CUCM中证书和授权的高级视图

目录

简介

本文档的目的是了解证书和证书颁发机构的基本知识。本文档补充了引用Cisco Unified Communications Manager(CUCM)中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。

证书用途

证书用于在终端之间建立信任/身份验证和数据加密。这确认了终端与预期设备通信，并且可以选择加密两个终端之间的数据。

从证书的角度定义信任

证书最重要的部分是定义哪些端点可以由端点信任。本文档帮助您了解并定义如何加密数据并与目标网站、电话、FTP服务器等共享数据。

当您的系统信任证书时，这意味着系统上有预安装的证书，表明它百分之百确信与正确的端点共享信息。否则，它会终止这些端点之间的通信。

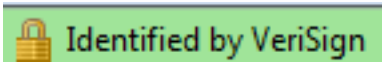
此示例的非技术性示例是您的驾照。您使用此许可证（服务器/服务证书）来证明您是您所说的自己；您从您所在地的机动车局（中级证书）处获得了您的许可证，该部门已获得您所在州（证书颁发机构）的机动车局(DMV)的许可。 当您需要向一名高级人员显示您的许可证（服务器/服务证书）时，该高级人员知道他们可以信任DMV分支机构（中间证书）和汽车部门（证书颁发机构），并且他们可以验证此许可证是由他们颁发的（证书颁发机构）。 你的身份已经向警官确认，现在他们相信你是你所说的。否则，如果您提供未由DMV（中间证书）签名的假许可证（服务器/服务证书），则他们将不信任您所说的您。本文档的其余部分提供证书层次结构的深入技术说明。

浏览器如何使用证书

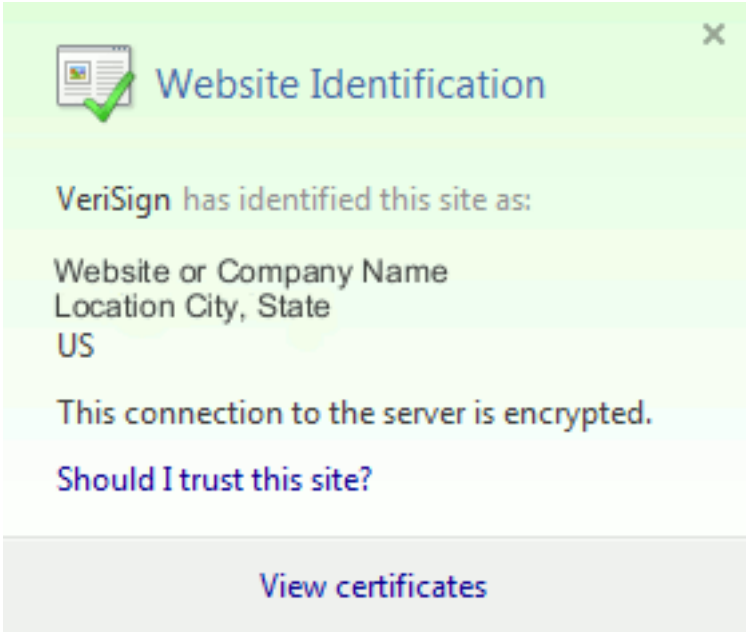
1. 访问网站时，请输入URL，例如http://www.cisco.com。
2. DNS会查找托管该站点的服务器的IP地址。
3. 浏览器导航到该站点。

如果没有证书，则无法知道是否使用了非法DNS服务器，或者您是否被路由到其他服务器。证书可确保您正确、安全地路由到您输入的个人信息或敏感信息安全的目标网站，如银行网站。

