CUCM中的證書和授權高級檢視

目錄

簡介

本文旨在瞭解憑證和憑證授權單位的基本資訊。本文檔補充了涉及Cisco Unified Communications Manager(CUCM)中的任何加密或身份驗證功能的其他思科文檔。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

憑證的用途

在端點之間使用證書來建立信任/驗證和資料加密。這確認端點與目標裝置通訊並且可以選擇加密兩個端點之間的資料。

從證書的角度定義信任

證書最重要的部分是定義您的終端可以信任哪些端點。本文檔幫助您瞭解和定義如何加密您的資料，以及如何與目標網站、電話、FTP伺服器等共用。

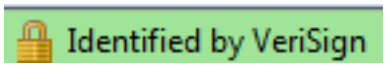
如果您的系統信任證書，則表示您的系統上存在預安裝的證書，該證書表明您完全確信它與正確的端點共用資訊。否則，它將終止這些端點之間的通訊。

非技術性的例子是您的駕駛執照。您使用此許可證（伺服器/服務證書）來證明您就是您所說的人；你已獲得你所在地區機動車部門分支機構的牌照（中間憑證），該部門已獲得你所在地區機動車部門（證書頒發機構）的許可。 當您需要將您的許可證（伺服器/服務證書）顯示給一名管理人員時，該管理人員知道他們可以信任DMV分支機構（中間證書）和機動車部門（證書頒發機構），並且他們可以驗證該許可證是由他們（證書頒發機構）頒發的。 您的身份由警官核實，現在他們相信您就是您所說的人。否則，如果您提供的虛假許可證（伺服器/服務證書）未由DMV（中間證書）簽名，則他們將不會信任您所說的您。本文的其餘部分提供憑證層級的深入技術說明。

