عرض عالي المستوى للشهادات والسلطات في CUCM

المحتويات

المقدمة

الغرض من هذا المستند هو فهم أساسيات الشهادات وسلطات الشهادات. يكمل هذا المستند مستندات Cisco الأخرى التي تشير إلى أي ميزات تشفير أو مصادقة في مدير الاتصالات الموحدة (CUCM) من Cisco.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

الغرض من الشهادات

يتم إستخدام الشهادات بين نقاط النهاية لبناء ثقة/مصادقة وتشفير البيانات. هذا يؤكد أن نقاط النهاية تتصل بالجهاز المرغوب ولديهم خيار تشفير البيانات بين نقطتي النهاية.

تعريف الثقة من وجهة نظر الشهادة

الجزء الأكثر أهمية من التراخيص هو تعريف نقاط النهاية التي يمكن الوثوق بها من خلال نقطة النهاية. يساعدك هذا المستند على معرفة كيفية تشفير بياناتك ومشاركتها مع موقع الويب والهاتف وخادم FTP الذي تريده وما إلى ذلك وتعريفها.

عندما يثق نظامك في شهادة ما، فهذا يعني وجود شهادة (شهادات) مثبتة مسبقا على نظامك، مما يعني أنه واثق بنسبة 100 بالمائة من مشاركته للمعلومات مع نقطة النهاية الصحيحة. وإلا، فإنها تنهي الاتصال بين نقاط النهاية هذه.

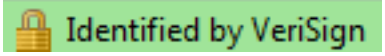
وخير مثال على ذلك هو رخصة القيادة الخاصة بك. تستخدم هذه الرخصة (شهادة خادم/خدمة) لتثبت أنك من تقولين أنك كذلك، حصلت على الرخصة من القسم المحلي لفرع المركبات الآلية (شهادة متوسطة) الذي حصل على إذن من قسم المركبات الآلية (DMV) في دولتك (سلطة شهادة). عندما تحتاج إلى إظهار رخصتك (شهادة خادم/خدمة) إلى أحد الضباط، يعلم الضابط أن بإمكانه الوثوق بفرع DMV (شهادة متوسطة) وقسم المركبات الآلية (سلطة شهادة)، ويمكنه التحقق من أن هذا الترخيص صادر من قبلهم (سلطة شهادة). تم التحقق من هويتك للضابط وهم الآن يثقون بأنك من أنت. وإلا، إذا قمت بإعطاء ترخيص غير صحيح (خادم/شهادة خدمة) لم يتم توقيعه بواسطة DMV (الشهادة الوسيطة)، فلن يثقوا بمن تقول أنك. يقدم باقي هذا المستند شرحا متعمقا وتقنيا للتدرج الهرمي للشهادات.

كيفية إستخدام المستعرضات للشهادات

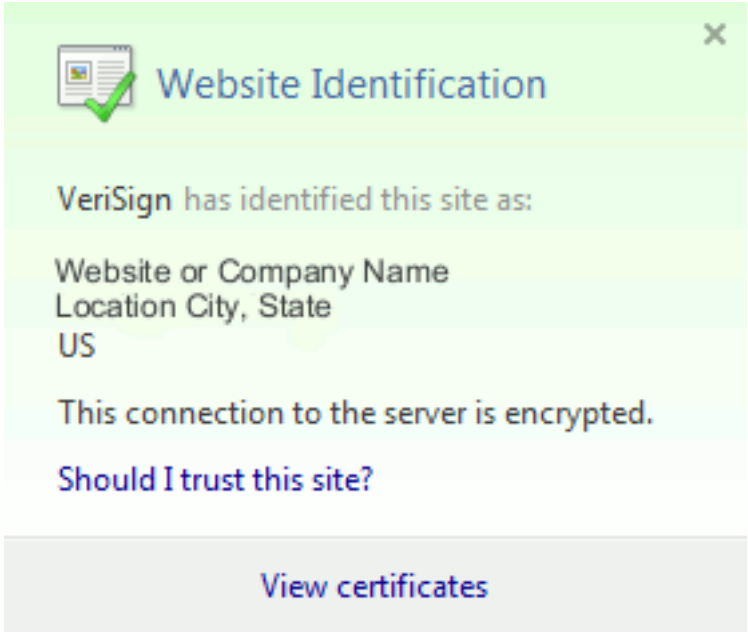
1. عندما تقوم بزيارة موقع ويب، أدخل عنوان URL، مثل http://www.cisco.com.
2. يعثر DNS على عنوان IP الخاص بالخادم الذي يستضيف هذا الموقع.
3. ينتقل المستعرض إلى هذا الموقع.

من دون شهادات، من المستحيل معرفة ما إذا كان خادم DNS مخادع قد تم إستخدامه، أو ما إذا تم توجيهك إلى خادم آخر. تضمن الشهادات توجيهك بشكل صحيح وآمن إلى موقع الويب المقصود، مثل موقع الويب الخاص بالبنك، حيث تكون المعلومات الشخصية أو الحساسة التي تدخلها آمنة.

