Allgemeine Übersicht über Zertifikate und Behörden in CUCM

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
  - Konventionen
- Zweck von Zertifikaten
  - Vertrauenswürdigkeit aus Sicht eines Zertifikats definieren
  - Verwendung von Zertifikaten durch Browser
- Unterschiede zwischen PEM- und DER-Zertifikaten
- Zertifikatshierarchie
  - Selbstsignierte Zertifikate im Vergleich zu Zertifikaten von Drittanbietern
- Gängige Namen und alternative Bezeichnungen
  - Platzhalterzertifikate
  - Identifizieren der Zertifikate
  - CSRs und deren Zweck
- Verwendung von Zertifikaten zwischen Endpunkt und SSL/TLS-Handshake-Prozess
- Verwendung von Zertifikaten durch CUCM
  - Der Unterschied zwischen Tomcat und Tomcat-Vertrauen
- Schlussfolgerung
- Zugehörige Informationen

Einleitung

Dieses Dokument beschreibt die Grundlagen von Zertifikaten und Zertifizierungsstellen. Es ergänzt andere Cisco Dokumente, die sich auf Verschlüsselungs- oder Authentifizierungsfunktionen in Cisco Unified Communications Manager (CUCM) beziehen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Zweck von Zertifikaten

Zertifikate werden zwischen Endpunkten verwendet, um Vertrauen/Authentifizierung und Datenverschlüsselung zu erstellen. Dadurch wird bestätigt, dass die Endpunkte mit dem beabsichtigten Gerät kommunizieren und die Möglichkeit haben, die Daten zwischen den beiden Endpunkten zu verschlüsseln.

Hinweis: Informationen zu den Auswirkungen der einzelnen Zertifikate finden Sie im Abschnitt Certificate Store unter Certificate Regeneration Process For Cisco Unified Communications Manager Impact by the Certificate Store.

Vertrauenswürdigkeit aus Sicht eines Zertifikats definieren

Der wichtigste Teil von Zertifikaten ist die Definition der Endpunkte, denen der Endpunkt vertrauen kann. Dieses Dokument hilft Ihnen zu wissen und zu definieren, wie Ihre Daten verschlüsselt sind und mit der beabsichtigten Website, Telefon, FTP-Server, und so weiter.

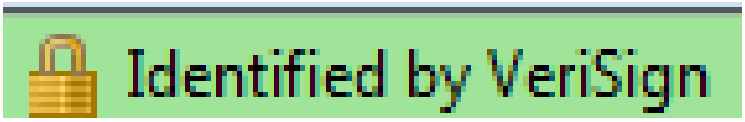
Wenn Ihr System einem Zertifikat vertraut, bedeutet dies, dass auf Ihrem System ein oder mehrere vorinstallierte Zertifikate vorhanden sind, die 100 % sicher sind, dass Informationen mit dem richtigen Endpunkt geteilt werden. Andernfalls wird die Kommunikation zwischen diesen Endpunkten beendet.

Ein nicht-technisches Beispiel dafür ist Ihr Führerschein. Sie verwenden diese Lizenz (Server-/Dienstleistungszertifikat), um zu beweisen, dass Sie der sind, der Sie sind; Sie haben Ihre Lizenz von Ihrer örtlichen Abteilung für Kraftfahrzeuge (Zwischenzertifikat) erhalten, die von der Abteilung für Kraftfahrzeuge (DMV) Ihres Staates (Zertifizierungsstelle) eine Genehmigung erhalten hat. Wenn Sie Ihre Lizenz (Server-/Servicebescheinigung) einem Offiziellen vorweisen müssen, weiß der Offizielle, dass er der DMV-Zweigstelle (Zwischenzertifikat) und der Division of Motor Vehicles (Zertifizierungsstelle) vertrauen kann, und er kann überprüfen, ob diese Lizenz von ihm ausgestellt wurde (Zertifizierungsstelle). Ihre Identität wird dem Offizier bestätigt, und jetzt vertrauen sie darauf, dass Sie der sind, der Sie zu sein behaupten. Wenn Sie andernfalls eine falsche Lizenz (Server-/Dienstzertifikat) vergeben, die nicht vom DMV (Zwischenzertifikat) signiert wurde, wird dem Benutzer nicht vertraut, der Sie angeblich sind. Im verbleibenden Teil dieses Dokuments finden Sie eine detaillierte technische Erläuterung der Zertifikatshierarchie.

