Vue de haut niveau des certificats et des autorités dans CUCM

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Conventions
Objet des certificats
Définir la confiance du point de vue d'un certificat
Utilisation des certificats par les navigateurs
Différences entre les certificats PEM et DER
Hiérarchie des certificats
Certificats auto-signés et certificats tiers
Noms communs et noms de remplacement des sujets
Certificats de carte générique
Identification des certificats
RSE et leurs objectifs
Utilisation de certificats entre le point de terminaison et le processus de connexion SSL/TLS
Comment CUCM utilise les certificats
La différence entre tomcat et tomcat-trust
Conclusion
Informations connexes

Introduction

Ce document a pour objet de comprendre les bases des certificats et des autorités de certification. Ce document complète les autres documents Cisco qui font référence à toutes les fonctions de chiffrement ou d'authentification dans Cisco Unified Communications Manager (CUCM).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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 points d'extrémité pour créer une confiance/authentification et un chiffrement des données. Cela confirme que les points de terminaison communiquent avec le périphérique prévu et ont la possibilité de chiffrer les données entre les deux points de terminaison.

Définir la confiance du point de vue d'un certificat

La partie la plus importante des certificats est la définition des points de terminaison auxquels votre point de terminaison peut faire confiance. Ce document vous aide à connaître et à définir comment vos données sont cryptées et partagées avec le site Web, le téléphone, le serveur FTP, etc.

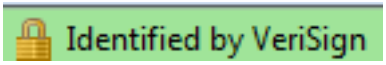
Lorsque votre système fait confiance à un certificat, cela signifie qu'il y a un ou plusieurs certificats préinstallés sur votre système qui indiquent qu'il est sûr à 100 % qu'il partage des informations avec le point de terminaison correct. Sinon, il met fin à la communication entre ces points d'extrémité.

Un exemple non technique de ceci est votre permis de conduire. Vous utilisez cette licence (certificat de serveur/service) pour prouver que vous êtes celui que vous déclarez être ; vous avez obtenu votre permis 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 présenter votre permis (certificat de serveur/service) à un agent, celui-ci sait qu'il peut faire confiance à la succursale du DMV (certificat intermédiaire) et à la Division des véhicules automobiles (autorité de certification), et il peut vérifier que cette licence a été délivrée par lui (autorité de certification). Votre identité est vérifiée auprès de l'agent et maintenant ils font confiance à vous qui dites être. Sinon, si vous donnez une fausse licence (certificat serveur/service) qui n'a pas été signée par le DMV (certificat intermédiaire), alors ils ne feront pas confiance à qui vous dites être. Le reste de ce document fournit une explication technique détaillée de la hiérarchie des certificats.

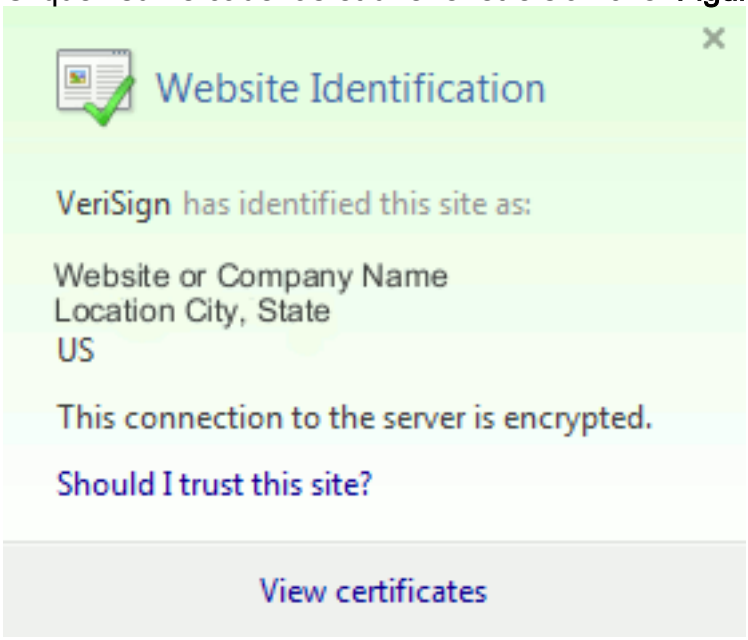
Utilisation des certificats par les navigateurs

