Vue de haut niveau des certificats et des autorités dans CUCM

Table des matières

Introduction

Ce document décrit les bases des certificats et des autorités de certification. Il complète d'autres documents Cisco qui font référence à toute fonctionnalité de cryptage ou d'authentification dans Cisco Unified Communications Manager (CUCM).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Objet des certificats

Les certificats sont utilisés entre les terminaux pour établir la confiance/l'authentification et le chiffrement des données. Cela confirme que les terminaux communiquent avec le périphérique prévu et ont la possibilité de chiffrer les données entre les deux terminaux.

Remarque : pour comprendre l'impact de chaque certificat, reportez-vous à la section Impact du processus de régénération des certificats pour Cisco Unified Communications Manager par la banque de certificats

---

Définir la confiance du point de vue d'un certificat

La partie la plus importante des certificats est la définition des points de terminaison qui peuvent être approuvés par votre point de terminaison. Ce document vous aide à connaître et à définir la manière dont vos données sont chiffrées et partagées avec le site Web, le téléphone, le serveur FTP, etc.

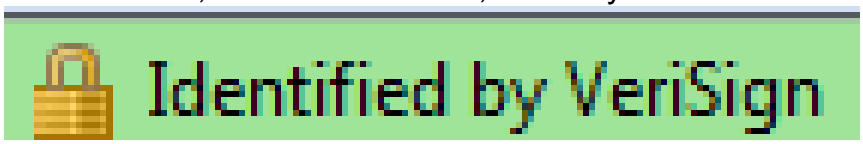
Lorsque votre système fait confiance à un certificat, cela signifie qu'il y a un ou plusieurs certificats préinstallés sur votre système qui indiquent qu'il est sûr à 100 % qu'il partage les informations avec le point d'extrémité correct. Sinon, il met fin à la communication entre ces points d'extrémité.

Le permis de conduire est un exemple non technique de cette situation. Vous utilisez cette licence (certificat de serveur/service) pour prouver que vous êtes qui vous dites être ; vous avez obtenu votre licence auprès de votre division locale des véhicules automobiles (certificat intermédiaire) qui a reçu l'autorisation de la division des véhicules automobiles (DMV) de votre État (autorité de certification). Lorsque vous devez montrer votre permis (certificat de serveur/service) à un agent, l'agent sait qu'il peut faire confiance à la succursale de la DMV (certificat intermédiaire) et à la Division des véhicules automobiles (autorité de certification), et il peut vérifier que ce permis a été délivré par eux (autorité de certification). Votre identité est vérifiée auprès de l'agent et maintenant il croit que vous êtes celui que vous dites être. Sinon, si vous donnez une fausse licence (certificat de serveur/service) qui n'a pas été signée par le DMV (certificat intermédiaire), alors ils ne feront pas confiance à qui vous dites que vous êtes. Le reste de ce document fournit une explication technique approfondie de la hiérarchie des certificats.

