Visualização de alto nível dos Certificados e das autoridades em CUCM

Índice

Introdução

A finalidade deste documento é compreender os princípios dos Certificados e das autoridades de certificação. Este documento felicita outros documentos Cisco que referem toda a criptografia ou características de autenticação no gerente das comunicações unificadas de Cisco (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.

Convenções

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

Finalidade dos Certificados

Os Certificados são usados entre pontos finais para construir uma confiança/autenticação e uma criptografia dos dados. Isto confirma que os valores-limite se comunicam com o dispositivo pretendido e se têm a opção para cifrar os dados entre os dois valores-limite.

Defina a confiança do ponto de vista de um certificado

A maioria de parte importante de Certificados é a definição de que os pontos finais podem ser confiados por seu ponto final. Este documento ajuda-o a saber e assim por diante e definir seus dados são cifrados e compartilhados com o Web site pretendido, telefone, servidor FTP.

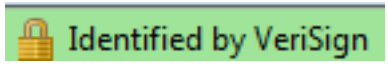
Quando seu sistema confia um certificado, este significa que há uns certificados instalados em seu sistema que indica que tem 100 por cento seguro que compartilha da informação com o ponto final correto. Se não, termina a comunicação entre estes pontos finais.

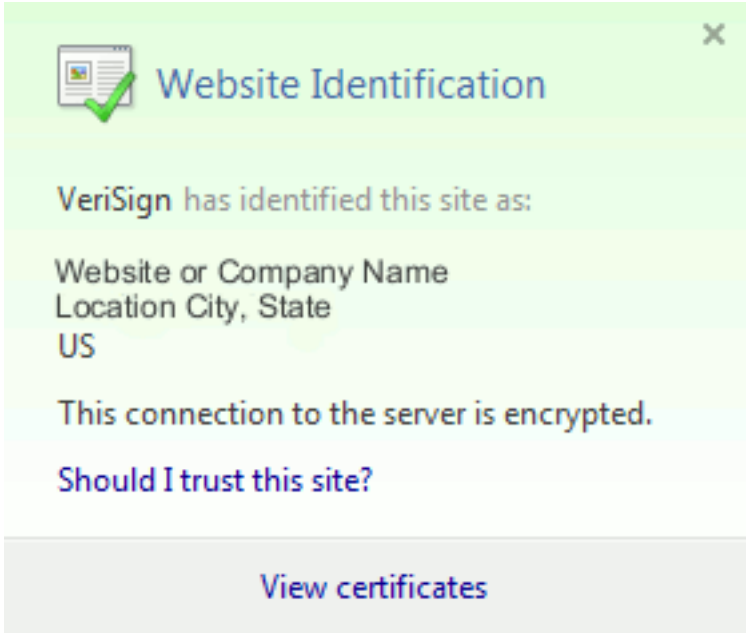
Um exemplo não técnico deste é sua licença de direcionador. Você usa esta licença (server/certificado do serviço) mostrar que você é quem você diz que você é; você obteve sua licença de sua divisão local do ramo dos veículos motorizados (certificado intermediário) que foi dado a permissão pela divisão dos veículos motorizados (DMV) de seu estado (Certificate Authority). Quando você precisa de mostrar sua licença (server/certificado do serviço) a um oficial, o oficial sabe que podem confiar o ramo DMV (certificado intermediário) e a divisão de veículos motorizados (Certificate Authority), e podem verificar que esta licença esteve emitida por eles (Certificate Authority). Sua identidade é verificada ao oficial e agora confiam que você é quem você diz que você é. Se não, se você dá uma licença falsa (server/certificado do serviço) que não seja assinada pelo DMV (certificado intermediário), a seguir não confiarão que quem você diz você é. O restante deste documento fornece uma explicação detalhada, técnica da hierarquia do certificado.

