CUCM中的證書和頒發機構高級檢視

目錄

簡介

本檔案介紹憑證和憑證授權單位的基本概念。它補充提及思科統一通訊管理器(CUCM)中的任何加密或身份驗證功能的思科其他文檔。

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。這可以確認終端與預定裝置通訊，並且可以選擇加密兩個終端之間的資料。

注意：要瞭解每個證書的影響請參考Cisco Unified Communications Manager的證書重新生成過程中證書儲存部分的影響

從證書的觀點定義信任

證書最重要的部分是定義您的終端可以信任哪些終端。本檔案可協助您瞭解並定義資料加密的方式，以及資料與預定網站、電話、FTP伺服器等的共用方式。

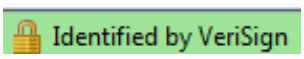
如果您的系統信任憑證，這表示您的系統上預先安裝憑證，表示它100%確信與正確的端點共用資訊。否則，它將終止這些終端之間的通訊。

非技術性範例就是您的駕駛執照。您使用本許可證（伺服器/服務證書）來證明自己就是您所說的人；您從在地機動車分公司處獲得了許可證（中間證書），該分公司已獲得您所在州機動車分公司（證書頒發機構）的許可。當您需要向主管出示您的許可證（伺服器/服務證書）時，主管知道他們可以信任DMV分支機構（中間證書）和機動車部門（證書頒發機構），並且他們可以驗證此許可證是由他們（證書頒發機構）頒發的。你的身份已經得到警官的確認現在他們相信你是你說的那個人。否則，如果您提供的錯誤許可證（伺服器/服務證書）未由DMV（中間證書）簽署，則他們將不會信任您所說的是誰。本文的其餘部分提供憑證階層的深入技術性說明。

瀏覽器如何使用憑證

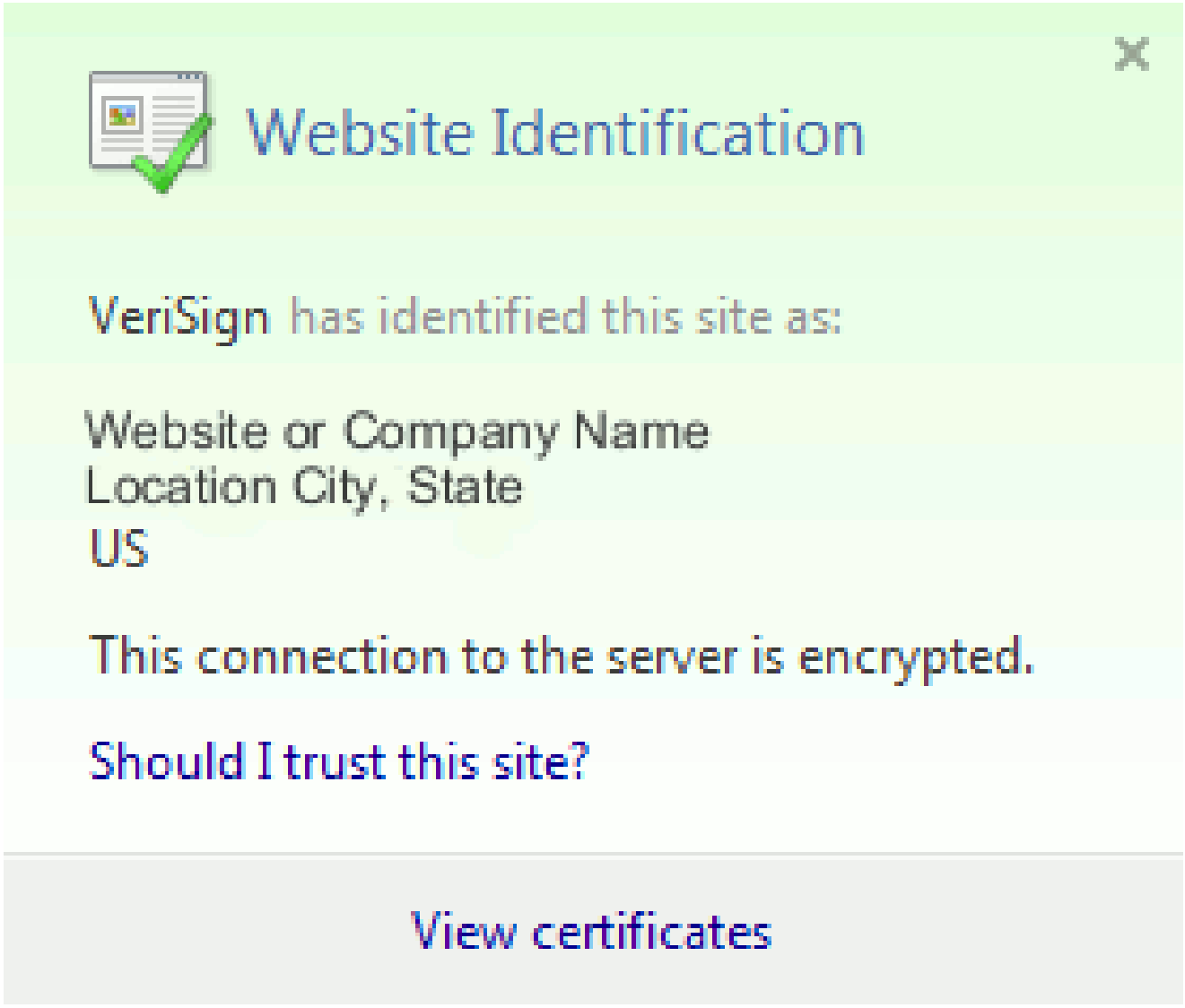
1. 當您訪問網站時，請輸入URL，例如http://www.cisco.com。
2. DNS會查詢託管該站點的伺服器的IP地址。
3. 瀏覽器會導覽至該網站。

