CUCM中的证书和颁发机构高级视图

目录

简介

本文档介绍证书和证书颁发机构的基本知识。它补充了引用Cisco Unified Communications Manager (CUCM)中的任何加密或身份验证功能的其他思科文档。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

证书的用途

证书在终端之间用于建立信任/验证和数据加密。这确认终端与预定设备通信，并且可以选择加密两个终端之间的数据。

注意：要了解每个证书的影响请参考“证书存储”部分的“Cisco Unified Communications Manager的证书重新生成过程”部分

从证书的角度定义信任

证书最重要的部分是定义哪些终端可受您的终端信任。本文档帮助您了解和定义如何加密您的数据，以及如何与目标网站、电话、FTP服务器等共享。

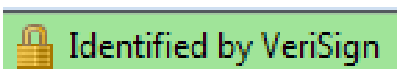
当您的系统信任证书时，这意味着您的系统中有一个预安装的证书，表明它100%确信它与正确的终端共享信息。否则，它将终止这些终端之间的通信。

非技术性的例子是您的驾驶执照。您使用此许可证（服务器/服务证书）来证明您是本人；您从您所在地的机动车部门分支机构（中间证书）处获得了许可证，该部门已经获得您所在州（证书颁发机构）机动车部门(DMV)的许可。当您需要将您的许可证（服务器/服务证书）显示给某个人员时，该人员知道他们可以信任DMV分支机构（中间证书）和机动车辆部门（证书颁发机构），并且他们可以验证此许可证是由他们颁发的（证书颁发机构）。您的身份已经得到警官的确认，现在他们相信您就是您所说的人。否则，如果您提供未由DMV（中间证书）签名的错误许可证（服务器/服务证书），则他们将不会信任您所说的人员。本文档的其余部分对证书层次结构提供了深入的技术说明。

浏览器如何使用证书

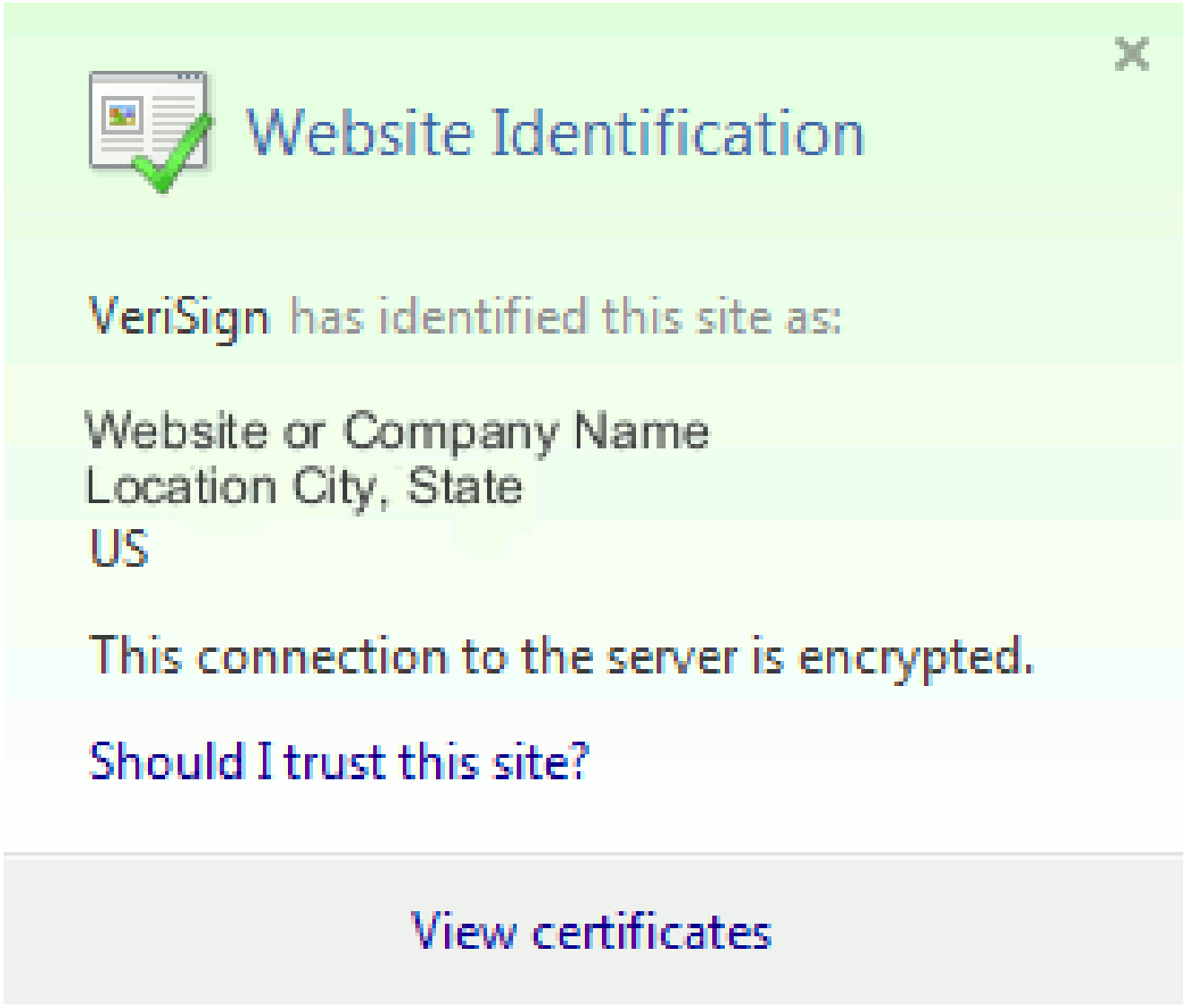
1. 当您访问网站时，请输入URL，例如http://www.cisco.com。
2. DNS会查找托管该站点的服务器的IP地址。
3. 浏览器导航至该站点。

