Visualização de alto nível de certificados e autoridades no CUCM

Contents

Introdução

Este documento descreve os fundamentos dos certificados e das autoridades de certificação. Ele complementa outros documentos da Cisco que se referem a qualquer recurso de criptografia ou autenticação no Cisco Unified Communications Manager (CUCM).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Finalidade dos certificados

Os certificados são usados entre endpoints para criar confiança/autenticação e criptografia de dados. Isso confirma que os endpoints se comunicam com o dispositivo pretendido e têm a opção de criptografar os dados entre os dois endpoints.

Observação: para entender o impacto de cada certificado, consulte Processo de regeneração de certificados para o Cisco Unified Communications Manager Impacto pela seção Armazenamento de certificados

---

Definir Confiança do Ponto de Vista de um Certificado

A parte mais importante dos certificados é a definição de quais endpoints podem ser confiáveis para seu endpoint. Este documento ajuda você a saber e definir como seus dados são criptografados e compartilhados com o site, telefone, servidor FTP e assim por diante.

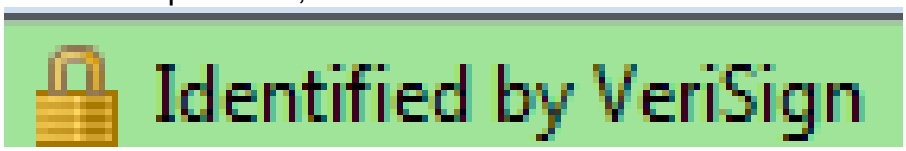
Quando o sistema confia em um certificado, isso significa que há um certificado pré-instalado no sistema que afirma que ele tem 100% de certeza de que compartilha informações com o endpoint correto. Caso contrário, ele encerra a comunicação entre esses endpoints.

Um exemplo não técnico disso é a sua carteira de motorista. Você usa esta licença (certificado de servidor/serviço) para provar que é quem você diz ser; você obteve sua licença de sua filial local da Divisão de Veículos Automotores (certificado intermediário) que recebeu permissão da Divisão de Veículos Automotores (DMV) de seu Estado (Autoridade de Certificação). Quando você precisa mostrar sua licença (certificado de servidor/serviço) para um funcionário, o funcionário sabe que pode confiar na filial DMV (certificado intermediário) e na Divisão de Veículos a Motor (autoridade de certificação) e pode verificar se esta licença foi emitida por eles (autoridade de certificação). Sua identidade é verificada pelo policial e agora eles confiam que você é quem você diz ser. Caso contrário, se você fornecer uma licença falsa (certificado de servidor/serviço) que não foi assinada pelo DMV (certificado intermediário), ele não confiará em quem você diz ser. O restante deste documento fornece uma explicação técnica detalhada da hierarquia de certificados.

Como os navegadores usam certificados

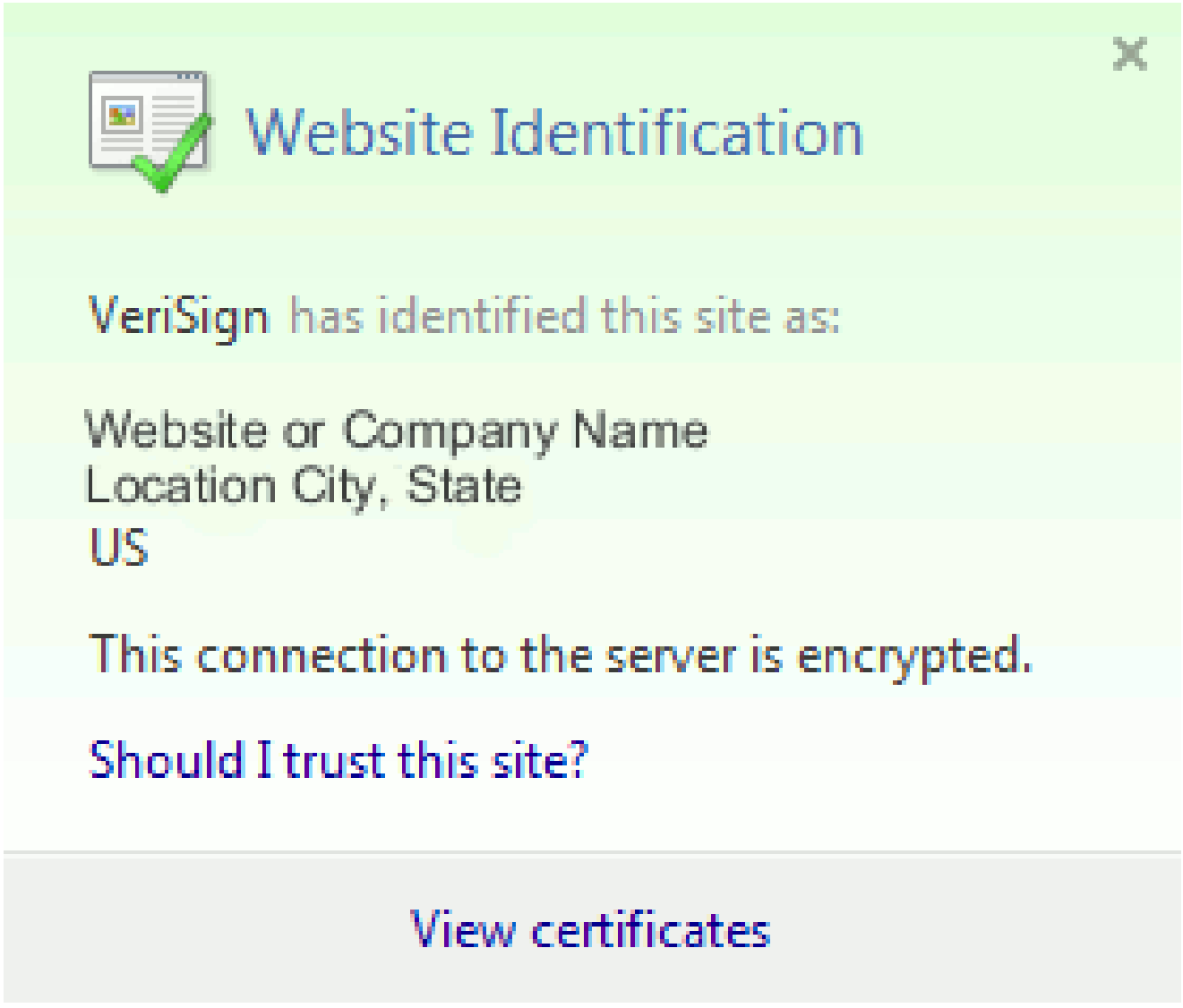
1. Quando você visita um site, digite o URL, como http://www.cisco.com.
2. O DNS encontra o endereço IP do servidor que hospeda esse site.
3. O navegador navega para esse site.