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

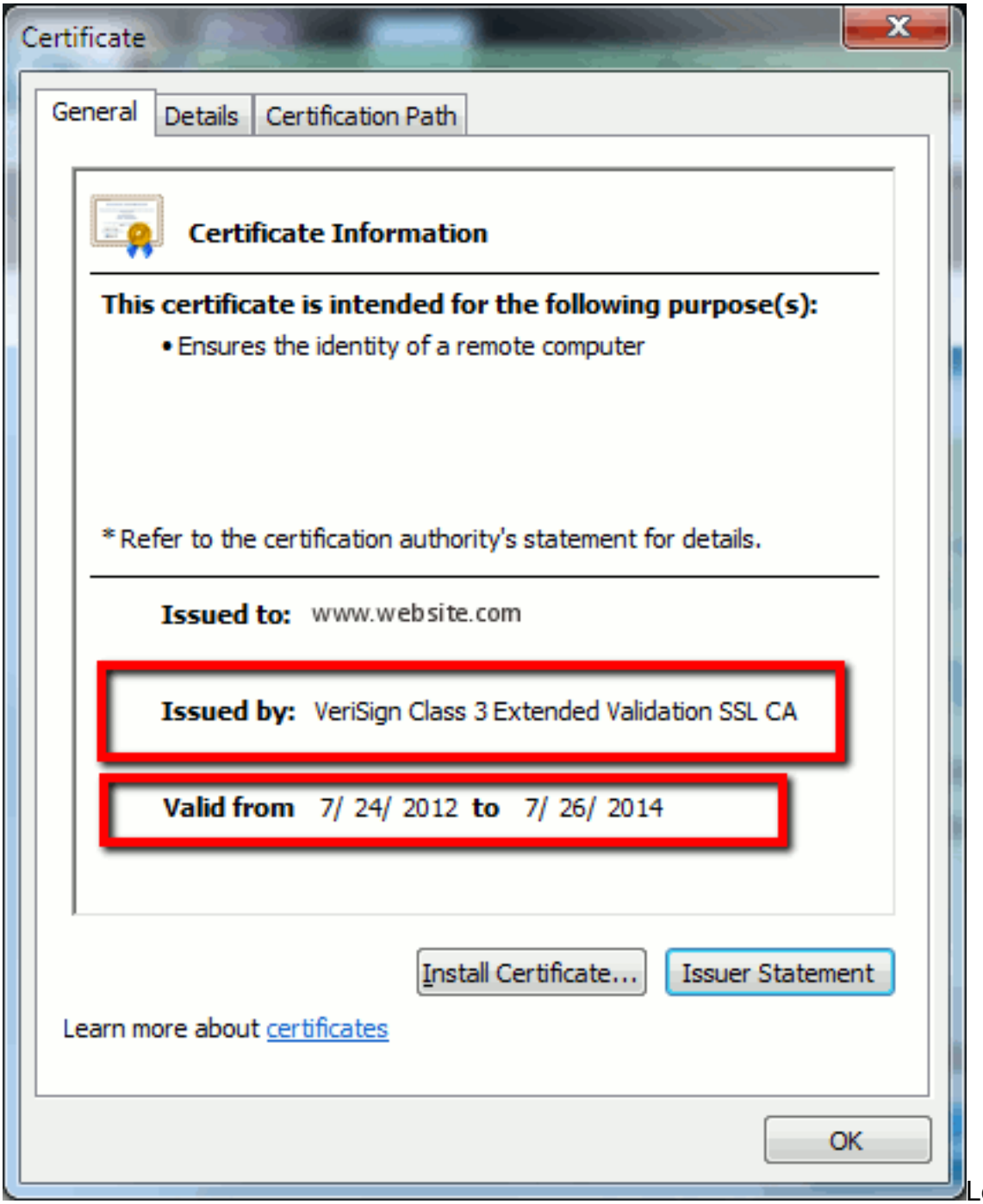
Sans certificat, il est impossible de savoir si un serveur DNS non autorisé a été utilisé ou si vous avez été routé vers un autre serveur. Les certificats s'assurent que vous êtes correctement et en toute sécurité acheminé vers le site Web prévu, tel que le site Web de votre banque, où les informations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