如果没有证书，就不可能知道是否使用了非法DNS服务器，或者您是否路由到其他服务器。证书可确保您正确和安全地路由到目标网站（例如您的银行网站），您输入的个人或敏感信息在该网站是安全的。

所有浏览器都使用不同的图标，但通常您在地址栏中会看到如下挂锁： 

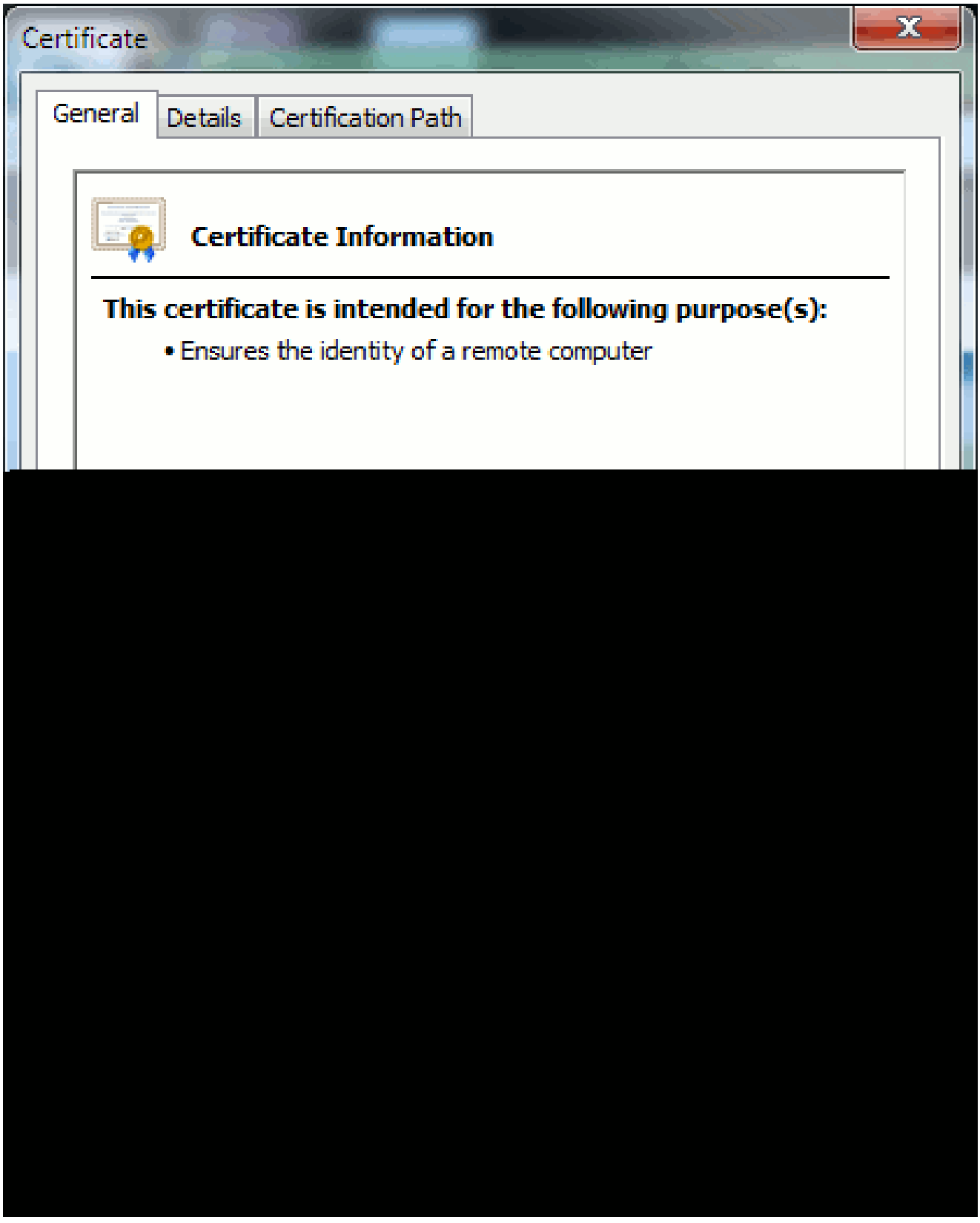
1. 单击挂锁将显示一个窗口：

   图1：网站标识



2. 单击View Certificates以查看站点证书，如下例所示：

图2： “Certificate Information”（证书信息）、“General”（常规）选项卡



突出显示的信息很重要。

- 颁发者是系统已信任的公司或证书颁发机构(CA)。
- Valid from/to是此证书可用的日期范围。(有时，您会看到一个您知道信任CA的证书，但您看到该证书无效。请始终检查日期，以便了解其是否已过期。)