Sem certificados, é impossível saber se um servidor DNS invasor foi usado ou se você foi roteado para outro servidor. Os certificados garantem que você seja encaminhado de forma adequada e segura para o site desejado, como o site do seu banco, onde as informações pessoais ou confidenciais inseridas são seguras.

Todos os navegadores têm ícones diferentes que usam, mas normalmente você vê um cadeado na barra de endereços como este: 

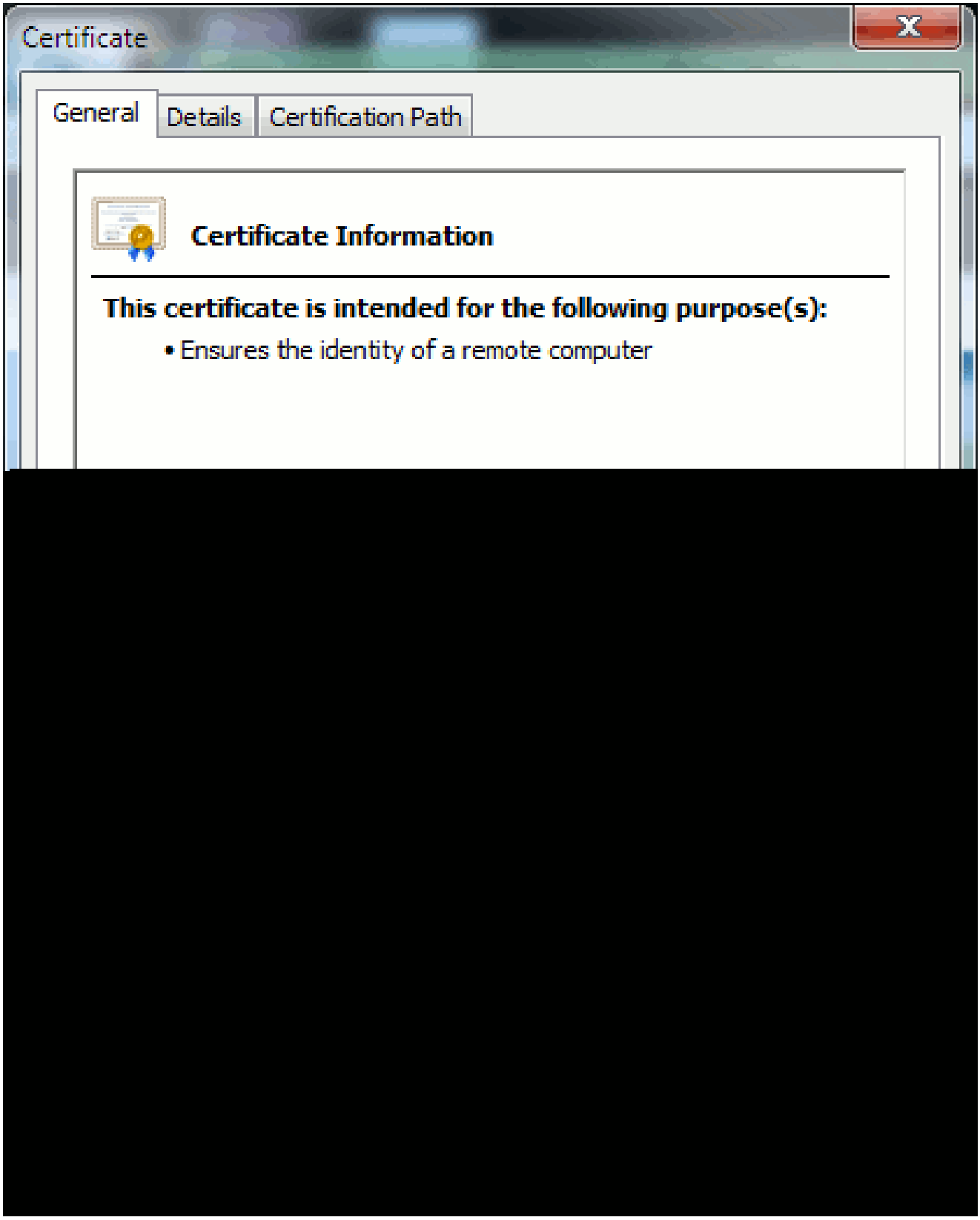
1. Clique no cadeado e uma janela será exibida:

   Figura 1: Identificação do site



2. Clique em View Certificates para ver o certificado do site como mostrado neste exemplo:

Figura 2: Informações do certificado, guia Geral



As informações destacadas são importantes.

- Emitido por é a Empresa ou Autoridade de Certificação (CA) em que o sistema já confia.

- Válido de/até é o intervalo de datas em que este certificado pode ser usado. (Às vezes, você vê um certificado em que sabe que confia na CA, mas vê que o certificado é inválido. Sempre verifique a data para saber se ela expirou.)

Dica: uma prática recomendada é criar um lembrete em seu calendário para renovar o certificado antes que ele expire. Isso evita problemas futuros.

Diferenças entre certificados PEM e DER

PEM é ASCII; DER é binário. A Figura 3 mostra o formato do certificado PEM.

Figura 3: Exemplo de certificado PEM

PEM Certificate

```
-----BEGIN CERTIFICATE-----
MIID2DCCAsCgAwIBAgIIDY2I6UJvckUwDQYJKoZIhvcNAQEFBQAwaTEXMBUGA1UE
AwwODUxUHViLmtqbC5jb20xDDAKBgNVBAsMA1RBQzERMA8GA1UECgwIQ1VDTV9M
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-----
```

A Figura 4 mostra o Certificado DER.

Figura 4: Exemplo de certificado DER

A maioria das empresas de CA, como a VeriSign ou Thawt, usa o formato PEM para enviar os certificados aos clientes, pois ele é amigável para e-mail. O cliente deve copiar a string inteira e incluir -----BEGIN CERTIFICATE— e -----END CERTIFICATE—, colá-la em um arquivo de texto e salvá-la com a extensão .PEM ou .CER.

O Windows pode ler os formatos DER e CER com seu próprio miniaplicativo de gerenciamento de certificados e mostra o certificado como mostrado na Figura 5.

