证书和权限高级观点在CUCM

Contents

Introduction

本文的目的将了解证书和认证权限基础。本文恭维是指所有加密或认证功能在Cisco Unified通信管理器的其他Cisco文档(CUCM)。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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

Refer to Cisco Technical Tips Conventions for more information on document conventions.

证书的目的

证书用于在端点之间建立数据的信任/认证和加密。这确认终端与打算的设备联络并且有加密的选项在两个终端之间的数据。

定义信任从认证的观点

证书的重要部分是端点可以由您的终点委托的定义。本文帮助您懂得和定义您的数据如何用打算的网站加密并且共享，电话， FTP服务器，等等。

当您的系统委托认证时，这意味着有在陈述的您的系统的一个被事先装配的认证是100%确信与正确的终点共享信息。否则，它终止这些端点之间的通信。

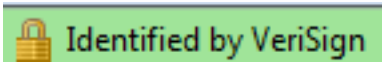
此的一个非技术性的示例是您的驾驶执照。您使用此许可证(服务器/服务认证)证明，您是谁您说您是;您获得了您的从由机动车产生了权限的机动车分组(中间证书)您的本地分部的许可证(DMV)分部您的状态(认证机关)。当您需要显示您的许可证(服务器/服务认证)时官员，官员知道他们能委托DMV分组(中间证书)和机动车(认证机关)分部，并且他们能验证他们发出此许可证(认证机关)。您的身份被验证给官员，并且他们当前相信，您是谁您说您是。否则，如果产生未由DMV的一个错误许可证(服务器/服务认证) (中间证书)签字，然后他们不会委托谁您说您是。本文档的剩余部分提供认证层次结构的一个详细，技术解释。

浏览器如何使用证书

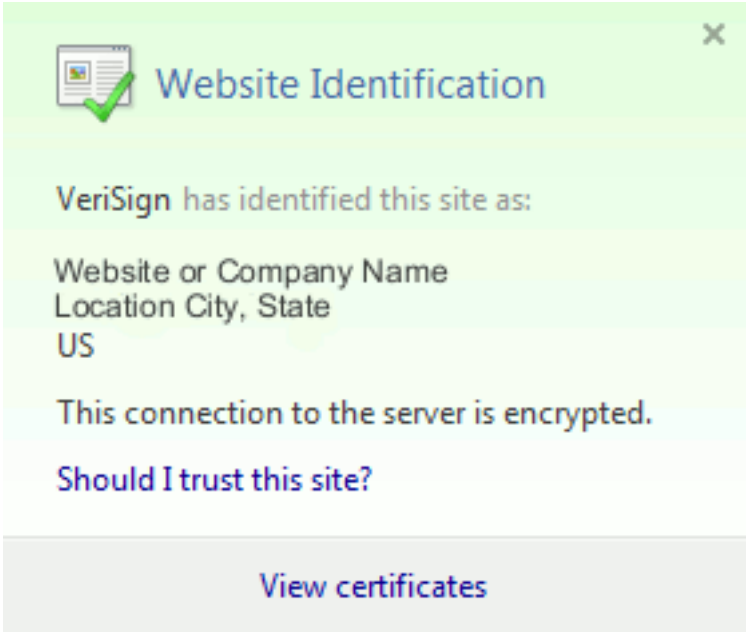
1. 当您访问一个网站时，请输入URL，例如http://www.cisco.com。
2. 主机该站点的DNS查找服务器的IP地址。
3. 浏览器连接到该站点。

没有证书，知道是不可能的是否使用了一个恶意DNS服务器，或者是否路由到另一个服务器。证书保证您适当地和安全地路由到打算的网站，例如您的内存段网站，私有或敏感信息您输入安全。