提示：最佳做法是在您的日历中创建提醒，以便在证书过期之前进行续订。这样可以防止将来出现问题。

PEM证书与DER证书之间的区别

PEM是ASCII；DER是二进制的。图3显示了PEM证书格式。

图3：PEM证书示例

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-----
```

图4显示了DER证书。

图4： DER证书示例

大多数CA公司（如VeriSign或Thawt）使用PEM格式将证书发送给客户，因为它对电子邮件友好。客户应复制整个字符串并包括-----BEGIN CERTIFICATE—和-----END CERTIFICATE—，将其粘贴到文本文件中，然后使用扩展名.PEM或.CER将其保存。

Windows可使用其自己的证书管理小程序读取DER和CER格式，并显示证书，如图5所示。

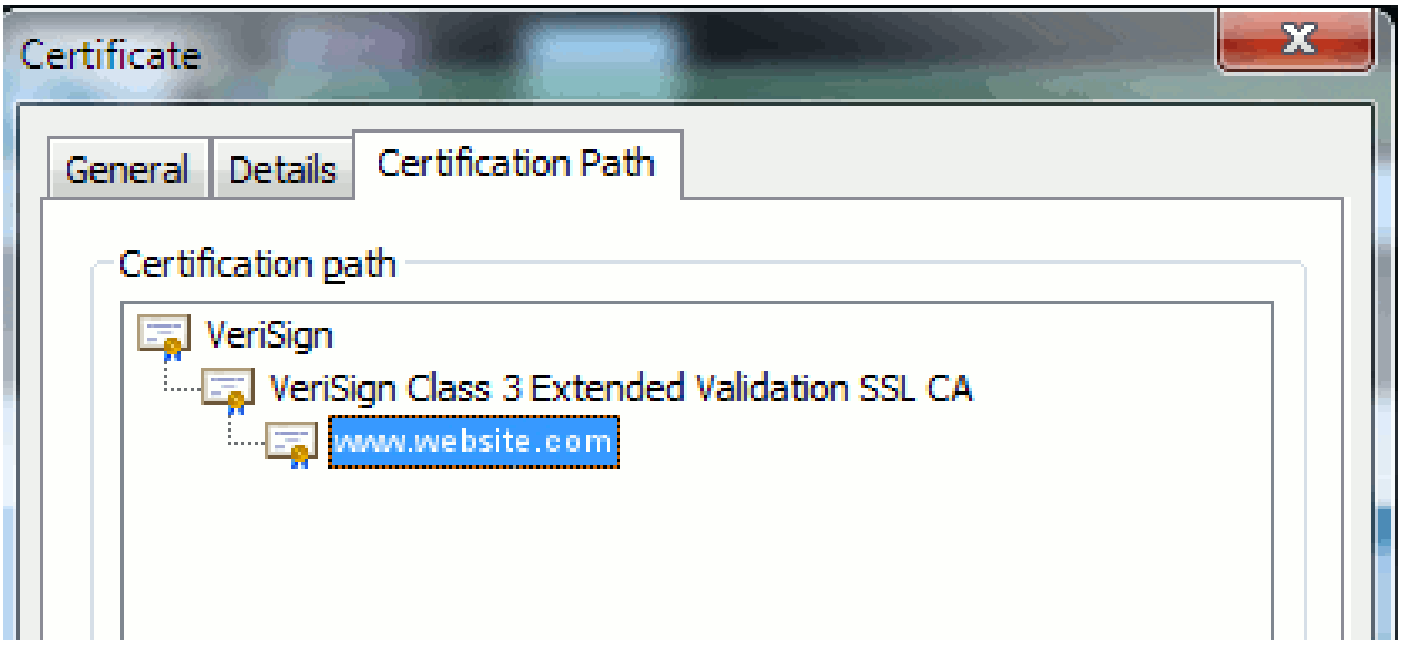
图5：证书信息

在某些情况下，设备需要特定格式（ASCII或二进制）。要更改此设置，请以所需格式从CA下载证书或使用SSL转换器工具，例如https://www.sslshopper.com/ssl-converter.html。

证书层次结构

要信任来自终端的证书，必须已经与第三方CA建立信任。例如，图6显示三个证书的层次结构。

图6：证书层次结构



- Verisign是一个CA。