Como os navegadores usam Certificados

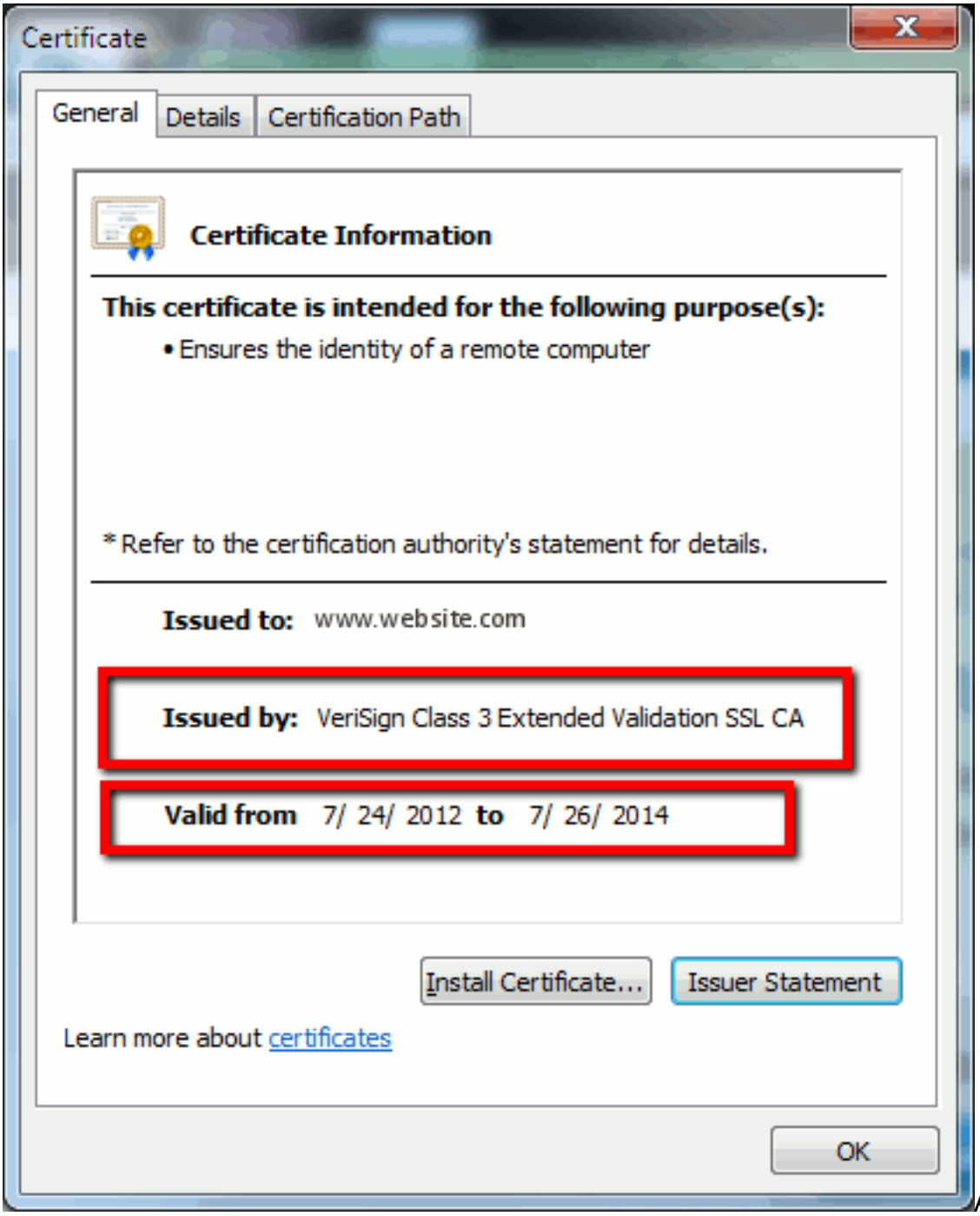
1. Quando você visita um Web site, incorpore a URL, tal como http://www.cisco.com.
2. O DNS encontra o endereço IP de Um ou Mais Servidores Cisco ICM NT do server que anfitrião esse local.
3. O navegador navega a esse local.

Sem Certificados, é impossível saber se um servidor DNS desonesto foi usado, ou se você foi distribuído a um outro server. Os Certificados asseguram-se de que você esteja distribuído corretamente e firmemente ao Web site pretendido, tal como seu Web site do banco, onde o pessoal ou a informação sensível que você incorpora são seguro.

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

1. Clique sobre os indicadores do cadeado e de um indicador:**Figura 1: Identificação do Web site**


2. Clique sobre **Certificados da vista** para ver o certificado do local segundo as indicações deste exemplo:**Figura 2: Informação do certificado, tab geral**



A informação destacada é importante.**São emitidos pela** empresa ou o Certificate Authority (CA) confianças desse suas sistema já.**Válida desde/até** é a escala da data que este certificado é útil. (Às vezes você vê um certificado onde você o conheça o confiança CA, mas vê que o certificado é inválido. Verifique sempre a data assim que você sabe mesmo se expirou.)**TIP**: Um melhor prática é criar um lembrete em seu calendário para renovar o certificado antes que expire. Isto impede as edições futuras.