如果沒有證書，就無法知道是否使用了非法DNS伺服器，或者您是否被路由到其他伺服器。憑證可確保您正確且安全地路由至預定網站，例如您的銀行網站，您輸入的個人或機密資訊在此是安全的。

所有瀏覽器都使用不同的圖示，但通常您會在地址列中看到掛鎖，如下所示： 

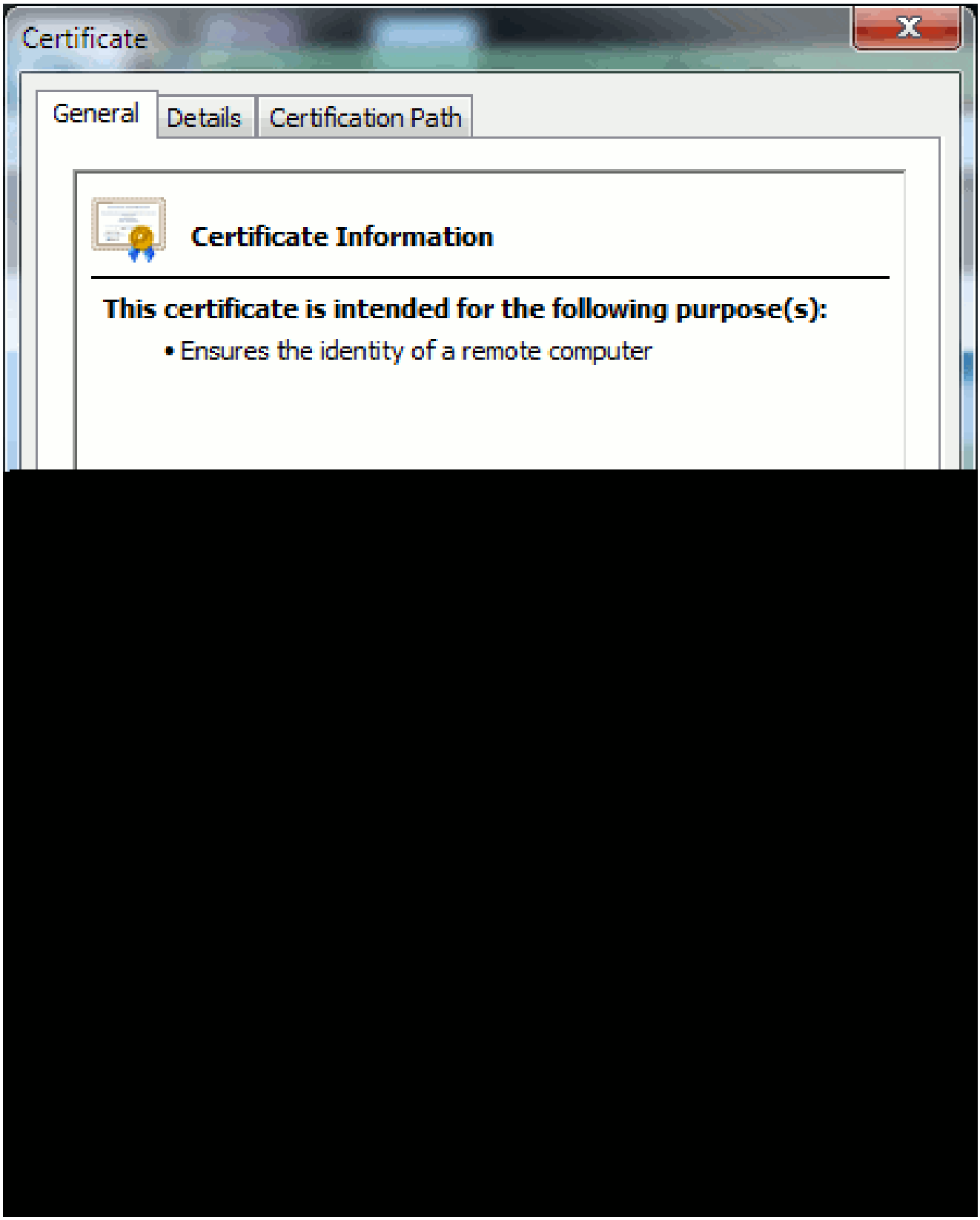
1. 按一下掛鎖，即會顯示一個視窗：

   圖1：網站標識



2. 按一下View Certificates以檢視站點證書，如下例所示：

圖2： 「Certificate Information（證書資訊）」 、 「General（常規）」頁籤



突出顯示的資訊非常重要。

- 頒發者是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，但您會看到憑證無效。請務必檢查日期，以便您知道日期是否已過期。)

