High Level View von Zertifikaten und Behörden in CUCM

Inhalt

Einführung

Zweck dieses Dokuments ist es, die Grundlagen der Zeugnisse und Zertifizierungsstellen zu verstehen. Dieses Dokument ergänzt andere Cisco Dokumente, die sich auf Verschlüsselungs- oder Authentifizierungsfunktionen in Cisco Unified Communications Manager (CUCM) beziehen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

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

Zweck der Zertifikate

Zertifikate werden zwischen Endpunkten verwendet, um eine Vertrauenswürdigkeit/Authentifizierung und Datenverschlüsselung zu erstellen. Damit wird bestätigt, dass die Endpunkte mit dem beabsichtigten Gerät kommunizieren und die Daten zwischen den beiden Endpunkten verschlüsseln können.

Definieren der Vertrauenswürdigkeit aus Sicht eines Zertifikats

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

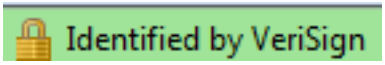
Wenn Ihr System einem Zertifikat vertraut, bedeutet dies, dass auf Ihrem System ein vorinstalliertes Zertifikat (bzw. vorinstallierte Zertifikate) vorhanden ist, das besagt, dass es zu 100 Prozent sicher ist, dass es Informationen mit dem richtigen Endpunkt austauscht. Andernfalls wird die Kommunikation zwischen diesen Endpunkten beendet.

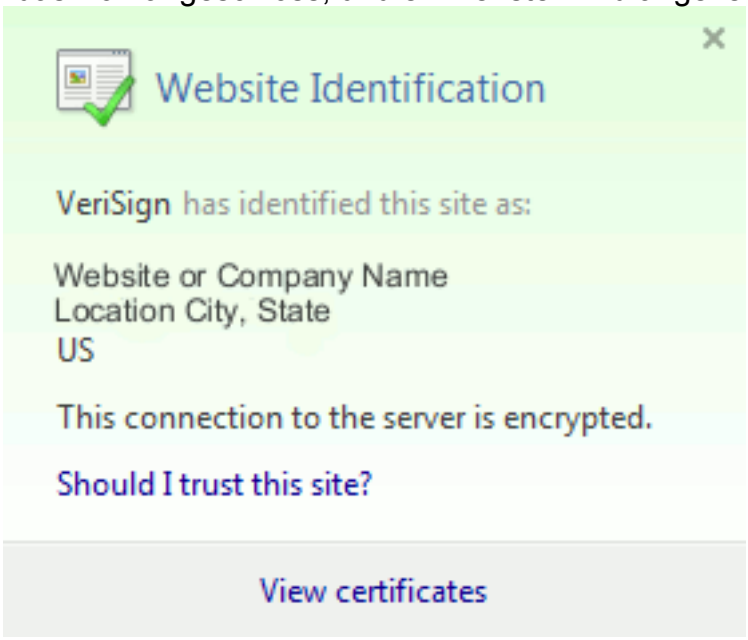
Ein nicht-technisches Beispiel dafür ist Ihr Führerschein. Sie verwenden diese Lizenz (Server-/Servicegutschrift), um zu beweisen, dass Sie der sind, für den Sie sich entschieden haben. Sie haben Ihren Führerschein von der örtlichen Zweigstelle für Kraftfahrzeuge (Zwischenzertifikat) erhalten, die von der Division der Kraftfahrzeuge (DMV) Ihres Staates (Zertifizierungsstelle) die Genehmigung erhalten hat. Wenn Sie einem Offizier Ihre Lizenz (Server-/Servicebescheinigung) vorlegen müssen, weiß der Offizier, dass er der DMV-Zweigstelle (Zwischenzertifikat) und der Division of Motor Vehicles (Zertifizierungsstelle) vertrauen kann, und er kann überprüfen, ob diese Lizenz von ihm erteilt wurde (Zertifizierungsstelle). Ihre Identität wird dem Offizier verifiziert, und jetzt vertrauen sie darauf, dass Sie sind, was Sie sagen. Andernfalls werden falsche Lizenzen (Server/Service-Zertifikat), die nicht von der DMV (Intermediate Certificate) signiert wurden, nicht vertrauenswürdig, wer Sie als sind. Im verbleibenden Teil dieses Dokuments finden Sie eine ausführliche technische Erläuterung der Zertifikatshierarchie.