Tous les navigateurs ont des icônes différentes, mais normalement, un cadenas s'affiche 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 voir le certificat du site comme indiqué dans cet exemple :**Figure 2 : Informations sur le certificat, onglet Général**



Les informations mises en évidence sont importantes.**Délivré par** est la société ou l'autorité de certification (CA) qui fait déjà confiance à votre système.**Valide de/à** est la plage de dates que ce certificat est utilisable. (Parfois, vous voyez un certificat où 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.)**CONSEIL :** Il est recommandé de créer un rappel dans votre calendrier pour renouveler le certificat avant son expiration. Cela évite les problèmes futurs.

Différences entre les certificats PEM et DER

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

Figure 3 : Exemple de certificat PEM

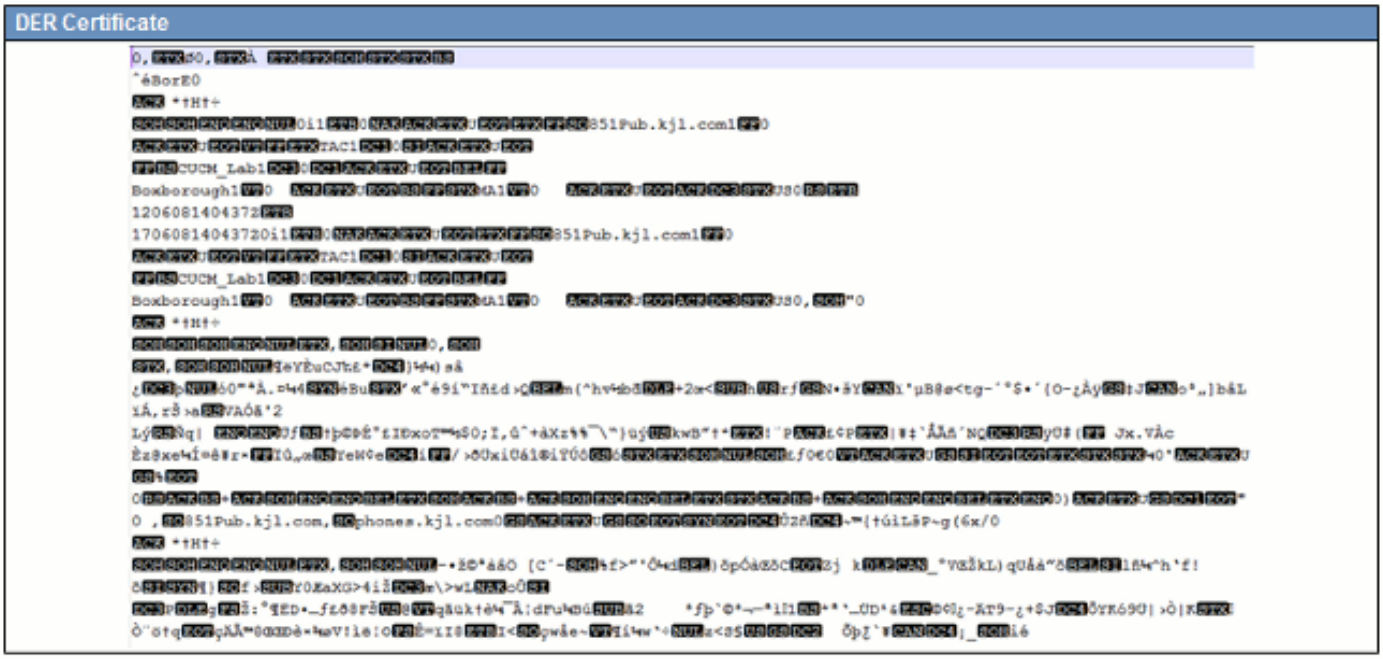
PEM Certificate

```
-----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
BQcDAgYIKwYBBQUHAwUwKQYDVR0RBCIwIIIODUxUHViLmtqbC5jb22CDnBob251
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

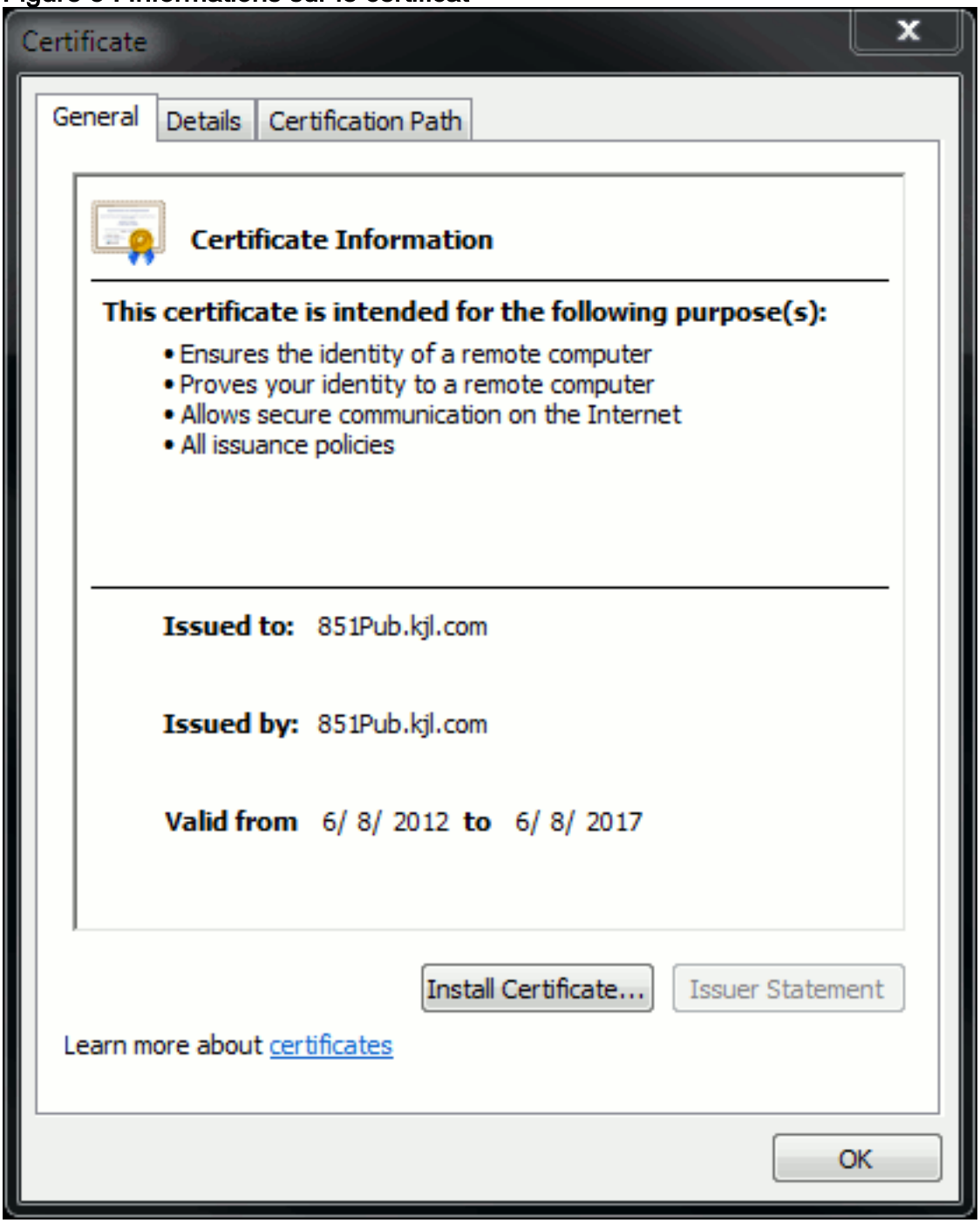
DER Certificate



La plupart des sociétés de CA comme VeriSign ou Thawt utilisent le format PEM pour envoyer les certificats aux clients, car il est convivial par courriel. 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

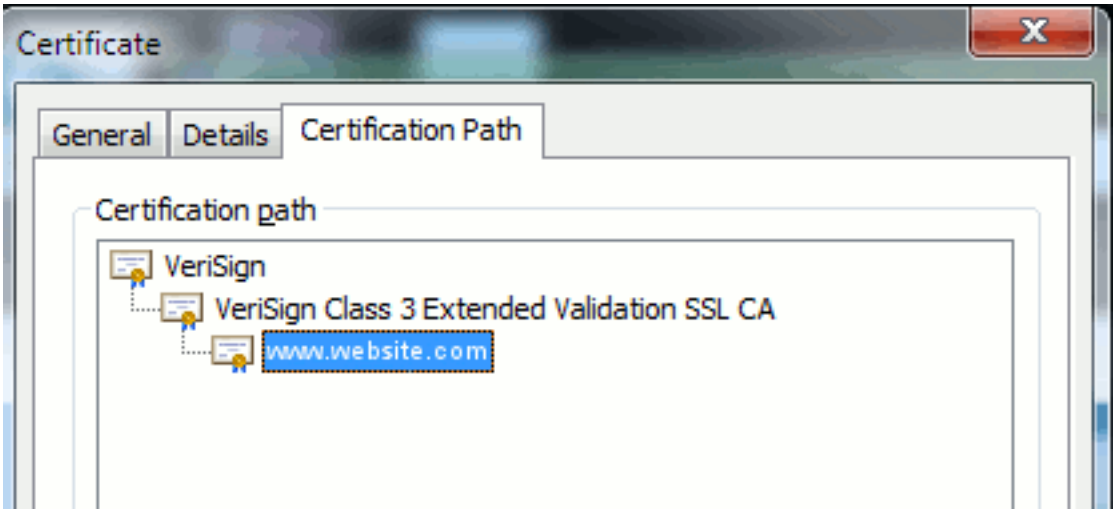


Dans certains cas, un périphérique nécessite un format spécifique (ASCII ou binaire). Afin de changer cela, téléchargez le certificat de l'autorité de certification au format requis ou utilisez un outil de conversion SSL, tel que https://www.sslshopper.com/ssl-converter.html.

