

# Visão de alto nível de certificados e autoridades no CUCM

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Finalidade dos certificados](#)

[Definir confiança do ponto de vista de um certificado](#)

[Como os navegadores usam certificados](#)

[As diferenças entre os certificados PEM e DER](#)

[Hierarquia de certificado](#)

[Certificados autoassinados versus certificados de terceiros](#)

[Nomes comuns e nomes alternativos do assunto](#)

[Certificados de curinga](#)

[Identificar os certificados](#)

[CSRs e suas finalidades](#)

[Uso de certificados entre o ponto final e o processo de handshake SSL/TLS](#)

[Como o CUCM usa certificados](#)

[A diferença entre tomcat e tomcat-trust](#)

[Conclusão](#)

[Informações Relacionadas](#)

## [Introduction](#)

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

## [Prerequisites](#)

## [Requirements](#)

Não existem requisitos específicos para este documento.

## [Componentes Utilizados](#)

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

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.

## 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 terminais para criar uma 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.

### Definir confiança do ponto de vista de um certificado

A parte mais importante dos certificados é a definição de quais endpoints podem ser confiáveis por seu endpoint. Este documento o ajuda 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(s) certificado(s) pré-instalado(s) no sistema que afirma que ele está 100% confiante em compartilhar informações com o ponto final correto. Caso contrário, ela encerra a comunicação entre esses terminais.


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

### Como os navegadores usam certificados

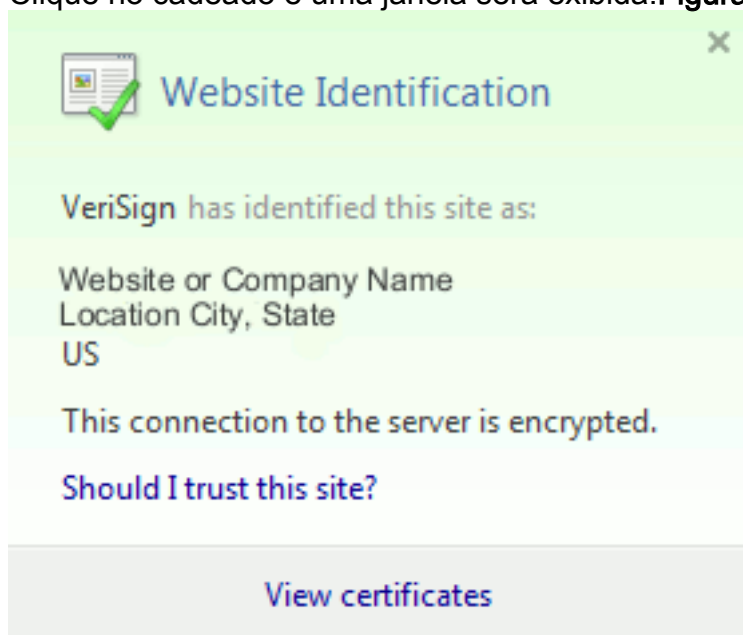
1. Ao visitar um site, digite o URL, como `http://www.cisco.com`.
2. O DNS encontra o endereço IP do servidor que hospeda esse site.
3. O navegador navega para esse site.

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 direcionado de forma correta e segura para o site desejado, como seu site do banco, onde as informações pessoais ou confidenciais que você digitar são seguras.