Utilisation des certificats par les navigateurs

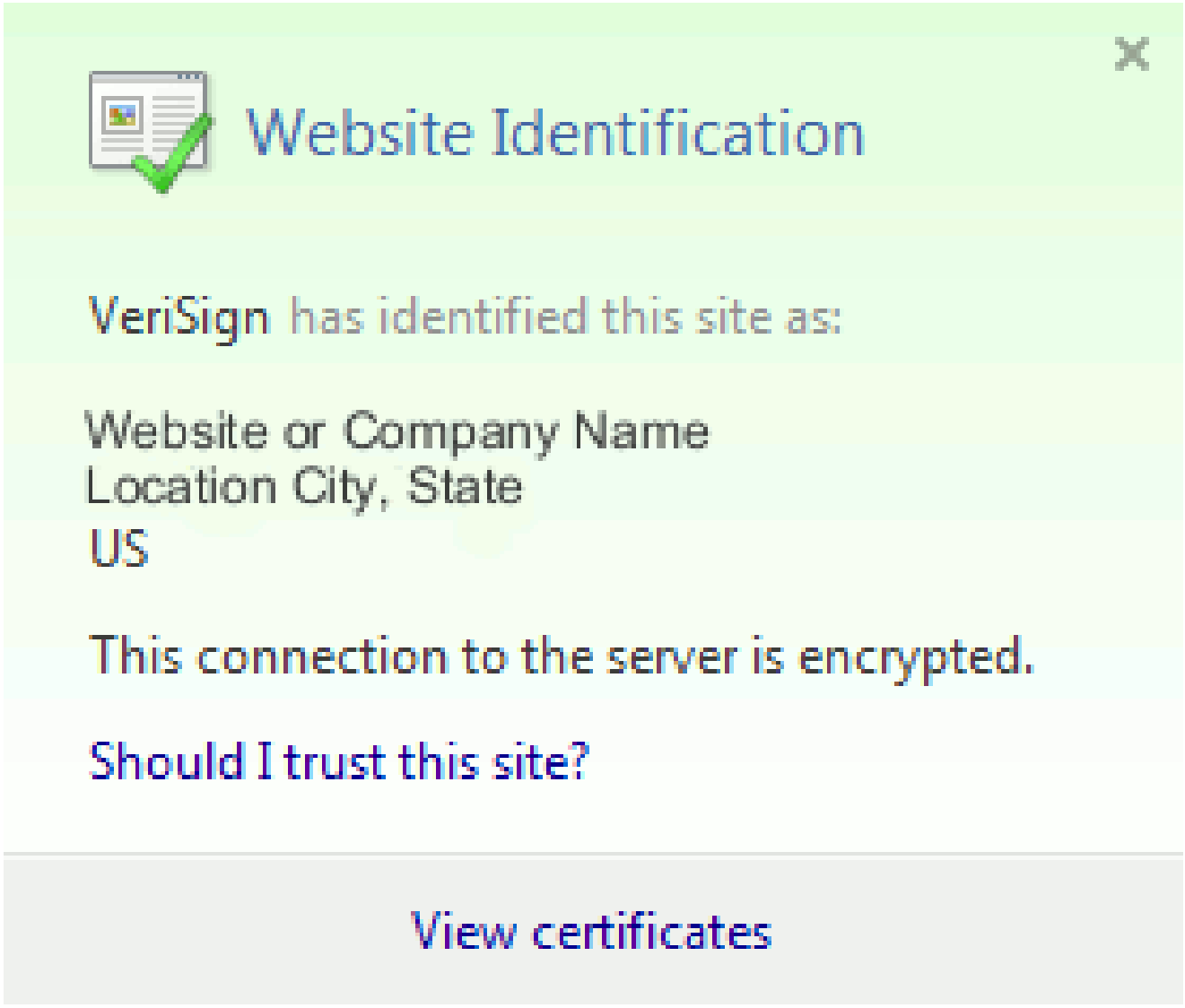
1. Lorsque vous visitez un site Web, entrez l'URL, telle que http://www.cisco.com.
2. Le serveur DNS recherche l'adresse IP du serveur qui héberge ce site.
3. Le navigateur accède à ce site.

Sans certificats, il est impossible de savoir si un serveur DNS non autorisé a été utilisé ou si vous avez été routé vers un autre serveur. Les certificats