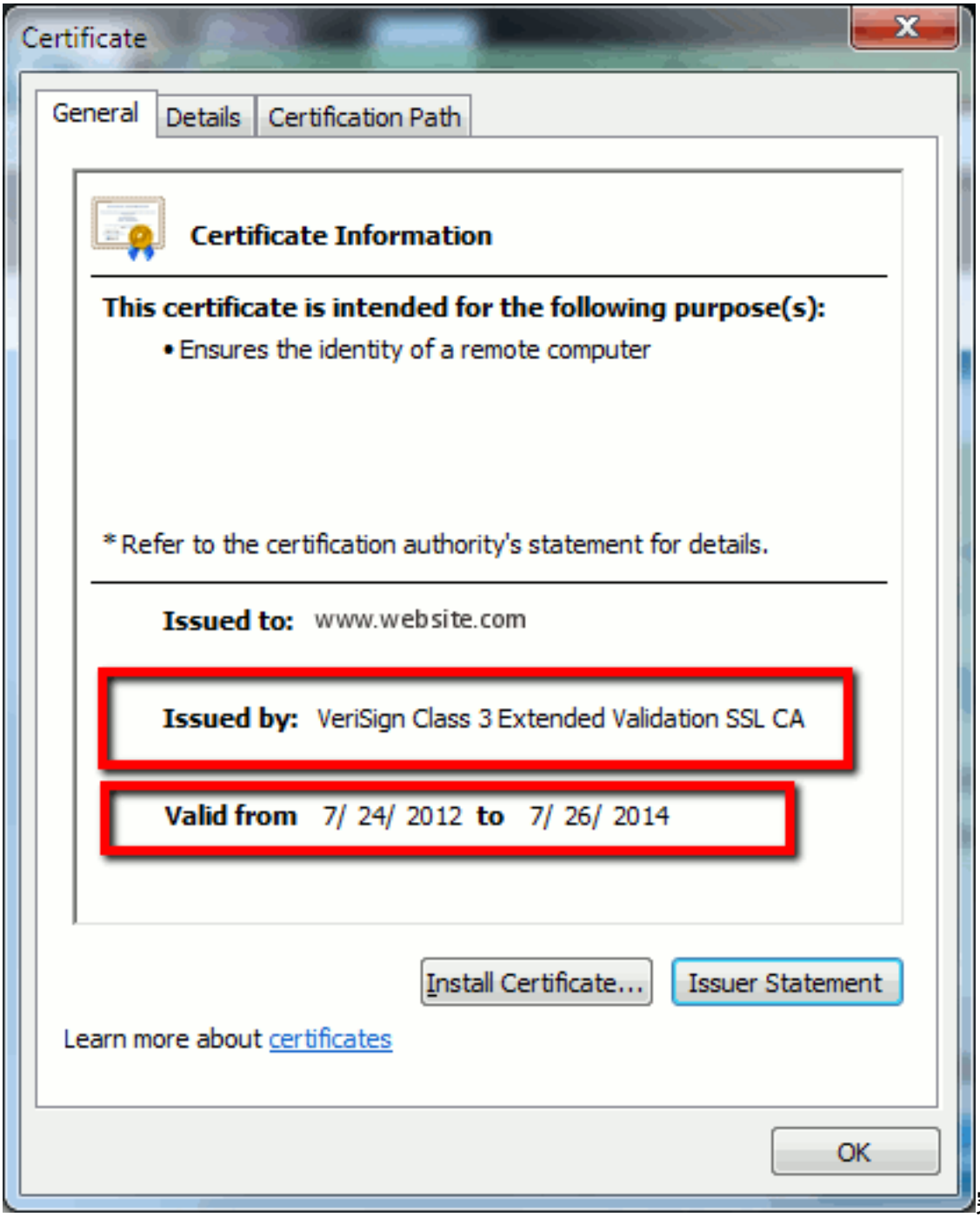
所有浏览器都使用不同的图标，但通常，您会在地址栏中看到这样的挂锁：



1. 单击挂锁，将显示一个窗口：**图 1：网站标识**



2. 单击View Certificates查看站点的证书，如本例所示：**图 2：证书信息，常规选项卡**



突出显示的信息非常重要。**颁发者**是您的系统已信任的公司或证书颁发机构(CA)。**有效自/至**是此证书可用的日期范围。(有时，您会看到您知道您信任CA的证书，但您看到证书无效。请务必检查日期，以便您知道日期是否已过期。)**提示：**最佳实践是在日历中创建提醒，以在证书过期前续订证书。这可以防止将来出现问题。