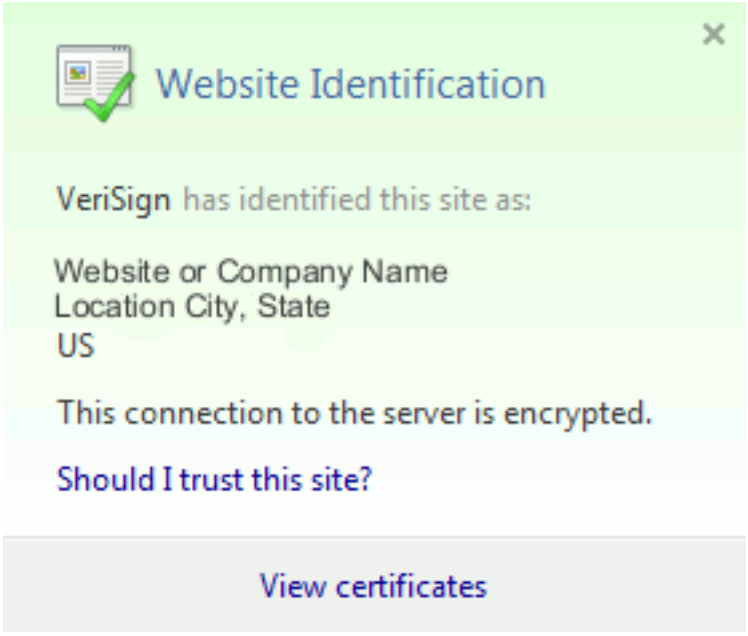
瀏覽器如何使用證書

1. 當您訪問網站時，請輸入URL，例如http://www.cisco.com。
2. DNS會查詢託管該站點的伺服器的IP地址。
3. 瀏覽器導航到該站點。

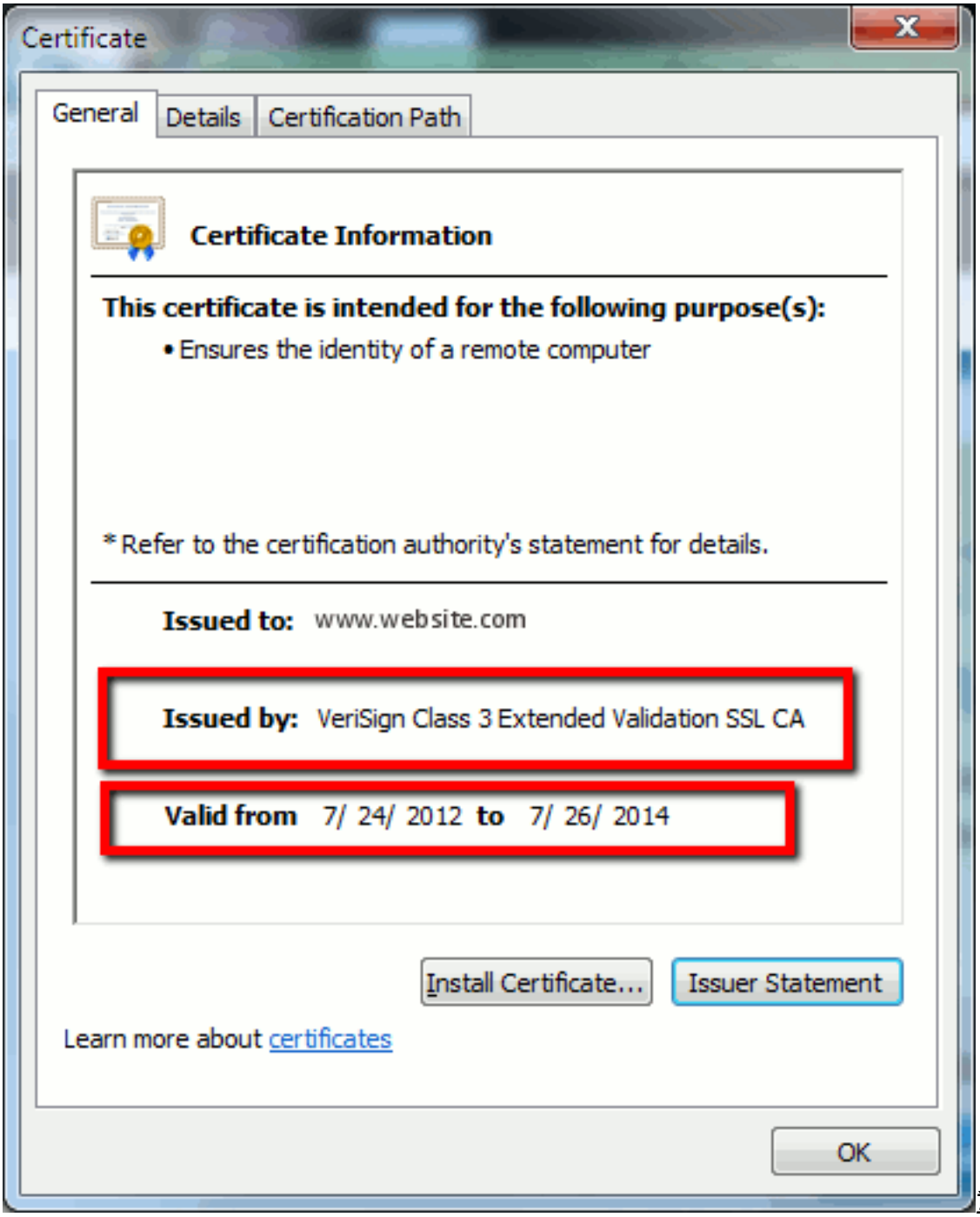
如果沒有證書，則無法知道是否使用了非法DNS伺服器，或者您是否路由到其他伺服器。證書確保您正確並安全地路由到目標網站（如您的銀行網站），您輸入的個人或敏感資訊在此網站是安全的。

所有瀏覽器都有不同的圖示，但通常您在位址列中會看到如下掛鎖： 

1. 按一下掛鎖，將顯示一個視窗：**圖1:網站標識**



2. 按一下**View Certificates**以檢視站點的證書，如以下示例所示：**圖2:證書資訊，常規頁籤**



重點介紹的資訊非常重要。**頒發者**是您的系統已經信任的公司或證書頒發機構(CA)。**Valid from/to是**此證書可用的日期範圍。(有時您會看到您知道信任CA的憑證，但您看到該憑證無效。請始終檢查日期，以便您知道它是否已過期。)**提示：**最佳作法是在您的日曆中建立提醒，以便在證書過期之前續訂。這可防止將來出現問題。

