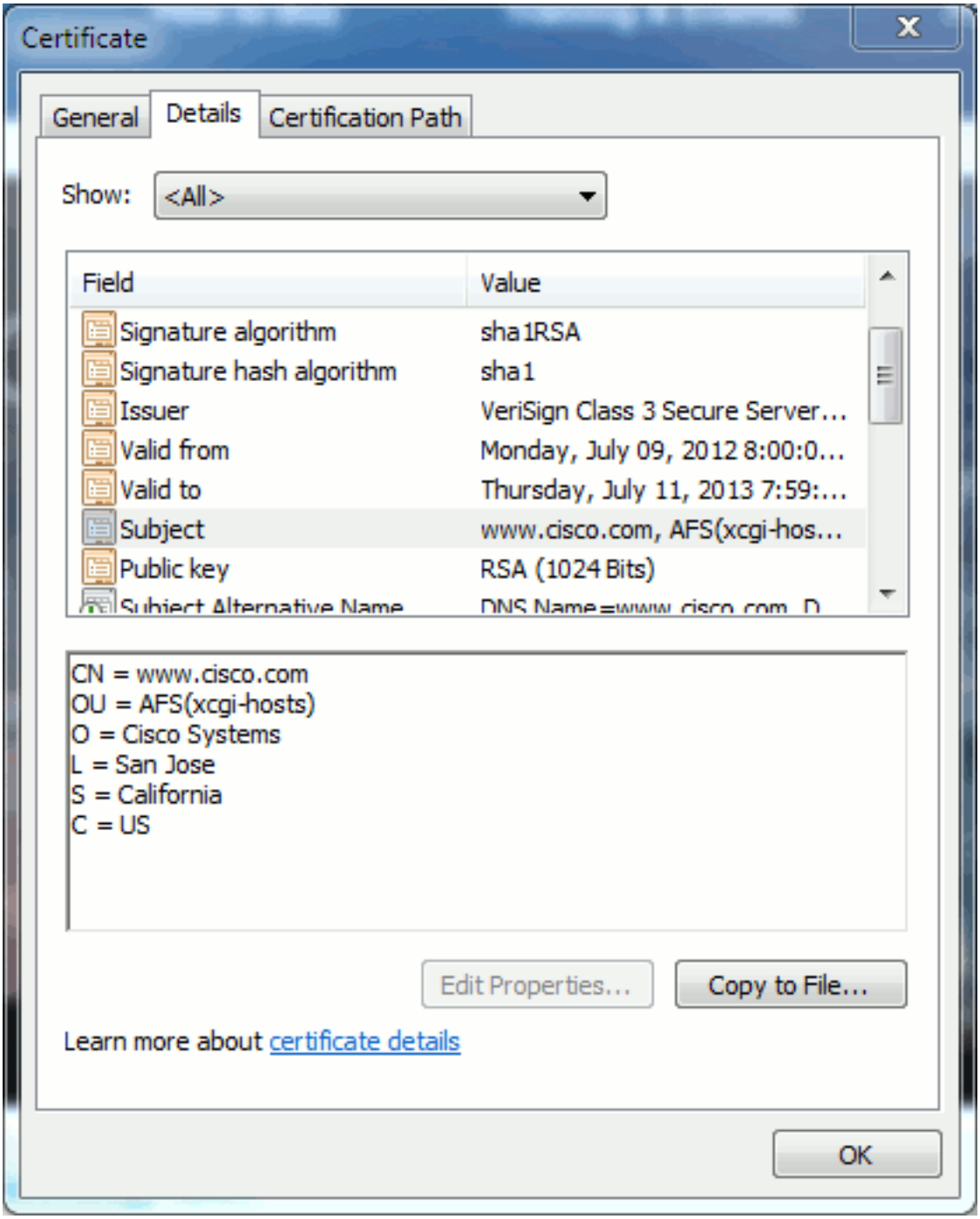
Cada una puede ser una CA. Si su sistema confía o no en la CA, es lo que más importa.

Nombres comunes y nombres alternativos de 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 introduce https://www.cisco.com, el CN o SAN debe tener www.cisco.com en el encabezado.