Verwendung von Zertifikaten durch Browser

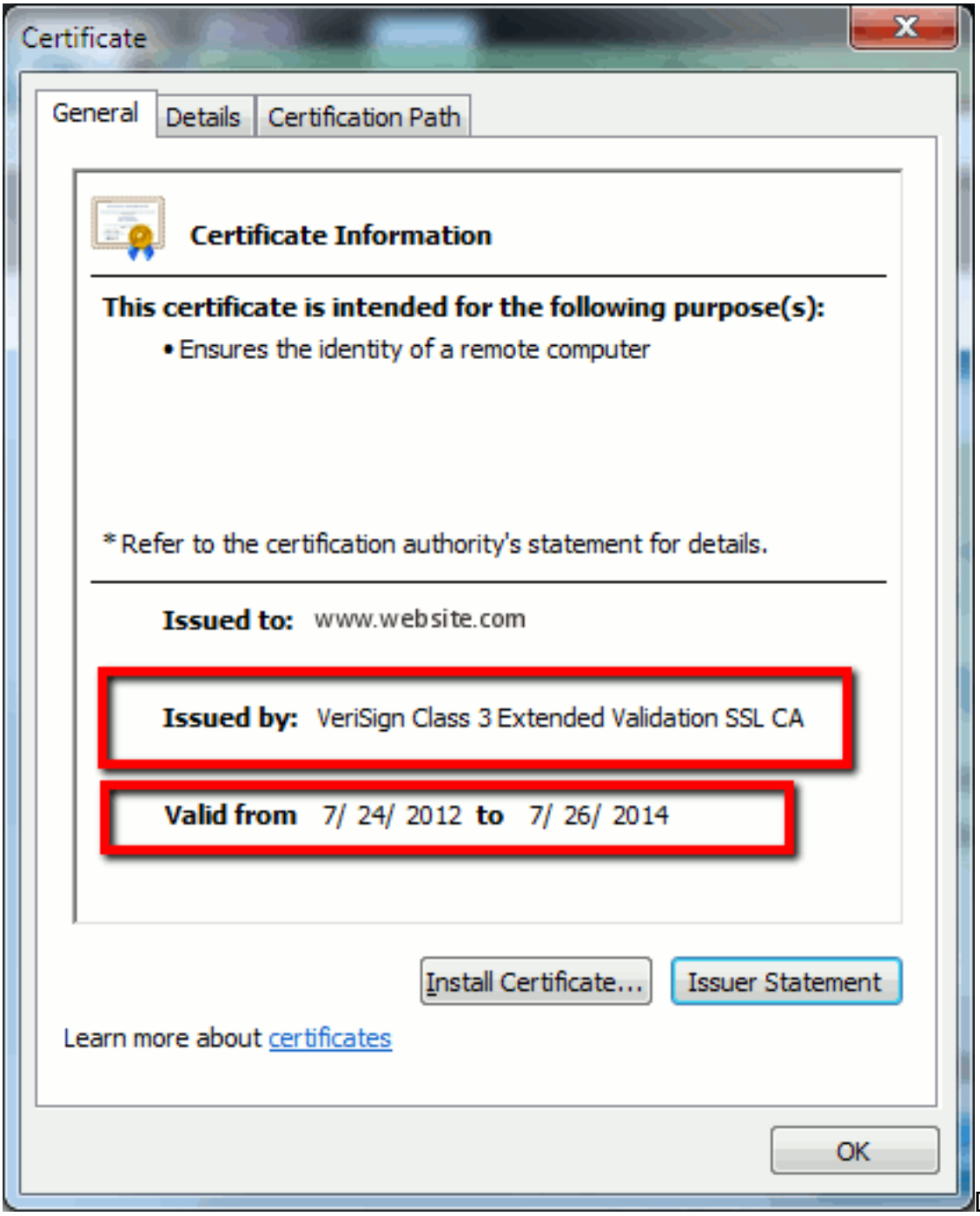
1. Wenn Sie eine Website besuchen, geben Sie die URL ein, z. B. http://www.cisco.com.
2. Der DNS sucht die IP-Adresse des Servers, der diese Site hostet.
3. Der Browser navigiert zu dieser Website.

Ohne Zertifikate ist es nicht möglich zu wissen, ob ein unberechtigter DNS-Server verwendet oder an einen anderen Server weitergeleitet wurde. Zertifikate stellen sicher, dass Sie ordnungsgemäß und sicher auf die beabsichtigte Website weitergeleitet werden, z. B. auf Ihre Bank-Website, wo die persönlichen oder vertraulichen Daten, die Sie eingeben, sicher sind.

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

1. Klicken Sie auf das Vorhängeschloss, und ein Fenster wird angezeigt:**Abbildung 1: Website-Identifizierung**


2. Klicken Sie auf **Zertifikate anzeigen**, um das Zertifikat der Website anzuzeigen, wie in diesem Beispiel gezeigt:**Abbildung 2: Zertifikatinformationen, Registerkarte "Allgemein"**



Die hervorgehobenen Informationen sind wichtig.**Ausgestellt von** ist die Firma oder Zertifizierungsstelle (Certificate Authority, CA), die Ihr System bereits vertraut.**Gültig von/bis** ist der Datumsbereich, in dem dieses Zertifikat verwendet werden kann. (Manchmal sehen Sie ein Zertifikat, von dem Sie wissen, dass Sie der Zertifizierungsstelle vertrauen, aber Sie sehen, dass das Zertifikat ungültig ist. Überprüfen Sie immer das Datum, damit Sie wissen, ob es abgelaufen ist.)**TIPP:** Eine Best Practice besteht darin, eine Erinnerung in Ihrem Kalender zu erstellen, um das Zertifikat zu verlängern, bevor es abläuft. Dadurch werden künftige Probleme vermieden.