PEM和DER證書之間的差異

PEM為ASCII;DER是二進位制的。圖3顯示了PEM證書格式。

圖3:PEM證書示例

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-----
```

圖4顯示了DER證書。

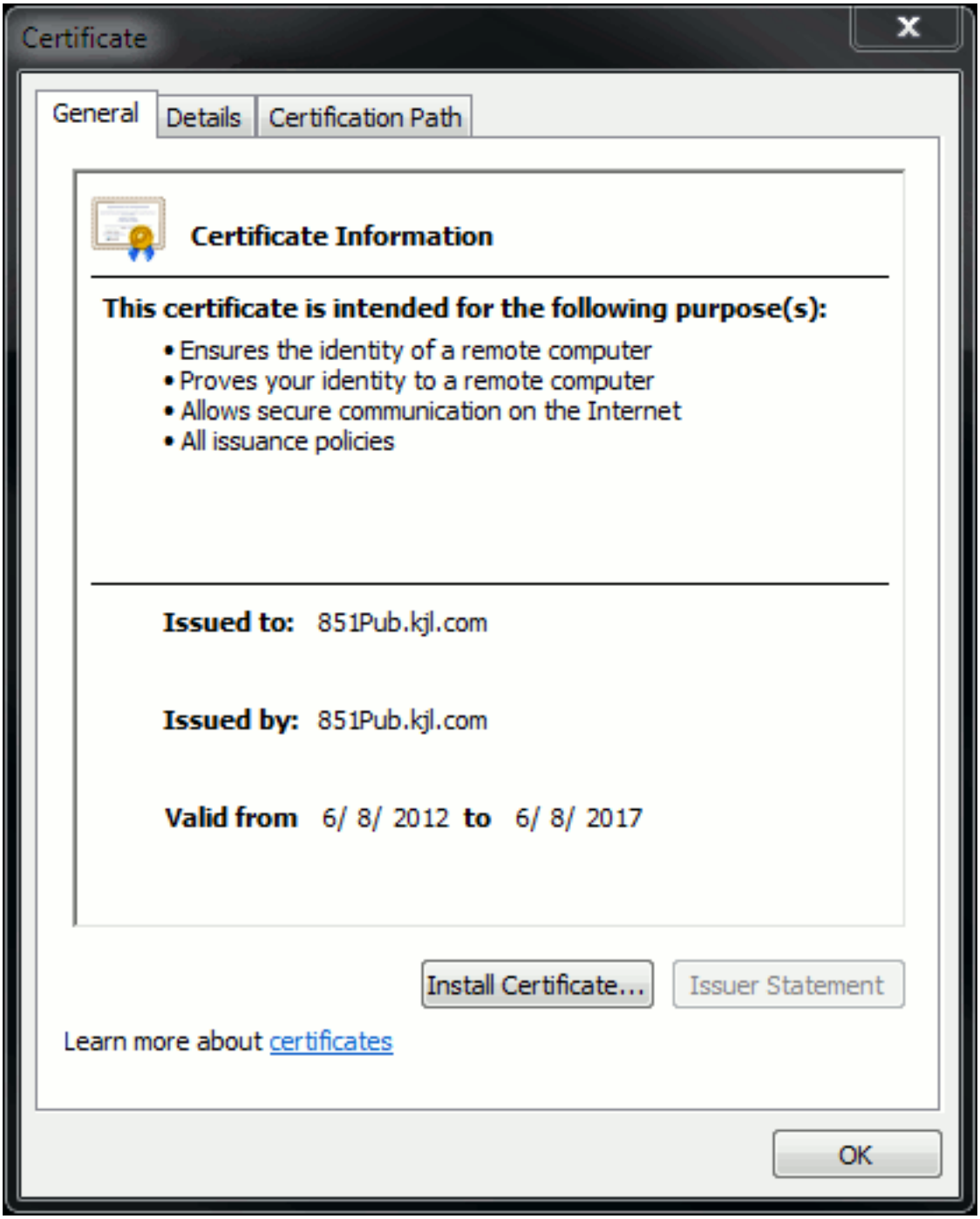
圖4:DER證書示例

DER Certificate

大多數CA公司（如VeriSign或Thawt）使用PEM格式將證書傳送給客戶，因為此格式適合使用電子郵件。客戶應複製整個字串並包括**-----BEGIN CERTIFICATE -** 和**-----END CERTIFICATE -** ，將其貼上到文本檔案中，然後使用.PEM或.CER副檔名進行儲存。

Windows可以使用自己的證書管理小程式讀取DER和CER格式，並顯示證書，如圖5所示。

圖5:憑證資訊

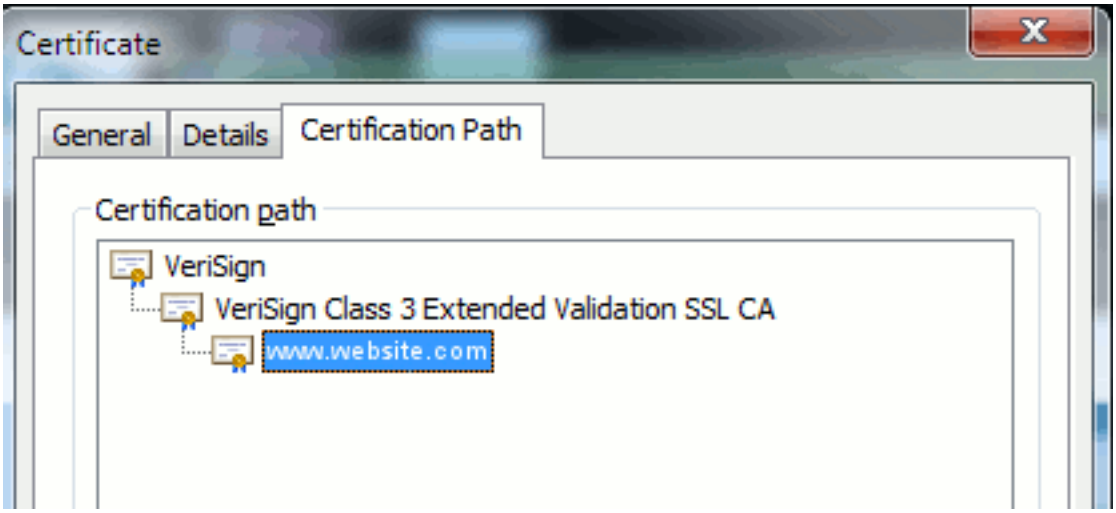


在某些情況下，裝置需要特定的格式（ASCII或二進位制）。 若要變更此設定，請以所需的格式從CA下載憑證或使用SSL轉換器工具，例如https://www.sslshopper.com/ssl-converter.html。

證書層次結構

若要信任來自端點的憑證，必須存在與第三方CA建立的信任。例如，圖6顯示了三個證書的層次結構。

圖6:證書層次結構



- **Verisign**是一個CA。