As diferenças entre o PEM contra Certificados DER

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

Figura 3: Exemplo do certificado PEM

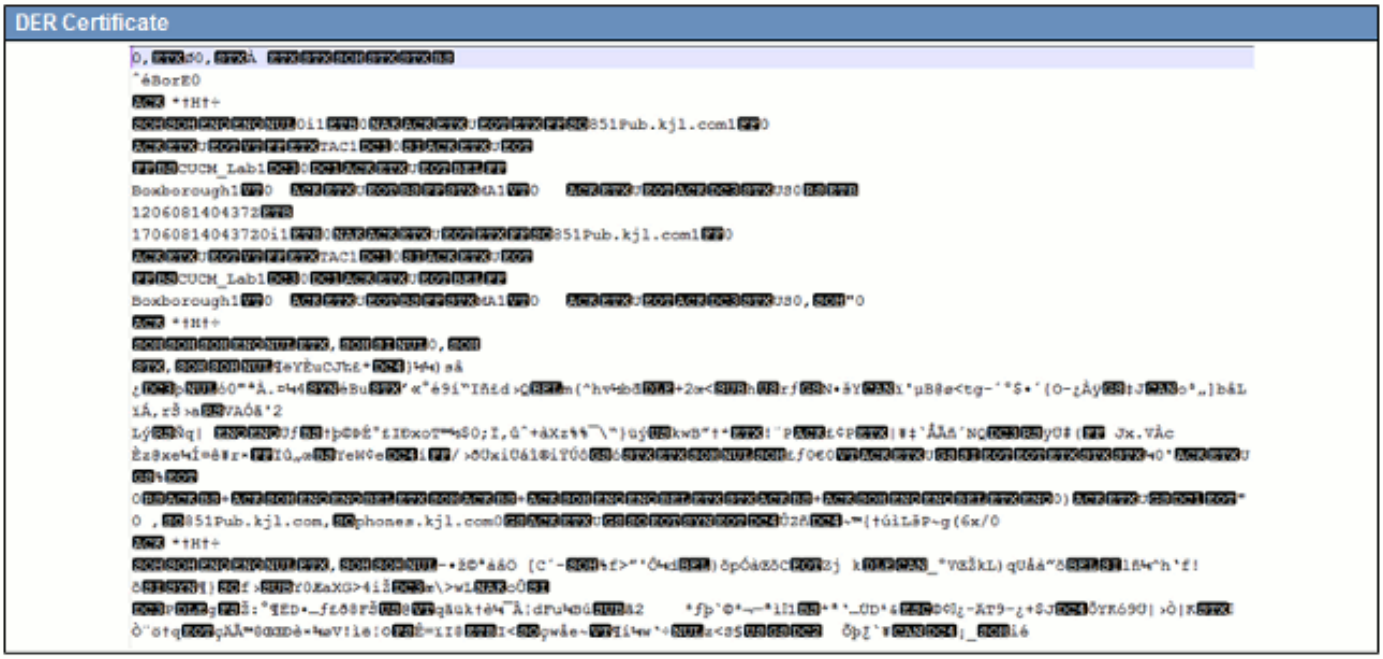
PEM Certificate

```
-----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
BQcDAgYIKwYBBQUHAwUwKQYDVR0RBCIwIIIODUxUHViLmtqbC5jb22CDnBob251
cy5ramwuY29tMB0GA1UdDgQWBBTbWvEUfpl7hvrsTJpQfmcoNpB4LzANBgkqhkiG
9w0BAQUFAAOCAQEArZWeqarg4tagW0O0rQElZj6UJ9S8ZAcp9XDT4Iz1QwRaaiBr
EBhfulaMjmtMKXFV5eCU9QcPbPG8XmiRZiEg9Q8Wtn0OZpuPGlkwxmFYRz40aY4T
5lw+d0wVb9sPChNQEGccjjqwtstElYWDo/A4RoqdH0ALceP8a4bovK/CpmRGdb5C
+hqP4zIJs4P+YKmzrJeq7H8xCCqqkYXcRLkmG6mif78txFQ5lr8rJEoU1VlL8znc
fJvSfEsCfwnSqPaGcQTnxMOZOIyM0OjXvvhWIezrpk8cyj3vSTgXSTwO53flZX4L
tu28d5H3AHo8U6cfHRIJ1f6Yv2ClGBShXwFp6Q==
-----END CERTIFICATE-----
```

Figura 4 mostra o certificado DER.