Die Unterschiede zwischen PEM und DER Zertifizierung

PEM ist ASCII. DER ist binär. Abbildung 3 zeigt das PEM-Zertifikatsformat.

Abbildung 3: PEM-Zertifikatbeispiel

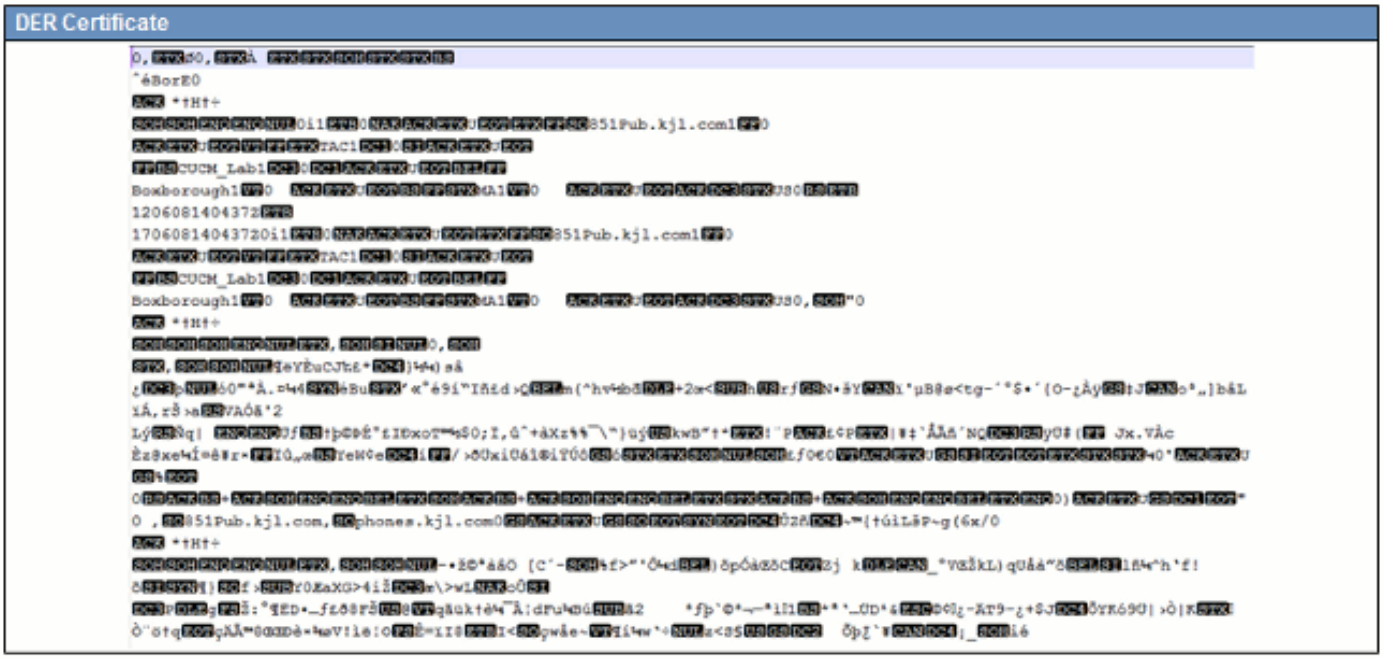
PEM Certificate

```
-----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-----
```

Abbildung 4 zeigt das DER-Zertifikat.