garantissent que vous êtes correctement et en toute sécurité acheminé vers le site Web souhaité, tel que le site Web de votre banque, où les informations personnelles ou sensibles que vous saisissez sont sécurisées.

Tous les navigateurs utilisent des icônes différentes, mais normalement, vous voyez un cadenas dans la barre d'adresse comme ceci : 

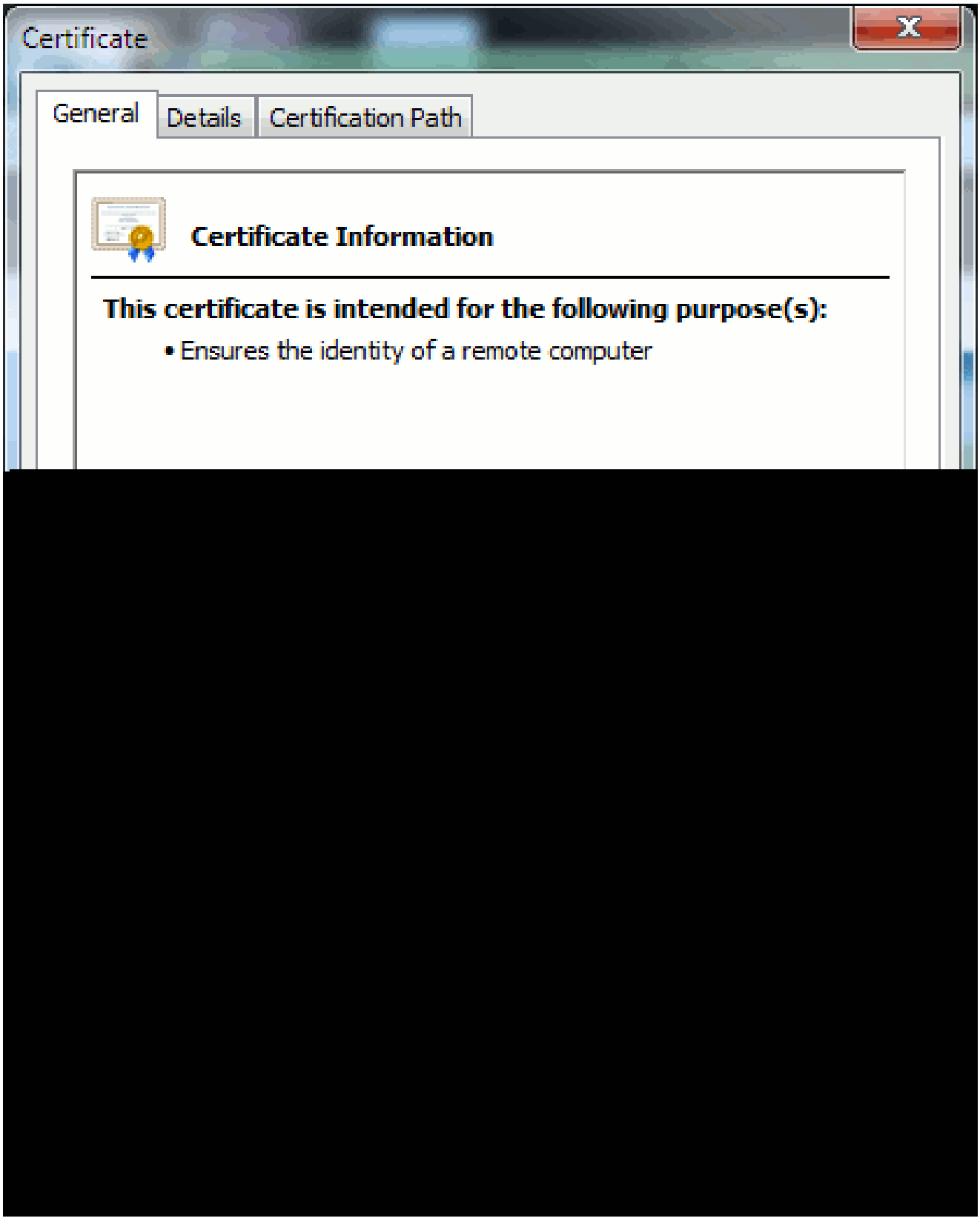
1. Cliquez sur le cadenas et une fenêtre s'affiche :