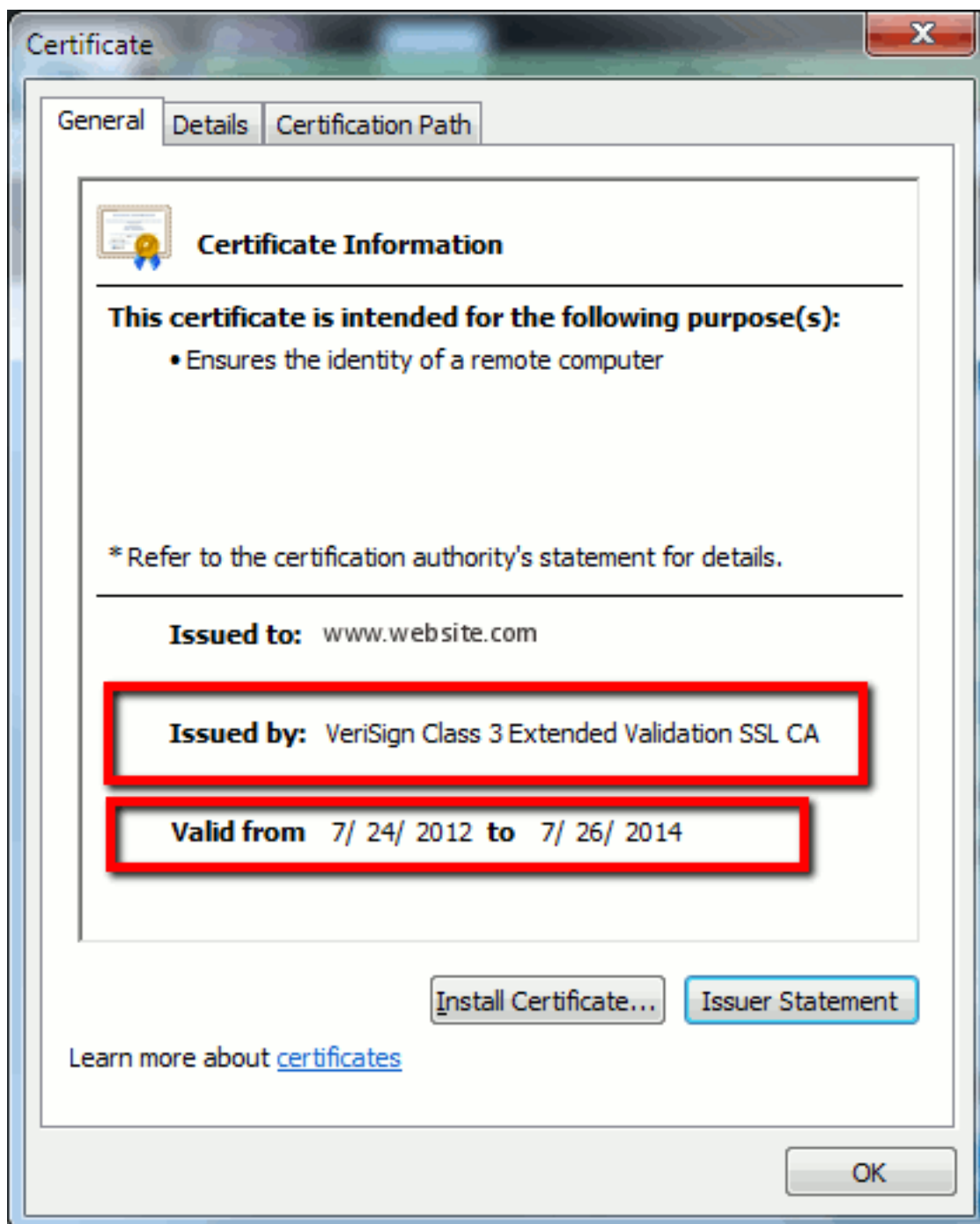
Todos os navegadores têm ícones diferentes que usam, mas normalmente você vê um cadeado

na barra de endereços como este:  Identified by VeriSign

1. Clique no cadeado e uma janela será exibida: **Figura 1: Identificação do site**



2. Clique em **Exibir certificados** 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/para** é o intervalo de datas 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 ou não.) **Dica:** Uma prática recomendada é criar um lembrete em seu calendário para renovar o certificado antes que ele expire. Isso evita problemas futuros.