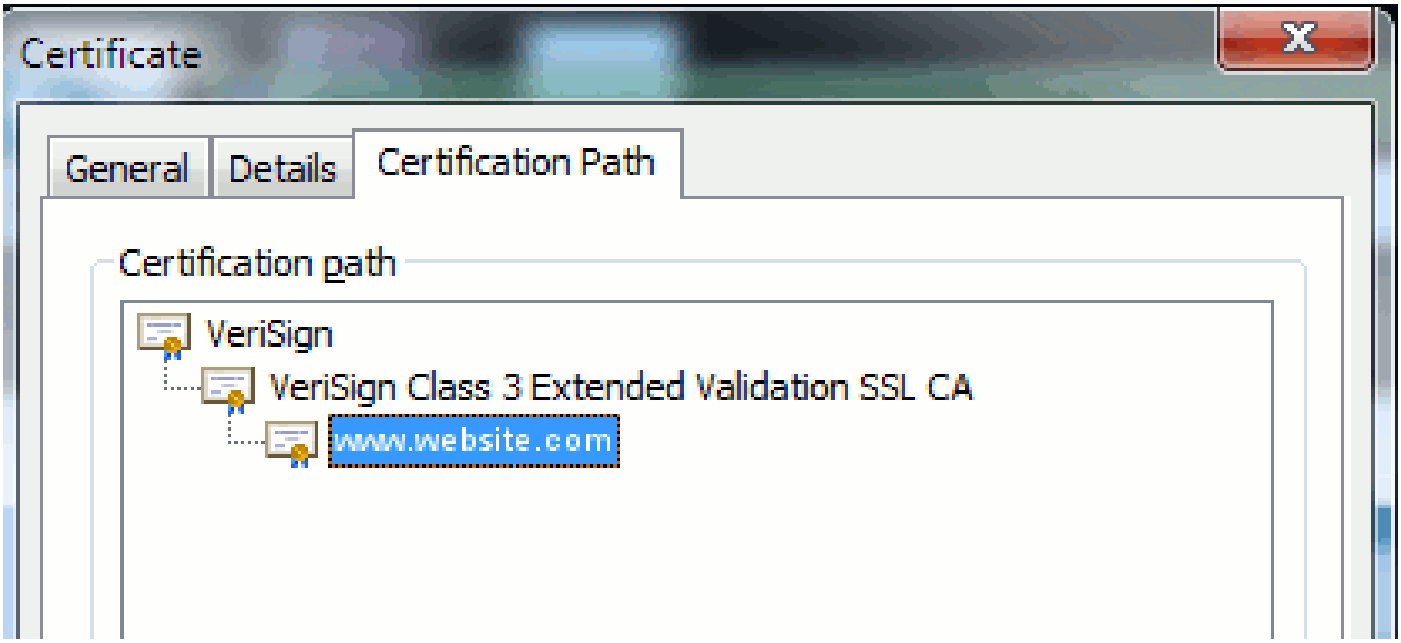
Figura 5: Informações do certificado

Em alguns casos, um dispositivo requer um formato específico (ASCII ou binário). Para alterar isso, baixe o certificado da CA no formato necessário ou use uma ferramenta de conversão SSL, como https://www.sslshopper.com/ssl-converter.html.

Hierarquia de Certificado

Para confiar em um certificado de um ponto de extremidade, deve haver uma confiança já estabelecida com uma CA de terceiros. Por exemplo, a Figura 6 mostra que há uma hierarquia de três certificados.

Figura 6: Hierarquia de certificados



- Verisign é uma CA.
- Verisign Classe 3 Validação Estendida A CA SSL é um certificado de servidor intermediário ou de assinatura (um servidor autorizado pela CA a emitir certificados em seu nome).
- www.website.com é um certificado de servidor ou serviço.

Seu ponto final precisa saber que pode confiar tanto na CA quanto nos certificados intermediários antes de saber que pode confiar no certificado do servidor apresentado pelo Handshake SSL (detalhes abaixo). Para entender melhor como essa relação de confiança funciona, consulte a seção neste documento: Definir "Relação de Confiança" do Ponto de Vista de um Certificado.

Certificados com assinatura automática versus certificados de terceiros

As principais diferenças entre certificados autoassinados e de terceiros são quem assinou o

certificado, se você confia neles.

Um certificado autoassinado é um certificado assinado pelo servidor que o apresenta; portanto, o certificado de servidor/serviço e o certificado CA são os mesmos.

Uma CA de terceiros é um serviço fornecido por uma CA pública (como Verisign, Entrust, Digicert) ou um servidor (como Windows 2003, Linux, Unix, IOS) que controla a validade do certificado de servidor/serviço.