- **Verisign Class 3 Extended Validation SSL CA是中間**或簽名伺服器證書（由CA授權以其名稱頒發證書的伺服器）。
- **www.website.com**是伺服器或服務證書。

您的終端需要先知道它可以信任CA和中間證書，然後才能知道它可以信任SSL握手提供的伺服器證書（詳細資訊如下）。 要更好地理解此信任的工作原理，請參閱本文檔中的部分：**從證書的角度定義「信任」**。

自簽名證書與第三方證書

自簽名證書和第三方證書之間的主要區別在於誰在證書上簽名，以及您是否信任它們。

自簽名證書是由提供證書的伺服器簽名的證書；因此，伺服器/服務證書和CA證書是相同的。

第三方CA是由公共CA（如Verisign、Entrust、Digicert）或伺服器（如Windows 2003、Linux、Unix、IOS）提供的服務，控制伺服器/服務證書的有效性。

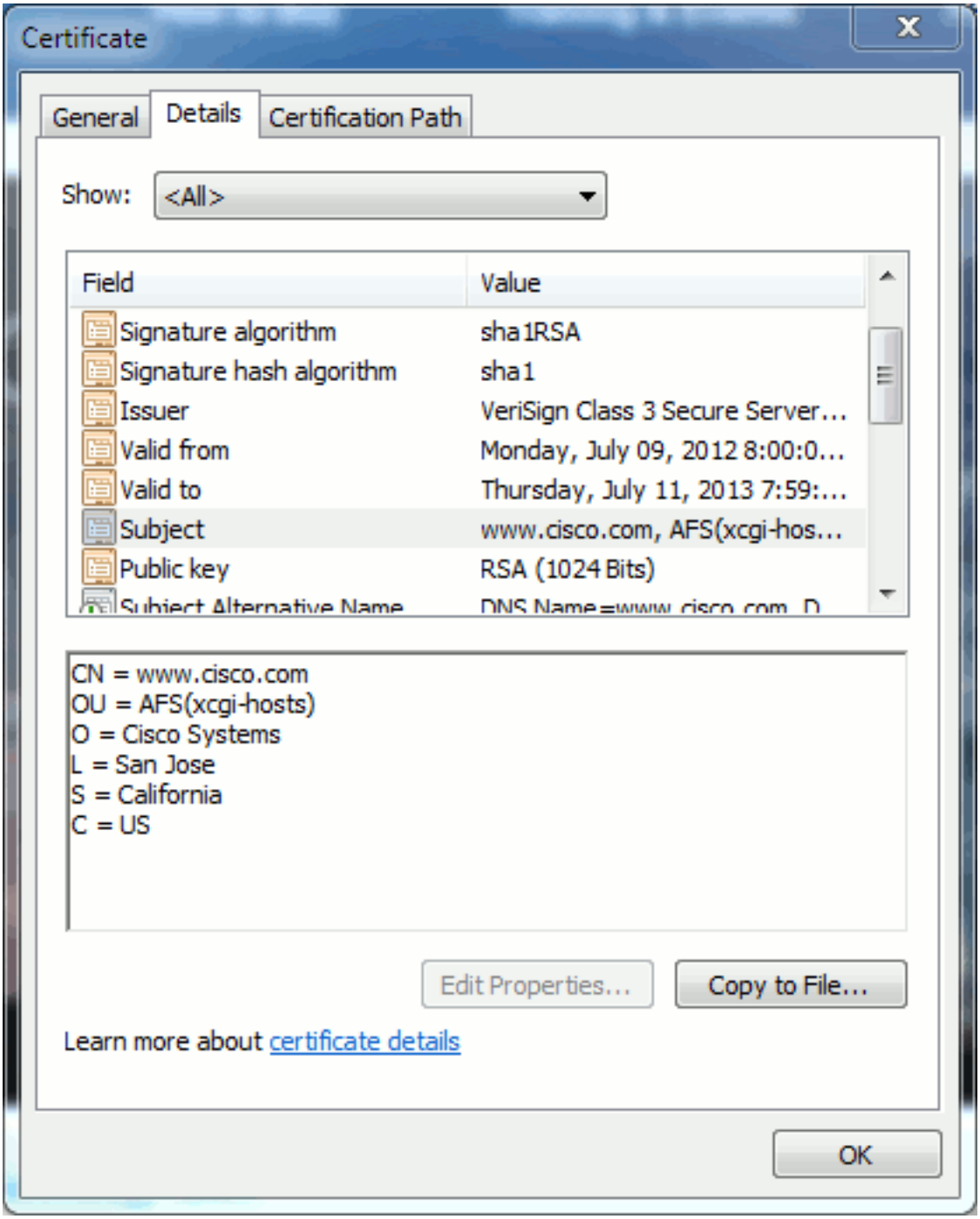
每個都可以是CA。系統是否信任該CA才是最重要的。

常用名稱和主題替代名稱

公用名(CN)和主體替代名稱(SAN)是所請求地址的IP地址或完全限定域名(FQDN)的引用。例如，如果您輸入https://www.cisco.com，則CN或SAN的報頭中必須包含www.cisco.com。

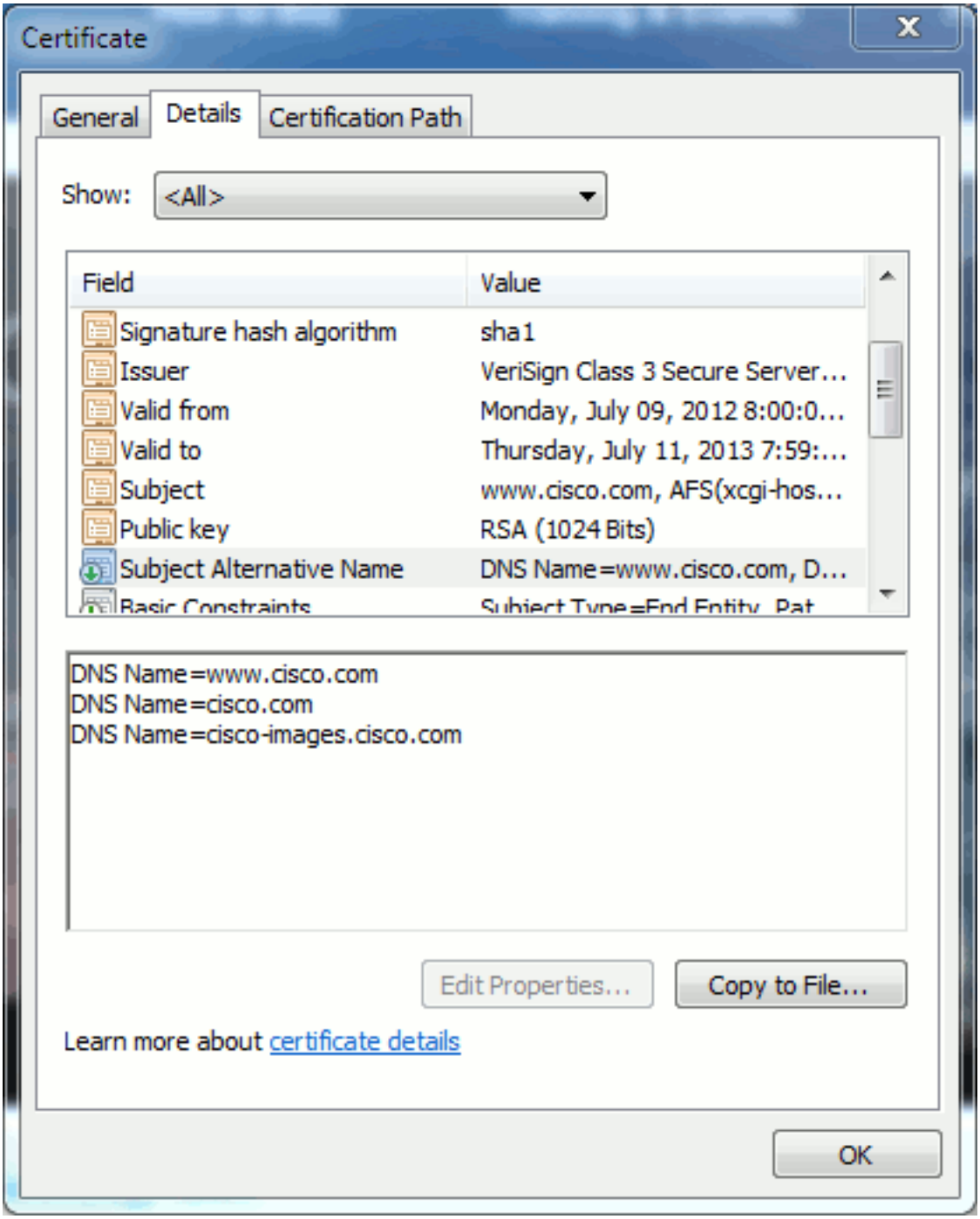