Figura 4: Exemplo do certificado DER

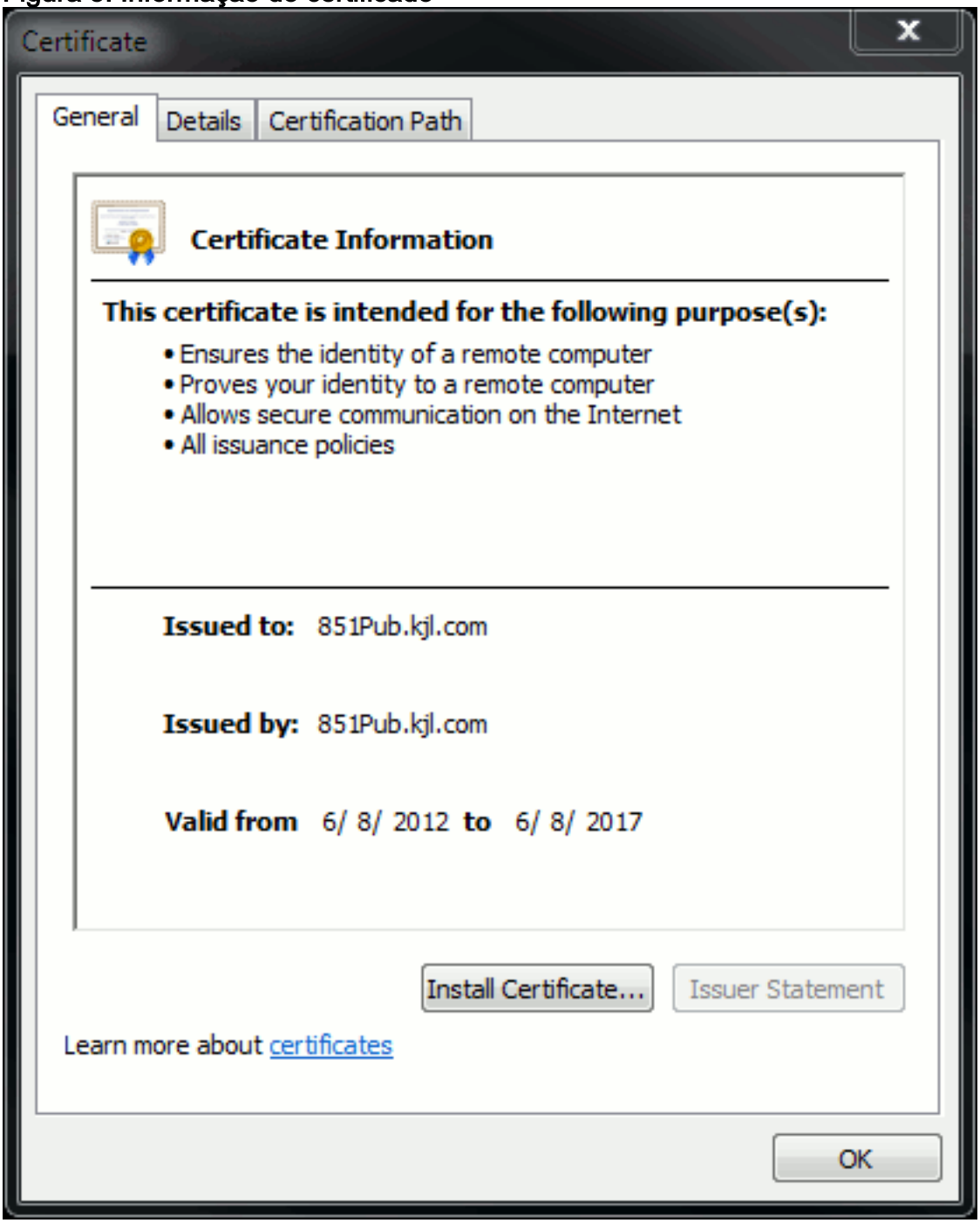
DER Certificate



A maioria de empresas de CA como formato do uso PEM de Verisign ou de Thawt para enviar os Certificados aos clientes, porque é email-amigável. O cliente deve copiar a corda inteira e inclui-la **-----COMECE O CERTIFICADO-----** e **-----CERTIFICADO DA EXTREMIDADE-----**, cole-o em um arquivo de texto, e salvar o com o .PEM da extensão ou o .CER.

Windows pode ler o DER e o CER formata com seu próprio applet do gerenciamento certificado e mostra o certificado segundo as indicações da figura 5.

Figura 5: Informação do certificado

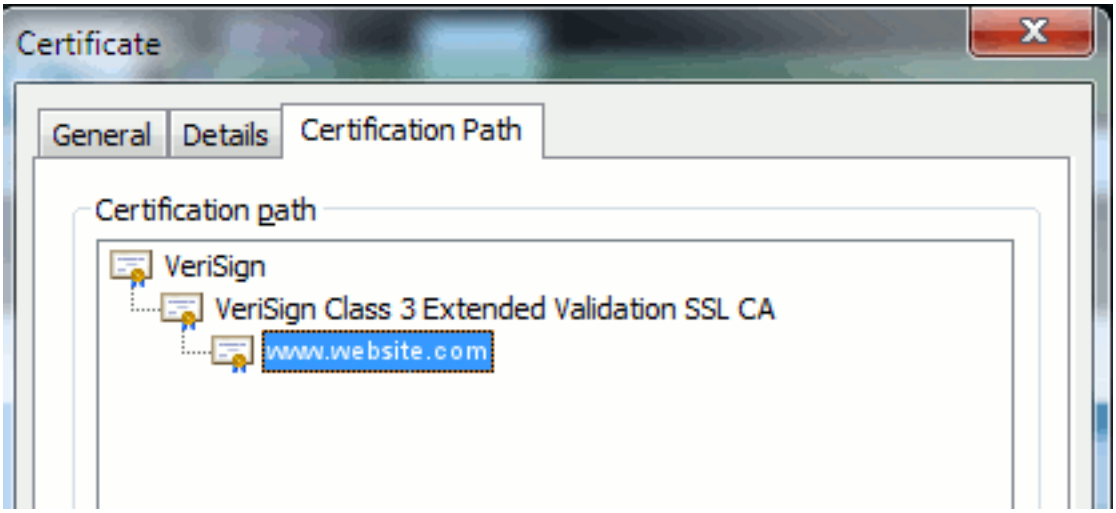


Em alguns casos, um dispositivo exige um formato específico (ASCII ou binário). A fim mudar isto, transfira o certificado de CA no formato necessário ou use uma ferramenta do conversor SSL, tal como https://www.sslshopper.com/ssl-converter.html.

Certificate a hierarquia

A fim confiar um certificado de um ponto final, deve haver uma confiança já estabelecida com uma terceira parte CA por exemplo, figura mostras 6 lá está uma hierarquia de três Certificados.

Figura 6: Hierarquia do certificado



- **Verisign** é CA.
- **A validação estendida SSL CA da classe 3 de Verisign** é um intermediário ou um certificado de servidor de assinatura (um server autorizado por CA para emitir Certificados em seu nome).
- **www.website.com** é um server ou um certificado do serviço.