提示：最佳做法是在日曆中建立提醒，以便在證書過期之前對其進行續訂。這可防止未來出現問題。

PEM與DER憑證之間的差異

PEM為ASCII；DER為二進位制。圖3顯示了PEM證書格式。

圖3： PEM證書示例

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-----
```

圖4顯示了DER證書。

圖4： DER證書示例

大多數CA公司（如VeriSign或Thawt）都使用PEM格式將證書傳送給客戶，因為這是一種電子郵件友好型格式。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，然後將其與副檔名.PEM或.CER一起儲存。

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

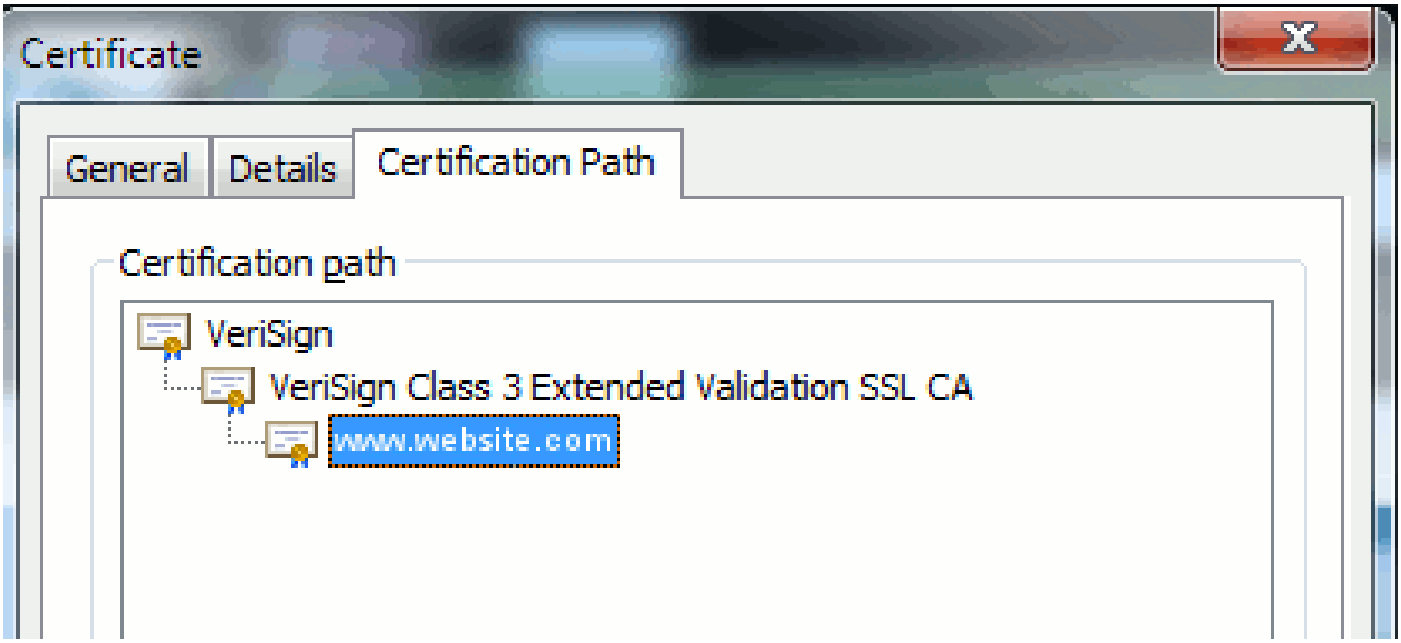
圖5：證書資訊

在某些情況下，裝置需要特定格式（ASCII或二進位制）。要更改此設定，請以所需格式從CA下載證書或使用SSL轉換器工具，例如https://www.sslshopper.com/ssl-converter.html。

憑證階層

要信任來自終端的證書，必須已經與第三方CA建立了信任。例如，圖6顯示了一個由三個證書組成的層次結構。

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自己可以信任CA和中間證書，才能知道自己可以信任SSL握手提供的伺服器證書（詳細資訊如下）。要更好地瞭解此信任如何工作，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證書的簽名者，以及您是否信任他們。