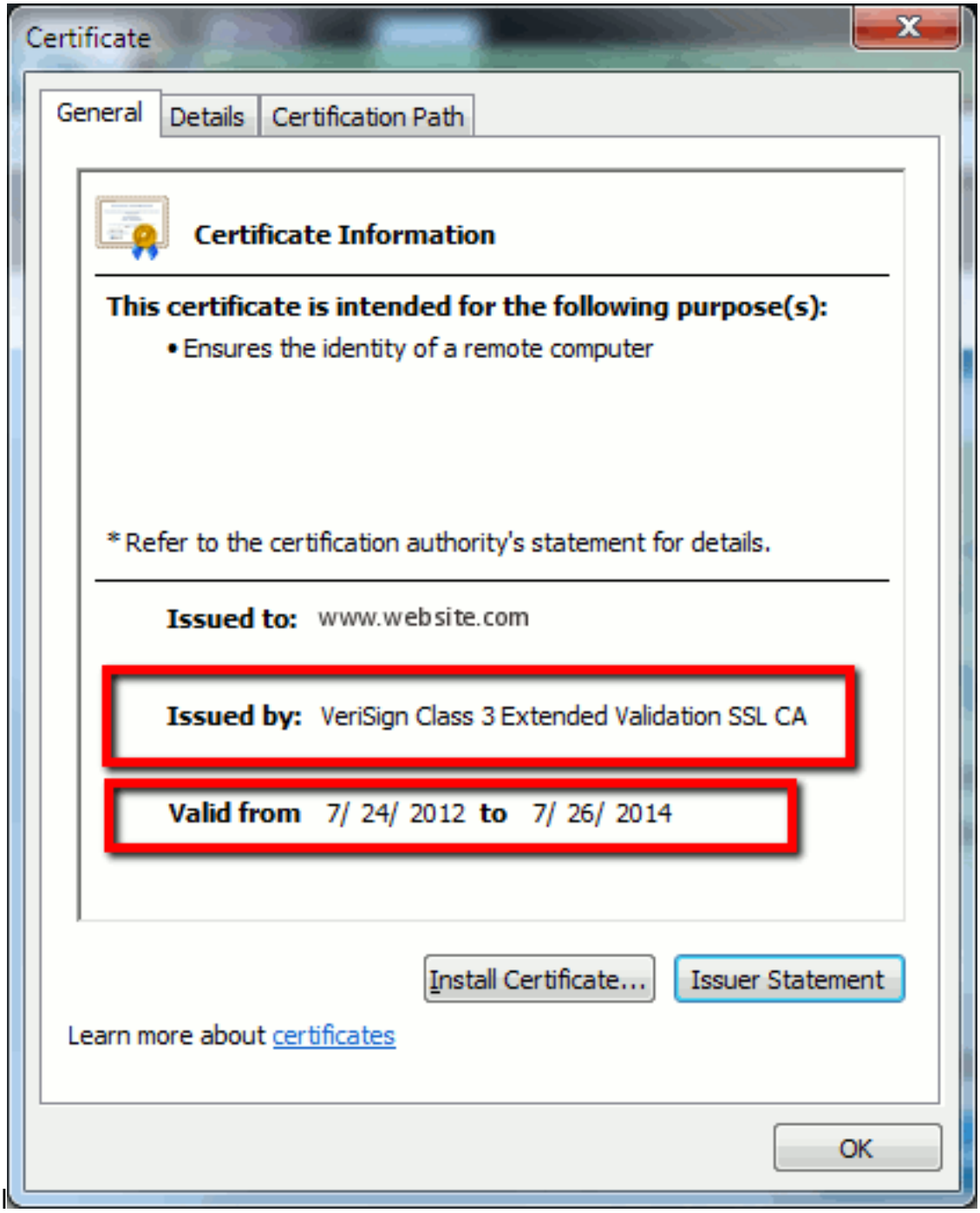
تحتوي جميع المستعرضات على أيقونات مختلفة تستخدمها، ولكن عادة ما ترى قفل في شريط العناوين كهذا:



1. انقر على القفل وتعرض النافذة:**الشكل 1: تحديد الموقع الشبكي**



2. انقر على **عرض الشهادات** لترى شهادة الموقع كما هو موضح في هذا المثال:**شكل 2: معلومات الشهادة، علامة التبويب العامة**



المعلومات المبرزة مهمة.**تم إصدارها بواسطة** الشركة أو جهة منح الشهادة (CA) التي يثق بها نظامك بالفعل.نطاق التاريخ الذي يمكن إستخدام هذه الشهادة فيه **صالح من/إلى**. (في بعض الأحيان ترى شهادة حيث تعلم أنك تثق في المرجع المصدق، لكنك ترى أن الشهادة غير صالحة. قم دائما بالتدقيق في التاريخ حتى تعرف ما إذا كان قد انتهت مدة صلاحيته أم لا.)**تلميح:** أفضل ممارسة هي إنشاء تذكير في التقويم لتجديد الشهادة قبل انتهاء صلاحيتها. وهذا يمنع حدوث مشاكل في المستقبل.

الفرق بين شهادات PEM مقابل شهادات DER

PEM هو ascii، DER هو ثنائي. الشكل 3 يوضح تنسيق شهادة PEM.