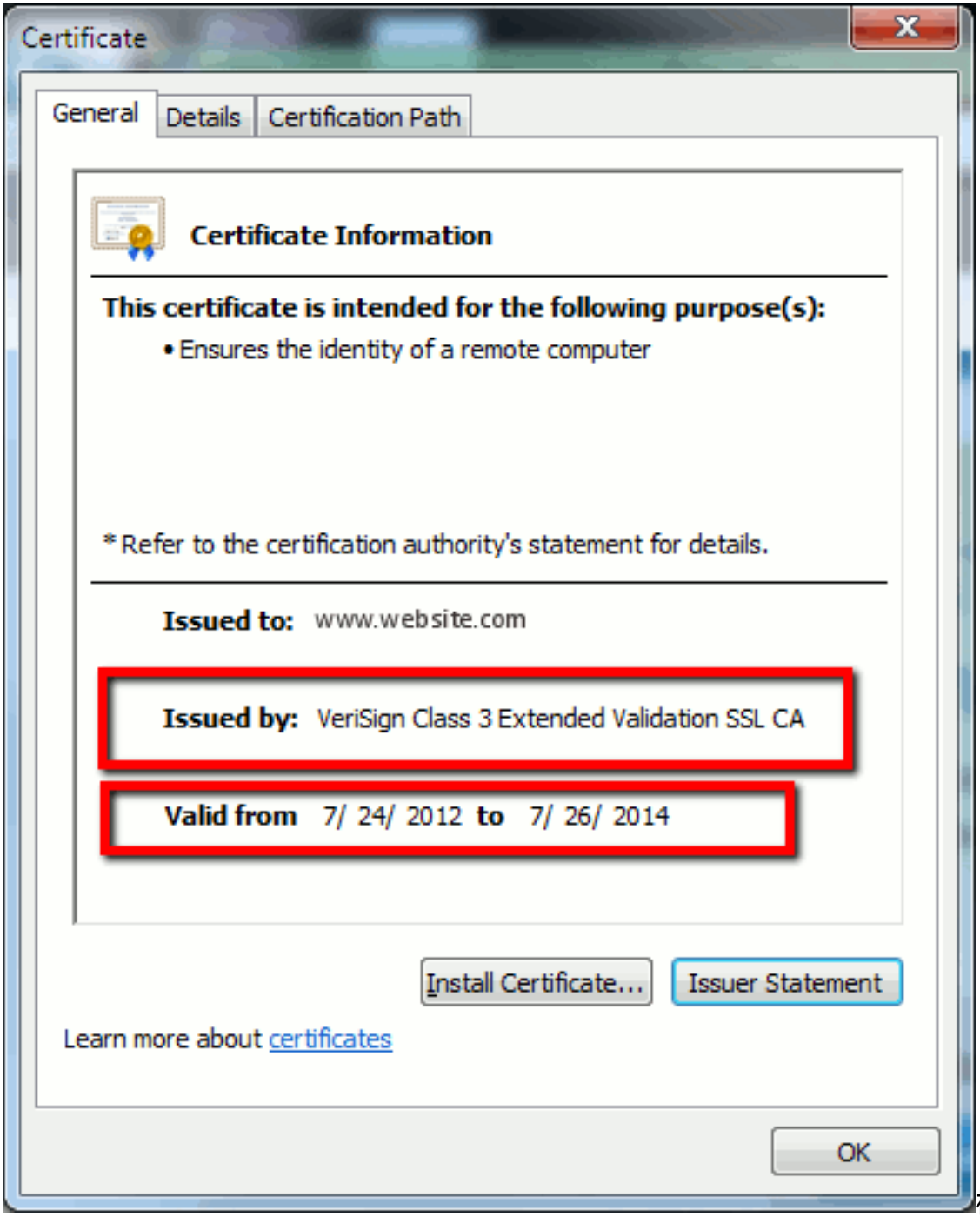
他们使用的所有浏览器有不同的图标，但是通常，您看到在地址栏的挂锁象这样：



1. 点击挂锁，并且窗口显示：**图 1：网站证明**



2. 如此示例所显示，点击**视图证书**发现站点的认证：**图 2：证书信息，一般选项**



被选定的信息是重要的。**发出由**已经公司或Certificate Authority (CA)该您的系统信任。**有效的从/至**是日期范围此认证是可用的。(您有时看到您认识您信任CA，但是的认证您看到认证无效。总是请检查日期，因此您知道它是否到期了。)**提示**：在到期前，最佳实践是创建在您的日历的一个提示更新认证。这防止将来问题。