Seu ponto final precisa de saber que pode confiar CA e Certificados intermediários primeiramente antes que saiba que pode confiar o certificado de servidor apresentado pela saudação de SSL (detalhes abaixo). Para compreender melhor como esta confiança trabalha, refira a seção neste documento: **Defina a "confiança" do ponto de vista de um certificado**.

Certificados auto-assinados contra Certificados da terceira

Os principais diferença entre Certificados auto-assinados e da terceira são quem assinados o certificado, se você os confia.

Um certificado auto-assinado é um certificado assinado pelo server que o apresenta; consequentemente, o server/certificado do serviço e o certificado de CA são o mesmo.

CA da terceira é um serviço proporcionado ou por CA público (como Verisign, confia, Digicert) ou um server (como Windows 2003, Linux, Unix, IO) esse controla a validez do server/certificado do serviço.

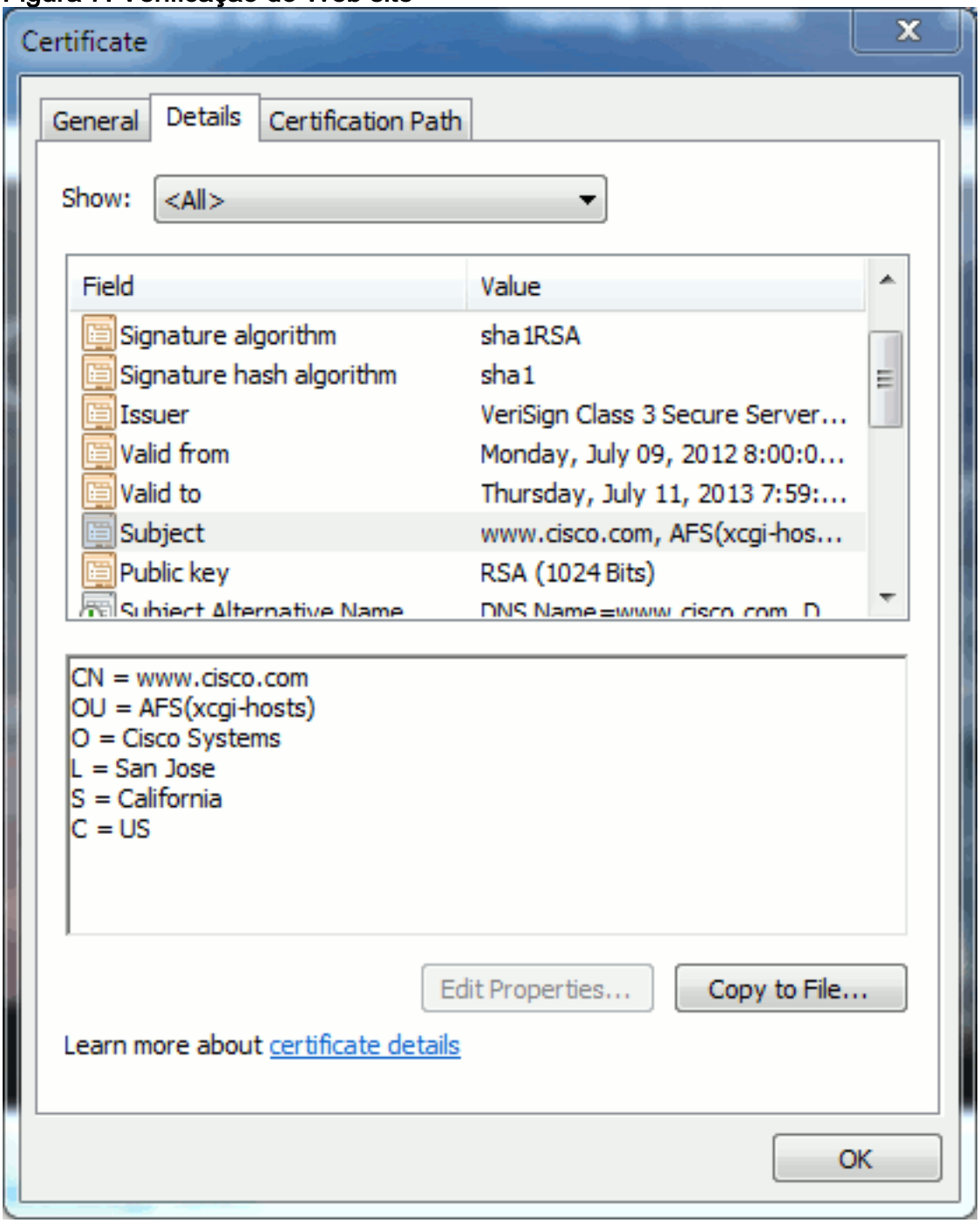
Cada um pode ser um CA mesmo se seu sistema confia esse CA, é o que importa mais.

Nomes comuns e nomes alternativos sujeitos

Os nomes comuns (CN) e os nomes alternativos sujeitos (SAN) são referências ao endereço IP de Um ou Mais Servidores Cisco ICM NT ou ao nome de domínio totalmente qualificado (FQDN) do endereço que é pedido. Por exemplo, se você entra em https://www.cisco.com, a seguir o CN ou o SAN devem ter www.cisco.com no encabeçamento.