- Verisign Class 3 Extended Validation SSL CA是中间或签名服务器证书（由CA授权以其名义签发证书的服务器）。
- www.website.com是服务器或服务证书。

您的终端需要知道它首先可以信任CA和中间证书，然后才能知道它可以信任SSL握手显示的服务器证书（详细信息如下）。要更好地了解此信任的工作原理，请参阅本文档中的部分：从证书的角度定义“信任”。

自签名证书与第三方证书

自签名证书和第三方证书之间的主要区别在于谁签署证书，以及您是否信任证书。

自签名证书是由提供自签名证书的服务器签名的证书；因此，服务器/服务证书和CA证书相同。

第三方CA是由公共CA（如Verisign、Entrust、Digicert）或控制服务器/服务证书有效性的服务器（如Windows 2003、Linux、Unix、IOS）提供的服务。

每个都可以是CA。您的系统是否信任CA是最重要的。

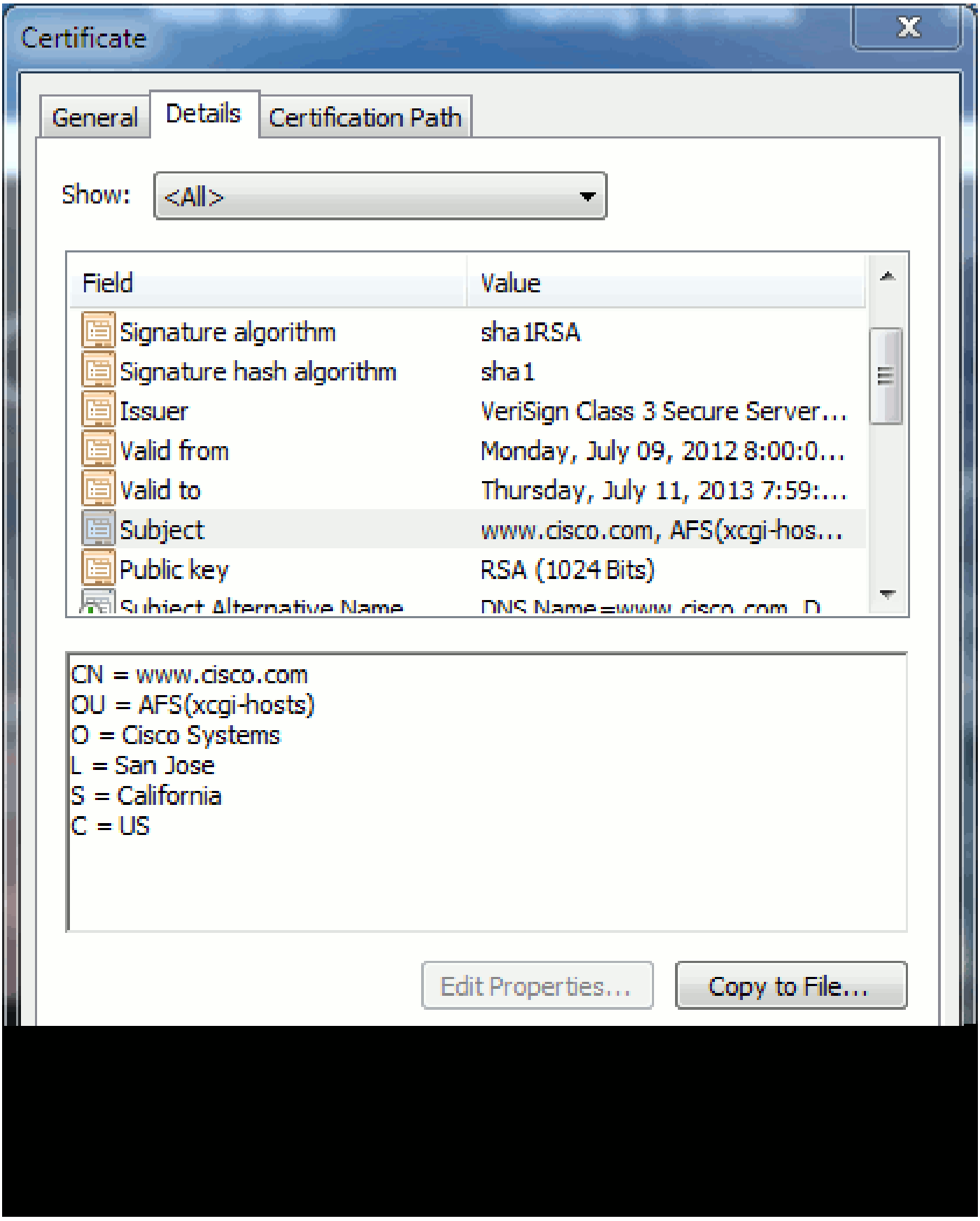
常用名称和主题备用名称

公用名(CN)和主题备用名(SAN)是指所请求地址的IP地址或完全限定域名(FQDN)。例如，如果您输

入https://www.cisco.com，则CN或SAN必须在报头中包含www.cisco.com。

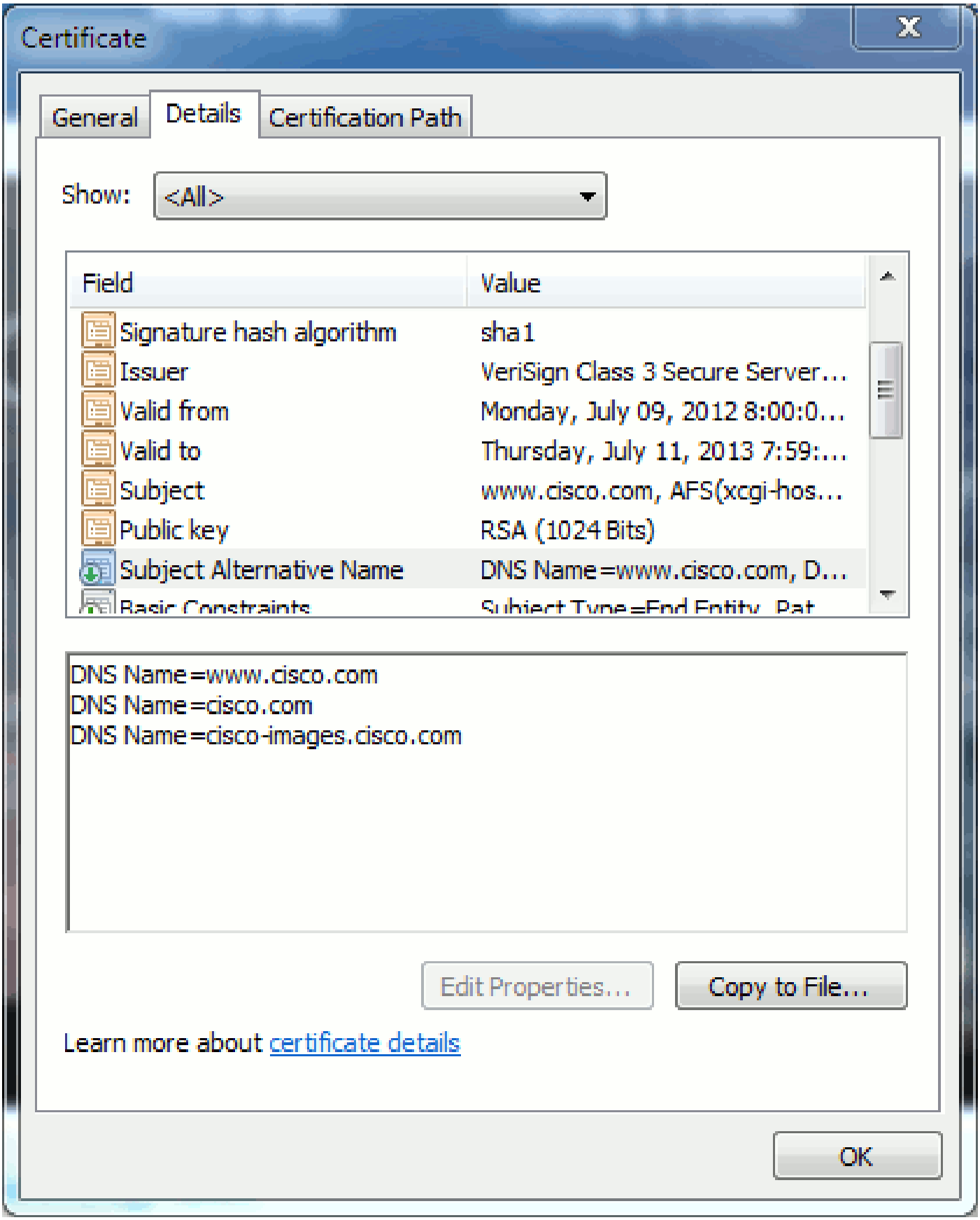