   Figure 1 : Identification du site Web



2. Cliquez sur Afficher les certificats pour afficher le certificat du site, comme indiqué dans cet exemple :

Figure 2 : Onglet Informations générales sur le certificat



Les informations mises en évidence sont importantes.

- Émis par est la société ou l'autorité de certification (CA) que votre système approuve déjà.
- Valide du/au est la plage de dates à laquelle ce certificat peut être utilisé. (Parfois, vous voyez un certificat dont vous savez que vous faites confiance à l'autorité de

certification, mais vous voyez que le certificat n'est pas valide. Vérifiez toujours la date afin de savoir si elle a expiré ou non.)

Conseil : il est recommandé de créer un rappel dans votre calendrier pour renouveler le certificat avant son expiration. Cela évite les problèmes futurs.

Les différences entre les certificats PEM et DER

PEM est ASCII ; DER est binaire. La Figure 3 illustre le format du certificat PEM.

Figure 3 : exemple de certificat 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
BQcDAgYIKwYBBQUHAwUwKQYDVR0RBCIwIIIOODUxUHViLmtqbC5jb22CDnBob25l
cy5ramwuY29tMB0GA1UdDgQWBBTbWvEUfpl7hvrsTJpQfmcoNpB4LzANBgkqhkiG
9w0BAQUFAAOCAQEArZWeqarg4tagW0O0rQElZj6UJ9S8ZAcp9XDT4Iz1QwRaaiBr
EBhfulaMjmtMKXFV5eCU9QcPbPG8XmiRZiEg9Q8Wtn0OZpuPGlkwxmFYRz40aY4T
5lw+d0wVb9sPChNQEGccjjqwtstElYWDo/A4RoqdH0ALceP8a4bovK/CpmRGdb5C
+hqP4zIJs4P+YKmzrJeq7H8xCCqqkYXcRLkmG6mif78txFQ5lr8rJEoU1VlL8znc
fJvSfEsCfwnSqPaGcQTnxMOZOIyM0OjXvvhWIezrpk8cyj3vSTgXSTwO53flZX4L
tu28d5H3AHo8U6cfHRIJ1f6Yv2ClGBShXwFp6Q==
-----END CERTIFICATE-----
```

La Figure 4 présente le certificat DER.

Figure 4 : Exemple de certificat DER

La plupart des sociétés AC comme VeriSign ou Thawt utilisent le format PEM pour envoyer les certificats aux clients, car il est facile d'envoyer des e-mails. Le client doit copier la chaîne entière et inclure -----BEGIN CERTIFICATE— et -----END CERTIFICATE—, la coller dans un fichier texte et l'enregistrer avec l'extension .PEM ou .CER.

Windows peut lire les formats DER et CER avec sa propre applet de gestion des certificats et

affiche le certificat comme illustré à la Figure 5.

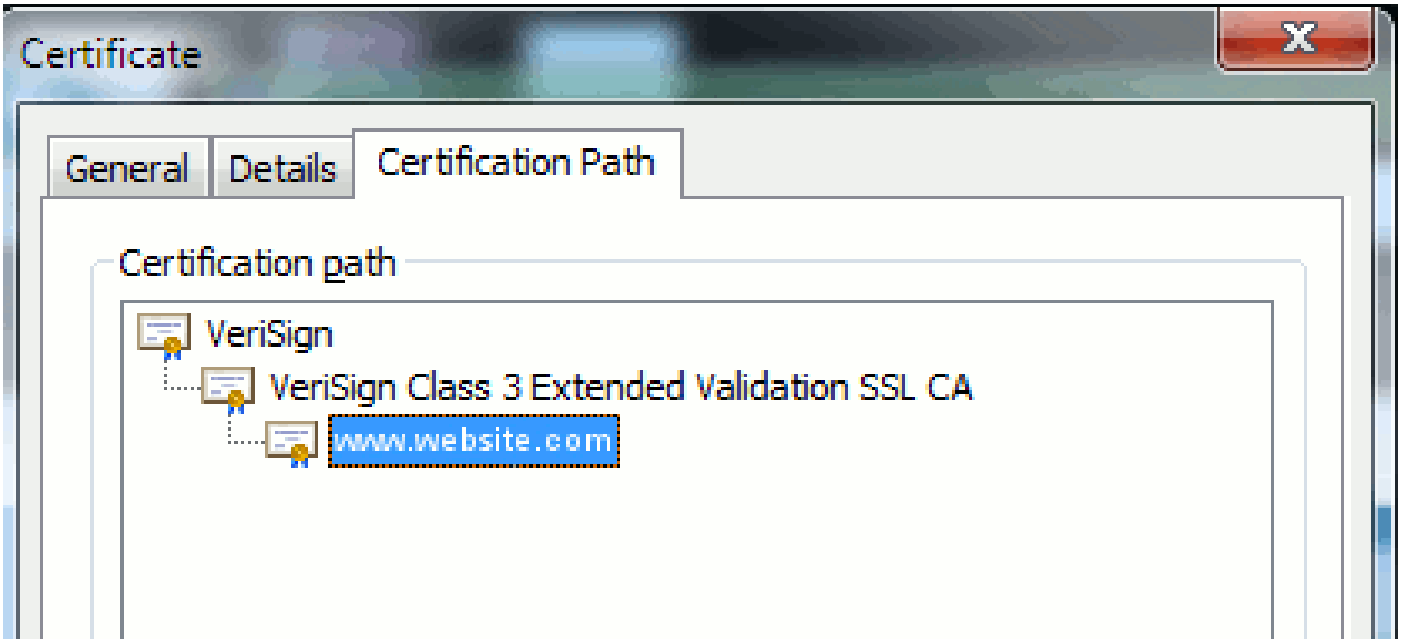
Figure 5 : Informations sur le certificat

Dans certains cas, un périphérique nécessite un format spécifique (ASCII ou binaire). Afin de changer cela, téléchargez le certificat de l'autorité de certification dans le format requis ou utilisez un outil de conversion SSL, tel que https://www.sslshopper.com/ssl-converter.html.