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

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，用於控制伺服器/服務證書的有效性。

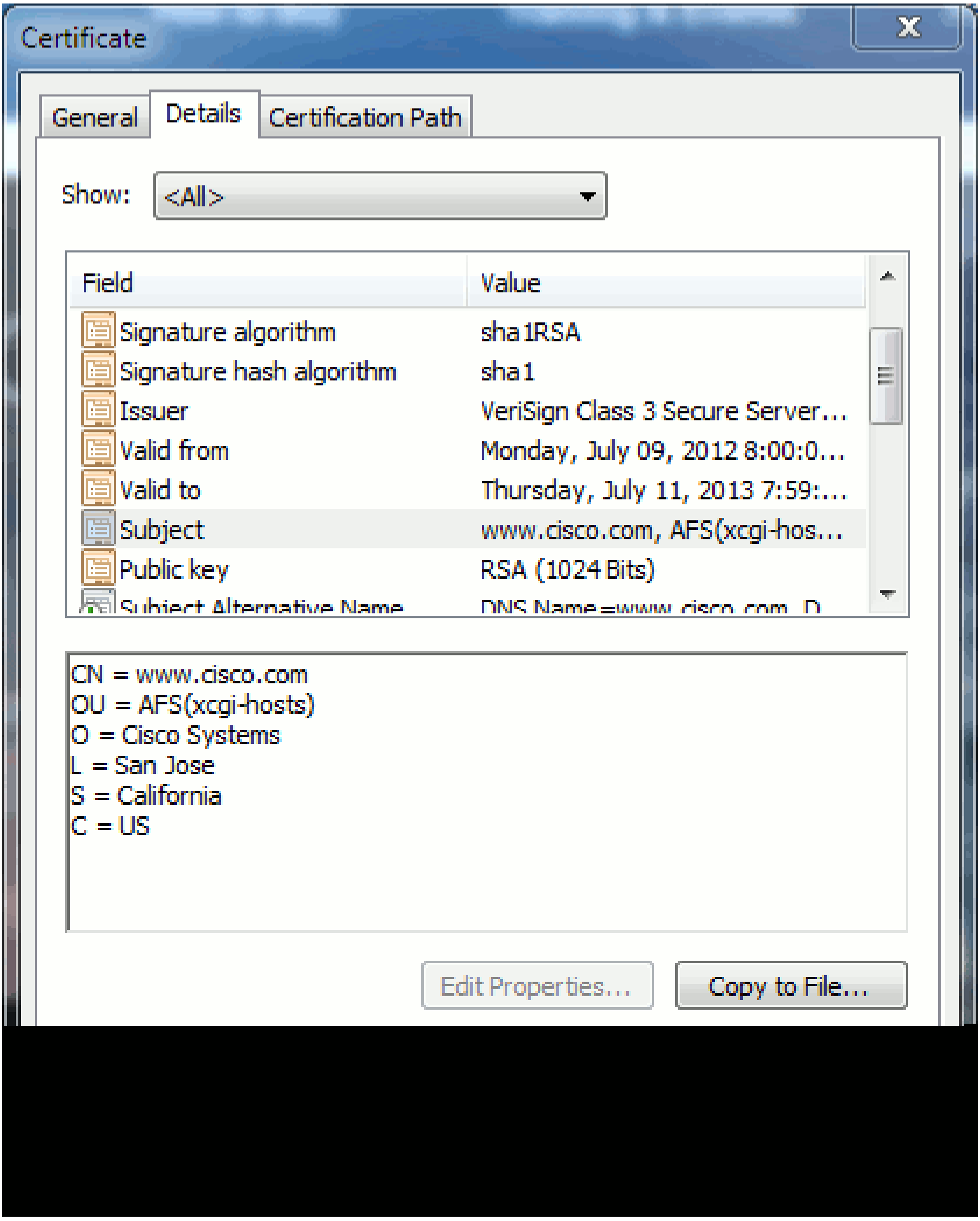
每個都可以是CA。系統是否信任該CA才是最重要的。

常用名稱和主題替代名稱

通用名稱(CN)和主題備用名稱(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。

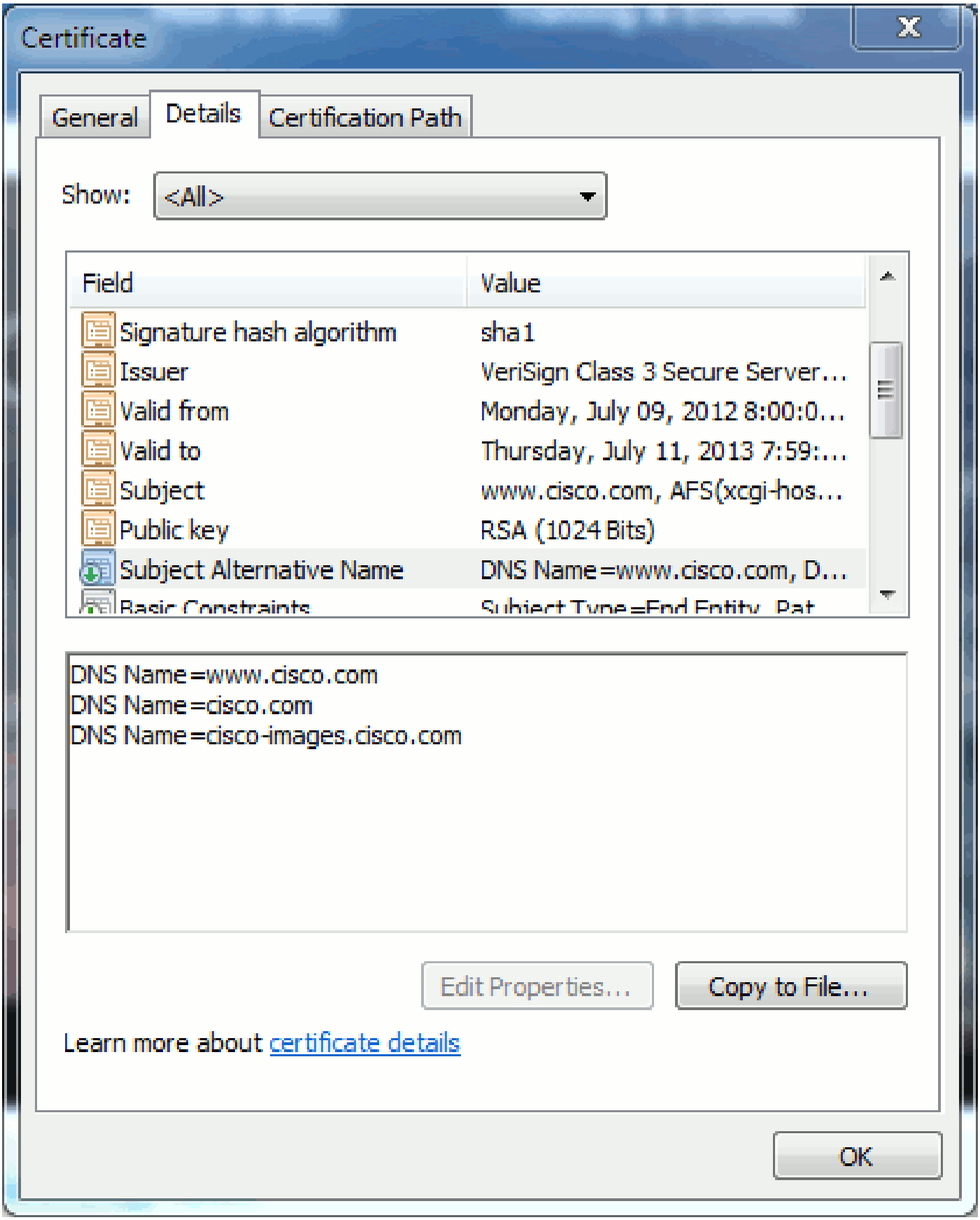
在圖7所示的示例中，證書的CN為www.cisco.com。瀏覽器對www.cisco.com的URL請求根據證書提供的資訊檢查URL FQDN。在本例中，它們匹配，並顯示SSL握手成功。此網站已經過驗證，是正確的網站，而且現在已加密案頭和網站之間的通訊。

圖7：網站驗證



在同一證書中，有三個FQDN/DNS地址的SAN報頭：

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。這表示您也可以輸入cisco.com，而此相同憑證也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，請參閱支援社群上的Jason Burn文檔CUCM上傳CCMAdmin Web GUI證書。