## [As diferenças entre os 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



Figura 5: Informações do certificado

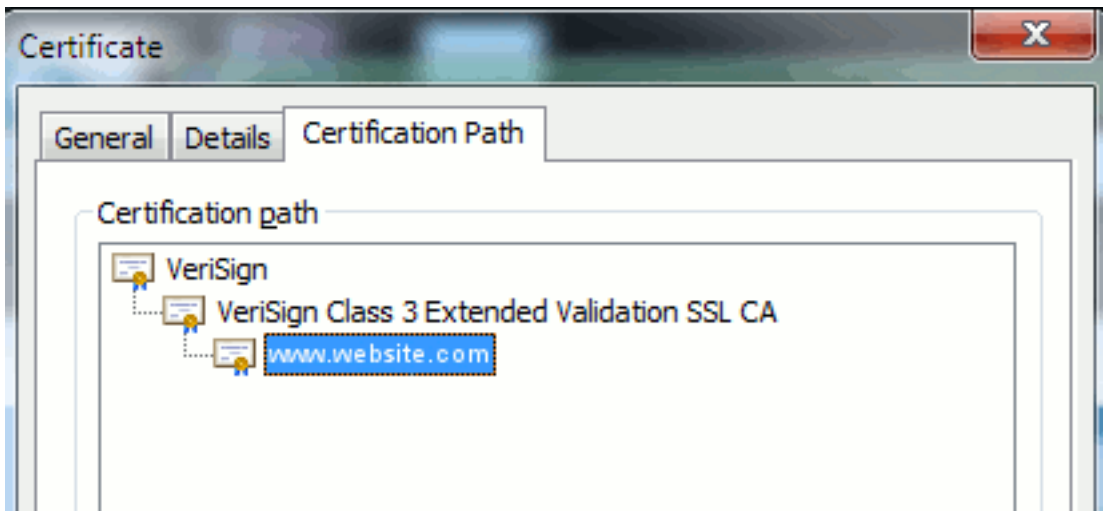


Em alguns casos, um dispositivo exige um formato específico (ASCII ou binário). Para alterar isso, baixe o certificado da CA no formato necessário ou use uma ferramenta conversora SSL, como <https://www.sslshopper.com/ssl-converter.html>.

## [Hierarquia de certificado](#)

Para confiar em um certificado de um ponto final, 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 certificado



- Verisign é uma CA.
- Verificando que a AC SSL de Validação Estendida de Classe 3 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 primeiro na CA e nos certificados intermediários antes de saber que pode confiar no certificado do servidor apresentado pelo Handshake SSL (detalhes abaixo). Para entender melhor como essa confiança funciona, consulte a seção neste documento: **Definir "Confiança" do ponto de vista de um certificado.**

## [Certificados autoassinados versus certificados de terceiros](#)

As principais diferenças entre certificados autoassinados e de terceiros são quem assinou o certificado, independentemente de você confiar neles.