Abbildung 4: Beispiel für ein Zertifikat der DER

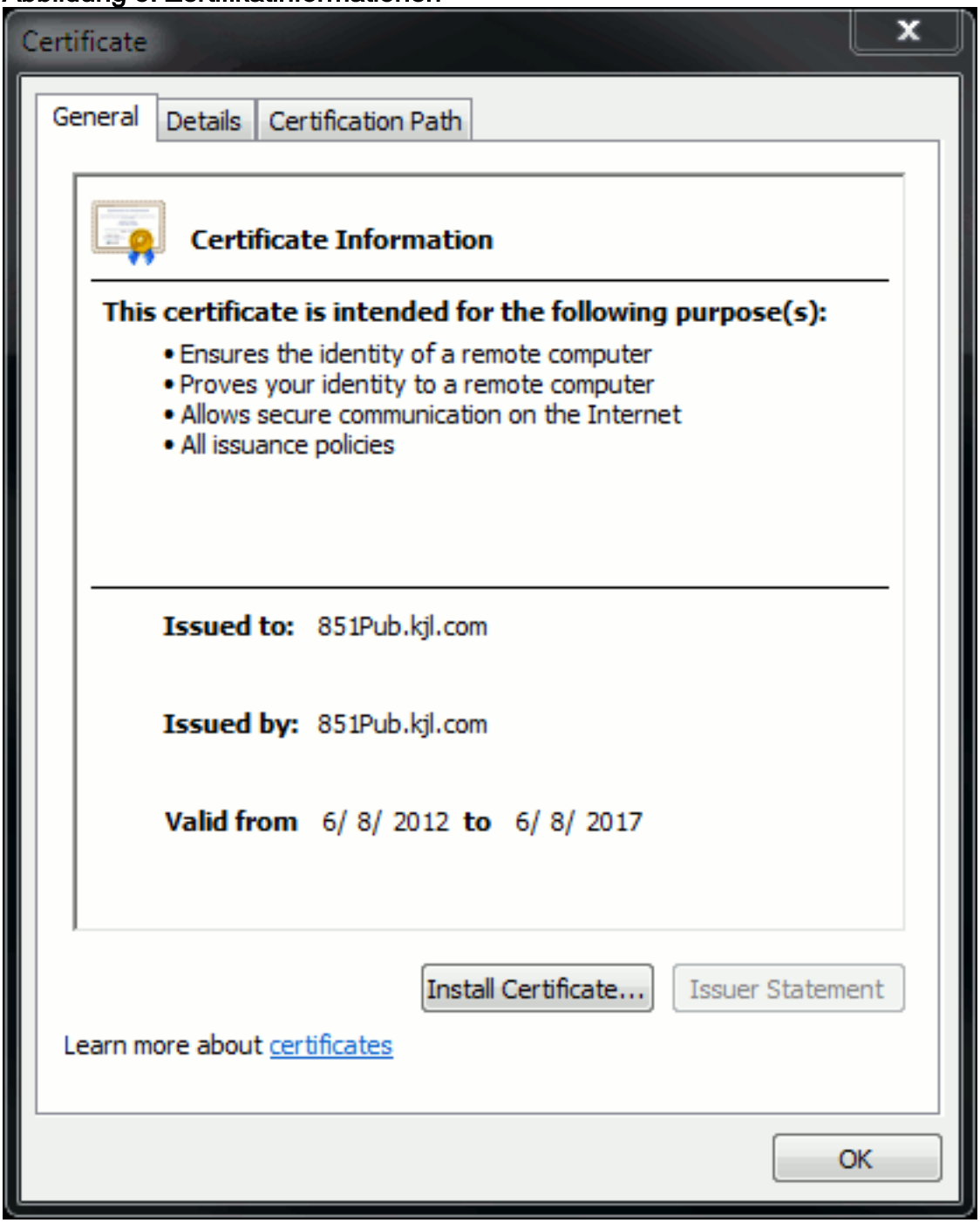
DER Certificate



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 **- BEGINNZERTIFIKAT** und **- ENDZERTIFIKAT** einschließen, in eine Textdatei einfügen und sie mit der Erweiterung .PEM oder .CER speichern.

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

Abbildung 5: Zertifikatinformationen

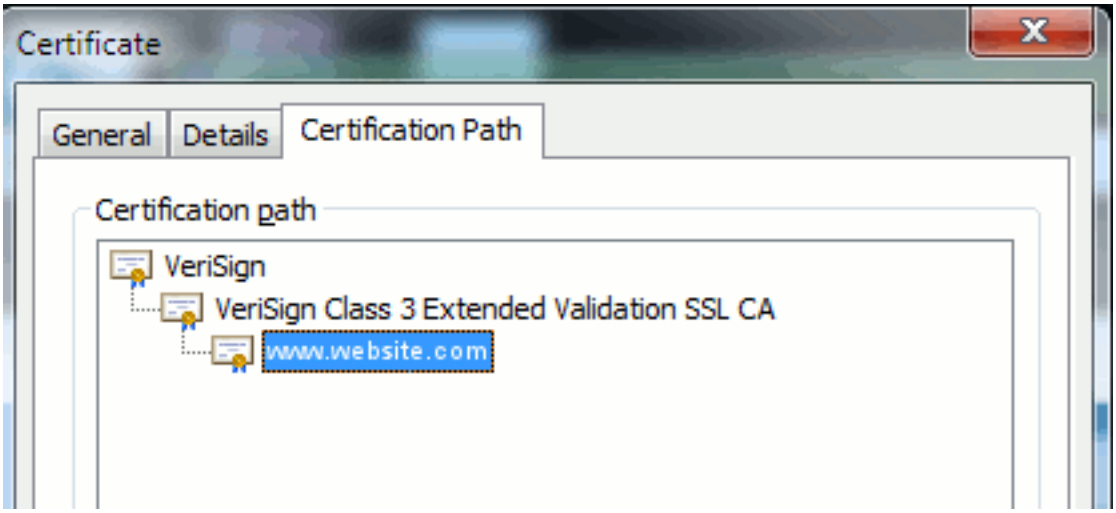


In einigen Fällen benötigt ein Gerät ein bestimmtes Format (ASCII oder binär). Um dies zu ändern, laden Sie das Zertifikat von der CA im benötigten Format herunter oder verwenden Sie ein SSL-Konverter-Tool wie https://www.sslshopper.com/ssl-converter.html.

Zertifikathierarchie

Damit ein Zertifikat von einem Endpunkt aus vertrauenswürdig ist, muss bereits eine Vertrauenswürdigkeit mit einer Zertifizierungsstelle eines Drittanbieters bestehen. Abbildung 6 zeigt eine Hierarchie von drei Zertifikaten.