Hiérarchie des certificats

Pour faire confiance à un certificat d'un point final, il doit y avoir une fiducie 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 l'autorité de certification à émettre des certificats dans son nom).
- **www.website.com** est un certificat de serveur ou de service.

Votre point de terminaison doit savoir qu'il peut faire confiance à la fois aux certificats CA et intermédiaire avant de savoir qu'il peut faire confiance au certificat serveur présenté par la connexion SSL (détails ci-dessous). Pour mieux comprendre le fonctionnement de cette approbation, reportez-vous à la section de ce document : **Définissez « Confiance » du point de vue d'un certificat**.

Certificats auto-signés et certificats tiers

Les principales différences entre les certificats auto-signés et les certificats tiers sont ceux qui ont signé le certificat, que vous leur fassiez confiance.

Un certificat auto-signé est un certificat signé par le serveur qui le présente ; par conséquent, le certificat serveur/service et le certificat CA 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 serveur/service.

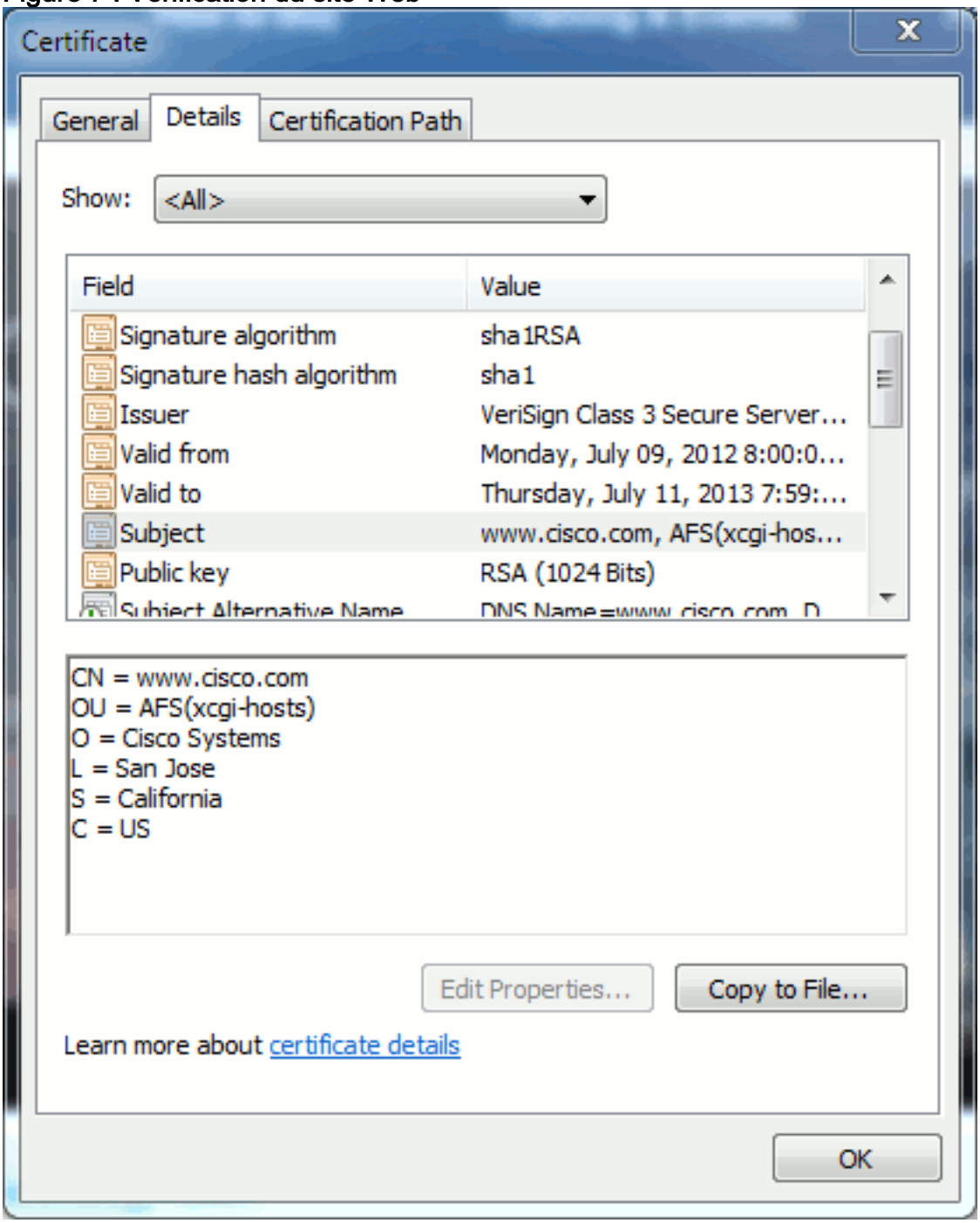
Chacun peut être une autorité de certification. Que votre système ait ou non confiance en cette CA, c'est ce qui compte le plus.

Noms communs et noms de remplacement des sujets

Les noms communs (CN) et les noms alternatifs d'objet (SAN) sont des références à l'adresse IP ou au nom de domaine complet (FQDN) de l'adresse demandée. Par exemple, si vous entrez https://www.cisco.com, le CN ou le SAN doit avoir www.cisco.com dans l'en-tête.