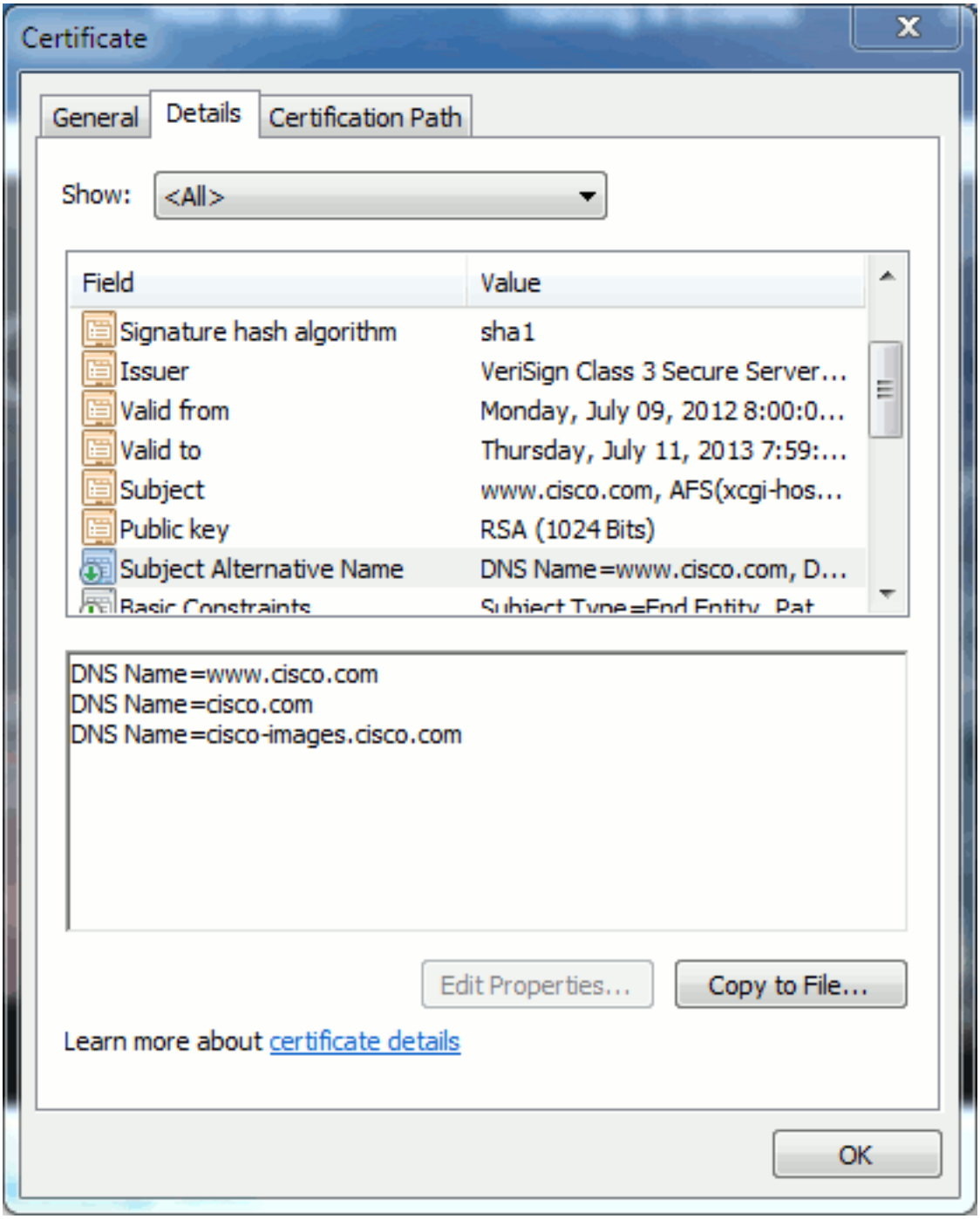
En el ejemplo que se muestra en la figura 7, el certificado tiene el CN como www.cisco.com. La solicitud de URL para www.cisco.com desde el explorador verifica el FQDN de URL con la información que presenta el certificado. En este caso, coinciden y muestra que el intercambio de señales SSL es exitoso. Este sitio web se ha comprobado que es el sitio web correcto y las comunicaciones se cifran ahora 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 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 Comunidad de soporte para obtener más información sobre los encabezados SAN.