在圖7所示的示例中，證書的CN為www.cisco.com。來自瀏覽器的www.cisco.com的URL請求根據證書提供的資訊檢查URL FQDN。在這種情況下，它們將匹配，並顯示SSL握手成功。此網站已被驗證為正確的網站，並且現在已加密案頭與網站之間的通訊。

圖7:網站驗證



在同一證書中，有三個FQDN/DNS地址的SAN標頭：

圖8:SAN報頭



此憑證可驗證/驗證www.cisco.com（亦在CN中定義）、cisco.com和cisco-images.cisco.com。這表示您還可以輸入cisco.com，而此相同的憑證可用於驗證和加密此網站。

CUCM可以建立SAN報頭。有關SAN報頭的詳細資訊，請參閱Jason Burn的文檔CUCM Uploading CCMAdmin Web GUI Certificates（CUCM在支援社群上上傳CCMAdmin Web GUI證書）。

萬用字元證書

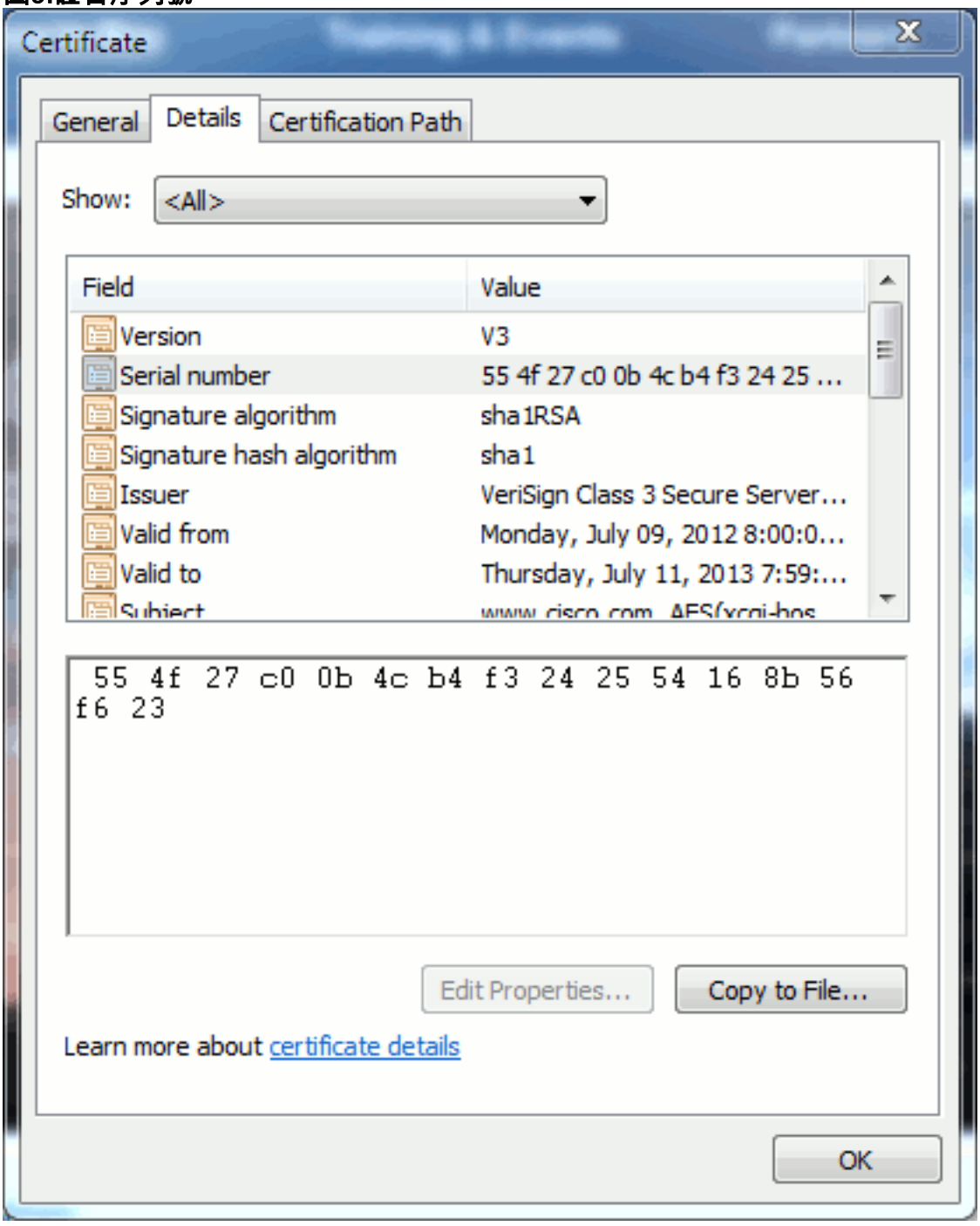
萬用字元證書是使用星號(*)表示URL部分中的任何字串的證書。例如，為了擁有www.cisco.com、ftp.cisco.com、ssh.cisco.com等的證書，管理員只需為*.cisco.com建立證書。為了節省資金，管理員只需購買一個證書，無需購買多個證書。

Cisco Unified Communications Manager(CUCM)目前不支援此功能。 但是您可以追蹤此增強功能：CSCta14114:請求在CUCM和私鑰匯入中支援萬用字元證書。

識別憑證