PEM之间的区别与DER证书

PEM是ASCII;DER二进制。图3显示PEM证书格式。

图 3：PEM认证示例

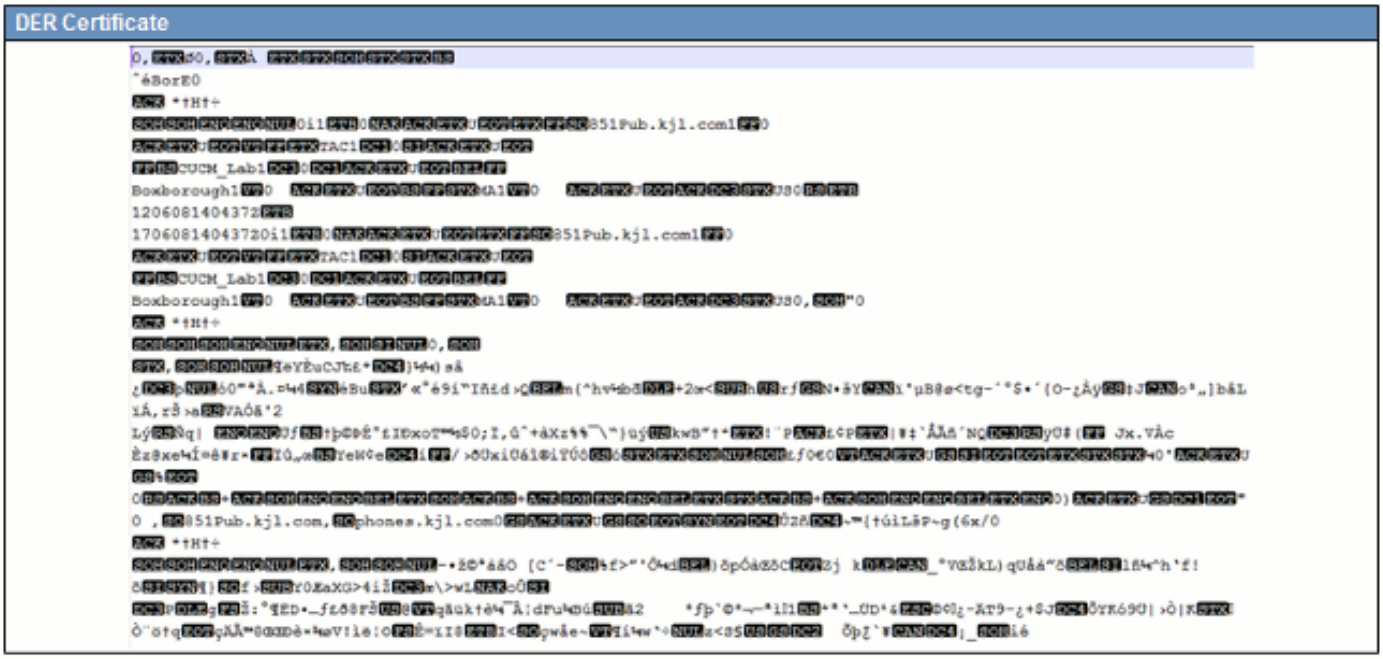
PEM Certificate

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

图4显示DER认证。

图 4：DER认证示例

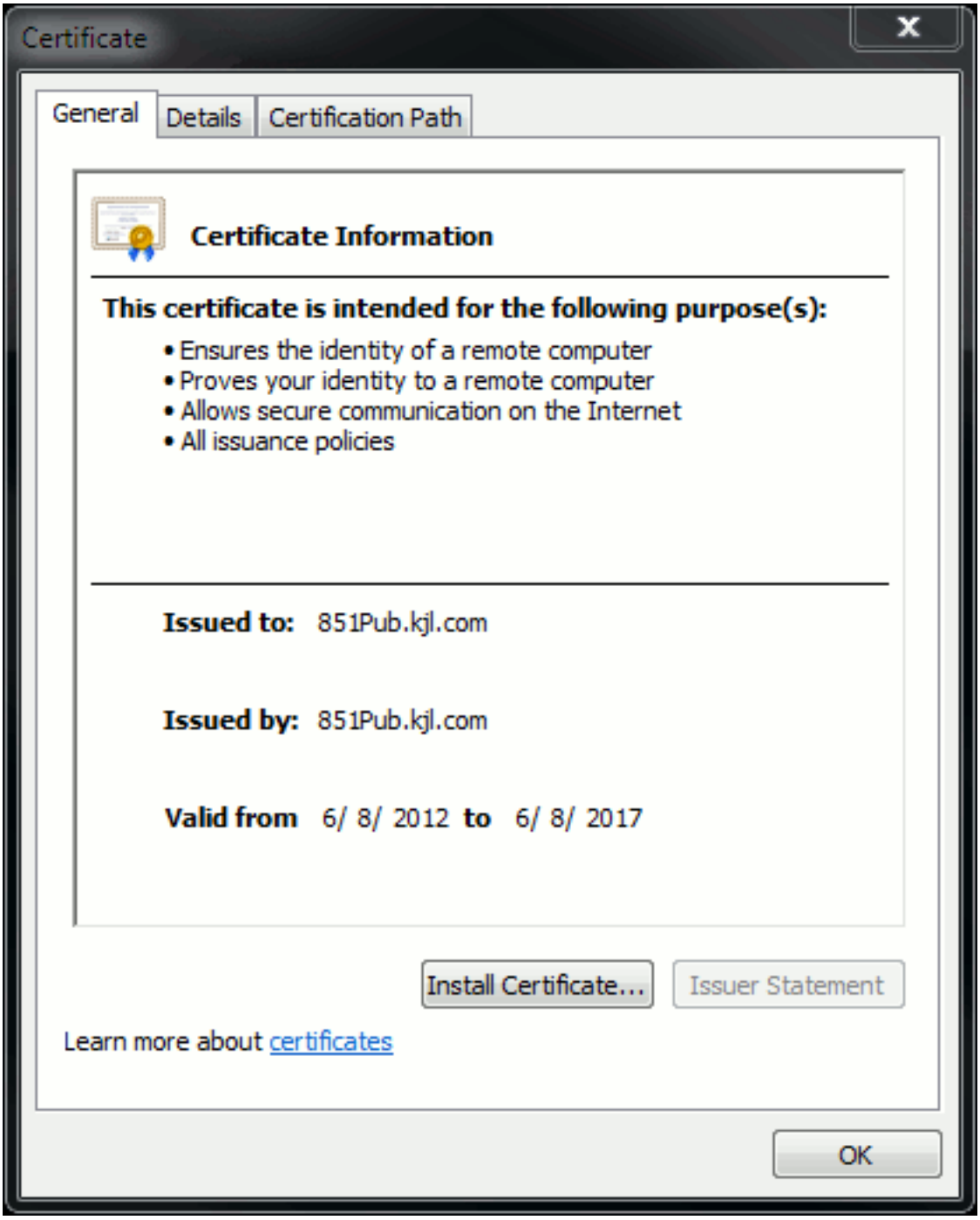
DER Certificate



多数CA公司类似VeriSign或Thawt使用发送证书的PEM格式到用户，因为是电子邮件友好。用户应该复制整个字符串和包括**-----开始认证-----**并且**-----END认证-----**请粘贴它到文本文件，并且保存它与扩展名.PEM或.CER。