萬用字元憑證

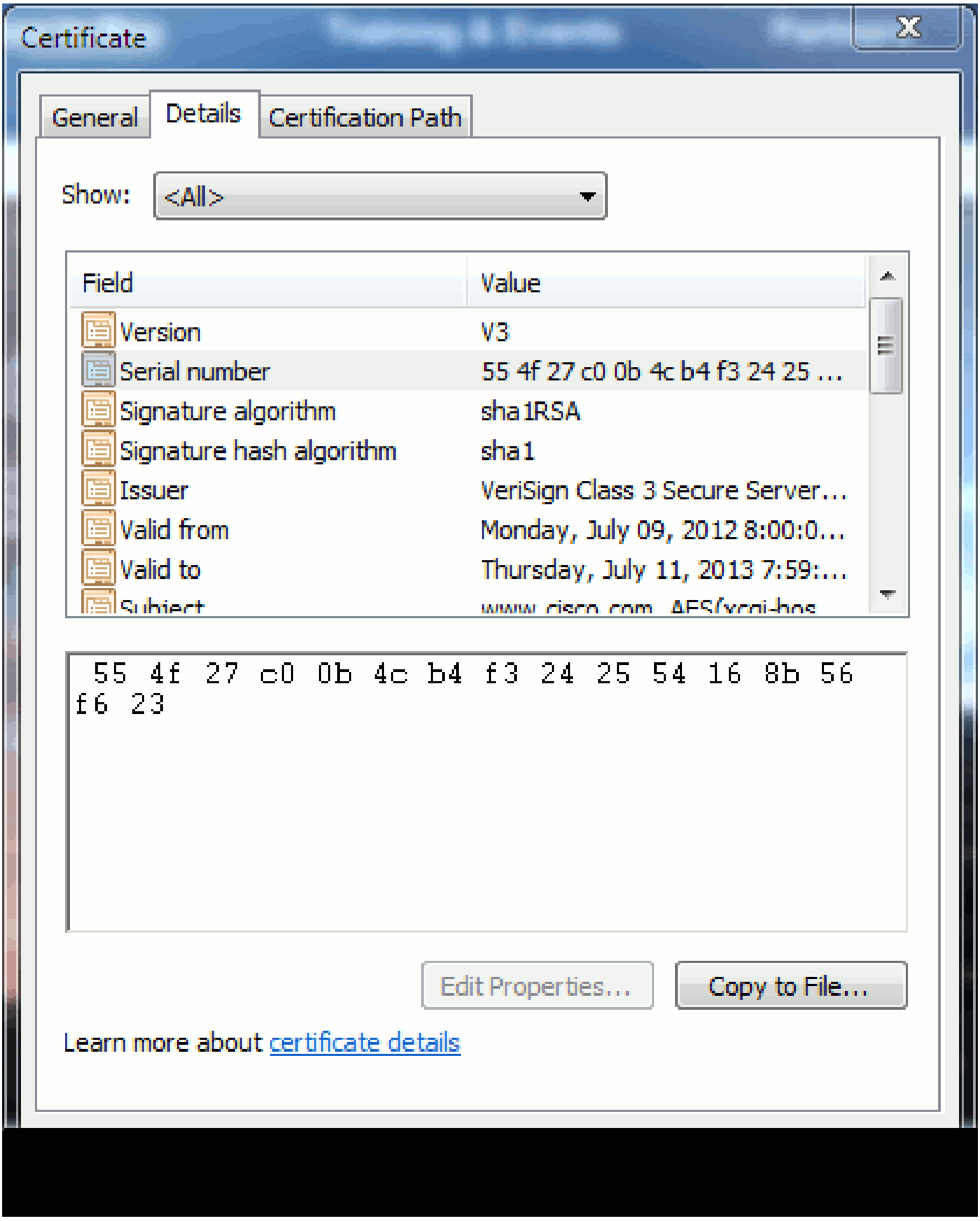
萬用字元憑證是使用星號(*)表示URL部分中的任何字串的證書。例如，要擁有www.cisco.com、ftp.cisco.com、ssh.cisco.com等的證書，管理員只需建立*.cisco.com的證書。為了節省成本，管理員只需要購買一個憑證，而不需要購買多個憑證。

Cisco Unified Communications Manager (CUCM)當前不支援此功能。但是，您可以跟蹤此增強功能：CSCta14114：請求支援CUCM和私鑰導入中的萬用字元憑證。

辨識憑證

當證書中包含相同資訊時，您可以看到它是否相同。所有證書都有唯一的序列號。如果證書是相同的證書、重新生成的證書或偽造的證書，您可以使用此命令進行比較。圖9提供了一個示例：

圖9：證書序列號



CSR及其目的

CSR代表憑證簽署請求。如果您要為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透過Web GUI自動建立CSR：思科統一作業系統管理>安全>證書管理>生成CSR，選擇您要建立證書的服務snf，然後生成CSR。每次使用此選項時，都會生成一個新的私鑰和CSR。

注意：私鑰是此伺服器和服務獨有的檔案。這個永遠不應該給任何人！如果向某人提供私鑰，則會危及證書提供的安全性。此外，如果您使用舊的CSR建立憑證，請勿為相同服務重新產生新的CSR。CUCM會刪除舊CSR和私鑰並替換兩者，從而使舊CSR毫無用處。