在图7所示的示例中，证书的CN是www.cisco.com。浏览器对www.cisco.com的URL请求会根据证书提供的信息检查URL FQDN。在本例中，它们匹配，并显示SSL握手成功。此网站已被验证为正确的网站，并且现在已加密桌面和网站之间的通信。

图7：网站验证



在同一证书中，有三个FQDN/DNS地址的SAN报头：

图8： SAN报头



此证书可以对以下内容进行身份验证/验证：www.cisco.com（在CN中也有定义）、cisco.com和cisco-images.cisco.com。这意味着您还可以键入cisco.com，并且此同一证书可用于验证和加密此网站。

CUCM可以创建SAN报头。有关SAN报头的详细信息，请参阅支持社区上的Jason Burn文档

CUCM上传CCMAdmin Web GUI证书。

通配符证书

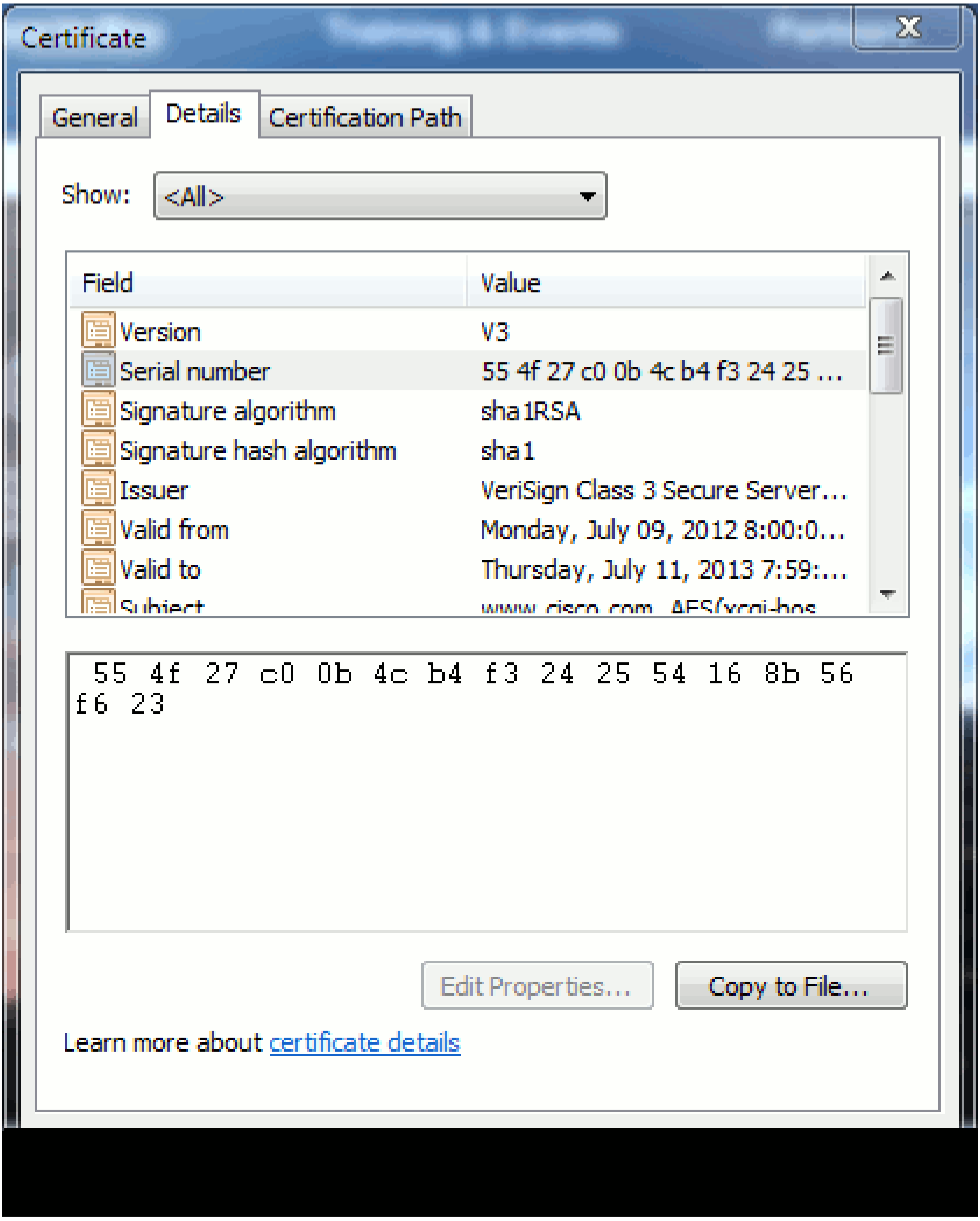
通配符证书是使用星号(*)表示URL部分中任何字符串的证书。例如，要拥有www.cisco.com、ftp.cisco.com、ssh.cisco.com等的证书，管理员只需为*.cisco.com创建证书。为了节省资金，管理员只需购买一个证书，无需购买多个证书。

Cisco Unified Communications Manager (CUCM)目前不支持此功能。不过，您可以跟踪此增强功能：CSCta14114：请求支持CUCM和私钥导入中的通配符证书。

识别证书