Verwendung von Zertifikaten durch Browser

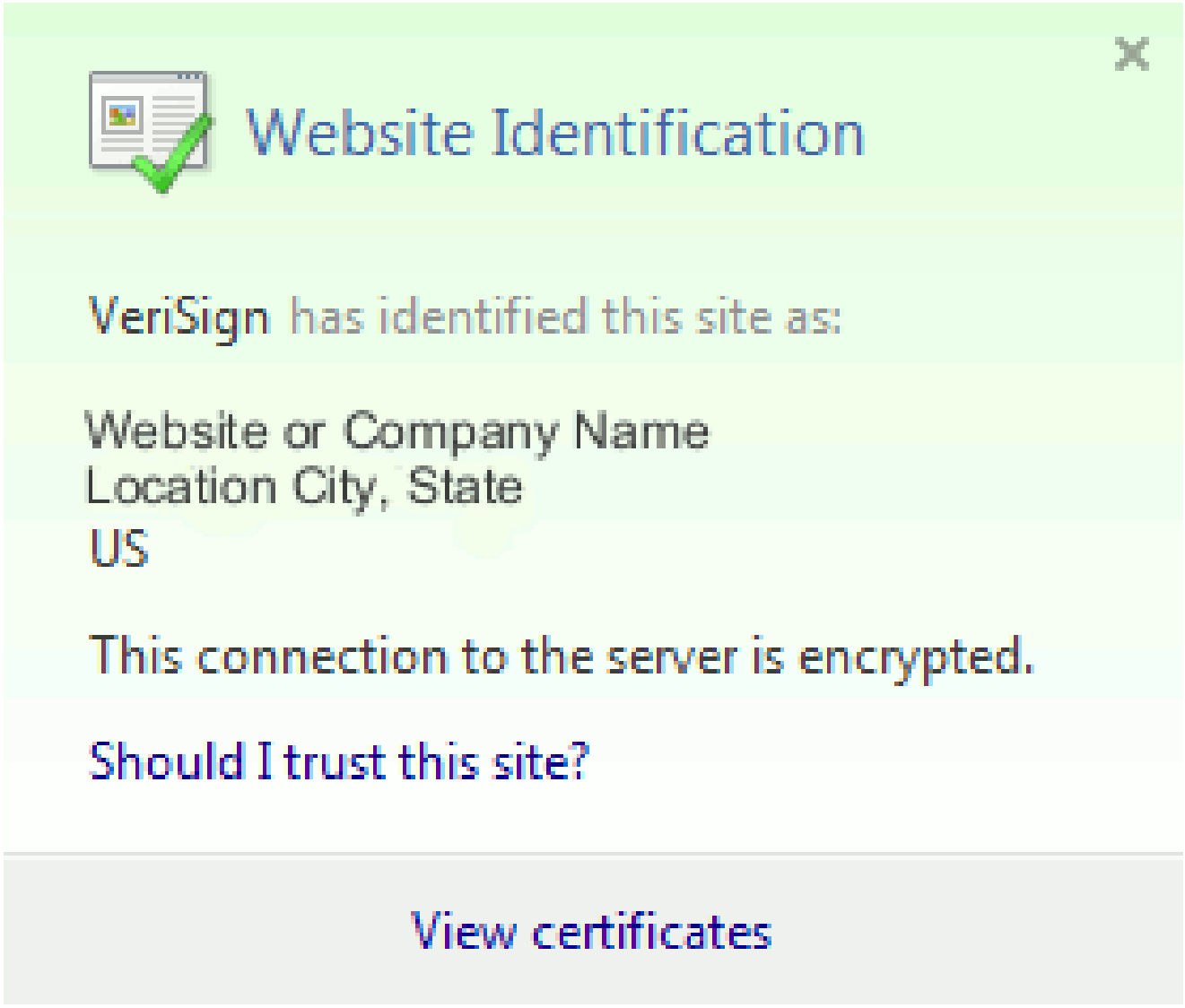
1. Wenn Sie eine Website besuchen, geben Sie die URL ein, z. B. http://www.cisco.com.
2. Der DNS findet die IP-Adresse des Servers, der diesen Standort hostet.
3. Der Browser navigiert zu dieser Site.

Ohne Zertifikate ist es unmöglich zu wissen, ob ein nicht autorisierter DNS-Server verwendet wurde oder ob Sie an einen anderen Server weitergeleitet wurden. Zertifikate stellen sicher, dass Sie ordnungsgemäß und sicher auf die beabsichtigte Website weitergeleitet werden, z. B. Ihre Bank-Website, auf der die von Ihnen eingegebenen persönlichen oder sensiblen Daten sicher sind.

Alle Browser verwenden unterschiedliche Symbole, aber normalerweise sieht man in der Adressleiste ein Vorhängeschloss wie dieses: 

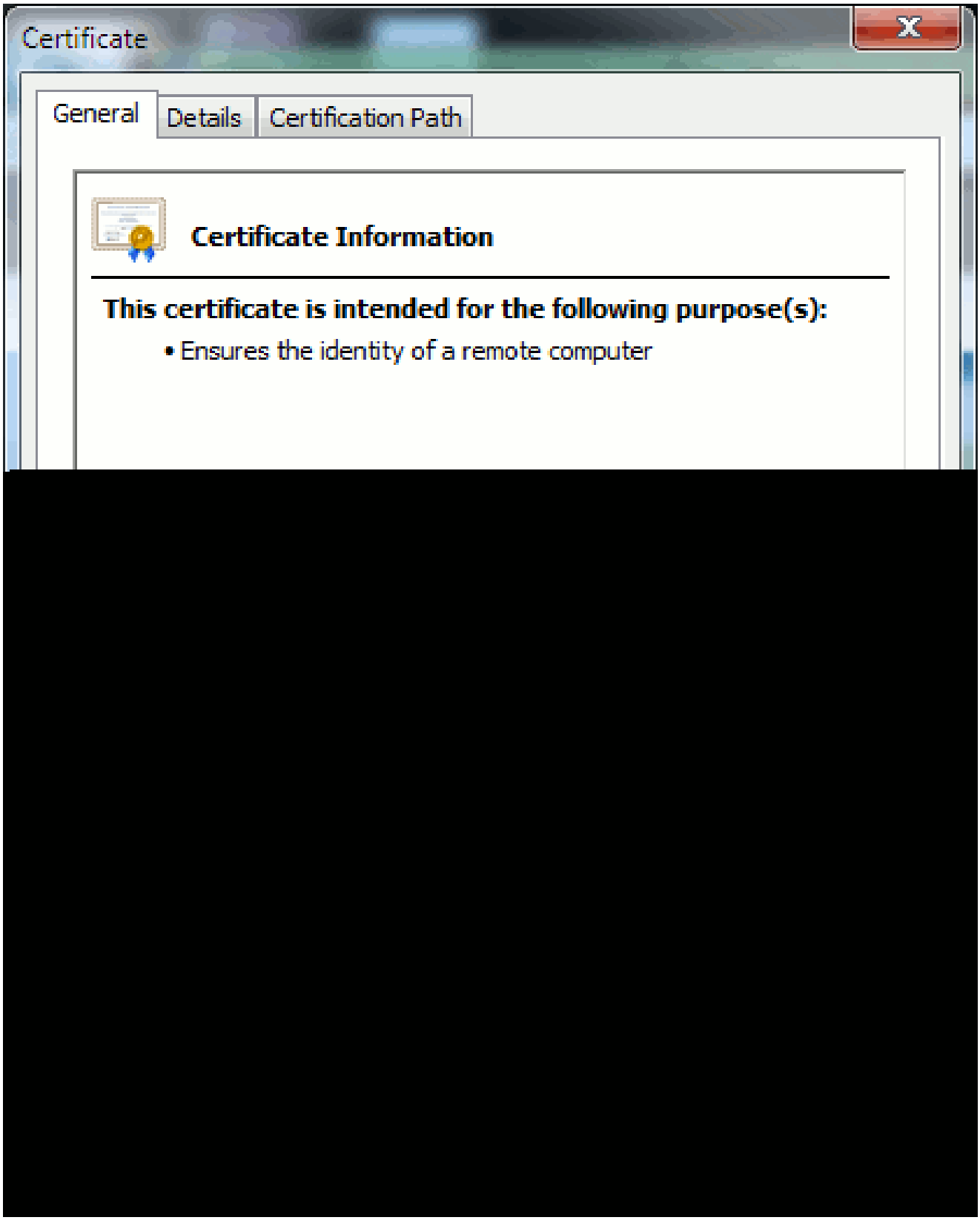
1. Klicken Sie auf das Vorhängeschloss, um ein Fenster anzuzeigen:

   Abbildung 1: Website-Identifizierung



2. Klicken Sie auf Zertifikate anzeigen, um das Zertifikat der Site anzuzeigen, wie in diesem Beispiel gezeigt:

   Abbildung 2: Zertifikatinformationen, Registerkarte "Allgemein"



Die hervorgehobenen Informationen sind wichtig.

- Ausgestellt von ist die Firma oder Zertifizierungsstelle, der Ihr System bereits vertraut.
- Gültig von/bis ist der Datumsbereich, in dem dieses Zertifikat verwendet werden kann. (Manchmal wird ein Zertifikat angezeigt, bei dem Sie wissen, dass Sie der Zertifizierungsstelle vertrauen, aber das Zertifikat ist ungültig. Überprüfen Sie immer

das Datum, damit Sie wissen, ob es abgelaufen ist.)

Tipp: Es empfiehlt sich, eine Erinnerung in Ihrem Kalender zu erstellen, um das Zertifikat vor Ablauf zu erneuern. So werden zukünftige Probleme vermieden.

Unterschiede zwischen PEM- und DER-Zertifikaten

PEM ist ASCII; DER ist binär. Abbildung 3 zeigt das PEM-Zertifikatformat.

Abbildung 3: PEM-Zertifikatbeispiel

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
BQcDAgYIKwYBBQUHAwUwKQYDVR0RBCIwIIIOODUxUHViLmtqbC5jb22CDnBob25l
cy5ramwuY29tMB0GA1UdDgQWBBTbWvEUfpl7hvrsTJpQfmcoNpB4LzANBgkqhkiG
9w0BAQUFAAOCAQEAr2Weqarg4tagW0O0rQElZj6UJ9S8ZAcp9XDT4Iz1QwRaaiBr
EBhfulaMjmtMKXFV5eCU9QcPbPG8XmiRZiEg9Q8Wtn0OZpuPGlkwxmFYRz40aY4T
5lw+d0wVb9sPChNQEGccjjqwtstElYWDo/A4RoqdH0ALceP8a4bovK/CpmRGdb5C
+hqP4zIJs4P+YKmzrJeq7H8xCCqqkYXcRLkmG6mif78txFQ5lr8rJEoU1VlL8znc
fJvSfEsCfwnSqPaGcQTnxMOZOIyM0OjXvvhWIezrpk8cyj3vSTgXSTwO53flZX4L
tu28d5H3AHo8U6cfHRIJ1f6Yv2ClGBShXwFp6Q==
-----END CERTIFICATE-----
```

Abbildung 4 zeigt das DER-Zertifikat.

Abbildung 4: Beispiel für das DER-Zertifikat

Die meisten CA-Unternehmen wie VeriSign oder Thawt verwenden das PEM-Format, um die Zertifikate an Kunden zu senden, da es E-Mail-freundlich ist. Der Kunde sollte die gesamte Zeichenfolge kopieren und -----BEGIN CERTIFICATE - und -----END CERTIFICATE - einschließen, sie in eine Textdatei einfügen und mit der Erweiterung .PEM oder .CER speichern.

Windows kann die DER- und CER-Formate mit einem eigenen Zertifikatsverwaltungs-Applet lesen und zeigt das Zertifikat wie in Abbildung 5 dargestellt an.