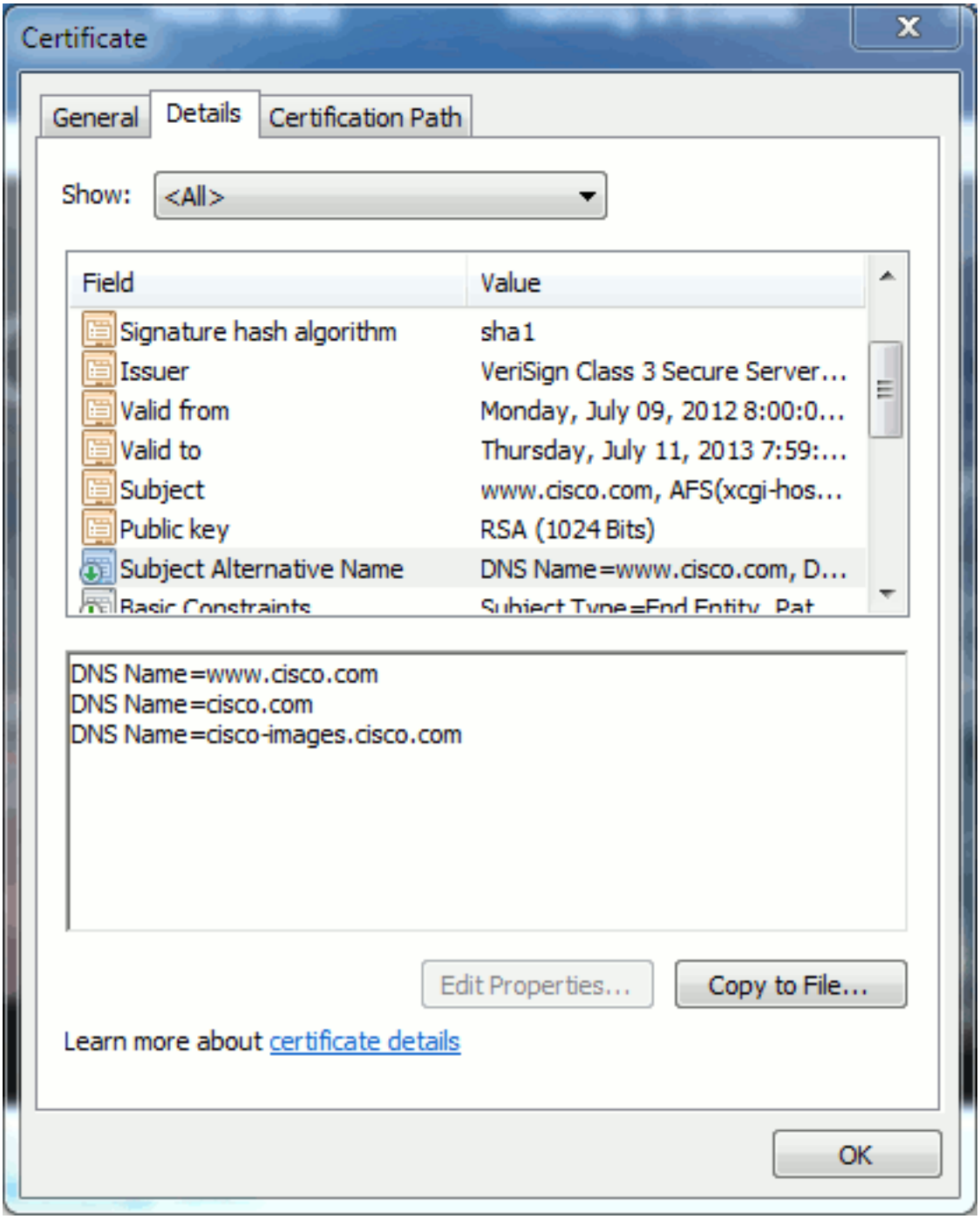
No exemplo mostrado na figura 7, o certificado tem o CN como www.cisco.com. O pedido URL para www.cisco.com do navegador verifica o FQDN URL contra a informação que o certificado apresenta. Neste caso, combinam, e mostra que a saudação de SSL é bem sucedida. Este Web site foi verificado para ser o Web site correto e as comunicações são cifradas agora entre o desktop e o Web site.

Figura 7: Verificação do Web site



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

Figura 8: Encabeçamento SAN



Este certificado pode autenticar/verifica www.cisco.com (igualmente definido no CN), cisco.com, e cisco-images.cisco.com. Isto significa que você pode igualmente datilografar cisco.com, e este mesmo certificado pode ser usado para autenticar e cifrar este Web site.

CUCM pode criar encabeçamentos SAN. Refira o documento da queimadura de Jason, Certificados transferindo arquivos pela rede da Web GUI do ccmadmin CUCM na comunidade do apoio para obter mais informações sobre dos encabeçamentos SAN.