شكل 3: مثال شهادة PEM

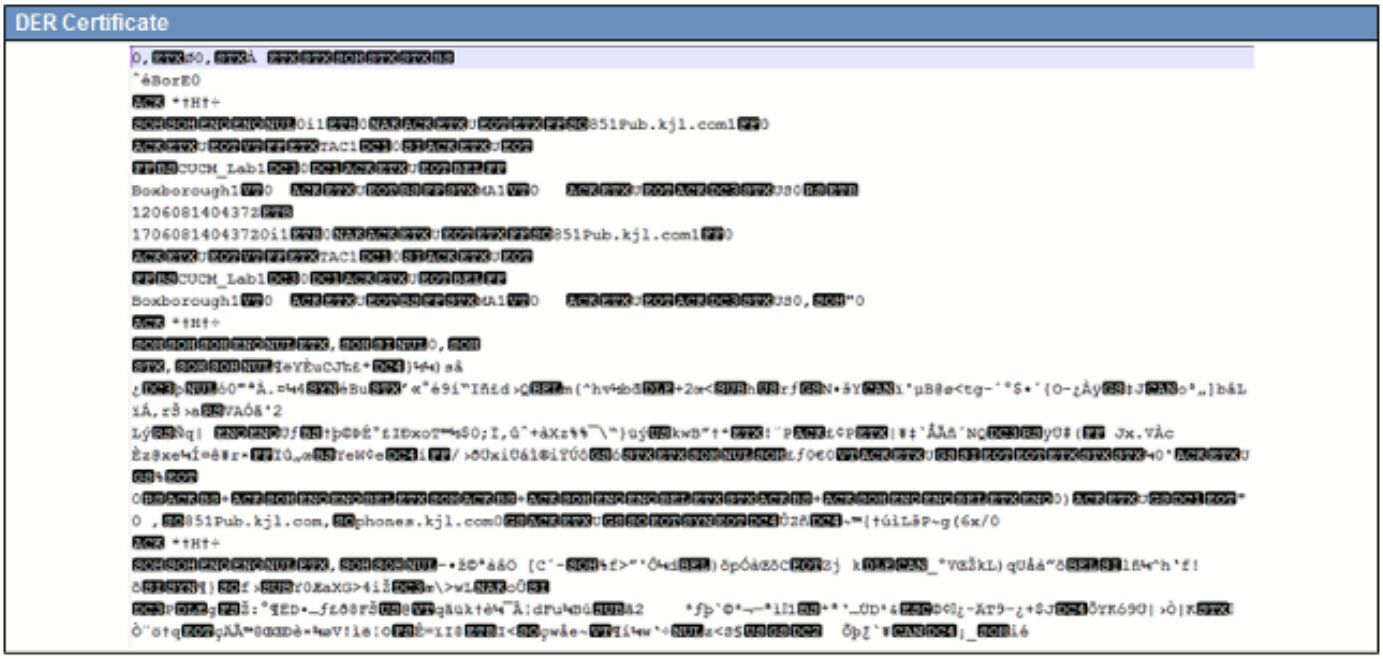
PEM Certificate

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

الشكل 4 يوضح شهادة DER.