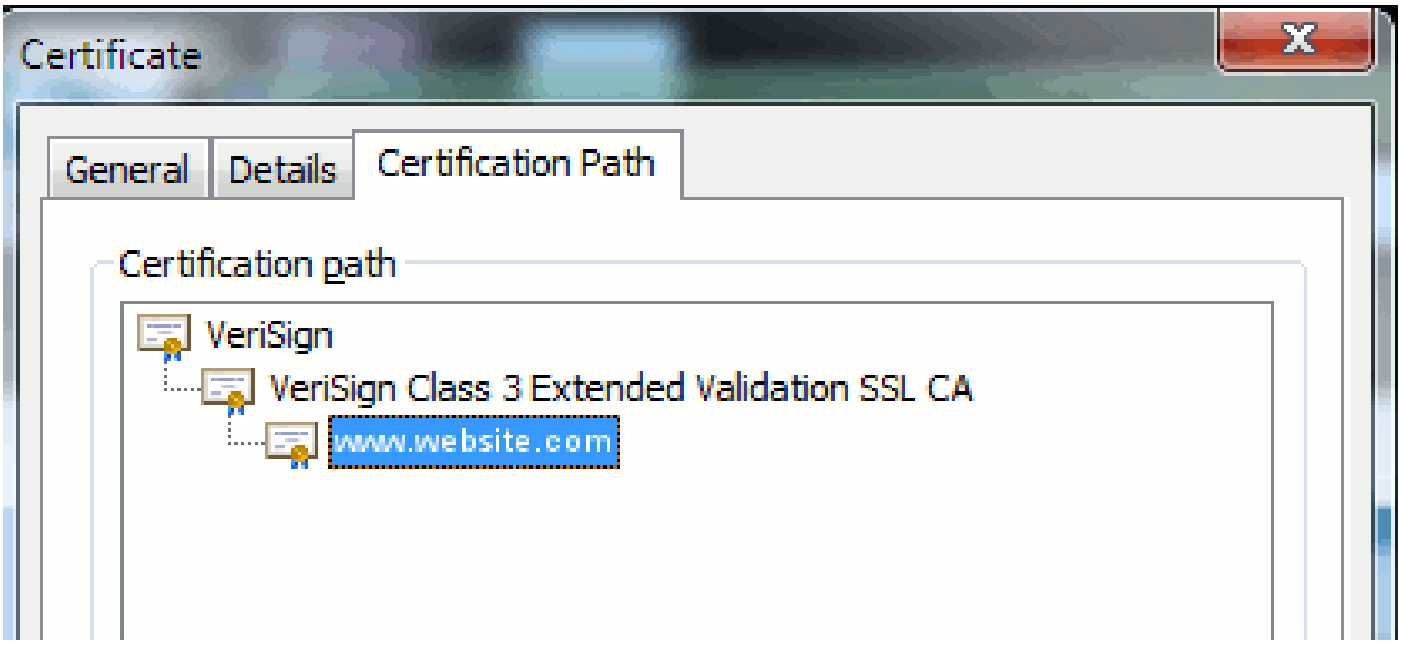
Abbildung 5: Zertifikatinformationen

In einigen Fällen benötigt ein Gerät ein bestimmtes Format (ASCII oder binär). Um dies zu ändern, laden Sie das Zertifikat von der Zertifizierungsstelle im erforderlichen Format herunter, oder verwenden Sie ein SSL-Konvertierungstool, z. B. https://www.sslshopper.com/ssl-converter.html.

Zertifikatshierarchie

Damit ein Zertifikat von einem Endpunkt als vertrauenswürdig eingestuft werden kann, muss bereits eine Vertrauensstellung mit einer Drittanbieter-Zertifizierungsstelle eingerichtet sein. Abbildung 6 zeigt beispielsweise eine Hierarchie von drei Zertifikaten.

Abbildung 6: Zertifikathierarchie



- Überprüfen, ob eine Zertifizierungsstelle vorhanden ist.
- Verisign Class 3 Extended Validation SSL CA ist ein Zwischenzertifikat oder ein signierendes Serverzertifikat (ein Server, der von CA autorisiert wurde, Zertifikate in seinem Namen auszustellen).
- www.website.com ist ein Server- oder Dienstzertifikat.

Der Endpunkt muss wissen, dass er zuerst sowohl dem CA- als auch dem Zwischenzertifikat vertrauen kann, bevor er weiß, dass er dem Serverzertifikat vertrauen kann, das vom SSL Handshake präsentiert wird (Details weiter unten). Um besser zu verstehen, wie diese Vertrauensstellung funktioniert, lesen Sie den Abschnitt in diesem Dokument: Definieren Sie "Vertrauen" aus der Sicht eines Zertifikats.

Selbstsignierte Zertifikate im Vergleich zu Zertifikaten von Drittanbietern

Die Hauptunterschiede zwischen selbstsignierten Zertifikaten und Zertifikaten von Drittanbietern

bestehen darin, wer das Zertifikat signiert hat, unabhängig davon, ob Sie es als vertrauenswürdig einstufen.

Ein selbstsigniertes Zertifikat ist ein Zertifikat, das vom Server signiert wird, der es präsentiert. Daher sind das Server-/Dienstzertifikat und das CA-Zertifikat identisch.

Eine Drittanbieter-Zertifizierungsstelle ist ein Dienst, der entweder von einer öffentlichen Zertifizierungsstelle (wie Verisign, Entrust, Digicert) oder von einem Server (wie Windows 2003, Linux, Unix, IOS) bereitgestellt wird, der die Gültigkeit des Servers/Dienstzertifikats steuert.