Abbildung 6: Zertifikathierarchie



- **Verisign** ist eine CA.
- **Verisign Class 3 Extended Validation SSL CA** ist ein vermitteltes oder signierendes Serverzertifikat (ein Server, der von der CA autorisiert ist, Zertifikate in seinem Namen auszustellen).
- **www.website.com** ist ein Server- oder Servicegutschrift.

Der Endpunkt muss wissen, dass er zunächst sowohl der CA als auch den Zwischenzertifikaten vertrauen kann, bevor er weiß, dass er dem vom SSL-Handshake präsentierten Serverzertifikat vertrauen kann (Details unten). Weitere Informationen zur Funktionsweise dieser Vertrauenswürdigkeit finden Sie im Abschnitt in diesem Dokument: **Definieren Sie "Vertrauenswürdigkeit" aus Sicht eines Zertifikats**.

Selbstsignierte Zertifikate gegenüber Drittanbieterzertifikaten

Die Hauptunterschiede zwischen selbstsignierten und Drittanbieterzertifikaten bestehen darin, wer das Zertifikat signiert hat, unabhängig davon, ob Sie ihnen vertrauen.

Ein selbstsigniertes Zertifikat ist ein vom Server signiertes Zertifikat. Daher sind das Server-/Service-Zertifikat und das Zertifizierungsstellenzertifikat identisch.

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

Jeder kann eine CA sein. Unabhängig davon, ob Ihr System dieser CA vertraut oder nicht, ist das, was am wichtigsten ist.

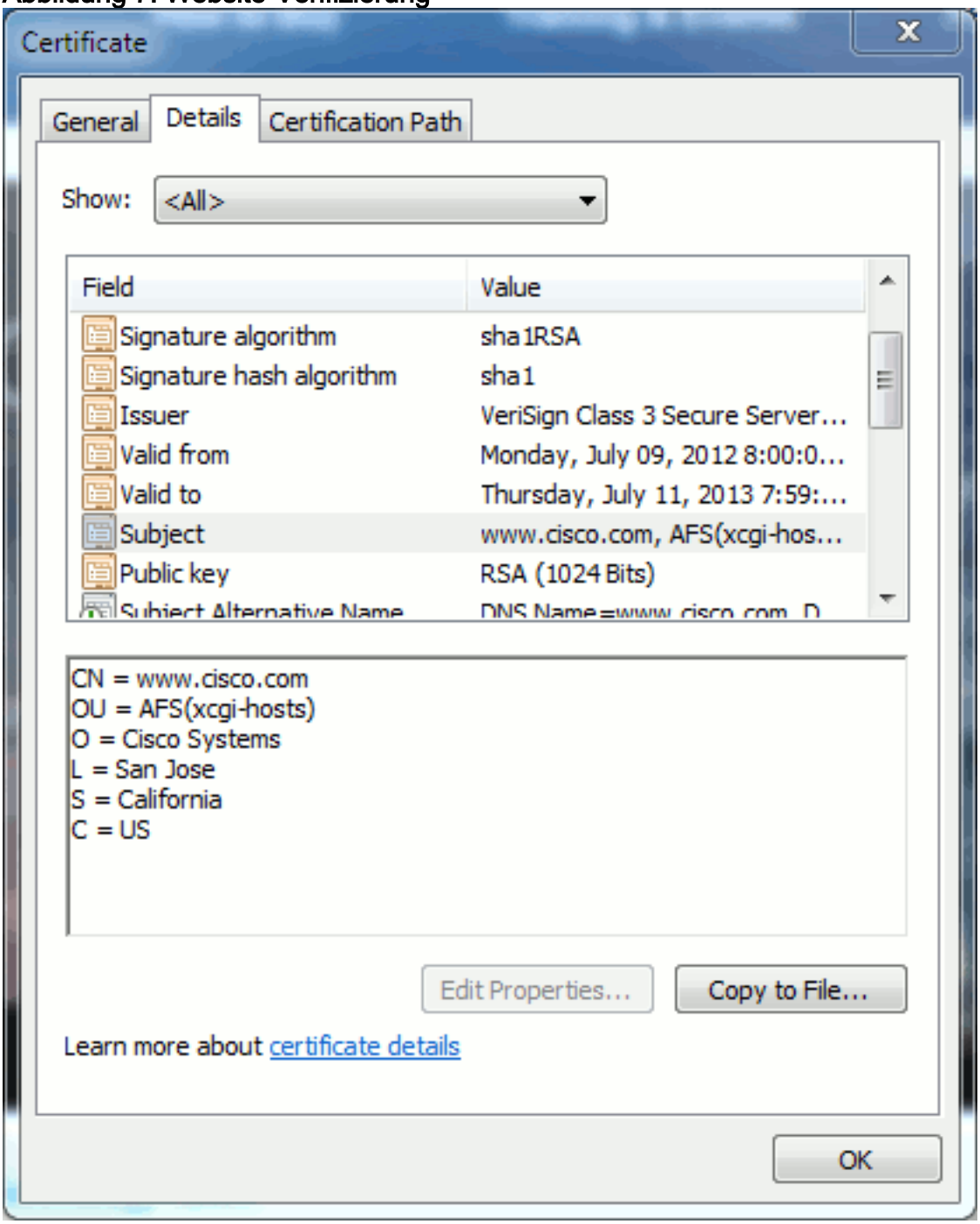
Häufige Namen und alternative Namen von Betreffenden