الشكل 4: مثال شهادة DER

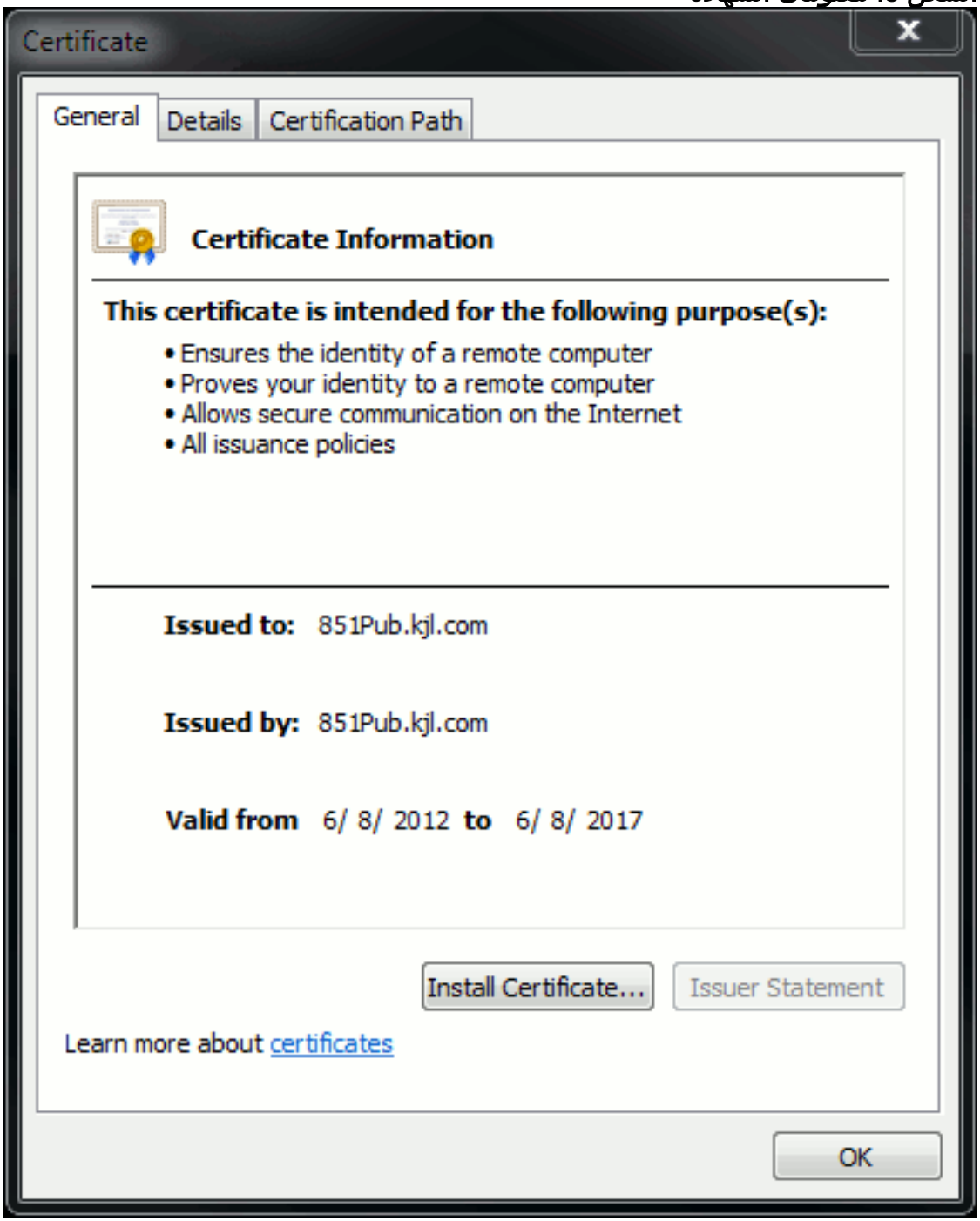
DER Certificate



تستخدم معظم شركات CA مثل VeriSign أو Thawt تنسيق PEM لإرسال الشهادات إلى العملاء، لأنها ملائمة للبريد الإلكتروني. يجب على العميل نسخ السلسلة بأكملها وتضمين **—BEGIN CERTIFICATE** و**—END CERTIFICATE—** ولصقها في ملف نصي وحفظها مع الملحق .PEM أو .CER.

يمكن ل Windows قراءة تنسيقات DER و CER باستخدام التطبيق الصغير الخاص بإدارة الشهادات وإظهار الشهادة كما هو موضح في الشكل 5.

الشكل 5: معلومات الشهادة

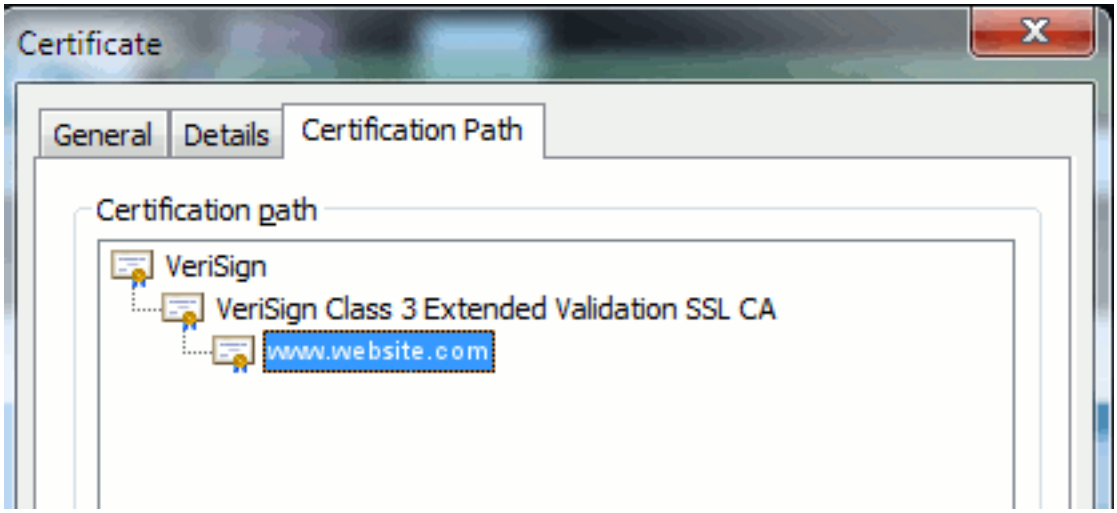


في بعض الحالات، يتطلب الجهاز تنسيق معين (ASCII أو ثنائي). لتغيير ذلك، قم بتنزيل الشهادة من المرجع المصدق بالتنسيق المطلوب أو أستخدم أداة محول SSL، مثل https://www.sslshopper.com/ssl-converter.html.

التدرج الهرمي للشهادة

من أجل الثقة في شهادة من نقطة نهاية، يجب أن تكون هناك ثقة منشأة بالفعل مع مرجع مصدق من طرف ثالث. على سبيل المثال، الشكل 6 يوضح أن هناك تسلسل هيكلي من ثلاثة شهادات.

شكل 6: التدرج الهرمي للشهادة



- **Verisign** هو CA.
- **مصادقة SSL الموسعة من الفئة 3** هي شهادة خادم وسيطة أو شهادة خادم توقيع (خادم مفوض من قبل CA لإصدار شهادات باسمها).
- **www.website.com** هو شهادة خادم أو خدمة.

تحتاج نقطة النهاية الخاصة بك إلى معرفة أنها يمكن أن تثق بكل من المرجع المصدق والشهادات الوسيطة أولا قبل أن تعرف أنها يمكن أن تثق بشهادة الخادم المقدمة من خلال مصافحة SSL (التفاصيل أدناه). لفهم كيفية عمل هذه الثقة بشكل أفضل، ارجع إلى القسم في هذا المستند: **قم بتعريف "الثقة" من وجهة نظر الشهادة**.

الشهادات الموقعة ذاتيا مقابل شهادات الطرف الثالث

الفروق الرئيسية بين شهادات التوقيع الذاتي وشهادات الطرف الثالث هي من وقع على الشهادة، سواء كنت تثق بها.

والشهادة الموقعة ذاتيا هي شهادة موقعة من قبل الخادم تقدمها؛ ولذلك فإن شهادة الخادم/الخدمة وشهادة المرجع المصدق هي نفسها.