当证书中包含相同信息时，您可以看到它是否为同一证书。所有证书都有一个唯一的序列号。如果证书是相同的证书、重新生成的证书或假冒证书，您可以使用此选项进行比较。图 9 提供了一个示例：

图9：证书序列号



企业社会责任及其目的

CSR代表证书签名请求。如果您要为CUCM服务器创建第三方证书，则需要将CSR提供给CA。此CSR看起来很像PEM (ASCII)证书。

注意：这不是证书，不能用作证书。

\

CUCM通过Web GUI自动创建CSR：思科统一操作系统管理>安全>证书管理>生成CSR，选择您想要创建证书snf的服务，然后生成CSR。每次使用此选项时，都会生成新的私钥和CSR。

注意：私钥是此服务器和服务独有的文件。这个不应该给任何人！如果向他人提供私钥，则会破坏证书提供的安全性。此外，如果使用旧CSR创建证书，请勿为同一服务重新生成新的CSR。CUCM会删除旧CSR和私钥并替换两者，从而使旧CSR失去作用。

请参阅Jason Burn在支持社区：CUCM上传CCMAdmin Web GUI证书上的文档了解有关如何创建CSR的信息。

在终端和SSL/TLS握手过程之间使用证书

握手协议是一系列用于协商数据传输会话安全参数的序列消息。请参阅SSL/TLS详细信息，其中记录握手协议中的消息序列。数据包捕获(PCAP)中可看到这些信息。详细信息包括在客户端和服务器之间发送和接收的初始消息、后续消息和最终消息。

CUCM如何使用证书

Tomcat和Tomcat-trust之间的区别