Hiérarchie de certificat

Pour faire confiance à un certificat à partir d'un point d'extrémité, il doit y avoir une confiance déjà établie avec une autorité de certification tierce. Par exemple, la Figure 6 montre qu'il existe une hiérarchie de trois certificats.

Figure 6 : Hiérarchie des certificats



- Verisign est une CA.
- Verisign Class 3 Extended Validation SSL CA est un certificat de serveur intermédiaire ou de signature (un serveur autorisé par CA à émettre des certificats en son nom).
- www.website.com est un certificat de serveur ou de service.

Votre point d'extrémité doit savoir qu'il peut faire confiance à la fois aux certificats CA et intermédiaires avant de savoir qu'il peut faire confiance au certificat de serveur présenté par la connexion SSL (détails ci-dessous). Pour mieux comprendre comment cette confiance fonctionne, référez-vous à la section dans ce document : Définir la "confiance" du point de vue d'un certificat.

Comparaison entre les certificats auto-signés et les certificats tiers

Les principales différences entre les certificats auto-signés et les certificats tiers sont la personne qui a signé le certificat, que vous les approuviez ou non.

Un certificat auto-signé est un certificat signé par le serveur qui le présente ; par conséquent, le certificat de serveur/service et le certificat d'autorité de certification sont identiques.

Une autorité de certification tierce est un service fourni par une autorité de certification publique (comme Verisign, Entrust, Digicert) ou un serveur (comme Windows 2003, Linux, Unix, IOS) qui contrôle la validité du certificat de serveur/service.

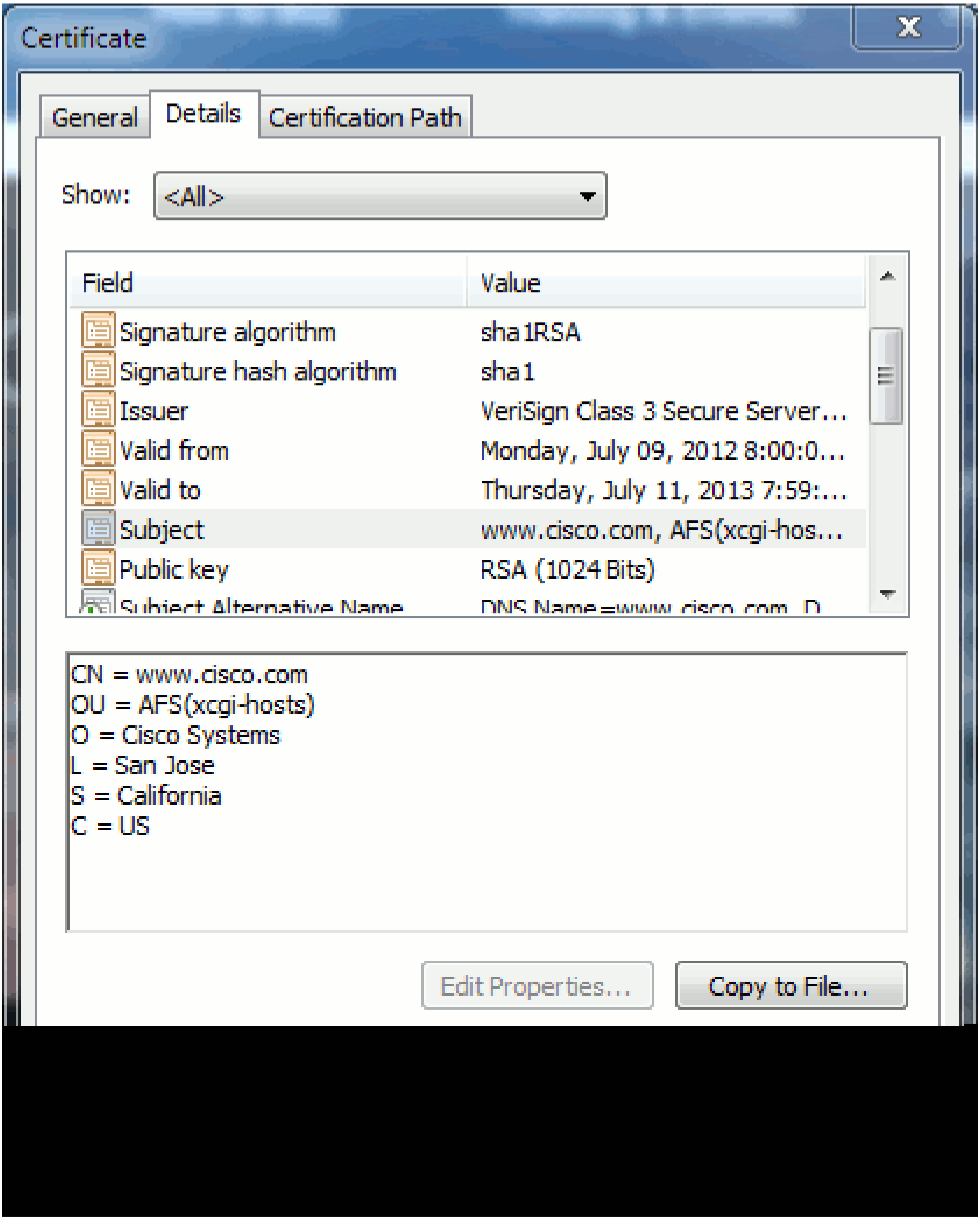
Chacun peut être une autorité de certification. Que votre système fasse confiance ou non à cette autorité de certification, c'est ce qui importe le plus.

Noms usuels et noms secondaires des sujets

Les noms communs (CN) et les autres noms de sujet (SAN) font référence à l'adresse IP ou au nom de domaine complet (FQDN) de l'adresse demandée. Par exemple, si vous entrez https://www.cisco.com, alors le CN ou le SAN doit avoir www.cisco.com dans l'en-tête.

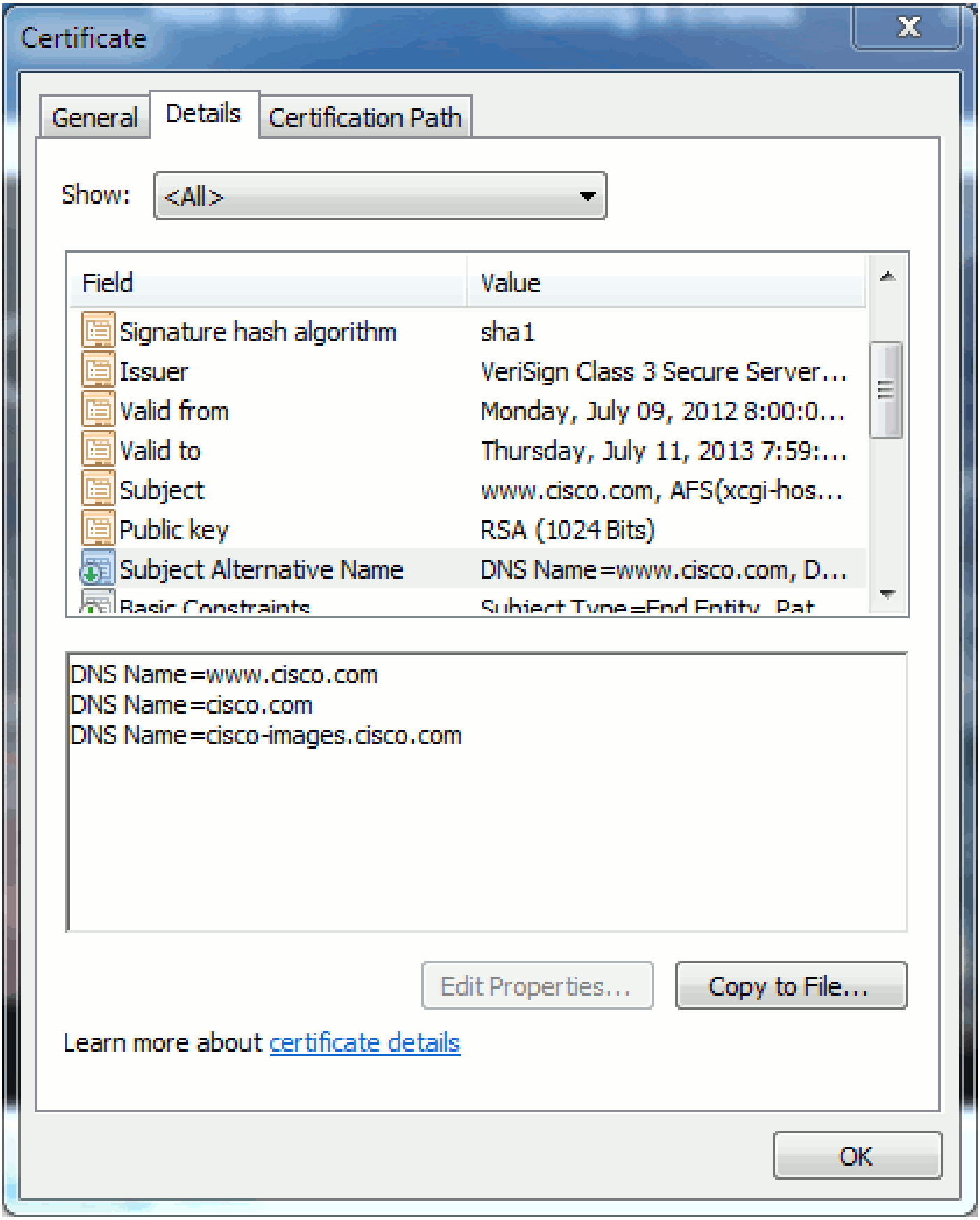
Dans l'exemple illustré à la Figure 7, le certificat a le CN comme www.cisco.com. La demande d'URL pour www.cisco.com du navigateur vérifie le nom de domaine complet de l'URL par rapport aux informations que le certificat présente. Dans ce cas, ils correspondent et cela indique que la connexion SSL a réussi. Ce site Web a été vérifié pour être le site Web correct et les communications sont maintenant chiffrées entre le bureau et le site Web.