Certificados Wild Card

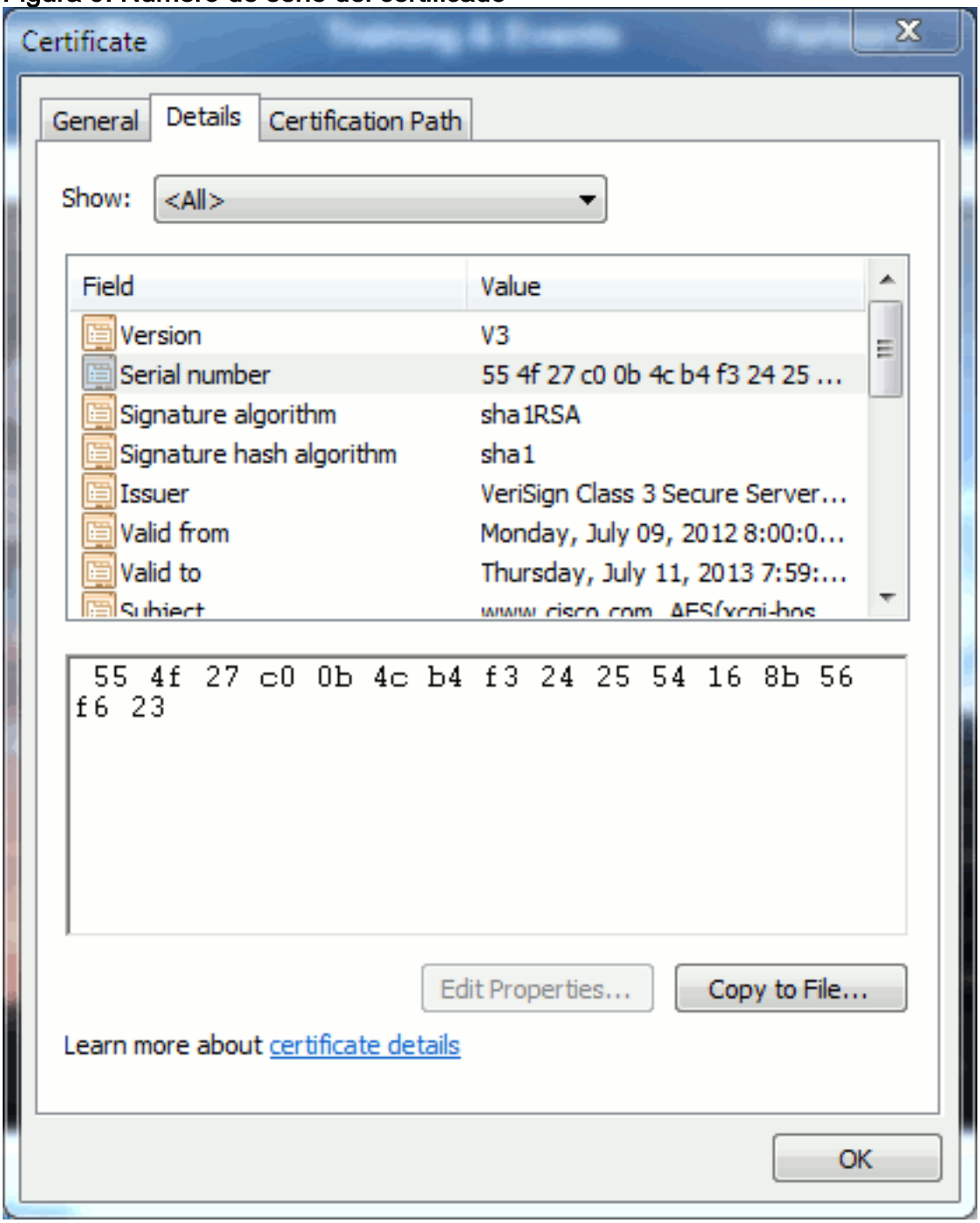
Los certificados comodín son certificados que utilizan un asterisco (*) para representar cualquier cadena en una sección de una dirección URL. Por ejemplo, para tener un certificado para www.cisco.com, ftp.cisco.com, ssh.cisco.com, etc., un administrador sólo tendría que crear un certificado para *.cisco.com.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

Cisco Unified Communications Manager (CUCM) no admite actualmente esta función. Sin embargo, puede realizar un seguimiento de esta mejora: CSCta14114: Solicitud de soporte del certificado comodín en CUCM y de importación de clave privada.

Identificación de los certificados

Cuando los certificados contienen la misma información, puede ver si es el mismo certificado. Todos los certificados tienen un número de serie único. Puede utilizarla 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



RSE y su finalidad

CSR significa solicitud de firma de certificado. Si desea crear un certificado de terceros para un

servidor CUCM, necesita un CSR para presentarlo a la CA. Esta CSR se parece mucho a un certificado PEM (ASCII).

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

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

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

Consulte la documentación de Jason Burn en Support Community: CUCM Cargando certificados CCMAdmin Web GUI para obtener información sobre cómo crear CSR.

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

El protocolo de intercambio de señales es una serie de mensajes secuenciados 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. Estos se pueden ver en una captura de paquetes (PCAP). Los detalles incluyen los mensajes iniciales, subsiguientes y finales 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 versión 8.0 y posteriores:

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

Refiérase a 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**, los **tomcat-trust** cargan la CA y los certificados intermedios para que este nodo 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 tomcat, el nodo CUCM necesita saber que puede confiar en la CA y en el servidor intermedio. Por lo tanto, es un requisito cargar la CA y los certificados intermedios antes de cargar el certificado tomcat (servicio).

Refiérase a Carga de Certificados GUI Web CCMAdmin de Jason Burn en la Comunidad de Soporte para obtener información que le ayudará a entender cómo cargar certificados en CUCM.

Cada servicio tiene su propio certificado de servicio y certificados de confianza. Ellos no se trabajan entre sí. 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 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 versión 8.5 y posteriores, hay un servicio que replica los certificados cargados al 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 cualquiera 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 asunto puede ser más profundo, pero este documento le familiariza lo suficiente para trabajar con los 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 CCMAdmin Web GUI
- Error CSCta14114: Solicitud de soporte del certificado comodín en CUCM e importación de clave privada
- Explicación de Cisco Emergency Responder (CER)
- Soporte Técnico y Documentación - Cisco Systems