CA الخاص بجهة خارجية هي خدمة مقدمة من مرجع مصدق عام (مثل Verisign و Entrust و Digicert) أو خادم (مثل Windows 2003 و Linux و Unix و IOS) يتحكم في صلاحية شهادة الخادم/الخدمة.

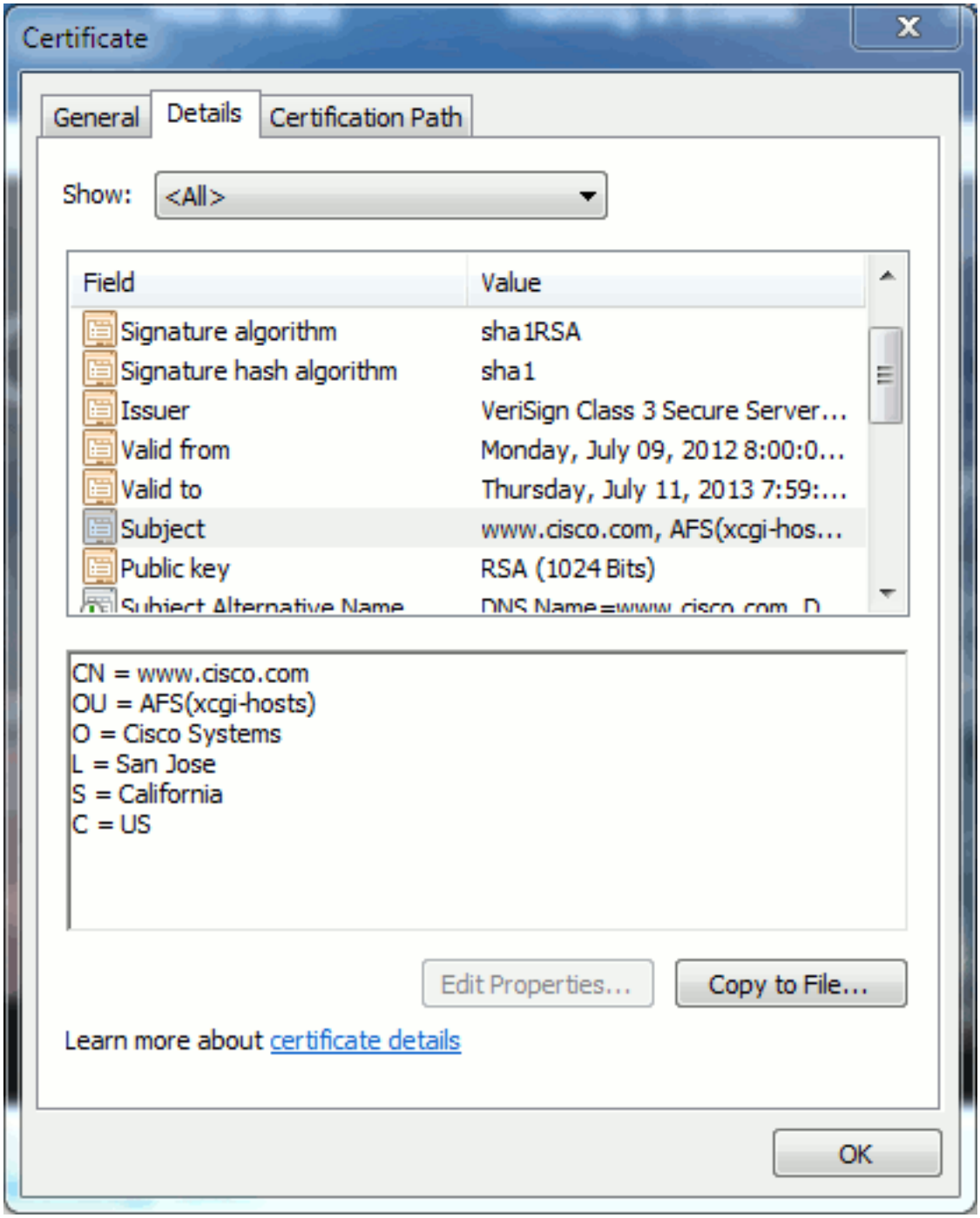
كل واحدة منها يمكن أن تكون المرجع المصدق. سواء كان النظام لديك يثق في CA أم لا، فإن هذا هو أكثر الأمور أهمية.

الأسماء الشائعة والموضوعات البديلة

الأسماء الشائعة (CN) والأسماء البديلة للموضوع (SAN) هي مراجع إلى عنوان IP أو اسم المجال المؤهل بالكامل (FQDN) للعنوان المطلوب. على سبيل المثال، إذا قمت بإدخال https://www.cisco.com، فيجب أن يحتوي CN أو SAN على www.cisco.com في الرأس.