Windows能读DER如图5.所显示，并且CER格式化与其自己的证书管理附属程序并且显示认证。

图 5：证书信息

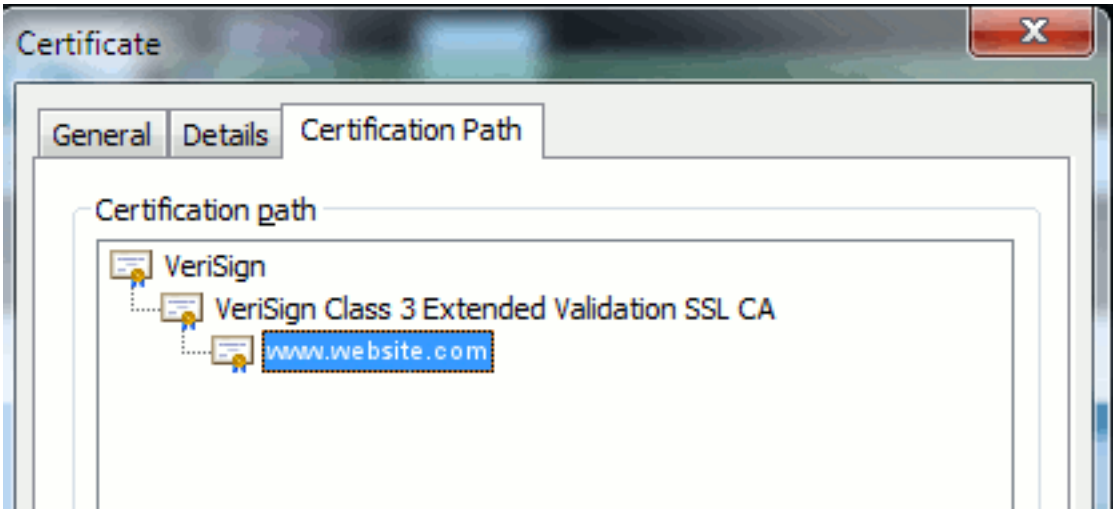


有时，设备要求一种特定格式(ASCII或二进制)。为了更改此，从CA请下载认证以需要的格式或请使用一个SSL交换器工具，例如https://www.sslshopper.com/ssl-converter.html。

认证层次结构

为了委托从终点的一个认证，必须有信任已经设立与第三方例如CA.，图6显示有三证书层次结构。

图 6： 认证层次结构



- Verisign是CA。
- Verisign等级3扩展的验证SSL CA是中间或签署的服务器证明(CA核准的服务器发行在其名字的证书)。
- www.website.com是服务器或服务认证。