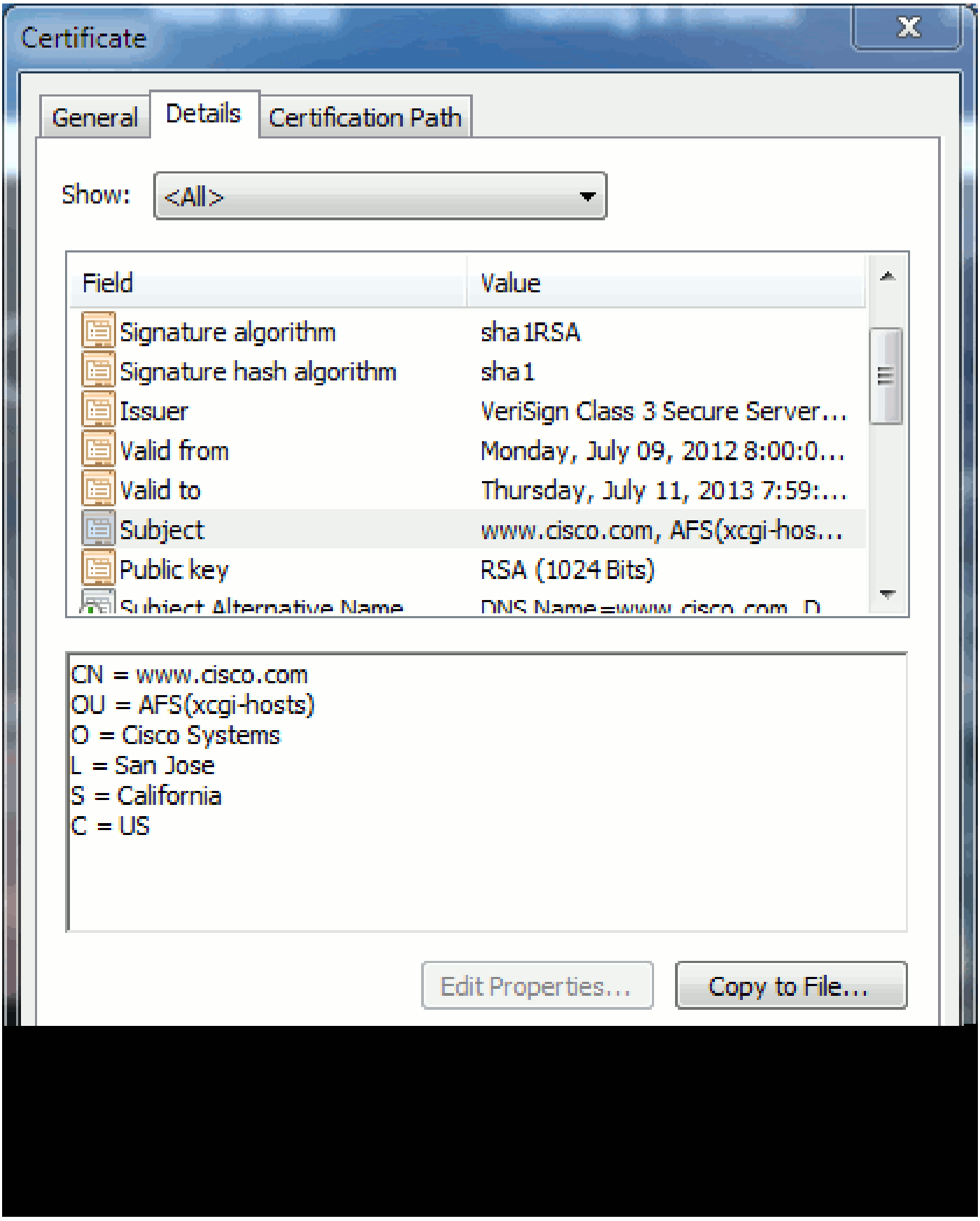
Cada um pode ser um CA. Se o seu sistema confia ou não na CA, é o que mais importa.

Nomes Comuns e Nomes Alternativos do Assunto

CN (Common Names, nomes comuns) e SAN (Subject Alternative Names, nomes alternativos de assunto) são referências ao endereço IP ou FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado) do endereço solicitado. Por exemplo, se você digitar https://www.cisco.com, o CN ou SAN deverá ter www.cisco.com no cabeçalho.

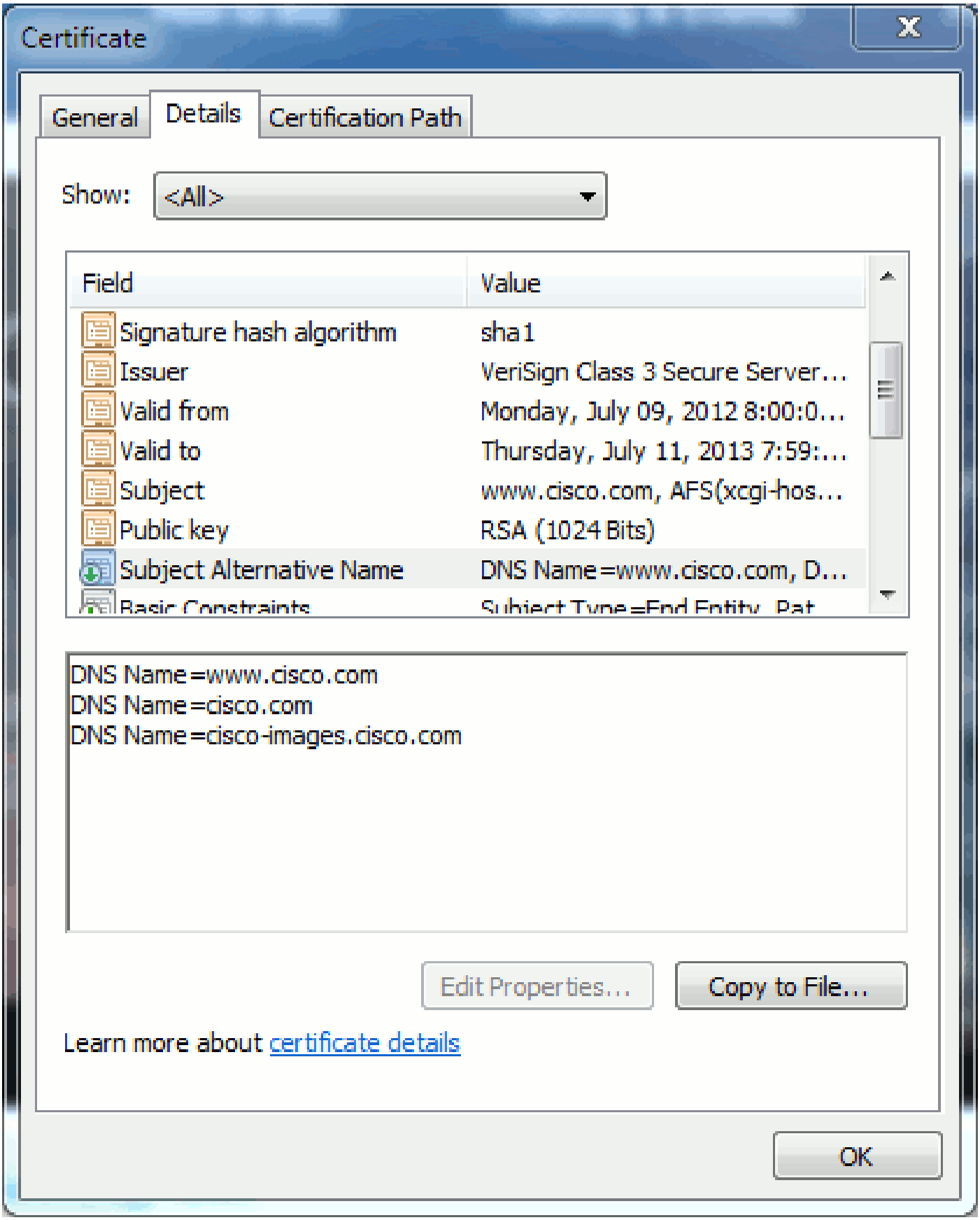
No exemplo mostrado na figura 7, o certificado tem o CN como www.cisco.com. A solicitação de URL para www.cisco.com do navegador verifica o FQDN da URL em relação às informações que o certificado apresenta. Nesse caso, eles correspondem e mostra que o handshake SSL foi bem-sucedido. Este site foi verificado para ser o site correto e as comunicações agora estão criptografadas entre o desktop e o site.