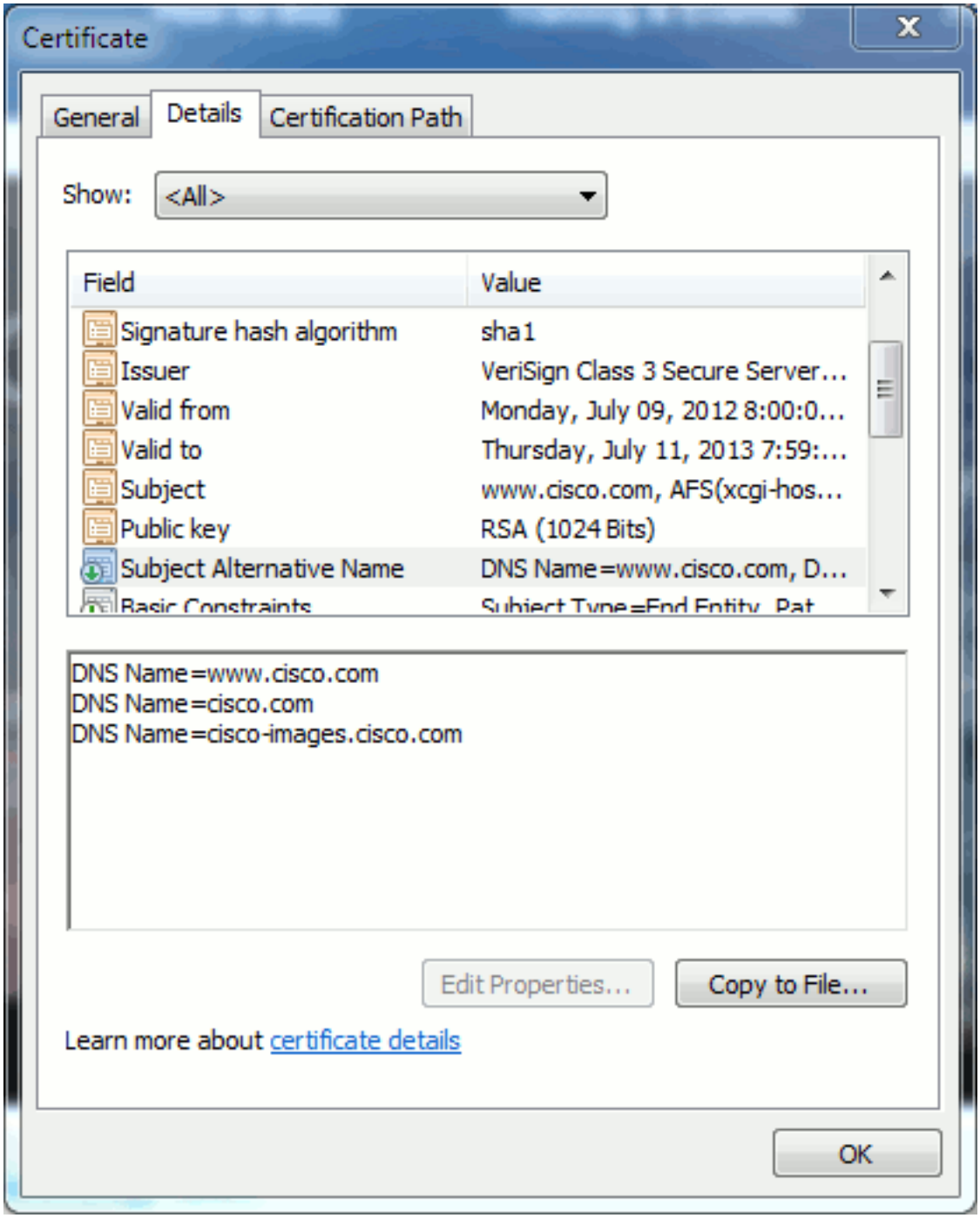
في المثال الموضح في الشكل 7، تحتوي الشهادة على CN مثل www.cisco.com. يتحقق طلب عنوان URL ل www.cisco.com من المستعرض من URL FQDN مقابل المعلومات التي يقدمها الترخيص. في هذه الحالة، تتطابق، وتظهر أن مصافحة SSL ناجحة. تم التحقق من أن موقع الويب هذا هو الموقع الصحيح، ويتم الآن تشفير الاتصالات بين سطح المكتب وموقع الويب.

الشكل 7: التحقق من الموقع الشبكي



في نفس الشهادة، يوجد رأس شبكة منطقة التخزين (SAN) لثلاثة عناوين FQDN/DNS:

شكل 8: رأس شبكة منطقة التخزين (SAN)



يمكن أن تصادق هذه الشهادة/تتحقق من www.cisco.com (المعرف أيضا في CN) و cisco.com و -cisco images.cisco.com. هذا يعني أنه يمكنك أيضا كتابة cisco.com، ويمكن إستخدام هذه الشهادة نفسها لمصادقة وتشفير موقع الويب هذا.

يمكن أن يقوم CUCM بإنشاء رؤوس SAN. ارجع إلى مستند CUCM، Jason Burn الذي يرفع شهادات CCMAdmin Web GUI على مجتمع الدعم للحصول على مزيد من المعلومات حول عناوين SAN.

شهادات البطاقة البرية

شهادات أحرف البدل هي شهادات تستخدم علامة نجمية (*) لتمثيل أي سلسلة في قسم من عنوان URL. على سبيل المثال، للحصول على شهادة ل www.cisco.com و ftp.cisco.com و ssh.cisco.com وما إلى ذلك، سيحتاج المسؤول فقط إلى إنشاء شهادة ل *.cisco.com. لتوفير المال، يحتاج المسؤول فقط إلى شراء شهادة واحدة ولا يحتاج إلى شراء شهادات متعددة.