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

Im Beispiel in Abbildung 7 weist das Zertifikat den CN auf www.cisco.com. Die URL-Anfrage für www.cisco.com vom Browser überprüft den URL-FQDN mit den Informationen, die das Zertifikat präsentiert. In diesem Fall stimmen sie überein, und es zeigt, dass der SSL-Handshake erfolgreich ist. Diese Website wurde als die richtige Website verifiziert, und die Kommunikation zwischen dem

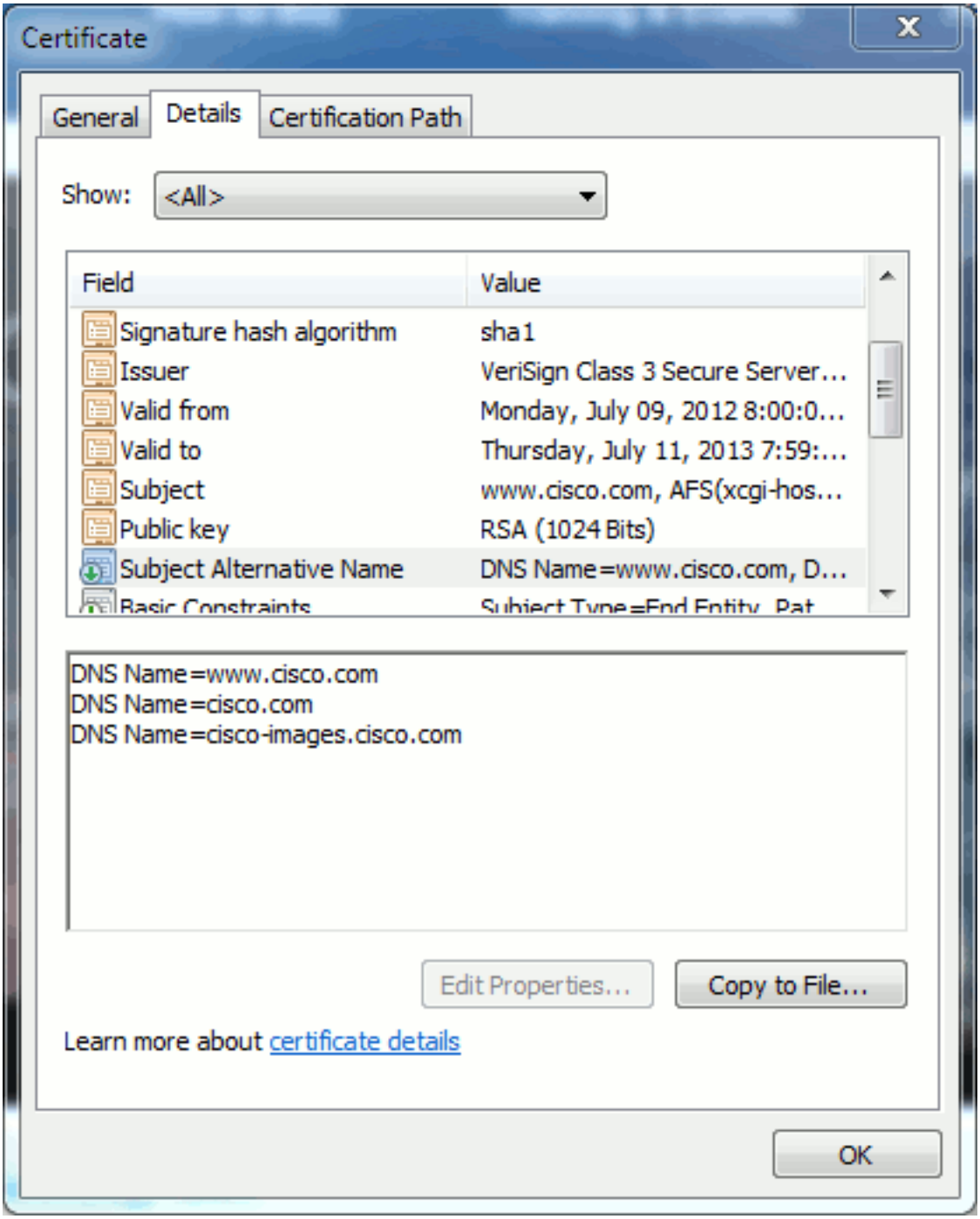
Desktop und der Website wird nun verschlüsselt.

Abbildung 7: Website-Verifizierung



Im gleichen Zertifikat befindet sich ein 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. Dies bedeutet, dass Sie auch cisco.com eingeben können, und dasselbe Zertifikat kann zur Authentifizierung und Verschlüsselung dieser Website verwendet werden.

CUCM kann SAN-Header erstellen. Weitere Informationen zu SAN-Headern finden Sie im Dokument von Jason Burn, CUCM Uploading CCMAdmin Web GUI Certificates on the Support Community.