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

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

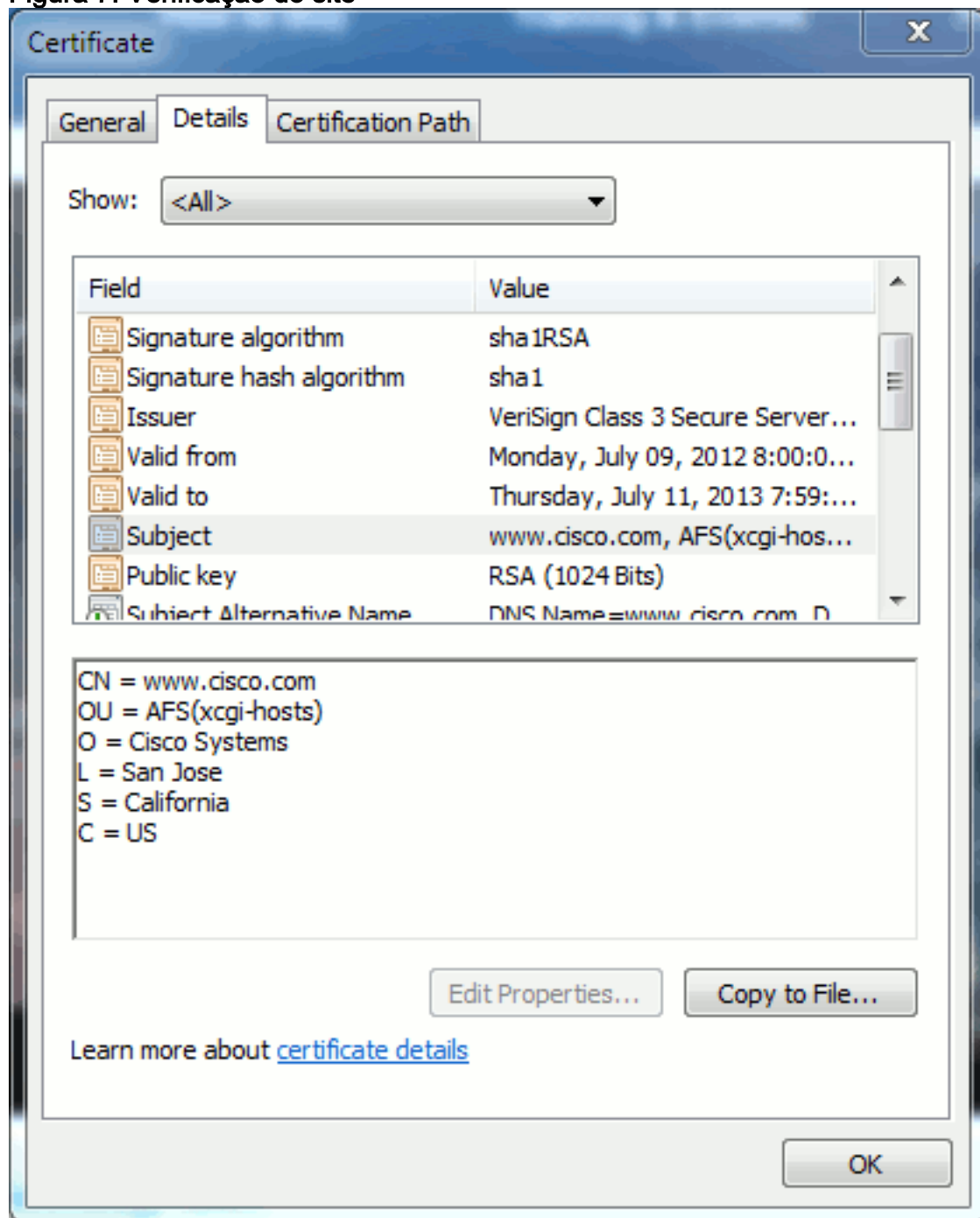
Cada um pode ser um CA. Se o seu sistema confia ou não na CA, é o que mais importa.

## [Nomes comuns e nomes alternativos do assunto](#)

Nomes comuns (CN) e nomes alternativos do assunto (SAN) são referências ao endereço IP ou ao 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 deve 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 URL FQDN 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 como o site correto e as comunicações agora são criptografadas entre o desktop e o site.