當證書中包含相同資訊時，您可以檢視它是否相同。所有證書都具有唯一的序列號。如果證書是相同的證書、重新生成的證書或偽造的證書，您可以使用此選項進行比較。圖9提供了一個示例：

圖9:證書序列號



企業社會責任及其目的

CSR代表證書簽名請求。如果要為CUCM伺服器建立第三方證書，則需要向CA提供CSR。此CSR看起來很像PEM(ASCII)憑證。

注意：這不是證書，不能用作證書。

CUCM通過Web GUI自動建立CSR:**Cisco Unified Operating System Administration > Security > Certificate Management > Generate CSR** >選擇要建立證書的服務>然後**Generate CSR**。每次使用

此選項時，都會生成新的私鑰和CSR。

注意：私鑰是此伺服器和服務所獨有的檔案。這個不應該給任何人！如果向某人提供私鑰，則會破壞憑證提供的安全性。此外，如果您使用舊的CSR建立憑證，請不要為相同服務重新產生新的CSR。CUCM會刪除舊的CSR和私密金鑰，並會替換這兩個金鑰，這使得舊的CSR毫無用處。

請參閱Jason Burn在支援社群上的文檔：CUCM上傳CCMAdmin Web GUI證書以瞭解有關如何建立CSR的資訊。

在終端和SSL/TLS握手流程之間使用證書

握手協定是一系列順序消息，用於協商資料傳輸會話的安全引數。有關詳細資訊，請參閱SSL/TLS，其中記錄了握手協定中的消息序列。這些可在封包擷取(PCAP)中看到。 詳細資訊包括在客戶端和伺服器之間傳送和接收的初始消息、後續消息和最終消息。