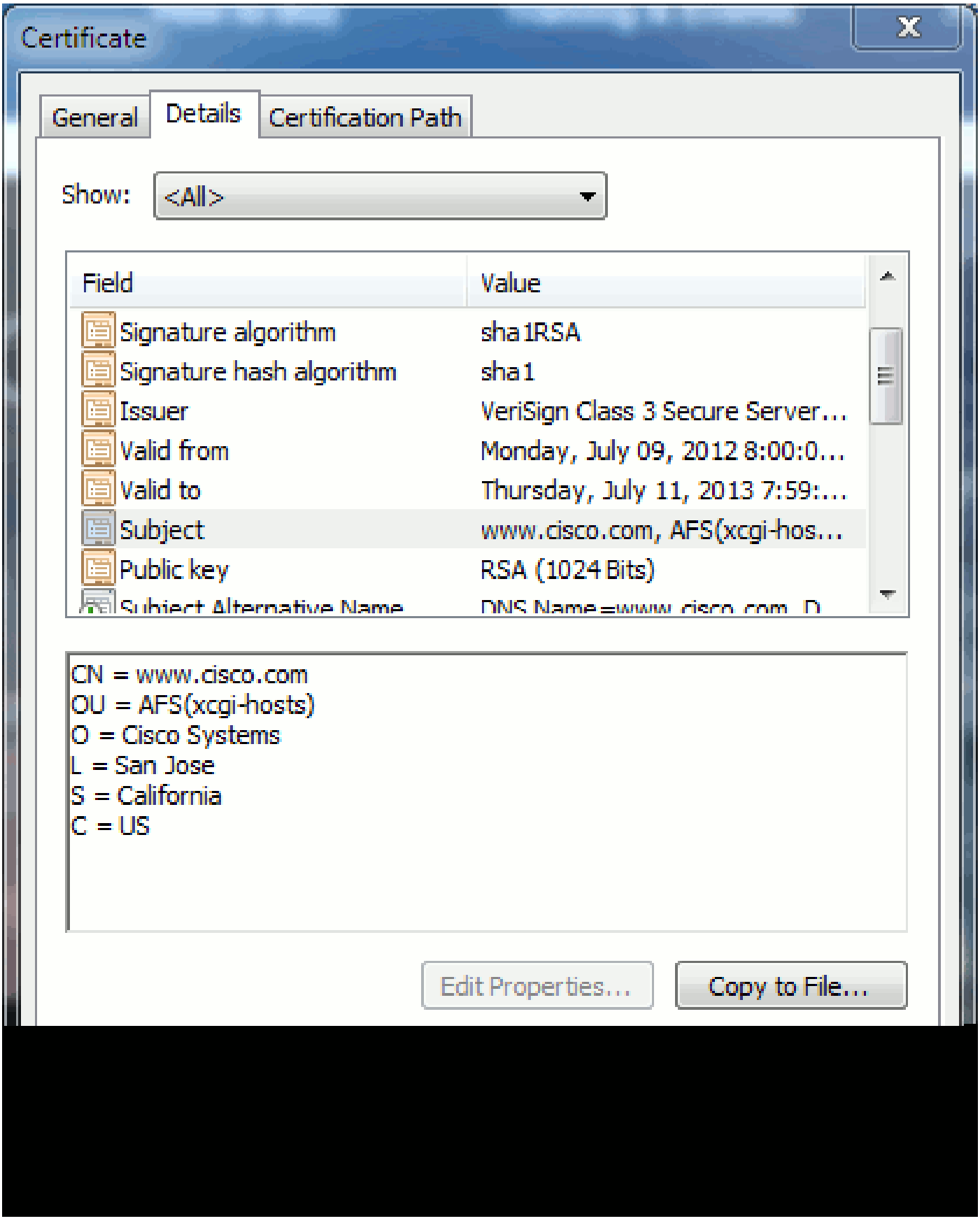
Jede kann eine Zertifizierungsstelle sein. Am wichtigsten ist, ob Ihr System dieser Zertifizierungsstelle vertraut oder nicht.

Gängige Namen und alternative Bezeichnungen

Common Names (CN) und Subject Alternative Names (SAN) sind Verweise auf die IP-Adresse oder den FQDN (Fully Qualified Domain Name) der angeforderten Adresse. Wenn Sie beispielsweise https://www.cisco.com eingeben, muss der CN oder SAN www.cisco.com im Header enthalten.

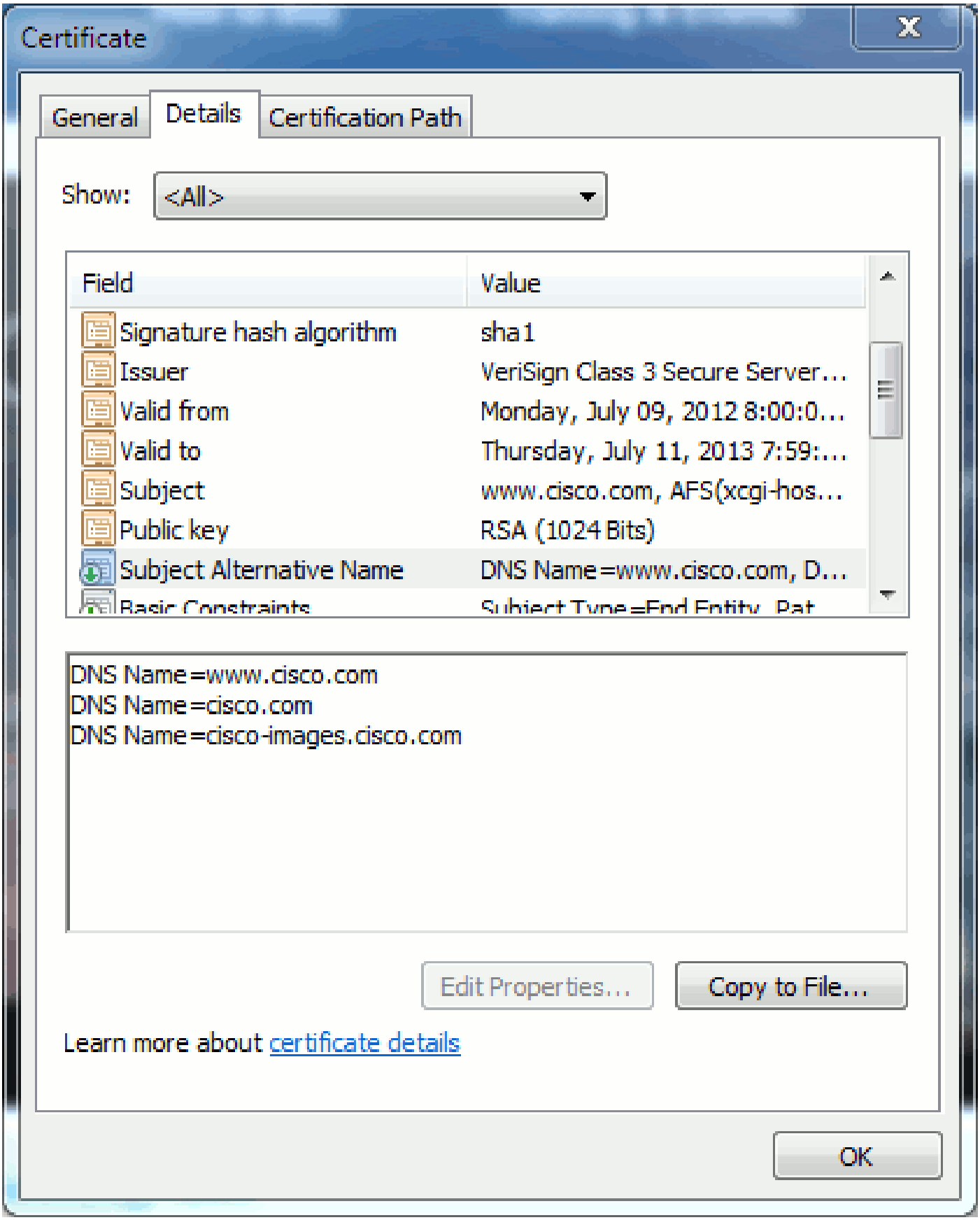
Im Beispiel in Abbildung 7 lautet der CN des Zertifikats www.cisco.com. Die URL-Anforderung für www.cisco.com vom Browser vergleicht den URL-FQDN mit den Informationen, die das Zertifikat enthält. In diesem Fall stimmen sie überein, und es zeigt an, dass der SSL-Handshake erfolgreich war. Diese Website wurde als korrekte Website verifiziert, und die Kommunikation zwischen dem Desktop und der Website wird jetzt verschlüsselt.

Abbildung 7: Überprüfung der Website



Im gleichen Zertifikat gibt es einen SAN-Header für drei FQDN/DNS-Adressen:

Abbildung 8: SAN-Header



Dieses Zertifikat kann www.cisco.com (auch in der CN definiert), cisco.com und cisco-images.cisco.com authentifizieren/verifizieren. Das bedeutet, dass Sie auch cisco.com eingeben können, und dasselbe Zertifikat kann verwendet werden, um diese Website zu authentifizieren und zu verschlüsseln.

CUCM kann SAN-Header erstellen. Weitere Informationen zu SAN-Headern finden Sie im Dokument "CUCM Uploading CCMAdmin Web GUI Certificates" (CCMAdmin-Web-GUI-Zertifikate) von Jason Burn in der Support Community.

Platzhalterzertifikate

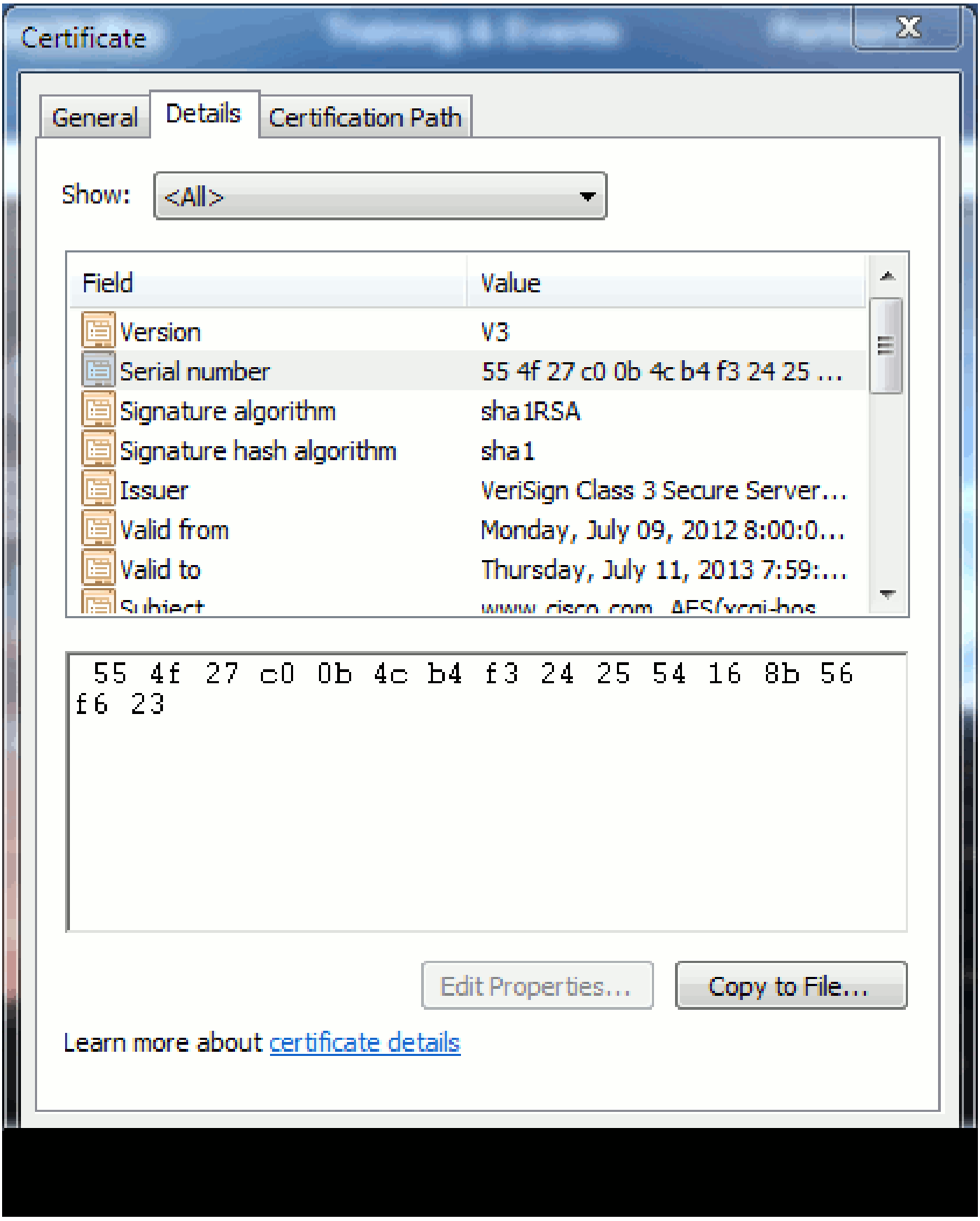
Platzhalterzertifikate sind Zertifikate, die ein Sternchen (*) verwenden, um eine beliebige Zeichenfolge in einem Abschnitt einer URL darzustellen. Um z. B. ein Zertifikat für www.cisco.com, ftp.cisco.com, ssh.cisco.com usw. zu erstellen, muss der Administrator nur ein Zertifikat für *.cisco.com erstellen. Um Geld zu sparen, muss der Administrator nur ein einzelnes Zertifikat erwerben und nicht mehrere Zertifikate.