PEM与DER证书的区别

PEM为ASCII;DER是二进制。图3显示PEM证书格式。

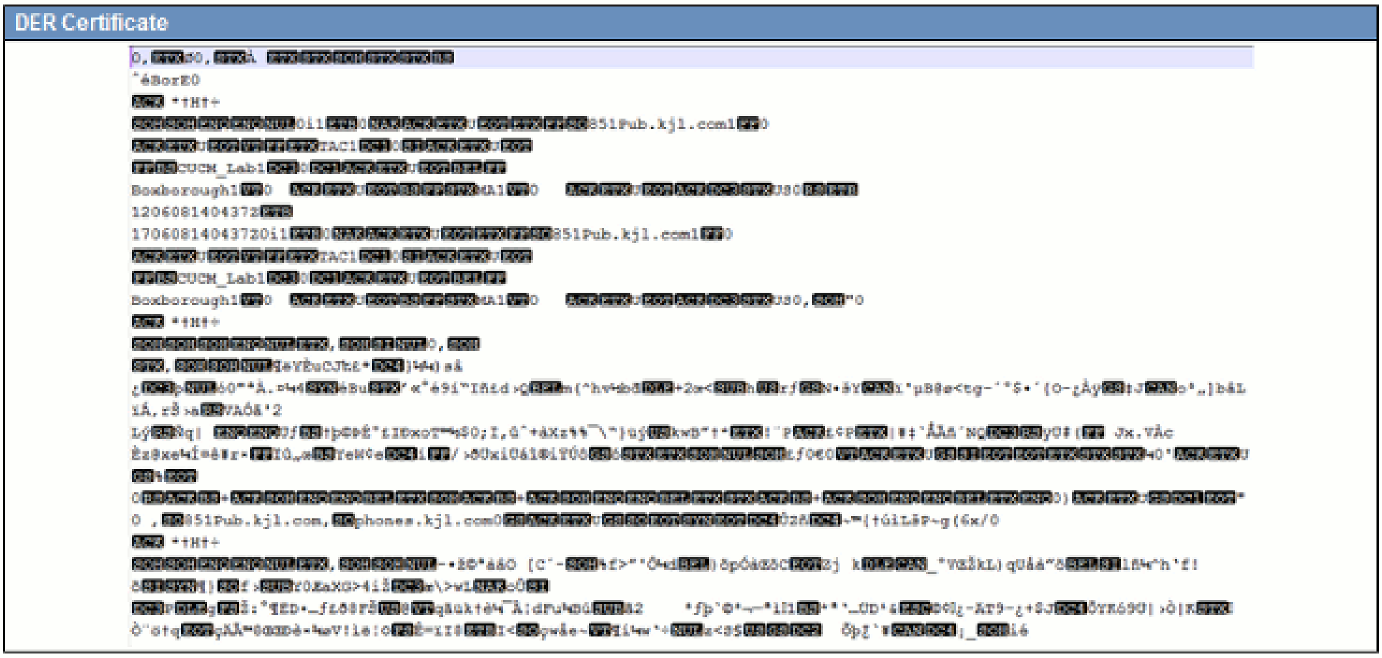
图 3：PEM证书示例

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-----
```


图4显示DER证书。

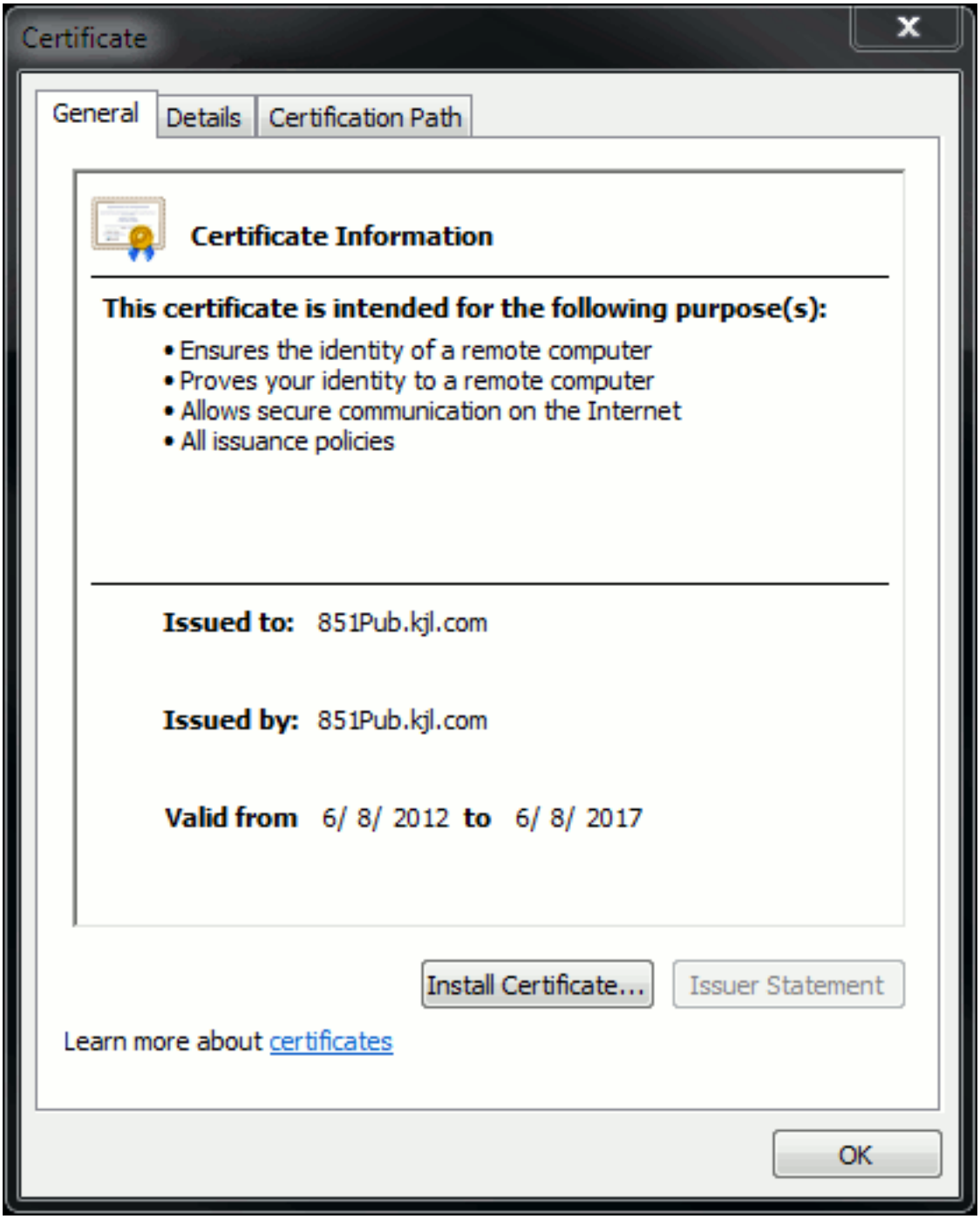
图 4：DER证书示例



大多数CA公司（如VeriSign或Thawt）都使用PEM格式向客户发送证书，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，并用扩展名.PEM或.CER保存。

Windows可以使用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

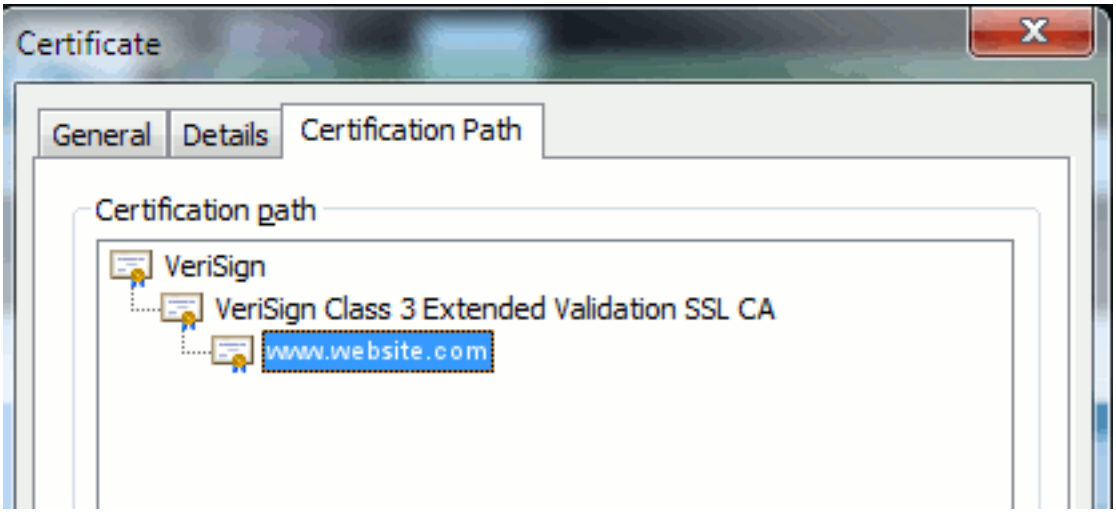


在某些情况下，设备需要特定格式（ASCII或二进制）。 要更改此设置，请以所需格式从CA下载证书或使用SSL转换器工具，如https://www.sslshopper.com/ssl-converter.html。

证书层次结构

要信任来自终端的证书，必须已与第三方CA建立信任。例如，图6显示有三个证书的层次结构。

图 6：证书层次结构



- **Verisign**是CA。