证书上传到CUCM时，通过思科统一操作系统管理>安全>证书管理 >查找为每个服务提供了两个选项。

允许您在CUCM中管理证书的五种服务是：

- tomcat
- ipsec
- callmanager
- capf
- tvs（在CUCM版本8.0及更高版本中）

以下是允许您将证书上传到CUCM的服务：

- tomcat
- tomcat-trust
- ipsec

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

以下是CUCM版本8.0及更高版本中提供的服务：

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

有关这些类型的证书的详细信息，请参阅各版本的CUCM安全指南。本部分仅说明服务证书和信任证书之间的区别。

例如，使用tomcat，tomcat-trusts上传CA和中间证书，以便此CUCM节点知道它可信任由CA和中间服务器签名的任何证书。如果终端向此服务器发出HTTP请求，则tomcat证书是此服务器上tomcat服务提供的证书。为了允许通过tomcat显示第三方证书，CUCM节点需要知道它可以信任CA和中间服务器。因此，在上传tomcat（服务）证书之前，需要上传CA和中间证书。

有关可帮助您了解如何将证书上传到CUCM的信息，请参阅支持社区中的Jason Burn的CUCM上传CCMAdmin Web GUI证书。

每个服务都有自己的服务证书和信任证书。他们彼此之间无法相互协作。换句话说，作为tomcat-trust服务上传的CA和中间证书不能被CallManager服务使用。

注意：CUCM中的证书基于每个节点。因此，如果您需要将证书上传到发布者，并且您需要订用者拥有相同的证书，则需要将其上传到CUCM版本8.5之前的每台服务器和节点。在CUCM版本8.5及更高版本中，有一个服务可将上传的证书复制到集群中的其余节点。

注意：每个节点具有不同的CN。因此，每个节点必须创建CSR才能使服务呈现自己的证书。

如果您对任何CUCM安全功能有其他具体问题，请参阅安全文档。

结论

本文档帮助和建立有关证书的高级知识。此主题可能会更加深入，但本文档会让您足够熟悉证书的使用。如果您对任何CUCM安全功能存在问题，请参阅各版本的CUCM安全指南以获取详细信息。

相关信息

- Cisco Unified Communications Manager (CallManager)维护和安全指南
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- 思科支持社区：CUCM上传CCMAdmin Web GUI证书
- 漏洞CSCta14114：请求支持CUCM中的通配符证书和私钥导入
- Cisco Emergency Responder (CER)介绍
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。