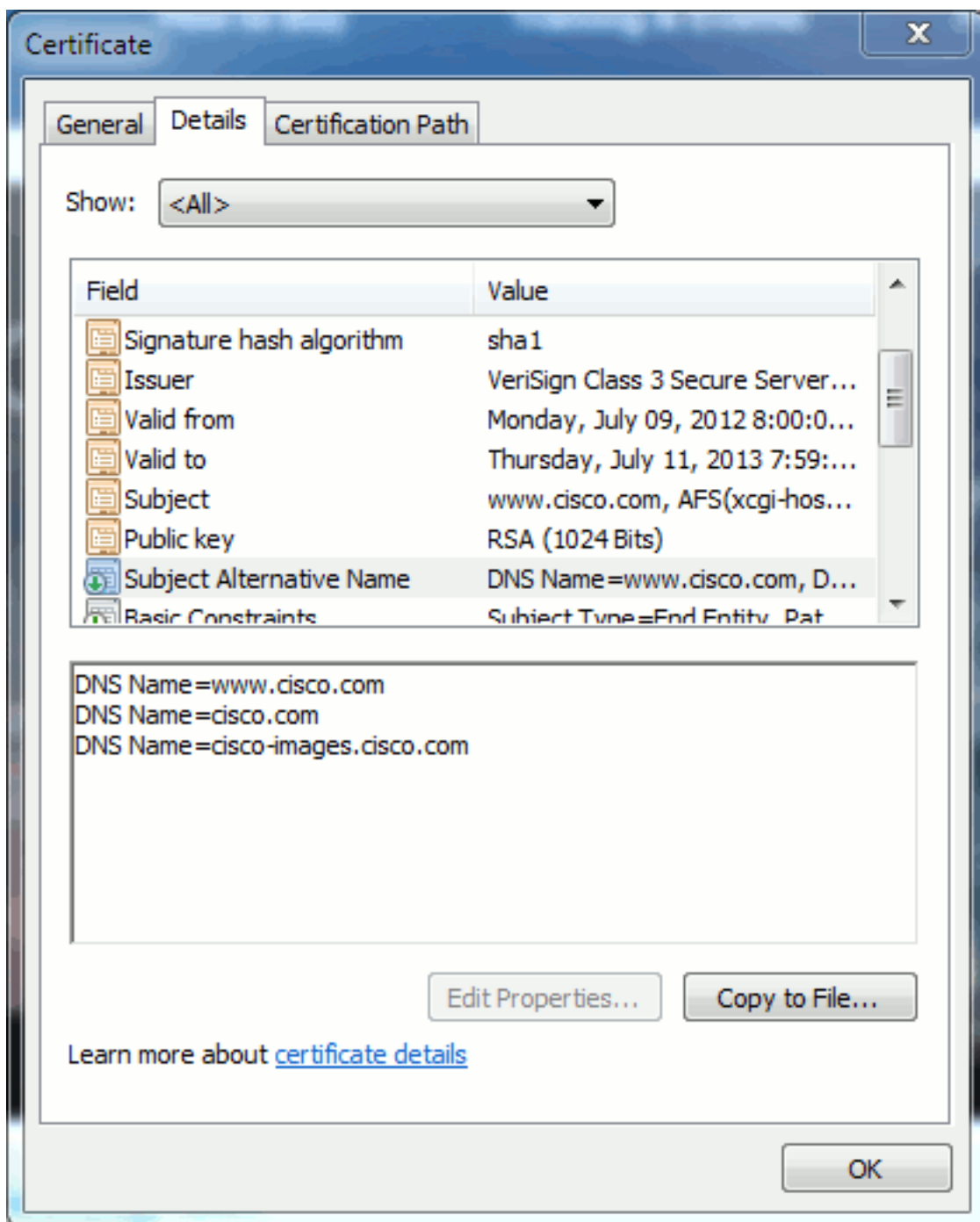
Figura 7: Verificação do site



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

Figura 8: Cabeçalho SAN





Este certificado pode autenticar/verificar [www.cisco.com](http://www.cisco.com) (também definido na CN), [cisco.com](http://cisco.com) e [cisco-images.cisco.com](http://cisco-images.cisco.com). Isso significa que você também pode digitar [cisco.com](http://cisco.com), e esse mesmo certificado pode ser usado para autenticar e criptografar este site.

O CUCM pode criar cabeçalhos de SAN. Consulte o documento de Jason Burn, [CUCM Uploading CCMAdmin Web GUI Certifications](#) na Comunidade de Suporte para obter mais informações sobre cabeçalhos de SAN.