- **Verisign Class 3 Extended Validation SSL CA是中间或签**名服务器证书（CA授权以其名称颁发证书的服务器）。
- **www.website.com**是服务器或服务证书。

您的终端需要先知道它可以信任CA和中间证书，然后才知道它可以信任SSL握手提供的服务器证书（详细信息如下）。 要更好地了解此信任的工作方式，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签署证书的人，无论您是否信任这些证书。

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证书是相同的。

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。

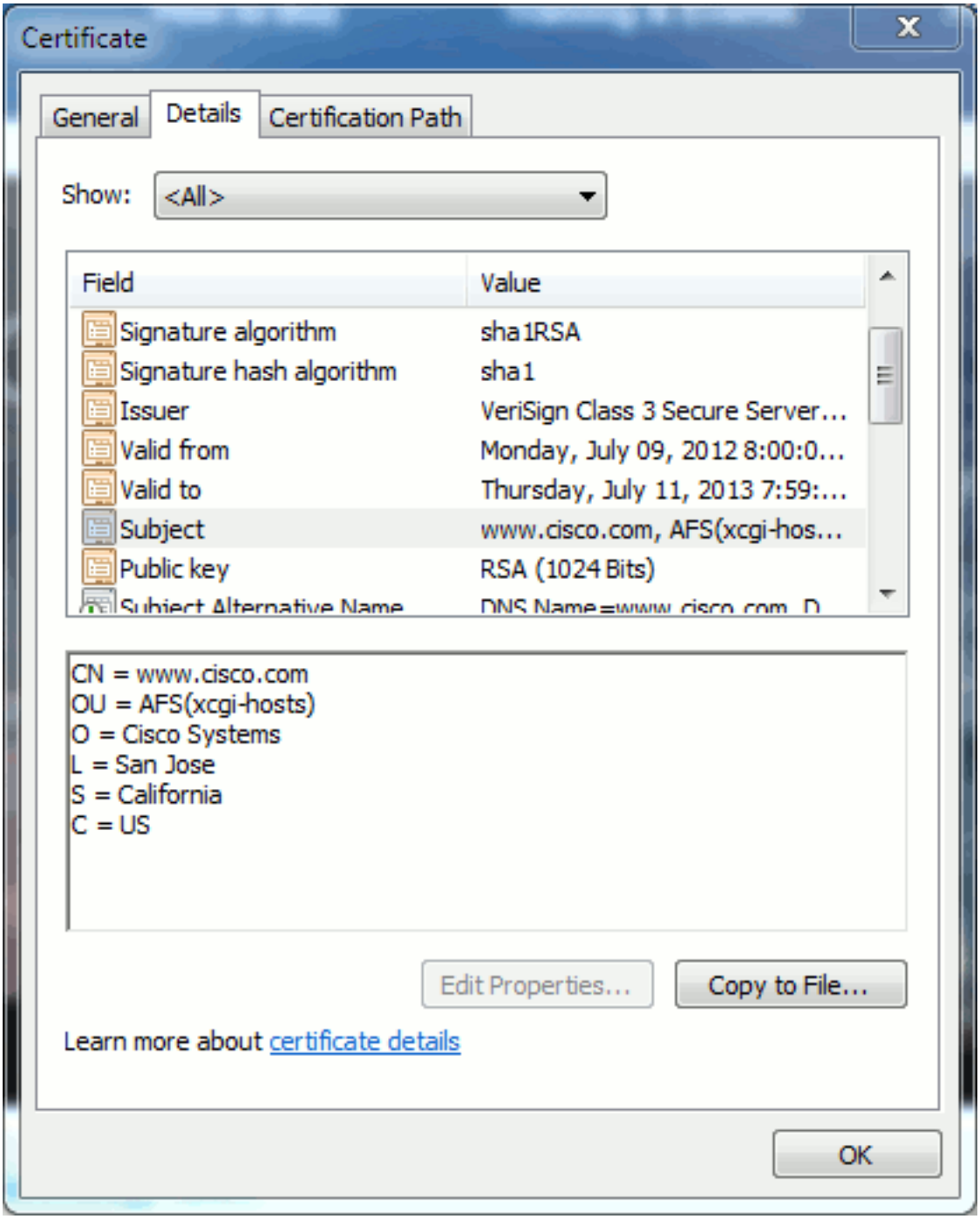
每个可以是CA。无论您的系统是否信任该CA，最重要的是。

常用名和主题替代名

公用名(CN)和使用者备用名(SAN)是对所请求地址的IP地址或完全限定域名(FQDN)的引用。例如，如果输入https://www.cisco.com，则CN或SAN的报头中必须包含www.cisco.com。

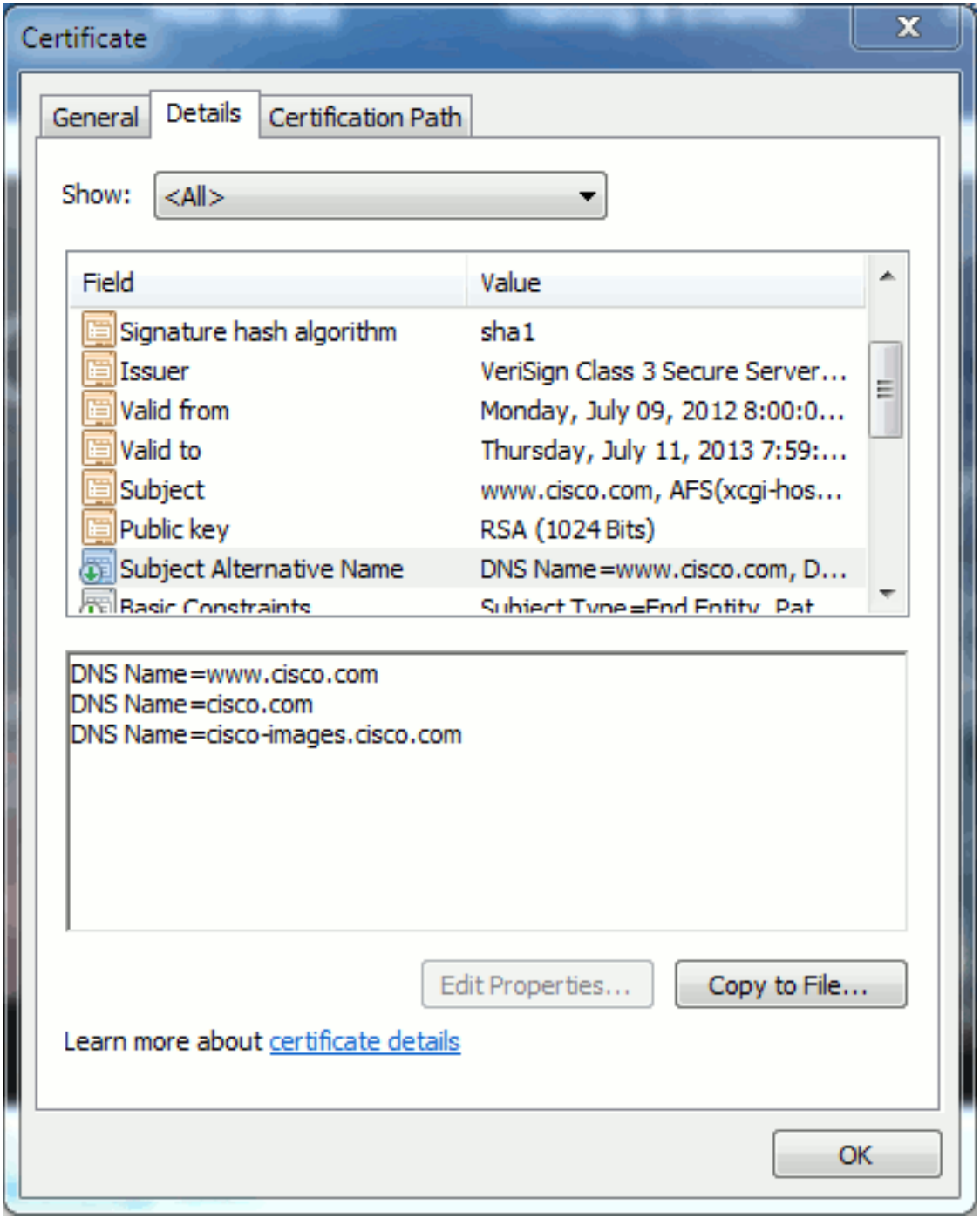