CUCM如何使用證書

Tomcat與tomcat-trust的區別

將證書上傳到CUCM時，通過**Cisco Unified Operating System Administration > Security > Certificate Management > Find**為每個服務提供兩個選項。

在CUCM中允許管理**證書**的五個服務是：

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

以下是允許您將憑證**上傳**到CUCM的服務：

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

以下是CUCM 8.0版及更高版本中提供的服務：

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

有關這些證書型別的詳細資訊，請參閱CUCM安全指南（按版本）。本節僅說明服務憑證和信任憑

證之間的差異。

例如，使用**tomcat**時，**tomcat-trust**會上傳CA和中間證書，以便此CUCM節點知道它可以信任由CA和中間伺服器簽署的任何證書。tomcat證書是此伺服器上tomcat服務提供的證書（如果終端向此伺服器發出HTTP請求）。為了允許通過tomcat顯示第三方證書，CUCM節點需要知道它可以信任CA和中間伺服器。因此，上傳tomcat（服務）憑證之前需要上傳CA和中間憑證。

請參閱Jason Burn的CUCM Uploading CCMAdmin Web GUI Certificates，瞭解可幫助您瞭解如何將證書上傳到CUCM的資訊。

每個服務都有自己的服務證書和信任證書。他們不是靠彼此來工作的。換句話說，Callmanager服務不能使用作為tomcat-trust服務上載的CA和中間證書。

注意：CUCM中的證書基於每個節點。因此，如果需要將證書上傳到發佈伺服器，並且需要訂閱者具有相同的證書，則需要在CUCM 8.5版之前將證書上傳到各個伺服器和節點。在CUCM 8.5版及更高版本中，有一個服務將上傳的證書複製到群集中的其餘節點。

註：每個節點具有不同的CN。因此，每個節點必須建立CSR，服務才能顯示自己的證書。

如果您對任何CUCM安全功能有其他特定問題，請參閱安全文檔。

結論

本文檔幫助並構建有關證書的高級知識。此主題可能會更加深入，但本文檔已足夠熟悉證書。如果您對任何CUCM安全功能有疑問，請參閱CUCM安全指南（按版本）瞭解更多資訊。

相關資訊

- **思科統一通訊管理器(CallManager)維護和安全指南**
- **思科整合通訊管理員(CallManager)**
- **Cisco整合通訊管理員Express版本**
- **思科支援社群：CUCM上傳CCMAdmin Web GUI證書**
- **錯誤CSCta14114:請求在CUCM和私鑰匯入中支援萬用字元證書**
- **已解釋Cisco Emergency Responder(CER)**
- **技術支援與文件 - Cisco Systems**