Figura 7: Verificação do site



No mesmo certificado, há um cabeçalho SAN para três endereços FQDN/DNS:

Figura 8: Cabeçalho SAN



Este certificado pode autenticar/verificar www.cisco.com (também definido no CN), cisco.com e cisco-images.cisco.com. Isso significa que você também pode digitar cisco.com, e esse mesmo certificado pode ser usado para autenticar e criptografar esse site.

O CUCM pode criar cabeçalhos SAN. Consulte o documento de Jason Burn, CUCM Uploading

CCMAdmin Web GUI Certificates na Comunidade de Suporte para obter mais informações sobre cabeçalhos de SAN.

Certificados curinga

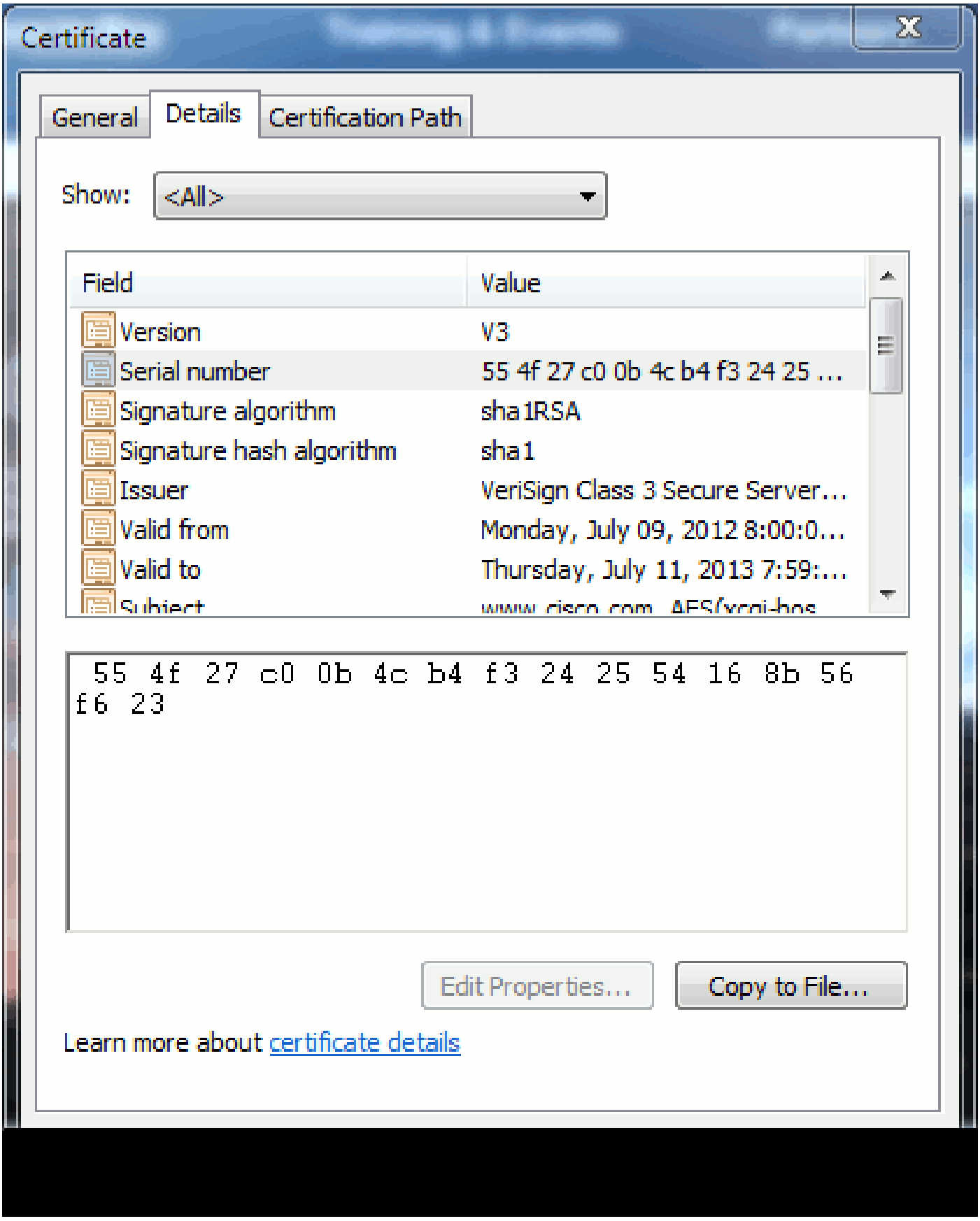
Os certificados curinga são certificados que usam um asterisco (*) para representar qualquer string em uma seção de um URL. Por exemplo, para ter um certificado para www.cisco.com, ftp.cisco.com, ssh.cisco.com e assim por diante, um administrador só precisaria criar um certificado para *.cisco.com. Para economizar dinheiro, o administrador só precisa comprar um único certificado e não precisa comprar vários certificados.