在图7所示的示例中，证书的CN为www.cisco.com。从浏览器对www.cisco.com的URL请求会根据证书显示的信息检查URL FQDN。在这种情况下，它们匹配，并且显示SSL握手成功。此网站已验证为正确的网站，现在桌面和网站之间的通信已加密。

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



此证书可以验证/验证www.cisco.com（也在CN中定义）、cisco.com和cisco-images.cisco.com。这意味着您也可以键入cisco.com，并且此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Jason Burn的文档“CUCM Uploading CCMAdmin Web GUI Certificates on the Support Community”（CCM在支持社区上上传CCMAdmin Web GUI证书）。

通配符证书

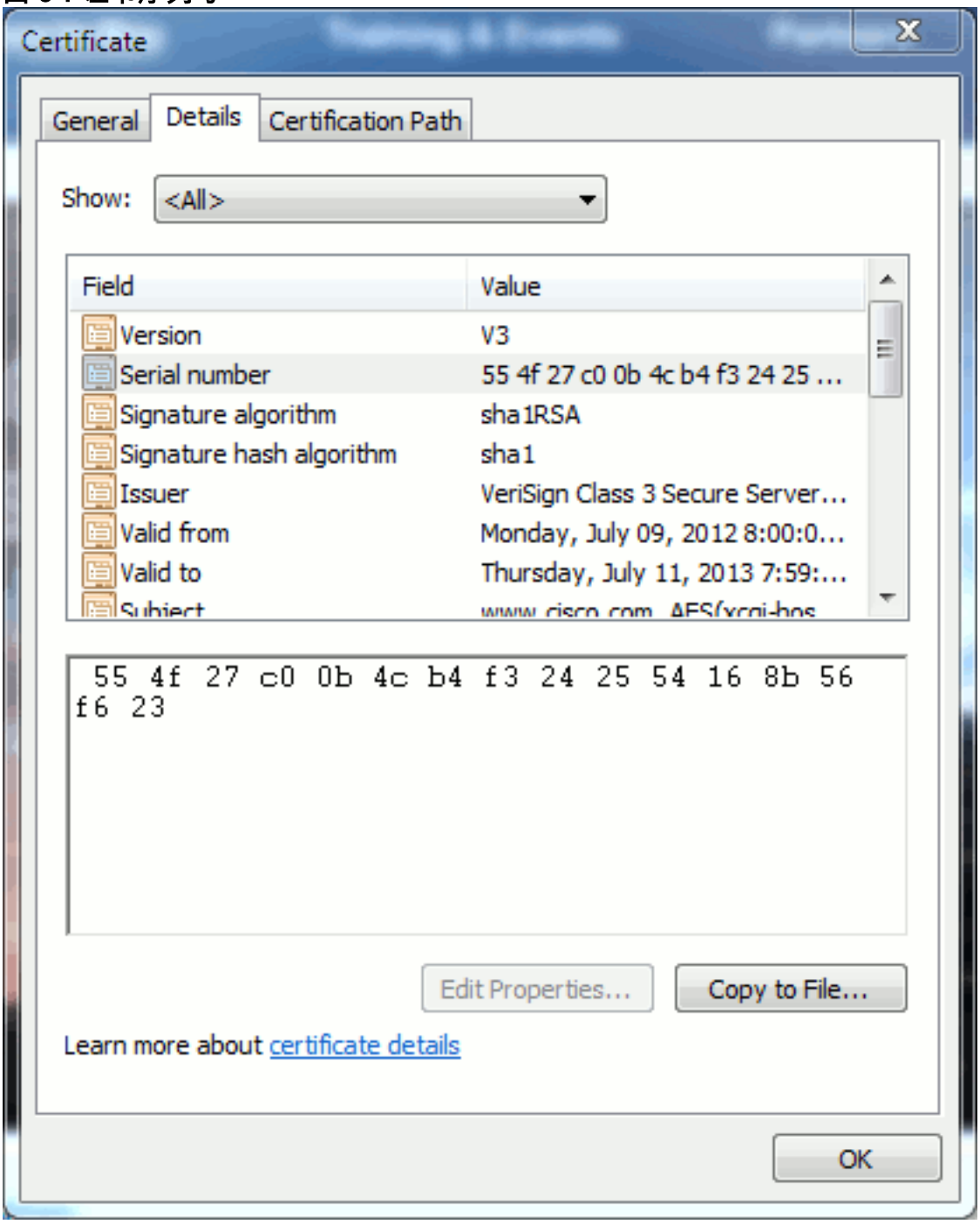
通配符证书是使用星号(*)表示URL部分中任何字符串的证书。例如，要获得www.cisco.com、ftp.cisco.com、ssh.cisco.com等的证书，管理员只需为*.cisco.com创建证书。为了节省资金，管理员只需购买一个证书，而无需购买多个证书。

思科统一通信管理器(CUCM)当前不支持此功能。 但是，您可以跟踪此增强功能：CSCta14114:请求在CUCM和私钥导入中支持通配符证书。