Figure 7 : Vérification du site Web



Dans le même certificat, il y a un en-tête SAN pour trois adresses FQDN/DNS :

Figure 8 : en-tête SAN



Ce certificat peut authentifier/vérifier www.cisco.com (également défini dans le CN), cisco.com et cisco-images.cisco.com. Cela signifie que vous pouvez également taper cisco.com, et ce même certificat peut être utilisé pour authentifier et chiffrer ce site Web.

CUCM peut créer des en-têtes SAN. Référez-vous au document de Jason Burn, CUCM Uploading

CCMAdmin Web GUI Certificates on the Support Community pour plus d'informations sur les en-têtes SAN.

Certificats de caractères génériques

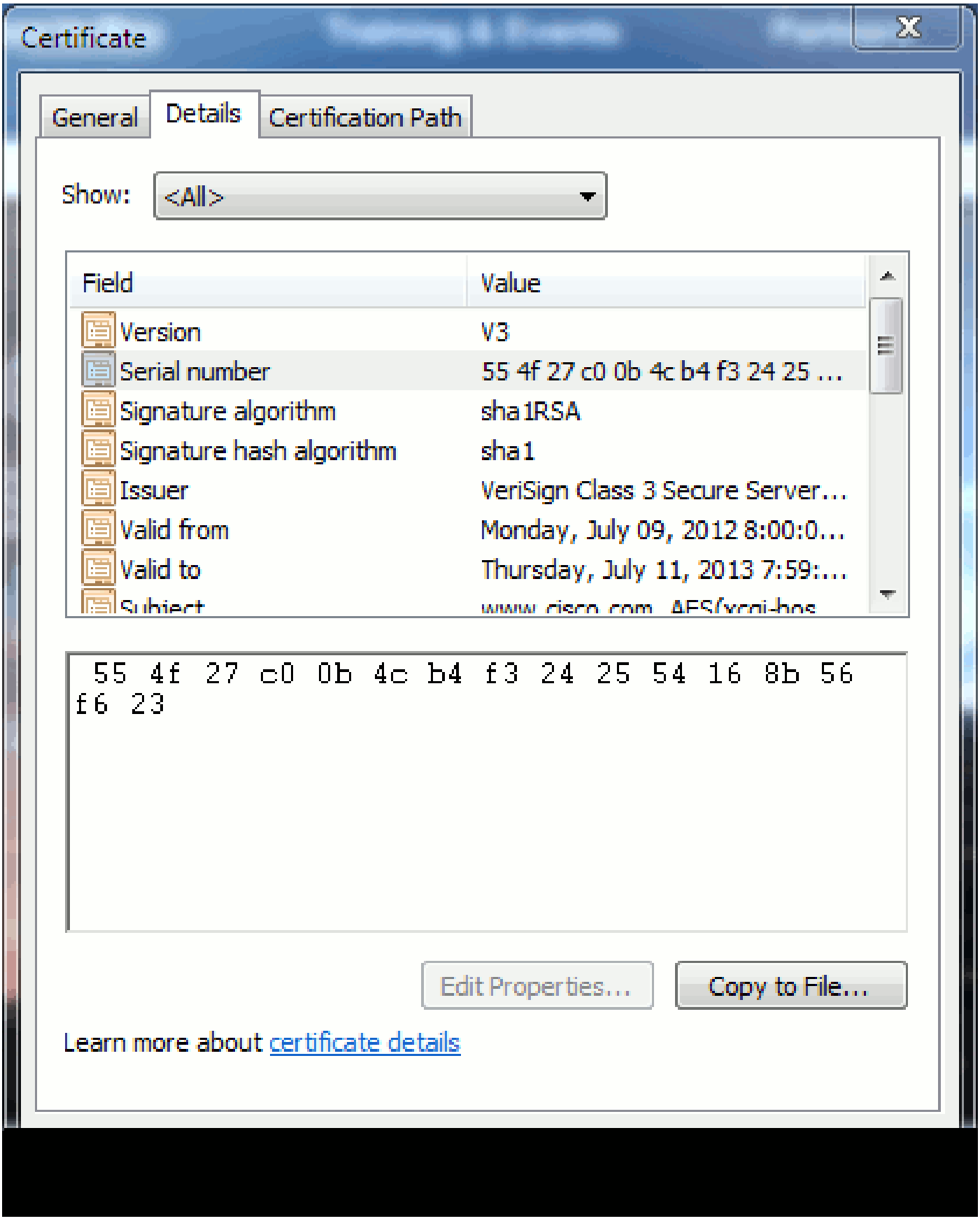
Les certificats génériques sont des certificats qui utilisent un astérisque (*) pour représenter n'importe quelle chaîne dans une section d'une URL. Par exemple, afin d'avoir un certificat pour www.cisco.com, ftp.cisco.com, ssh.cisco.com, et ainsi de suite, un administrateur aurait seulement besoin de créer un certificat pour *.cisco.com. Afin d'économiser de l'argent, l'administrateur n'a besoin d'acheter qu'un seul certificat et n'a pas besoin d'acheter plusieurs certificats.

Cette fonctionnalité n'est actuellement pas prise en charge par Cisco Unified Communications Manager (CUCM). Cependant, vous pouvez garder une trace de cette amélioration : CSCta14114 : Demande de support de certificat générique dans CUCM et importation de clé privée.

Identifier les certificats

Lorsque les certificats contiennent les mêmes informations, vous pouvez voir s’il s’agit du même certificat. Tous les certificats ont un numéro de série unique. Vous pouvez l'utiliser pour comparer si les certificats sont identiques, régénérés ou contrefaits. La figure 9 fournit un exemple :

Figure 9 : Numéro de série du certificat



RSE et leur objectif

CSR signifie Certificate Signing Request. Si vous souhaitez créer un certificat tiers pour un serveur CUCM, vous avez besoin d'un CSR à présenter à l'autorité de certification. Ce CSR

ressemble beaucoup à un certificat PEM (ASCII).

Remarque : il ne s'agit pas d'un certificat et ne peut pas être utilisé comme tel.

\

CUCM crée automatiquement des CSR via l'interface utilisateur graphique Web : Cisco Unified Operating System Administration > Security > Certificate Management > Generate CSR, choisissez le service que vous souhaitez créer le certificat snf puis Generate CSR. Chaque fois que cette option est utilisée, une nouvelle clé privée et un nouveau CSR sont générés.