Wild Card-Zertifikate

Wildcard-Zertifikate sind Zertifikate, die mit einem Sternchen (*) eine beliebige Zeichenfolge in einem Abschnitt einer URL darstellen. Um beispielsweise über ein Zertifikat für www.cisco.com, ftp.cisco.com, ssh.cisco.com usw. zu verfügen, muss ein Administrator lediglich ein Zertifikat für *.cisco.com erstellen. Um Geld sparen zu können, muss der Administrator nur ein einziges

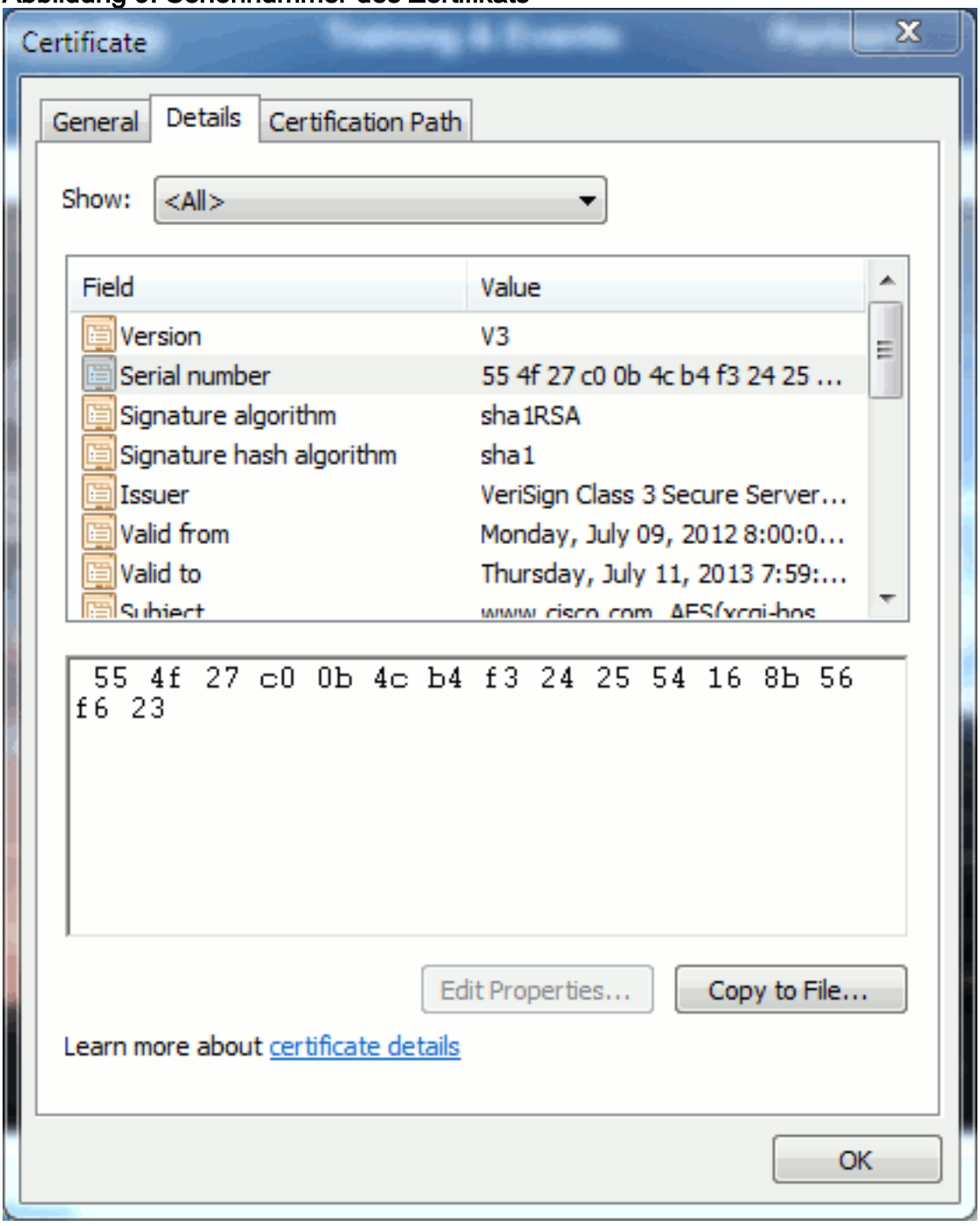
Zertifikat erwerben und muss nicht mehrere Zertifikate erwerben.

Diese Funktion wird derzeit nicht von Cisco Unified Communications Manager (CUCM) unterstützt. Sie können diese Erweiterung jedoch verfolgen: CSCta14114: Anforderung zur Unterstützung von Platzhalterzertifikaten in CUCM und für den 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, um regenerierte oder gefälschte Zertifikate. Abbildung 9 zeigt ein Beispiel:

Abbildung 9: Seriennummer des Zertifikats



CSR 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 CA präsentiert werden soll. Dieser CSR ähnelt einem PEM-Zertifikat (ASCII-Zertifikat).