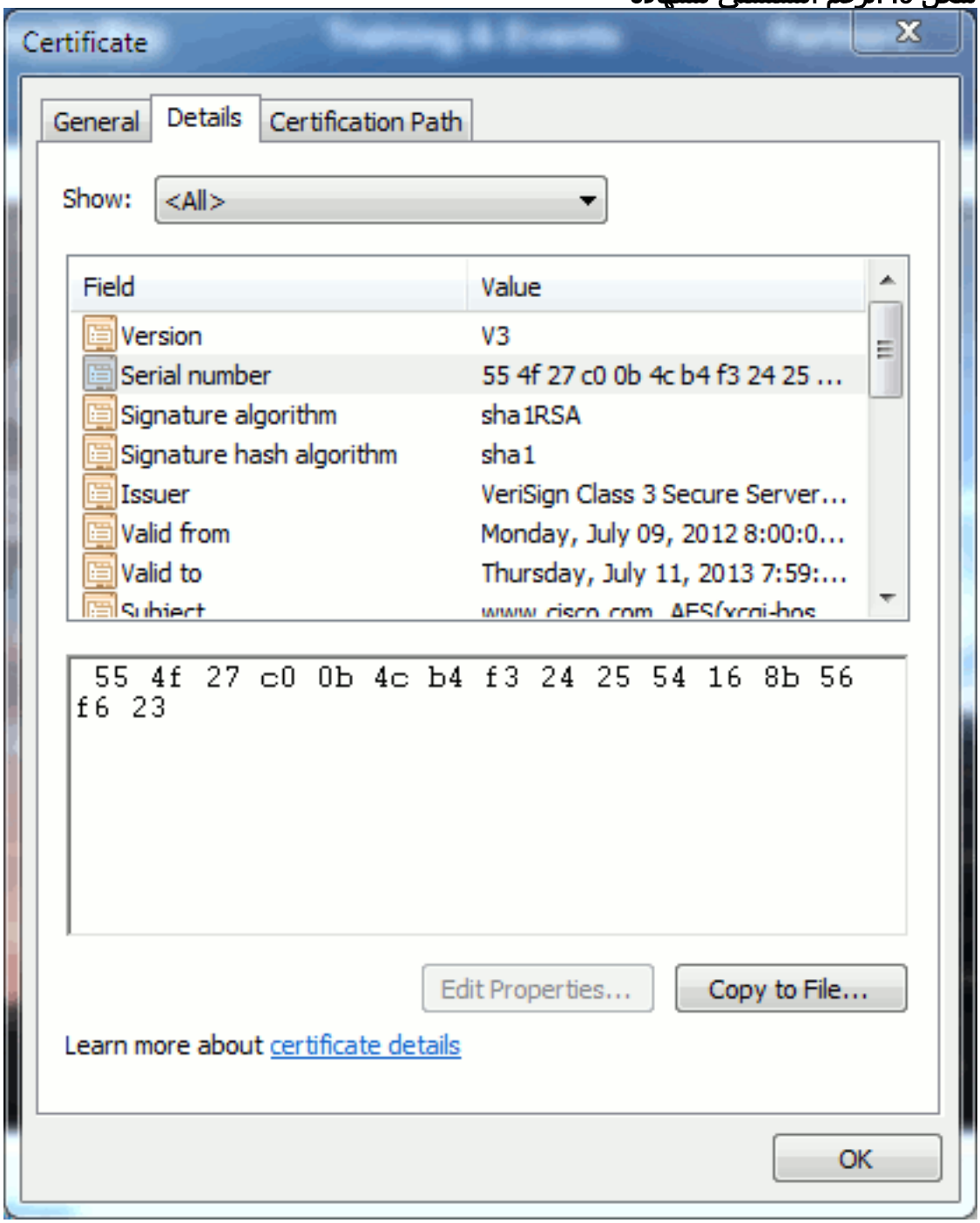
لا تدعم CUCM (Cisco Unified Communications Manager) هذه الميزة حاليا. ومع ذلك، يمكنك تعقب هذا

التحسين: CSCta14114: طلب دعم شهادة أحرف البدل في إستيراد CUCM والمفتاح الخاص.

تعريف الشهادات

عندما تحتوي الشهادات على نفس المعلومات، يمكنك أن ترى إذا كانت نفس الشهادة. تحتوي جميع الشهادات على رقم تسلسلي فريد. يمكنك إستخدام هذا للمقارنة إذا كانت الشهادات هي نفس الشهادات، معاد توليدها، أو مزيفة. الشكل 9 يقدم مثالا:

شكل 9: الرقم التسلسلي للشهادة



المسؤولية الاجتماعية للشركات والغرض منها

CSR يمثل طلب توقيع الشهادة. إذا كنت تريد إنشاء شهادة جهة خارجية لخادم CUCM، فأنت بحاجة إلى CSR لتقديمها إلى CA. هذه CSR تشبه كثيرا شهادة (ASCII PEM).

ملاحظة: هذه الشهادة ليست شهادة ولا يمكن إستخدامها كشهادة واحدة.

يقوم CUCM بإنشاء CSRs تلقائيا عبر واجهة المستخدم الرسومية (GUI) على الويب: إدارة نظام التشغيل الموحد من Cisco > **الأمان > إدارة الشهادات > إنشاء CSR >** إختيار الخدمة التي تريد إنشاء الشهادة > ثم إنشاء CSR. كل مرة يتم إستخدام هذا الخيار، يتم إنشاء مفتاح خاص جديد و CSR.

ملاحظة: المفتاح الخاص هو ملف فريد لهذا الخادم والخدمة. ولا يجب ان يعطى ذلك ابدا لأي شخص! إذا قمت بتوفير مفتاح خاص لشخص ما، فإنه يخل بالأمان الذي توفره الشهادة. أيضا، لا تقم بإعادة إنشاء CSR جديد لنفس الخدمة إذا كنت تستخدم CSR القديم لإنشاء شهادة. يقوم CUCM بحذف CSR القديم والمفتاح الخاص ويحل محلهما، مما يجعل CSR القديم غير ذي فائدة.