Remarque : une clé privée est un fichier unique pour ce serveur et ce service. Cela ne devrait jamais être donné à personne ! Si vous fournissez une clé privée à quelqu'un, cela compromet la sécurité que le certificat fournit. En outre, ne régénérez pas un nouveau CSR pour le même service si vous utilisez l'ancien CSR pour créer un certificat. CUCM supprime l'ancienne CSR et la clé privée et les remplace toutes les deux, ce qui rend l'ancienne CSR inutile.

Reportez-vous à la documentation de Jason Burn sur la communauté de support : CUCM Uploading CCMAdmin Web GUI Certificates pour plus d'informations sur la façon de créer des CSR.

Utilisation de certificats entre le point d'extrémité et le processus de connexion SSL/TLS

Le protocole d'échange est une série de messages séquencés qui négocient les paramètres de sécurité d'une session de transfert de données. Référez-vous à SSL/TLS in Detail , qui documente la séquence de messages dans le protocole d'échange. Elles sont visibles dans la capture de paquets (PCAP). Les détails incluent les messages initiaux, ultérieurs et finaux envoyés et reçus entre le client et le serveur.

Comment CUCM utilise les certificats

La différence entre tomcat et tomcat-trust

Lorsque des certificats sont téléchargés vers CUCM, il existe deux options pour chaque service via Cisco Unified Operating System Administration > Security > Certificate Management > Find.

Les cinq services qui vous permettent de gérer les certificats dans CUCM sont :

- tomcat

- ipsec
- callmanager
- capf
- téléviseurs (dans CUCM version 8.0 et ultérieure)

Voici les services qui vous permettent de télécharger des certificats vers CUCM :

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

Voici les services disponibles dans CUCM version 8.0 et ultérieure :

- tvs
- télétrust
- phone-trust
- phone-vpn-trust
- phone-sast-trust
- phone-ctl-trust

Référez-vous aux Guides de sécurité CUCM par version pour plus de détails sur ces types de certificats. Cette section explique uniquement la différence entre un certificat de service et un certificat d'approbation.