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

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

Hinweis: Ein privater Schlüssel ist eine Datei, die nur für diesen Server und Dienst gilt. Das sollte nie jemandem gegeben werden! Wenn Sie jemandem einen privaten Schlüssel bereitstellen, beeinträchtigt dies die Sicherheit, die das Zertifikat bietet. Generieren Sie auch keine neue CSR-Anfrage für denselben Service, wenn Sie mit der alten CSR ein Zertifikat erstellen. CUCM löscht den alten CSR und den privaten Schlüssel und ersetzt beide, wodurch der alte CSR nutzlos wird.

Weitere Informationen finden Sie in der Dokumentation von Jason Burn zur Support Community: CUCM Hochladen von CCMAdmin-GUI-Zertifikaten für die Web-GUI für Informationen zum Erstellen von CSRs.

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

Das Handshake-Protokoll ist eine Reihe aufeinander folgender Meldungen, die die Sicherheitsparameter einer Datenübertragungssitzung aushandeln. Weitere Informationen finden Sie unter SSL/TLS in Detail , das die Nachrichtensequenz im Handshake-Protokoll dokumentiert. Diese werden in einer Paketerfassung (PCAP) angezeigt. Die Details umfassen die zwischen Client und Server gesendeten und empfangenen ersten, nachfolgenden und letzten Nachrichten.

Verwendung von Zertifikaten durch CUCM

Der Unterschied zwischen tomcat und tomcat trust

Beim Hochladen von Zertifikaten in CUCM stehen für jeden Service zwei Optionen zur Verfügung: **Cisco Unified Operating System Administration > Security > Certificate Management > Find**.

Die fünf Dienste, mit denen Sie Zertifikate in CUCM **verwalten** können, sind:

- Tomate
- IPS
- Callmanager
- Kap
- tvs (ab CUCM Version 8.0)

Hier sind die Dienste, mit denen Sie Zertifikate auf CUCM **hochladen** können:

- Tomate
- tomcat trust
- IPS

- ipsec-trust
- Callmanager
- callmanager trust
- Kap
- capf-trust

Dies sind die in CUCM Version 8.0 und höher verfügbaren Services:

- Fernseher
- Vertrauenswürdige Fernseher
- Telefonvertrauen
- phone-vpn-trust
- telefonvertrauen
- 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.

Mit **tomcat** laden die **tomcat-trusts** die CA und Zwischenzertifikate hoch, sodass dieser CUCM-Knoten weiß, dass er jedem Zertifikat vertrauen kann, das von der CA und dem Zwischenserver signiert wurde. Das tomcat-Zertifikat ist das Zertifikat, das der Tomcat-Dienst auf diesem Server vorlegt, wenn ein Endpunkt eine HTTP-Anforderung an diesen Server stellt. Um die Darstellung von Zertifikaten von Drittanbietern nach Tomcat zu ermöglichen, muss der CUCM-Knoten wissen, dass er der CA und dem Zwischenserver vertrauen kann. Daher müssen die Zertifizierungsstelle und Zwischenzertifikate hochgeladen werden, bevor das Tomcat (Service)-Zertifikat hochgeladen wird.

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

Jeder Dienst verfügt über ein eigenes Dienstzertifikat und Vertrauenszertifikate. Sie arbeiten sich nicht gegenseitig aus. Anders ausgedrückt: Eine CA und ein Zwischenzertifikat, die als tomcat-trust-Dienst hochgeladen wurden, können vom Anrufmanager-Dienst nicht verwendet werden.

Hinweis: Zertifikate in CUCM sind auf Knotenbasis. Wenn Sie also Zertifikate an den Herausgeber hochladen müssen und die Abonnenten dieselben Zertifikate benötigen, müssen Sie diese vor CUCM Release 8.5 auf jeden einzelnen Server und Knoten hochladen. In CUCM 8.5 und höher gibt es einen Dienst, der hochgeladene Zertifikate auf die übrigen Knoten im Cluster repliziert.

Hinweis: Jeder Knoten verfügt über eine andere CN. Daher muss von jedem Knoten eine CSR-Anfrage erstellt werden, damit der Dienst eigene Zertifikate präsentieren kann.

Wenn Sie weitere spezifische Fragen zu CUCM-Sicherheitsfunktionen haben, lesen Sie die Sicherheitsdokumentation.

Schlussfolgerung

Dieses Dokument unterstützt und baut ein hohes Maß an Wissen über Zertifikate auf. Dieses Thema kann vielleicht noch tiefer gehen, aber dieses Dokument gibt Ihnen genug Informationen für die Arbeit mit Zertifikaten. Wenn Sie Fragen zu CUCM-Sicherheitsfunktionen haben, finden Sie in den CUCM-Sicherheitsleitfäden nach Release weitere Informationen.

Zugehörige Informationen

- Wartungs- und Sicherheitsleitfäden für Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- Cisco Support Community: CUCM Hochladen der CCMAdmin-Webbenutzeroberfläche-Zertifikate
- Bug CSCta14114: Antrag auf Unterstützung eines Wildcard-Zertifikats in CUCM und Import von privaten Schlüsseln
- Cisco Emergency Responder (CER) - Erläuterung
- Technischer Support und Dokumentation - Cisco Systems