您的终点需要知道能首先委托CA和半成品证书，在知道前能委托SSL握手(见下)提交的服务器证明。更好知道此信任如何工作，请参见在本文的部分：**定义"信任"从认证的观点**。

自署名的认证与第三方证书

自已签署的和第三方证书之间的主要区别是谁签字认证，您是否委托他们。

自签证书是提交它的服务器签字的认证;因此，服务器/服务认证和CA证书是相同的。

第三方CA是或者公共CA提供的服务(类似Verisign、Entrust， Digicert)或该的服务器(类似Windows 2003， Linux， Unix， IOS)控制服务器/服务认证的正确性。

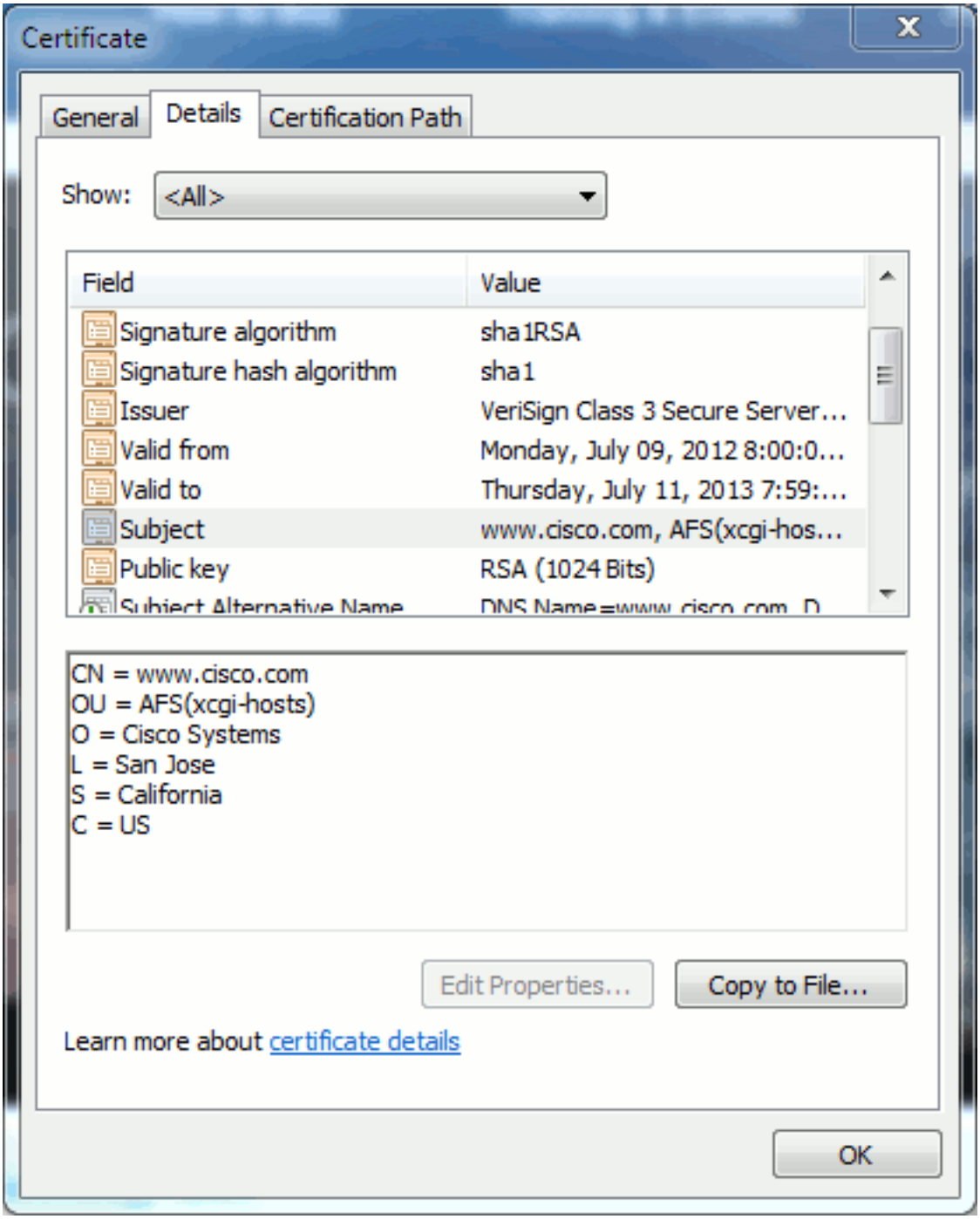
每一个可以是CA.您的系统是否委托该CA，是什么最要紧。

普通的名字和附属的代替名字

普通的名字(CN)和附属的代替名字(SAN)是在被请求地址的IP地址或完全合格的域名(FQDN)的参考。例如，如果输入https://www.cisco.com，然后CN或SAN必须有在报头的www.cisco.com。