Diese Funktion wird derzeit von Cisco Unified Communications Manager (CUCM) nicht unterstützt. Sie können diese Verbesserung jedoch verfolgen: CSCta14114: Anfrage nach Unterstützung eines Platzhalterzertifikats in CUCM und Import von privaten Schlüsseln.

Identifizieren der Zertifikate

Wenn Zertifikate dieselben Informationen enthalten, können Sie sehen, ob es sich um dasselbe Zertifikat handelt. Alle Zertifikate haben eine eindeutige Seriennummer. Sie können dies verwenden, um zu vergleichen, ob es sich bei den Zertifikaten um dieselben Zertifikate handelt, ob sie neu generiert oder gefälscht wurden. Abbildung 9 zeigt ein Beispiel:

Abbildung 9: Seriennummer des Zertifikats



CSRs und deren Zweck

CSR steht für Certificate Signing Request. Wenn Sie ein Drittanbieterzertifikat für einen CUCM-Server erstellen möchten, benötigen Sie einen CSR, der der Zertifizierungsstelle präsentiert wird.

Dieser CSR ähnelt stark einem PEM-Zertifikat (ASCII).

Hinweis: Dies ist kein Zertifikat und kann nicht als solches verwendet werden.

\

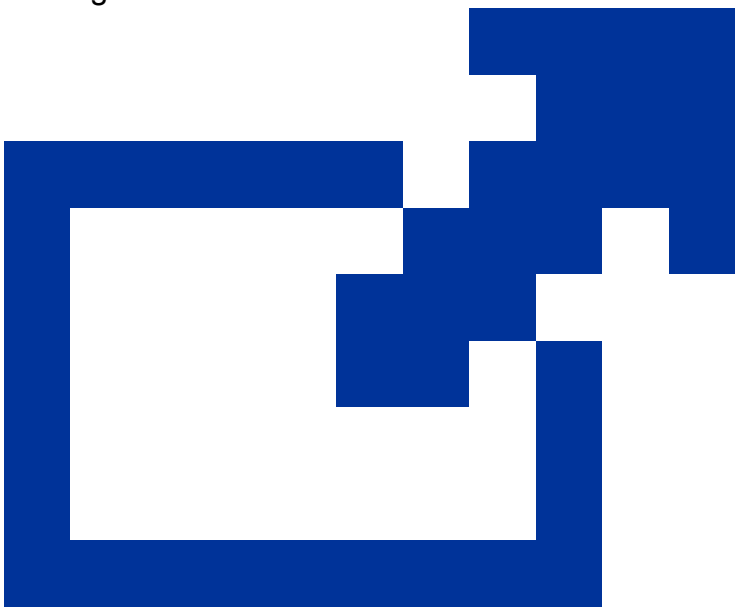
CUCM erstellt CSRs automatisch über die Web-GUI: Cisco Unified Operating System Administration > Security > Certificate Management > Generate CSR, wählen Sie den Service aus, den Sie für das Zertifikat erstellen möchten, und klicken Sie dann auf Generate CSR (CSR generieren). Bei jeder Verwendung dieser Option werden ein neuer privater Schlüssel und eine CSR-Anfrage generiert.

Hinweis: Ein privater Schlüssel ist eine Datei, die für diesen Server und Dienst eindeutig ist. Das sollte man niemals jemandem geben! Wenn Sie jemandem einen privaten Schlüssel bereitstellen, beeinträchtigt dies die Sicherheit, die das Zertifikat bietet. Generieren Sie auch keinen neuen CSR für denselben Service, wenn Sie den alten CSR zum Erstellen eines Zertifikats verwenden. CUCM löscht den alten CSR und den privaten Schlüssel und ersetzt beide, wodurch der alte CSR nutzlos wird.

Weitere Informationen zum Erstellen von CSRs finden Sie in der Dokumentation von Jason Burn zur Support Community: CUCM Uploading CCMAdmin Web GUI Certificates (CCMAdmin-Web-GUI-Zertifikate).