Certificados da curinga

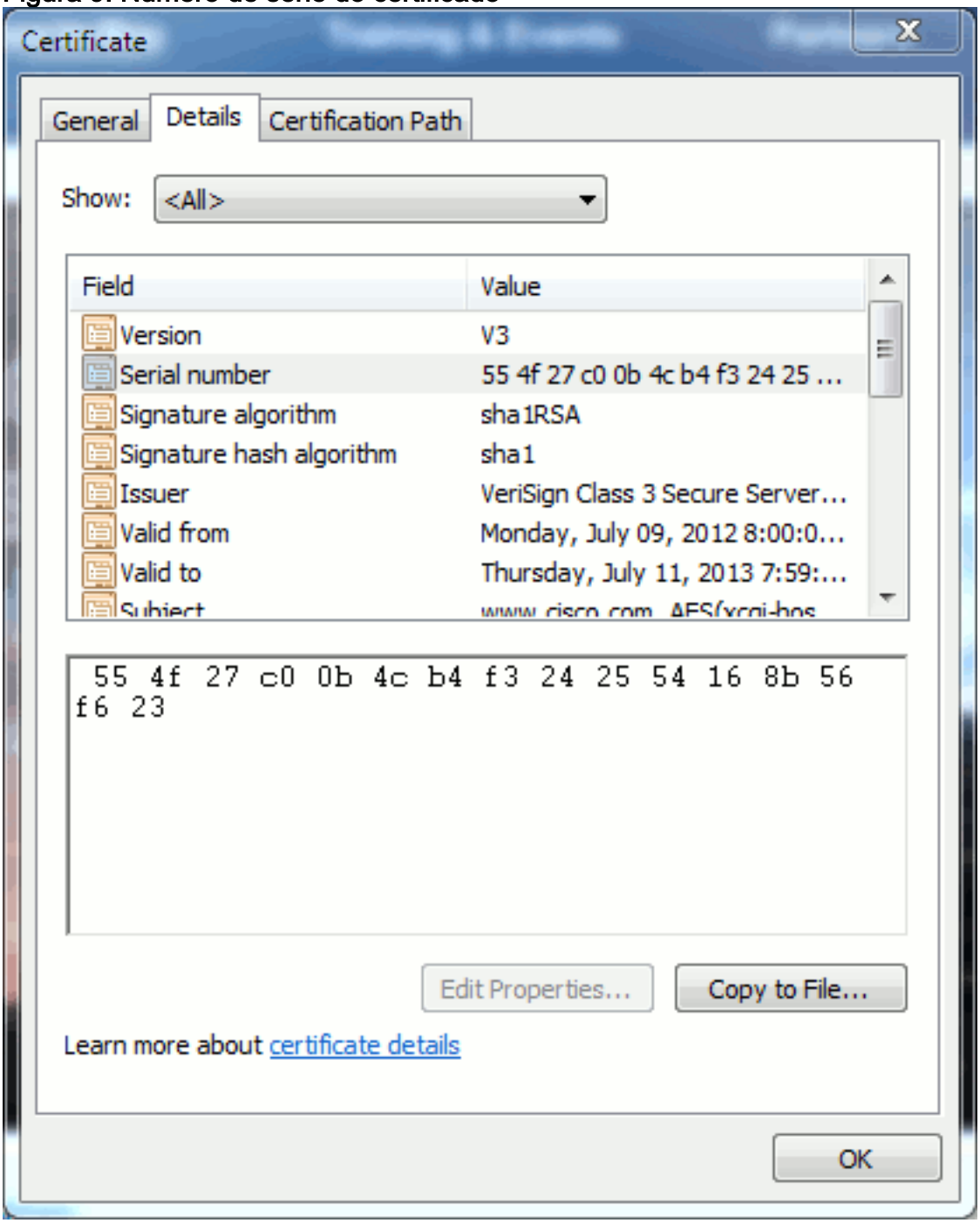
Os Certificados do convite são os Certificados que usam um asterisco (*) para representar toda a corda em uma seção de uma URL. Por exemplo, a fim ter um certificado para www.cisco.com, ftp.cisco.com, ssh.cisco.com, e assim por diante, um administrador precisaria somente de criar um certificado para *.cisco.com. A fim salvar o dinheiro, as necessidades do administrador somente de comprar um único certificado e não precisam de comprar certificados múltiplos.

Esta característica não é apoiada atualmente pelo gerente das comunicações unificadas de Cisco (CUCM). Contudo, você pode manter-se a par deste realce: CSCta14114: Pedido para o apoio do certificado do convite em CUCM e em importação da chave privada.

Identifique os Certificados

Quando os Certificados têm a mesma informação neles, você pode ver se é o mesmo certificado. Todos os Certificados têm um número de série original. Você pode usar este para comparar se os Certificados são os mesmos Certificados, regenerado, ou moeda falsa. A figura 9 fornece um exemplo:

Figura 9: Número de série do certificado



CSR e sua finalidade

O CSR representa a solicitação de assinatura de certificado. Se você quer criar um certificado da

terceira para um server CUCM, você precisa um CSR de apresentar a CA. Este CSR olha muito como um certificado PEM (ASCII).

Note: Este não é um certificado e não pode ser usado como um.