Este recurso não é suportado atualmente pelo Cisco Unified Communications Manager (CUCM). No entanto, você pode acompanhar esse aprimoramento: CSCta14114: Solicitação de suporte de certificado curinga no CUCM e importação de chave privada.

Identificar os certificados

Quando os certificados tiverem as mesmas informações, você poderá ver se é o mesmo certificado. Todos os certificados têm um número de série exclusivo. Você pode usar isso para comparar se os certificados são os mesmos, gerados novamente ou falsificados. A Figura 9 fornece um exemplo:

Figura 9: Número de série do certificado



CSRs e seu objetivo

CSR significa Certificate Signing Request (Solicitação de assinatura de certificado). Se quiser criar um certificado de terceiros para um servidor CUCM, você precisará de um CSR para

apresentar à CA. Esse CSR se parece muito com um certificado PEM (ASCII).

Observação: este não é um certificado e não pode ser usado como um.

\

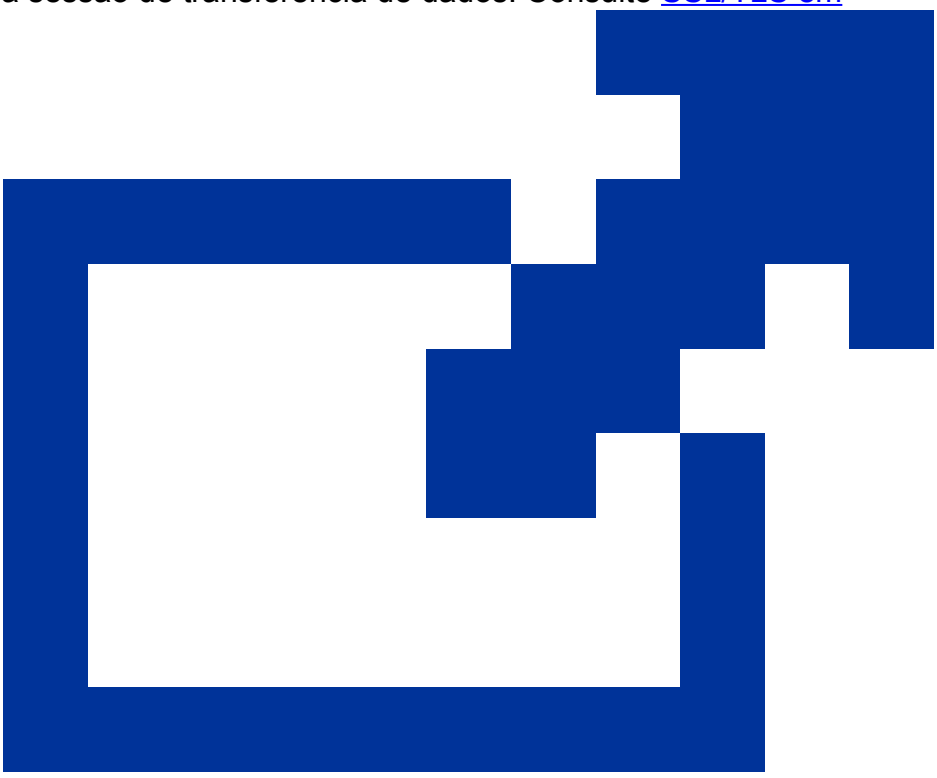
O CUCM cria CSRs automaticamente por meio da GUI da Web: Cisco Unified Operating System Administration > Security > Certificate Management > Gerar CSR, escolha o serviço que você deseja criar o certificado snf e Gerar CSR. Toda vez que essa opção é usada, uma nova chave privada e CSR são geradas.