Verwendung von Zertifikaten zwischen Endpunkt und SSL/TLS-Handshake-Prozess

Beim Handshake-Protokoll handelt es sich um eine Reihe sequenzierter Nachrichten, die die Sicherheitsparameter einer Datenübertragungssitzung aushandeln. Weitere Informationen finden



Sie unter SSL/TLS im Detail
, das die Nachrichtensequenz im Handshake-Protokoll dokumentiert. Diese sind in der Paketerfassung (PCAP) erkennbar. Zu den Details gehören die ersten, nachfolgenden und letzten

Nachrichten, die zwischen dem Client und dem Server gesendet und empfangen wurden.

Verwendung von Zertifikaten durch CUCM

Der Unterschied zwischen Tomcat und Tomcat-Vertrauen

Wenn Zertifikate in CUCM hochgeladen werden, stehen für jeden Service zwei Optionen zur Verfügung: Cisco Unified Operating System Administration (Cisco Unified Operating System-Verwaltung) > Security (Sicherheit) > Certificate Management (Zertifikatsverwaltung) > Find (Suchen).

Die folgenden fünf Dienste ermöglichen das Verwalten von Zertifikaten in CUCM:

- tomcat
- IPsec
- callmanager
- capf
- tvs (in CUCM Version 8.0 und höher)

Mit den folgenden Services können Sie Zertifikate in CUCM hochladen:

- tomcat
- Tomcat-Trust
- IPsec
- IPSec-Trust
- callmanager
- Callmanager-Trust
- capf
- CAPF-Trust

Folgende Services sind in CUCM Version 8.0 und höher verfügbar:

- tvs
- TV-Trust
- phone-trust
- phone-vpn-trust

- phone-sast-trust
- phone-ctl-trust

Weitere Informationen zu diesen Zertifikatstypen finden Sie in den CUCM-Sicherheitsleitfäden nach Version. In diesem Abschnitt wird nur der Unterschied zwischen einem Dienstzertifikat und einem Vertrauenszertifikat erläutert.

Bei tomcat laden die tomcat-trusts beispielsweise die Zertifizierungsstelle und Zwischenzertifikate hoch, sodass dieser CUCM-Knoten weiß, dass er allen von der Zertifizierungsstelle und dem Zwischenzeitserver signierten Zertifikaten vertrauen kann. Das Tomcat-Zertifikat ist das Zertifikat, das vom Tomcat-Dienst auf diesem Server vorgelegt wird, wenn ein Endpunkt eine HTTP-Anforderung an diesen Server sendet. Um die Darstellung von Drittanbieterzertifikaten durch tomcat zu ermöglichen, muss der CUCM-Knoten wissen, dass er der CA und dem Zwischenserver vertrauen kann. Daher müssen die CA- und Zwischenzertifikate hochgeladen werden, bevor das Tomcat-(Service-)Zertifikat hochgeladen wird.