有關如何建立CSR的資訊，請參閱Jason Burn在支援社群：CUCM上傳CCMAdmin Web GUI證書上的文檔。

在終端和SSL/TLS握手進程之間使用證書

握手協定是一系列經過排序的消息，用於協商資料傳輸會話的安全引數。請參閱SSL/TLS in Detail，其中記錄了握手協定中的消息序列。這些可以在封包擷取(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、後續和最終消息。

CUCM如何使用證書

Tomcat和tomcat-trust之間的區別

當證書上傳到CUCM時，透過思科統一作業系統管理>安全>證書管理 >查詢為每個服務提供了兩個選項。

允許您管理CUCM中證書的五種服務是：

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

以下是允許您上傳證書到CUCM的服務：

- 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務：

- tvs
- tvs-trust
- 電話信任
- Phone-vpn-trust
- Phone-sast-trust
- phone-ctl-trust

有關這些型別的證書的更多詳細資訊，請參閱各版本的CUCM安全指南。本節僅說明服務憑證與信任憑證之間的差異。

例如，對於tomcat，tomcat-trust會上傳CA和中間證書，以便此CUCM節點知道它可信任由CA和中間伺服器簽署的任何證書。Tomcat證書是終端向此伺服器發出HTTP請求時，Tomcat服務在此伺服器上提供的證書。為了允許透過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）憑證前必須先上傳CA和中間憑證。

有關可幫助您瞭解如何將證書上傳到CUCM的資訊，請參閱支援社群上的Jason Burn的CUCM上傳CCMAdmin Web GUI證書。

每個服務都有自己的服務證書和信任證書。它們不會相互依賴。換句話說，作為tomcat-trust服務上傳的CA和中間證書不能由CallManager服務使用。

注意：CUCM中的證書按節點分配。因此，如果您需要將證書上傳到發佈伺服器，並且您需要使用者具有相同的證書，則需要將這些證書上傳到CUCM版本8.5之前的每個伺服器和節點。在CUCM版本8.5及更高版本中，有一種服務可將上傳的證書複製到集群中的其餘節點。

注意：每個節點都有不同的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安全功能有其他具體問題，請參閱安全文檔。

結論

本文檔幫助和建立有關證書的高水準知識。此主題可能會更加深入，但本文檔已足夠熟悉證書的使用。如果您對任何CUCM安全功能有疑問，請參閱各版本的CUCM安全指南瞭解更多資訊。

相關資訊

- Cisco Unified Communications Manager (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和私鑰導入中支援萬用字元憑證
- Cisco Emergency Responder (CER)介紹
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。