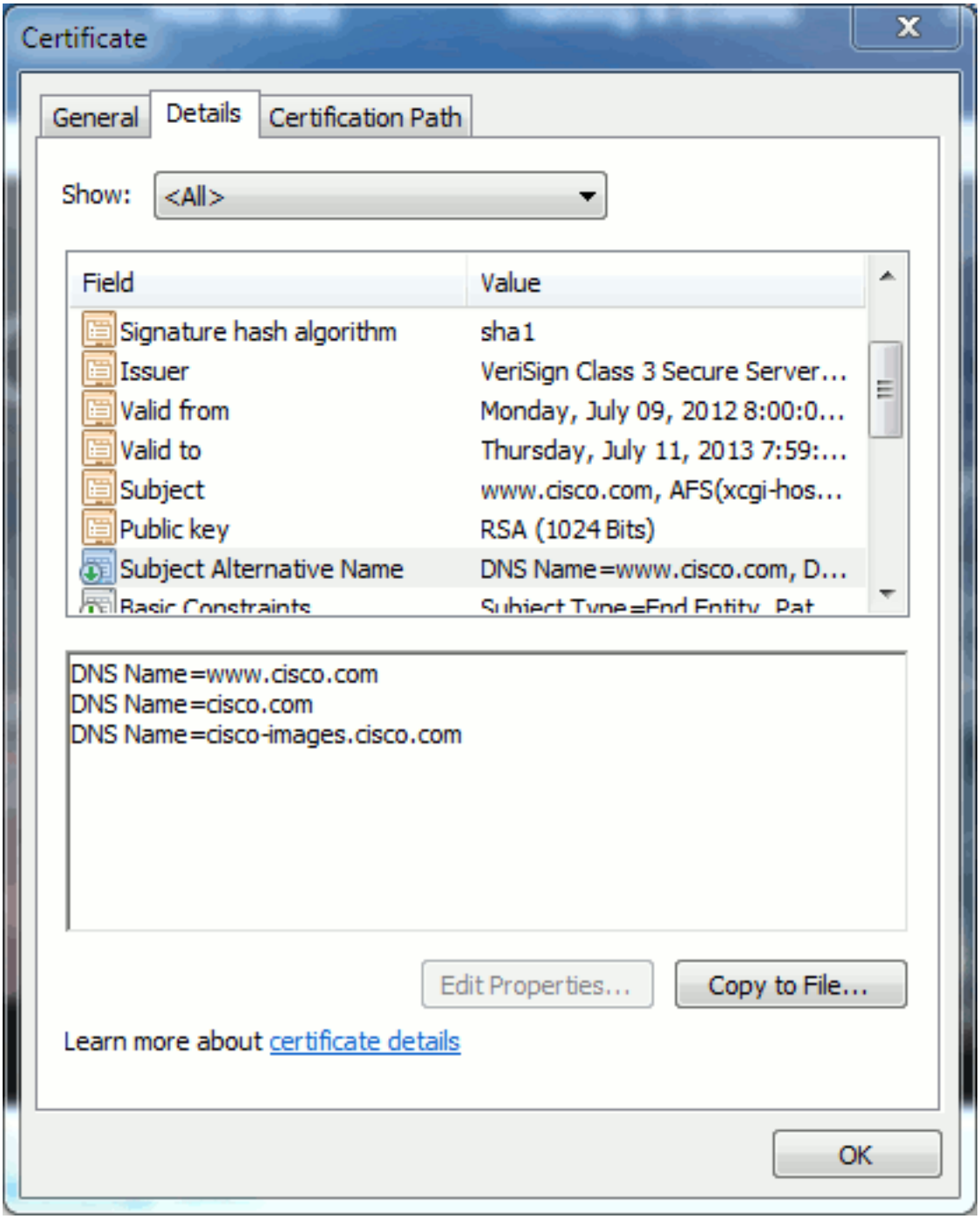
在Figure7显示的示例中，认证有CN作为www.cisco.com。URL请求从浏览器的www.cisco.com根据认证引见的信息检查URL FQDN。在这种情况下，他们配比，并且它显示SSL握手是成功的。此网站被验证是正确的网站，并且通信当前被加密在桌面和网站之间。