识别证书

当证书中包含相同信息时，您可以看到它是否是相同的证书。所有证书都有唯一的序列号。如果证书是相同的证书、重新生成的证书或伪造的证书，则可以使用此项进行比较。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。如果要为CUCM服务器创建第三方证书，则需要CSR向CA提供。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:**Cisco Unified Operating System Administration > Security >**

Certificate Management > Generate CSR >选择要创建证书的服务>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的唯一文件。这不应该给任何人！如果您向某人提供私钥，则会损害证书提供的安全性。此外，如果使用旧CSR创建证书，请勿为同一服务重新生成新CSR。CUCM删除旧CSR和私钥并替换两者，这使旧CSR无用。

请参阅Jason Burn在支持社区的文档：CUCM上传CCMAdmin Web GUI证书，了解如何创建CSR的信息。

在终端和SSL/TLS握手过程之间使用证书

握手协议是一系列顺序消息，用于协商数据传输会话的安全参数。请参阅SSL/TLS详细信息 ，它记录握手协议中的消息序列。在数据包捕获(PCAP)中可以看到这些。 详细信息包括客户端和服务器之间发送和接收的初始、后续和最终消息。

CUCM如何使用证书

tomcat与tomcat-trust的区别

当证书上传到CUCM时，通过Cisco Unified Operating System Administration > **Security** > **Certificate Management** > **Find**为每个服务提供两个选项。

允许您在CUCM中管理证书的五种服务是：

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

以下是允许您将证书上传到CUCM的服务：

- tomcat
- tomcat-trust
- ipsec
- IPSec信任
- callmanager
- callmanager-trust
- capf
- capf-trust

以下是CUCM 8.0版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CUCM安全指南（按版本）。本节仅说明服务证书和信任证书之间的区别。

例如，使用**tomcat**时，**tomcat-trusts**会上传CA和中间证书，以便此CUCM节点知道它可以信任由CA和中间服务器签名的任何证书。tomcat证书是此服务器上的tomcat服务提供的证书，如果终端向此服务器发出HTTP请求。为了允许Tomcat演示第三方证书，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，必须上传CA和中间证书。

请参阅Jason Burn的CUCM在支持社区上传CCMAdmin Web GUI证书，以了解如何将证书上传到CUCM的信息。

每项服务都有自己的服务证书和信任证书。他们不能互相合作。换句话说，CA和中间证书无法被CallManager服务使用，这些证书以tomcat-trust服务形式上传。

注意：CUCM中的证书是每个节点的证书。因此，如果您需要将证书上传到发布者，并且需要订用者具有相同的证书，则需要在CUCM版本8.5之前将证书上传到每个单独的服务器和节点。在CUCM版本8.5及更高版本中，有一项服务将上传的证书复制到集群中的其余节点。

注意：每个节点有不同的CN。因此，CSR必须由每个节点创建，服务才能提供自己的证书。

如果您对任何CUCM安全功能有其他特定问题，请参阅安全文档。

结论

本文档帮助并建立有关证书的高级知识。此主题可能会更加深入，但本文档对您足够熟悉，可以使用证书。如果您对任何CUCM安全功能有任何疑问，请参阅CUCM安全指南按版本了解详细信息。

相关信息

- **思科统一通信管理器(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:请求在CUCM和私钥导入中支持通配符证书**
- **思科应急响应器(CER)说明**
- **技术支持和文档 - Cisco Systems**