## [Certificados de curinga](#)

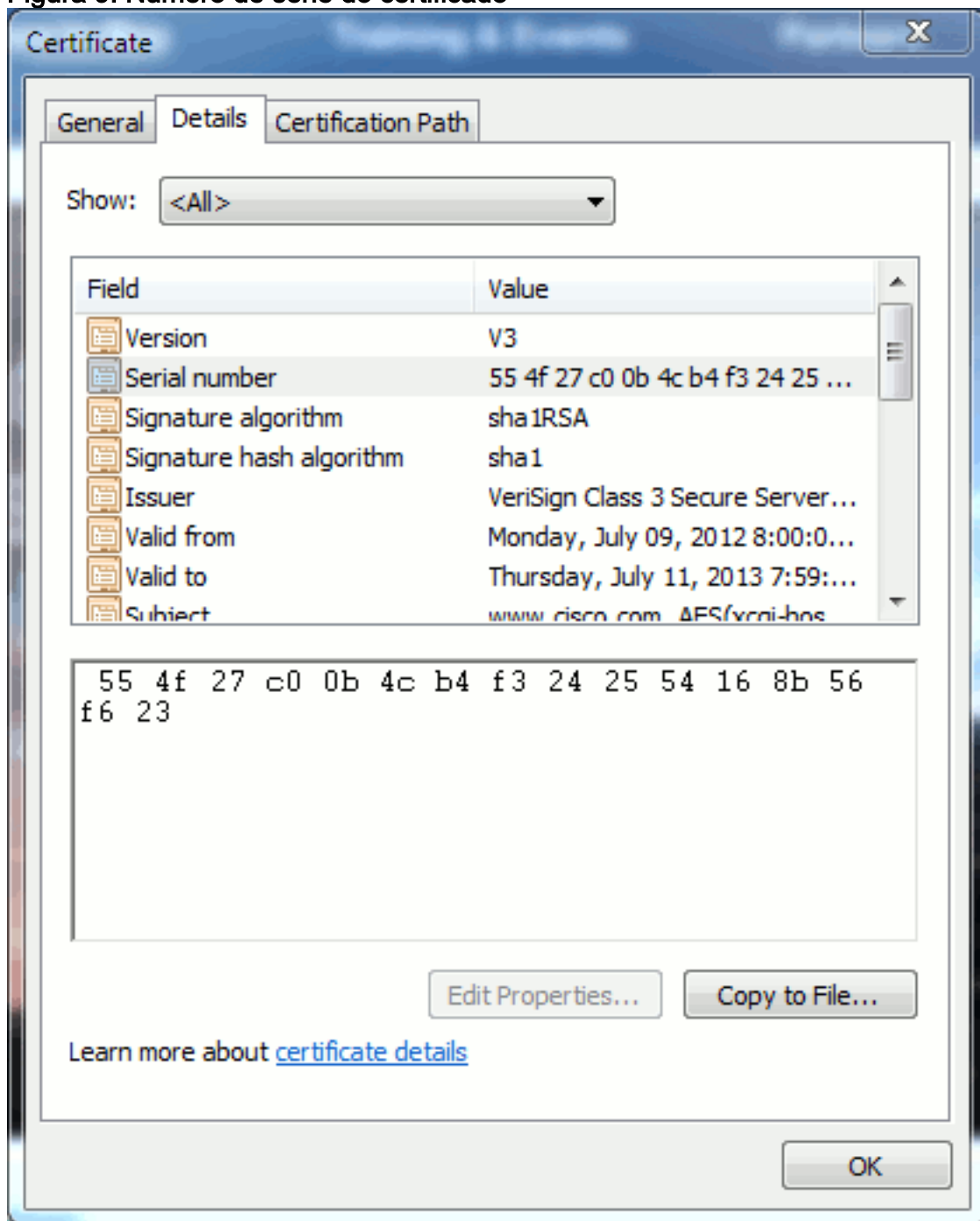
Certificados curinga são certificados que usam um asterisco (\*) para representar qualquer string em uma seção de um URL. Por exemplo, para ter um certificado para [www.cisco.com](http://www.cisco.com), [ftp.cisco.com](http://ftp.cisco.com), [ssh.cisco.com](http://ssh.cisco.com) e assim por diante, um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