图 7：网站验证



在同一个认证，有三个FQDN/DNS地址的一个SAN报头：

图8 ：SAN报头



此认证能验证/验证www.cisco.com (也定义在CN)， cisco.com和cisco-images.cisco.com。这意味着您能也键入cisco.com，并且此同样认证可以用于验证和加密此网站。

CUCM能创建SAN报头。参考贾森预烧硬件的文件，加载CCMAdmin Web在支持公共的CUCM GUI证书关于SAN报头的更多信息。

通配符证书

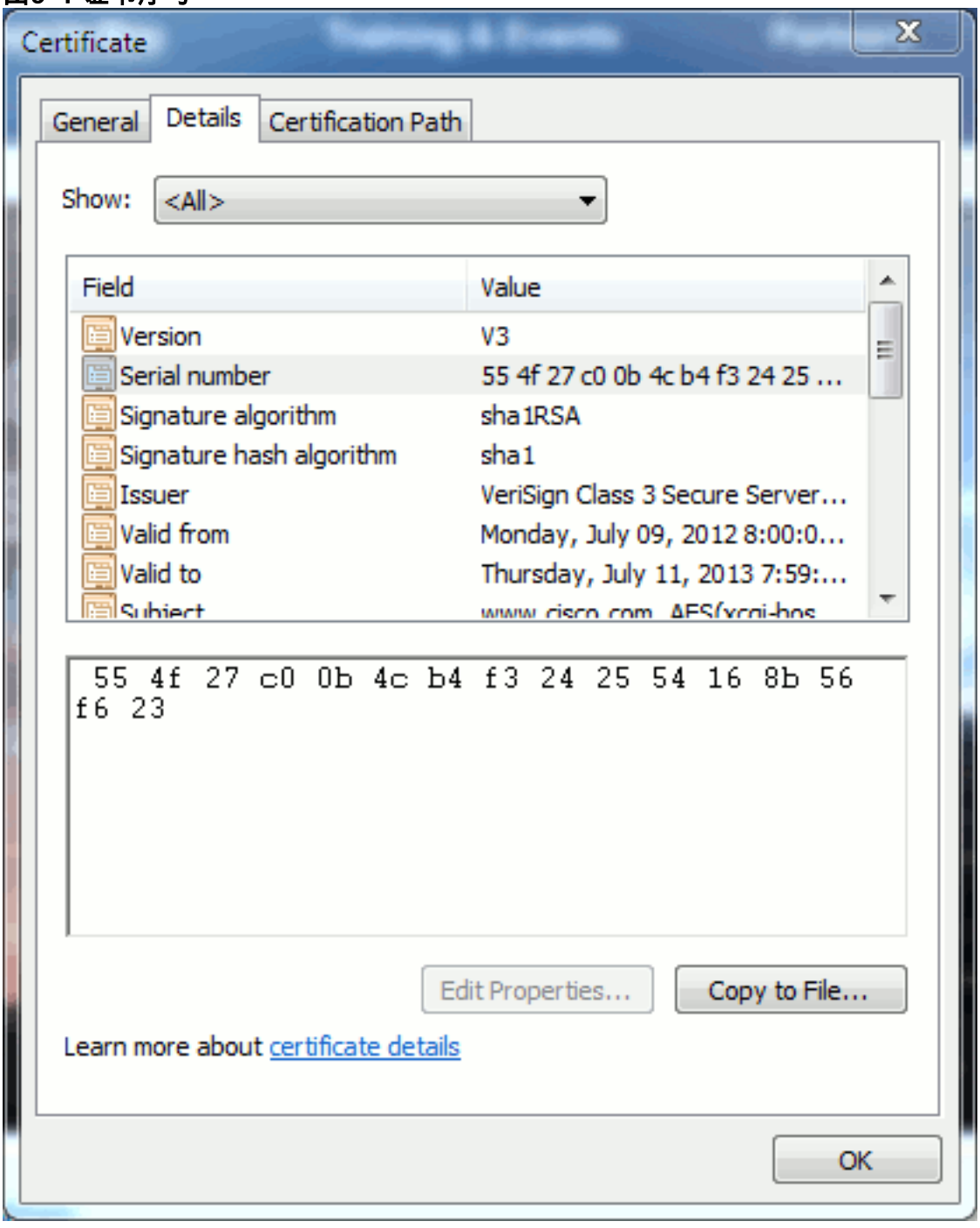
通配符证书是使用星号(*)表示在URL的部分的所有字符串的证书。例如，为了有www.cisco.com的一个认证， ftp.cisco.com， ssh.cisco.com，等等，管理员只将需要创建*.cisco.com的一个认证。为了存金钱，仅管理员需要采购单个认证，并且不需要购买多重证明。