Observação: uma chave privada é um arquivo exclusivo para este servidor e serviço. Isso nunca deve ser dado a ninguém! Se você fornecer uma chave privada a alguém, isso comprometerá a segurança fornecida pelo certificado. Além disso, não gere novamente um novo CSR para o mesmo serviço se você usar o CSR antigo para criar um certificado. O CUCM exclui o CSR antigo e a chave privada e substitui ambos, o que torna o CSR antigo inútil.

Consulte a documentação de Jason Burn na Comunidade de suporte: CUCM Uploading CCMAdmin Web GUI Certificates para obter informações sobre como criar CSRs.

Uso de certificados entre o ponto final e o processo de handshake SSL/TLS

O protocolo de handshake é uma série de mensagens sequenciadas que negociam os parâmetros de segurança de uma sessão de transferência de dados. Consulte SSL/TLS em



Detalhes

, que documenta a sequência de mensagens no protocolo de handshake. Eles podem ser vistos na captura de pacotes (PCAP). Os detalhes incluem as mensagens iniciais, subsequentes e finais enviadas e recebidas entre o cliente e o servidor.

Como o CUCM usa certificados

A diferença entre tomcat e tomcat-trust

Quando os certificados são carregados no CUCM, há duas opções para cada serviço via Cisco Unified Operating System Administration > Security > Certificate Management > Find.

Os cinco serviços que permitem gerenciar certificados no CUCM são:

- tomcat
- ipsec
- callmanager
- capf
- tvs (no CUCM versão 8.0 e posterior)

Estes são os serviços que permitem que você carregue certificados para o CUCM:

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

Estes são os serviços disponíveis no CUCM Versão 8.0 e posterior:

- tvs
- tvs-trust
- phone-trust
- phone-vpn-trust

- phone-sast-trust
- phone-ctl-trust

Consulte os Guias de segurança do CUCM por versão para obter mais detalhes sobre esses tipos de certificados. Esta seção explica apenas a diferença entre um certificado de serviço e um certificado confiável.

Por exemplo, com tomcat, o tomcat-trusts carrega a CA e os certificados intermediários de modo que este nó do CUCM saiba que pode confiar em qualquer certificado assinado pela CA e pelo servidor intermediário. O certificado tomcat é o certificado apresentado pelo serviço tomcat neste servidor se um ponto de extremidade fizer uma solicitação HTTP a este servidor. Para permitir a apresentação de certificados de terceiros pelo tomcat, o nó do CUCM precisa saber que pode confiar no CA e no servidor intermediário. Portanto, é necessário carregar a CA e os certificados intermediários antes de carregar o certificado tomcat (serviço).

Consulte Jason Burn's CUCM Uploading CCMAdmin Web GUI Certificates na Comunidade de Suporte para obter informações que ajudarão você a entender como carregar certificados no CUCM.

Cada serviço tem seu próprio certificado de serviço e certificados confiáveis. Eles não trabalham um com o outro. Em outras palavras, uma CA e um certificado intermediário carregados como um serviço tomcat-trust não podem ser usados pelo serviço CallManager.

Observação: os certificados no CUCM são baseados em nó. Portanto, se você precisar que os certificados sejam carregados no editor e que os assinantes tenham os mesmos certificados, será necessário carregá-los em cada servidor e nó individual antes do CUCM Versão 8.5. No CUCM versão 8.5 e posterior, há um serviço que replica certificados carregados para o restante dos nós no cluster.

Observação: cada nó tem um CN diferente. Portanto, um CSR deve ser criado por cada nó para que o serviço apresente seus próprios certificados.

Se você tiver mais perguntas específicas sobre qualquer um dos recursos de segurança do CUCM, consulte a documentação de segurança.

Conclusão

Este documento auxilia e constrói um alto nível de conhecimento sobre certificados. Este assunto pode ser importante e pode ser mais aprofundado, mas este documento o familiariza o suficiente para trabalhar com certificados. Se você tiver dúvidas sobre qualquer recurso de segurança do CUCM, consulte os Guias de segurança do CUCM por versão para obter mais informações.

Informações Relacionadas

- Guias de manutenção e segurança do Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- Comunidade de suporte da Cisco: CUCM fazendo upload de certificados de interface gráfica do usuário da Web CCMAdmin
- Bug CSCta14114: Solicitação de suporte de certificado curinga no CUCM e importação de chave privada
- Cisco Emergency Responder (CER) Explicado
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.