Par exemple, avec tomcat, le tomcat-trusts télécharge les certificats d'autorité de certification et intermédiaires de sorte que ce noeud CUCM sache qu'il peut faire confiance à n'importe quel certificat signé par l'autorité de certification et le serveur intermédiaire. Le certificat tomcat est le certificat présenté par le service tomcat sur ce serveur si un point de terminaison envoie une requête HTTP à ce serveur. Afin de permettre la présentation de certificats tiers par tomcat, le noeud CUCM doit savoir qu'il peut faire confiance à l'autorité de certification et au serveur intermédiaire. Par conséquent, il est nécessaire de télécharger les certificats d'autorité de

certification et intermédiaires avant le téléchargement du certificat tomcat (service).

Référez-vous à Téléchargement CUCM CCMAdmin Web GUI Certificates de Jason Burn sur la communauté de support pour des informations qui vous aideront à comprendre comment télécharger des certificats vers CUCM.

Chaque service possède son propre certificat de service et des certificats de confiance. Ils ne fonctionnent pas les uns des autres. En d'autres termes, une autorité de certification et un certificat intermédiaire téléchargés en tant que service tomcat-trust ne peuvent pas être utilisés par le service CallManager.

Remarque : les certificats dans CUCM sont basés sur un noeud. Par conséquent, si vous avez besoin de certificats téléchargés vers l'éditeur et que vous avez besoin que les abonnés aient les mêmes certificats, vous devez les télécharger vers chaque serveur et noeud individuel avant la version 8.5 de CUCM. Dans CUCM version 8.5 et ultérieure, il existe un service qui réplique les certificats téléchargés vers le reste des noeuds du cluster.

Remarque : chaque noeud a un CN différent. Par conséquent, un CSR doit être créé par chaque noeud afin que le service présente ses propres certificats.

Si vous avez d'autres questions spécifiques sur l'une des fonctions de sécurité de CUCM, reportez-vous à la documentation de sécurité.

Conclusion

Ce document fournit une assistance et établit un niveau élevé de connaissances sur les certificats. Ce sujet peut devenir plus approfondi, mais ce document vous familiarise suffisamment pour travailler avec les certificats. Si vous avez des questions sur les fonctions de sécurité de CUCM, référez-vous aux Guides de sécurité de CUCM par version pour plus d'informations.

Informations connexes

- Guides de maintenance et de sécurité de Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- Communauté d'assistance Cisco : CUCM Téléchargement des certificats CCMAdmin Web GUI
- Bogue CSCta14114 : Demande de prise en charge du certificat générique dans CUCM et de l'importation de clé privée
- Présentation de Cisco Emergency Responder (CER)
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.