Cisco Unified通信管理器当前不支持此功能(CUCM)。然而，您能记录此增进：CSCta14114 ：要求通配符认证技术支持在CUCM和专用密钥导入的。

识别证书

当证书有同样信息在他们时，您能看到它是否是同一个认证。所有证书有一唯一序列号。您能使用此比较，如果证书是同一证书，重新生成或者假劣。图9提供一个示例：

图9 ：证书序号



CSR和他们的目的

CSR代表认证署名请求。如果要创建CUCM服务器的一个第三方认证，您需要CSR出席到CA。此CSR看起来很多PEM (ASCII)认证。

Note: 这不是认证，并且不可能使用作为一个。

CUCM通过Web GUI自动地创建CSR ：**Cisco Unified操作系统的管理>** Security > Certificate Management **>生成CSR** >选择您要创建认证>然后**生成CSR的**服务。在使用时候此选项，一把新的

专用密钥和CSR生成。

Note: 一把专用密钥是对此服务器和服务是唯一的文件。不应该产生这任何人!如果提供一把专用密钥给某人，危及该的安全认证提供。并且，如果使用老CSR创建认证，请勿重新生成同一项服务的新的CSR。CUCM删除老CSR和专用密钥并且替换他们两个，使老CSR无用。

参考贾森在支持公共的预烧硬件的文档：加载CCMAdmin Web GUI证书的CUCM关于如何创建CSR的信息。

使用在终点和SSL/TLS握手进程之间的证书

握手协议是协商数据传输会话的安全参数的一系列的程序化的消息。详细请参见SSL/TLS ，描述在握手协议的消息序列。这些在信息包获取(PCAP)能被看到。详细资料包括首字母，随后和最终发送的消息和接受在客户端和服务器之间。

CUCM如何使用证书

在Tomcat和Tomcat信任之间的区别

当证书被加载到CUCM时，有每项服务的两个选项通过**Cisco Unified操作系统的管理>** Security > Certificate Management **>查找**。

允许您**管理**在CUCM的证书的五服务是：

- Tomcat
- ipsec
- 呼叫管理器
- capf
- 电视(在CUCM版本8.0及以后)

这是允许您**加载**证书到CUCM的服务：

- Tomcat
- Tomcat信任
- ipsec
- ipsec信任
- 呼叫管理器
- 呼叫管理器信任
- capf
- CAPF信任

这些是服务可用在CUCM版本8.0及以后：

- 电视
- 电视信任
- phone-trust
- phone-vpn-trust
- phone-sast-trust
- phone-ctl-trust

由版本欲了解更详细的信息请参见CUCM安全指南在证书的这些类型。此部分只说明在服务认证和

信任认证之间的区别。

例如，与**Tomcat**， Tomcat**信任**加载CA，并且半成品证书，以便此CUCM节点认识它能委托CA和半成品服务器签字的所有认证。Tomcat认证是由在此服务器的Tomcat服务提交的认证，如果终点做一个HTTP请求到此服务器。为了由Tomcat允许第三方证书的介绍， CUCM节点需要知道能委托CA和半成品服务器。所以，它是需求加载CA和半成品证书，在Tomcat (服务)前认证被加载。

参考贾森加载CCMAdmin Web在支持公共的预烧硬件的CUCM GUI证书将帮助您知道如何加载证书到CUCM的信息。

每项服务有其自己的服务认证和信任认证。他们不工作彼此。换句话说，作为Tomcat信任服务和中间证书被加载的CA不可能由呼叫管理服器务使用。

Note: 在CUCM的证书是a每个节点基本类型。所以，如果需要证书被加载到发布人和您请需要订户有同一证书，您需要加载他们到每个单个服务器和节点在CUCM版本8.5之前。在CUCM版本8.5中及以后，有复制被加载的证书对节点其余在簇的服务。

Note: 每个节点有不同的CN。所以，必须由每个节点创建CSR为了服务能提交他们自己的证书。

如果有对的另外的特定问题任何CUCM安全功能，请参见安全文档。

结论

本文协助解决并且构件高级在证书的知识。此主题能要紧能变得更加详细，但是本文熟悉足够您与证书一起使用。如果有对任何CUCM安全功能的问题，由版本请参见CUCM安全指南欲知更多信息。

Related Information

- 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：加载CCMAdmin Web GUI证书的CUCM
- Bug CSCta14114 ：要求通配符认证技术支持在CUCM和专用密钥导入的
- (CER)解释的Cisco Emergency Responder
- Technical Support & Documentation - Cisco Systems