Informationen zum Hochladen von Zertifikaten für die CCMAdmin-Web-GUI in der Support Community finden Sie unter CUCM von Jason Burn.

Jeder Dienst verfügt über ein eigenes Dienstzertifikat und Vertrauenszertifikate. Sie arbeiten nicht voneinander ab. Mit anderen Worten: Eine CA und ein Zwischenzertifikat, die als ein Tomcat-Trust-Dienst hochgeladen wurden, können vom CallManager-Dienst nicht verwendet werden.

Hinweis: Zertifikate in CUCM gelten pro Knoten. Wenn Sie also Zertifikate in den Publisher hochladen müssen und die Abonnenten über dieselben Zertifikate verfügen müssen, müssen Sie diese vor CUCM 8.5 auf jeden einzelnen Server und Knoten hochladen. In CUCM Version 8.5 und höher gibt es einen Dienst, der hochgeladene Zertifikate auf die übrigen Knoten im Cluster repliziert.

Hinweis: Jeder Knoten hat eine andere CN. Aus diesem Grund muss von jedem Knoten ein CSR erstellt werden, damit der Dienst seine eigenen Zertifikate präsentieren kann.

Wenn Sie weitere spezifische Fragen zu den CUCM-Sicherheitsfunktionen haben, lesen Sie in der Sicherheitsdokumentation nach.

Schlussfolgerung

Dieses Dokument unterstützt Sie dabei, ein hohes Maß an Fachwissen über Zertifikate zu erwerben. Dieses Thema kann vertieft werden, aber dieses Dokument macht Sie ausreichend vertraut, um mit Zertifikaten zu arbeiten. Wenn Sie Fragen zu den CUCM-Sicherheitsfunktionen haben, finden Sie weitere Informationen in den CUCM-Sicherheitsleitfäden nach Version.

Zugehörige Informationen

- Cisco Unified Communications Manager (CallManager) - Wartungs- und Sicherheitsleitfäden
- Cisco Unified Communications Manager (Call Manager)
- Cisco Unified Communications Manager Express
- Cisco Support Community: CUCM lädt GUI-Zertifikate für CCMAdmin hoch
- Bug CSCta14114: Anfrage nach Unterstützung eines Platzhalter-Zertifikats in CUCM und Import eines privaten Schlüssels
- Cisco Emergency Responder (CER) im Überblick
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.