Este recurso não é suportado atualmente pelo Cisco Unified Communications Manager (CUCM). Entretanto, você pode acompanhar essa melhoria: [CSCta14114: Solicitação de suporte para certificado curinga no CUCM e importação de chave privada](#).

## Identificar os certificados

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

Figura 9: Número de série do certificado



## CSRs e suas finalidades

CSR significa Certificate Signing Request (Solicitação de assinatura de certificado). Para criar um

certificado de terceiros para um servidor CUCM, você precisa de um CSR para apresentar à CA. Este CSR se parece muito com um certificado PEM (ASCII).

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

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

**Observação:** uma chave privada é um arquivo exclusivo deste servidor e serviço. Isso nunca deve ser dado a ninguém! Se você fornecer uma chave privada a alguém, ela comprometerá a segurança fornecida pelo certificado. Além disso, não regenere 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 sobre a Comunidade de Suporte: CUCM Carregando certificados da Web CCMAAdmin](#) para obter informações sobre como criar CSRs.

## [Uso de certificados entre o ponto final e o processo de handshake SSL/TLS](#)

O protocolo handshake é uma série de mensagens sequenciadas que negociam os parâmetros de segurança de uma sessão de transferência de dados. Consulte [SSL/TLS em Detalhe](#) , que documenta a sequência de mensagens no protocolo de handshake. Eles podem ser vistos em uma captura de pacote (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 através do **Cisco Unified Operating System Administration > Security > Certificate Management > Find**.

Os cinco serviços que permitem que você **gerencie** 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 no CUCM:

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

- callmanager-trust
- capf
- capf-trust

Estes são os serviços disponíveis no CUCM versão 8.0 e posteriores:

- 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**, os **tomcat-trusts** carregam a CA e os certificados intermediários para que esse nó 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 final fizer uma solicitação HTTP para este servidor. Para permitir a apresentação de certificados de terceiros por tomcat, o nó CUCM precisa saber que pode confiar na CA e no servidor intermediário. Portanto, é necessário carregar a CA e os certificados intermediários antes que o certificado tomcat (serviço) seja carregado.

Consulte o [CUCM](#) de Jason Burn [Carregando certificados da Web CCMAdmin](#) na Comunidade de Suporte para obter informações que o ajudarão a entender como carregar certificados para o 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 de confiança tomcat não podem ser usados pelo serviço callmanager.

**Observação:** os certificados no CUCM são baseados em nó. Portanto, se você precisar de certificados carregados no editor e precisar 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 resto 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 dúvidas específicas adicionais sobre qualquer um dos recursos de segurança do CUCM, consulte a documentação de segurança.

## [Conclusão](#)

Este documento auxilia e cria um alto nível de conhecimento em certificados. Este assunto pode se aprofundar mais, mas este documento o familiariza o suficiente para trabalhar com certificados. Se tiver dúvidas sobre algum recurso de segurança do CUCM, consulte os [Guias de Segurança do CUCM por Versão](#) para obter mais informações.

## Informações Relacionadas

- [Guias de segurança e manutenção do Cisco Unified Communications Manager \(CallManager\)](#)
- [Cisco Unified Communications Manager \(CallManager\)](#)
- [Cisco Unified Communications Manager Express](#)
- [Comunidade de suporte técnico da Cisco: CUCM fazendo upload de certificados da Web CCMAAdmin](#)
- [Erro CSCta14114: Solicitação de suporte para certificado curinga no CUCM e importação de chave privada](#)
- [Explicação do Cisco Emergency Responder \(CER\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)