ارجع إلى وثائق جابسون بيرن في مجتمع الدعم: تحميل CUCM لشهادات واجهة المستخدم الرسومية (GUI) عبر الويب ل CCMAdmin للحصول على معلومات حول كيفية إنشاء أدوات تحديد المعدل المستندة إلى الأجهزة (CSR).

إستخدام الشهادات بين نقطة النهاية وعملية مصافحة SSL/TLS

بروتوكول المصافحة هو سلسلة من الرسائل المتسلسلة التي تتفاوض على معلمات الأمان لجلسة نقل البيانات. ارجع إلى SSL/TLS بالتفصيل ، والذي يوثق تسلسل الرسائل في بروتوكول المصافحة. ويمكن ملاحظة ذلك في التقاط الحزمة (PCAP). وتتضمن التفاصيل الرسائل الأولية واللاحقة والنهائية التي يتم إرسالها واستقبالها بين العميل والخادم.

كيفية إستخدام CUCM للشهادات

الفرق بين التومت وثقة التومت

عند تحميل الشهادات إلى CUCM، هناك خياران لكل خدمة عبر **إدارة نظام التشغيل الموحد من Cisco > الأمان > إدارة الشهادة>البحث**.

الخدمات الخمس التي تسمح لك **بإدارة** الشهادات في CUCM هي:

- tomcat
- IPsec
- callmanager
- capf
- TVS (في CUCM الإصدار 8.0 والإصدارات الأحدث)

فيما يلي الخدمات التي تسمح لك **بتحميل** الشهادات إلى CUCM:

- tomcat
- تومكات ترست
- IPsec
- ثقة IPSec
- callmanager
- برنامج CallManager-Trust
- capf
- CAPF-trust

هذه هي الخدمات المتاحة في CUCM الإصدار 8.0 والإصدارات الأحدث:

- tvs
- تقنية TVS-Trust
- phone-trust

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

راجع أدلة أمان CUCM بواسطة الإصدار للحصول على مزيد من التفاصيل حول هذه الأنواع من الشهادات. يشرح هذا القسم الفرق بين شهادة الخدمة وشهادة الضمان فقط.

على سبيل المثال، مع **tomcat**، **فإنTomcatTrust** تحمل ال CA والشهادات الوسيطة بحيث تعرف هذه العقدة CUCM أنها يمكن أن تثق في أي شهادة موقعة من CA والخادم الوسيط. شهادة TOMCAT هي الشهادة التي يتم تقديمها بواسطة خدمة TOMCAT على هذا الخادم، إذا كانت نقطة نهاية تقوم بطلب HTTP إلى هذا الخادم. للسماح بعرض شهادات الطرف الثالث بواسطة TOMCAT، يجب أن تعرف عقدة CUCM أنها يمكن أن تثق في CA والخادم الوسيط. لذلك، فمن الضروري تحميل CA والشهادات الوسيطة قبل تحميل شهادة (خدمة) tomcat.

راجع شهادات CCMAdmin الخاصة ب Jason Burn لتحميل CUCM على مجتمع الدعم للحصول على معلومات تساعدك على فهم كيفية تحميل الشهادات إلى CUCM.

تحتوي كل خدمة على شهادة خدمة وشهادات ثقة خاصة بها. لا يعمل كل منهما على الآخر. بمعنى آخر، لا يمكن إستخدام CA والشهادة الوسيطة المحملتين كخدمة توثيق من قبل خدمة CallManager.

ملاحظة: الشهادات في CUCM هي أساس كل عقدة. لذلك، إذا كنت بحاجة إلى شهادات تم تحميلها إلى الناشر، وتحتاج إلى أن يكون للمشتركين نفس الشهادات، فأنت بحاجة لتحميلها إلى كل خادم فردي وعقدة قبل إصدار CUCM 8.5. في الإصدار 8.5 من CUCM والإصدارات الأحدث، توجد خدمة مماثلة للشهادات التي تم تحميلها إلى بقية العقد في نظام المجموعة.

ملاحظة: لكل عقدة CN مختلف. لذلك، يجب إنشاء CSR بواسطة كل عقدة لكي تقدم الخدمة شهاداتها الخاصة.

إذا كانت لديك أسئلة إضافية محددة حول أي من ميزات أمان CUCM، فارجع إلى وثائق الأمان.

القرار

يساعد هذا المستند ويبني مستوى عال من المعرفة بالشهادات. من الممكن أن يصبح هذا الموضوع أكثر تعمقا، لكن هذا المستند يعرفك بما يكفي للعمل مع الشهادات. إذا كانت لديك أسئلة عن أي من ميزات أمان CUCM، راجع أدلة أمان CUCM عن طريق الإصدار للحصول على مزيد من المعلومات.

معلومات ذات صلة

- أدلة الأمان والصيانة لبرنامج Cisco Unified Communications Manager (إختصاره CallManager)
- Cisco Unified Communications Manager (إختصاره CallManager)
- مدير الاتصالات الموحدة الفائق من Cisco
- مجتمع دعم Cisco: تحميل CUCM لشهادات واجهة المستخدم الرسومية (GUI) عبر الويب ل CCMAdmin
- الخطأ CSCta14114: طلب دعم شهادة البدل في إستيراد مفتاح CUCM ومفتاح خاص
- شرح (Cisco Emergency Responder (CER
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).