CUCM cria CSR automaticamente através da Web GUI: **Cisco unificou o >** gerenciamento de certificado do **>** segurança da **administração do sistema operacional > gerencie CSR >** escolhe o serviço que você quer criar o certificado **> gerencie** então o **CSR**. Cada vez que esta opção é usada, uma chave privada e um CSR novos estão gerados.

Note: Uma chave privada é um arquivo que seja original a estes server e serviço. Isto deve nunca ser dado a qualquer um! Se você fornece uma chave privada a alguém, compromete a Segurança que o certificado fornece. Também, não regenere um CSR novo para o mesmo serviço se você usa o CSR velho para criar um certificado. CUCM suprime do CSR e da chave privada velhos e substitui ambos eles, que faz o CSR velho inútil.

Refira a documentação da queimadura de Jason na comunidade do apoio: Certificados transferindo arquivos pela rede da Web GUI do ccmadmin CUCM para obter informações sobre de como criar CSR.

Uso dos Certificados entre o processo do ponto final e do aperto de mão SSL/TLS

O protocolo de handshake é uma série de mensagens arranjadas em sequência que negociam os parâmetros de segurança de uma sessão de transferência de dados. Refira o SSL/TLS em detalhe , que documenta a sequência de mensagem no protocolo de handshake. Estes podem ser vistos em uma captura de pacote de informação (PCAP). Os detalhes incluem a inicial, subsequente, e os mensagens finais enviados e recebidos entre o cliente e servidor.

Como CUCM usa Certificados

A diferença entre TomCat e a Tomcat-confiança

Quando os Certificados são transferidos arquivos pela rede a CUCM, há duas opções para cada serviço através de **Cisco unificou o >** gerenciamento de certificado **>** o **achado do >** segurança da **administração do sistema operacional**.

Os cinco serviços que permitem que você **controle** Certificados em CUCM são:

- TomCat
- IPsec
- callmanager
- capf
- tevês (na liberação 8.0 CUCM e mais atrasado)

Estão aqui os serviços que permitem que você **transfira arquivos pela rede** Certificados a CUCM:

- TomCat
- Tomcat-confiança
- IPsec

- IPsec-confiança
- callmanager
- CallManager-confiança
- capf
- CAPF-confiança

Estes são os serviços disponíveis na liberação 8.0 CUCM e mais atrasado:

- tevês
- TV-confiança
- telefone-confiança
- telefone-VPN-confiança
- telefone-SAST-confiança
- telefone-CTL-confiança

Refira os guias da Segurança CUCM pela liberação para mais detalhes nestes tipos de Certificados. Esta seção explica somente a diferença entre um certificado do serviço e um certificado de confiança.

Por exemplo, com **TomCat**, as Tomcat-**confianças** transferem arquivos pela rede CA e os Certificados intermediários de modo que este nó CUCM o conheça podem confiar todo o certificado assinado por CA e pelo server intermediário. O certificado de TomCat é o certificado que está apresentado pelo serviço de TomCat neste server, se um ponto final faz um pedido do HTTP a este server. A fim permitir a apresentação de Certificados da terceira por TomCat, o nó CUCM precisa de saber que pode confiar CA e o server intermediário. Consequentemente, é uma exigência transferir arquivos pela rede CA e os Certificados intermediários antes que o certificado de TomCat (serviço) esteja transferido arquivos pela rede.

Refira Certificados transferindo arquivos pela rede da Web GUI do ccmadmin CUCM da queimadura de Jason na comunidade do apoio para a informação que o ajudará a compreender como transferir arquivos pela rede Certificados a CUCM.

Cada serviço tem seus próprios certificado do serviço e Certificados de confiança. Não trabalham fora de se. Ou seja CA e um certificado intermediário transferidos arquivos pela rede como um serviço da Tomcat-confiança não podem ser usados pelo serviço do callmanager.

Note: Os Certificados em CUCM são a pela base de nó. Consequentemente, se você precisa os Certificados transferidos arquivos pela rede ao editor, e você precise os assinantes de ter os mesmos Certificados, você precisa de transferi-los arquivos pela rede a cada servidor individual e nó antes da liberação 8.5 CUCM. Em CUCM libere 8.5 e mais atrasado, há um serviço que replicates Certificados transferidos arquivos pela rede ao resto dos Nós no conjunto.

Note: Cada nó tem um CN diferente. Consequentemente, um CSR deve ser criado por cada nó para que o serviço apresente seus próprios Certificados.

Se você tem perguntas específicas adicionais em alguns dos recursos de segurança CUCM, refira a documentação da Segurança.

Conclusão

Este documento ajuda e constrói a um nível alto do conhecimento em Certificados. Este assunto pode importar pode tornar-se mais detalhado, mas este documento familiariza-o bastante para

trabalhar com Certificados. Se você tem perguntas em quaisquer recursos de segurança CUCM, refira os guias da Segurança CUCM pela liberação para mais informação.

Informações Relacionadas

- Guias da manutenção e da Segurança do Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- Cisco apoia a comunidade: Certificados transferindo arquivos pela rede da Web GUI do ccmadmin CUCM
- Erro CSCta14114: Pedido para o apoio do certificado do convite em CUCM e em importação da chave privada
- Cisco Emergency Responder (CER) explicado
- Suporte Técnico e Documentação - Cisco Systems