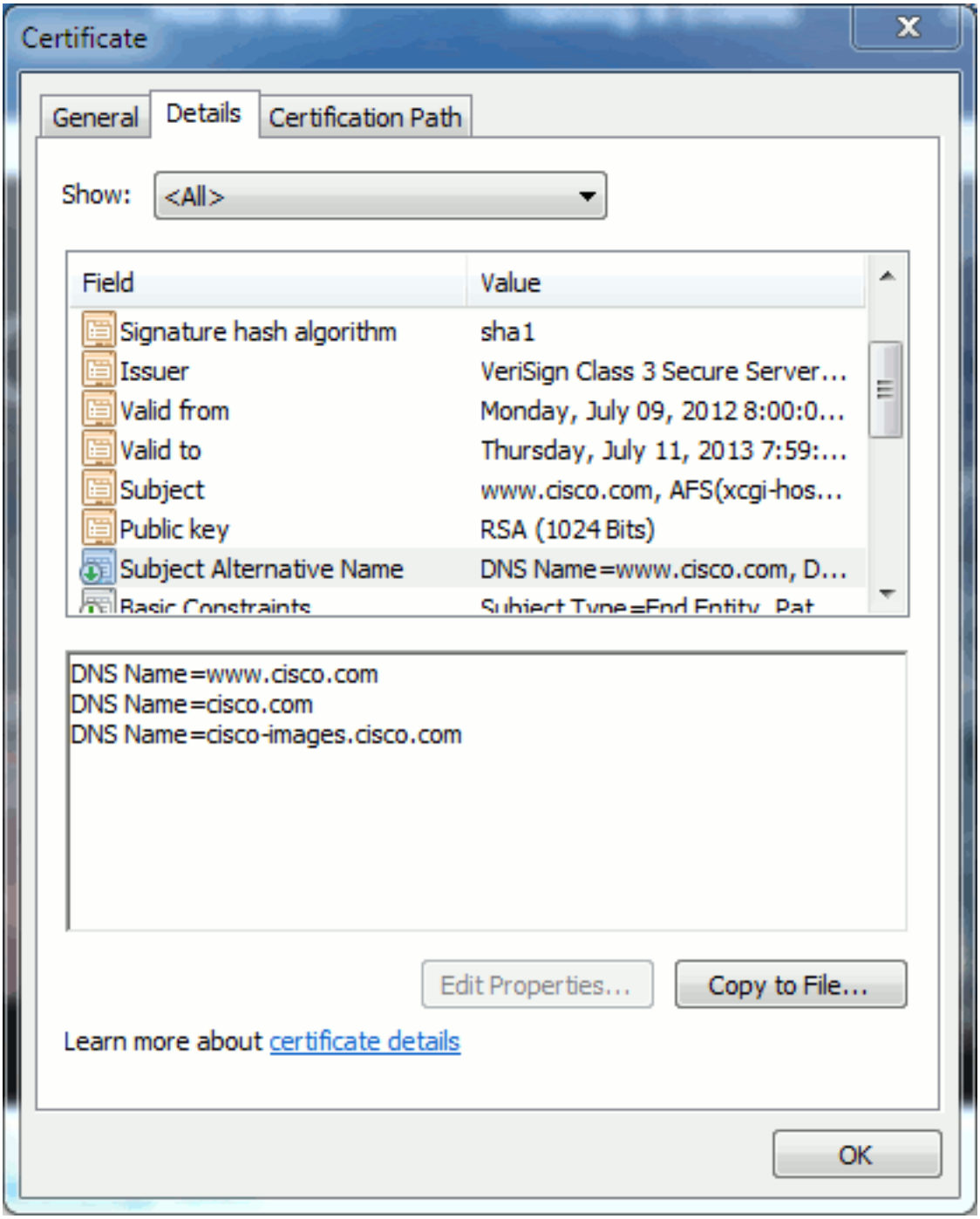
Dans l'exemple illustré à la Figure 7, le certificat a le code CN comme www.cisco.com. La demande d'URL pour www.cisco.com à partir du navigateur vérifie le nom de domaine complet de l'URL par rapport aux informations fournies par le certificat. Dans ce cas, ils correspondent et cela montre que la connexion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

Figure 7 : Vérification du site Web



Dans le même certificat, il existe 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 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. Reportez-vous au document de Jason Burn, CUCM Uploading CCMAdmin Web GUI Certificates sur la communauté de support pour plus d'informations sur les en-têtes SAN.

Certificats de carte générique

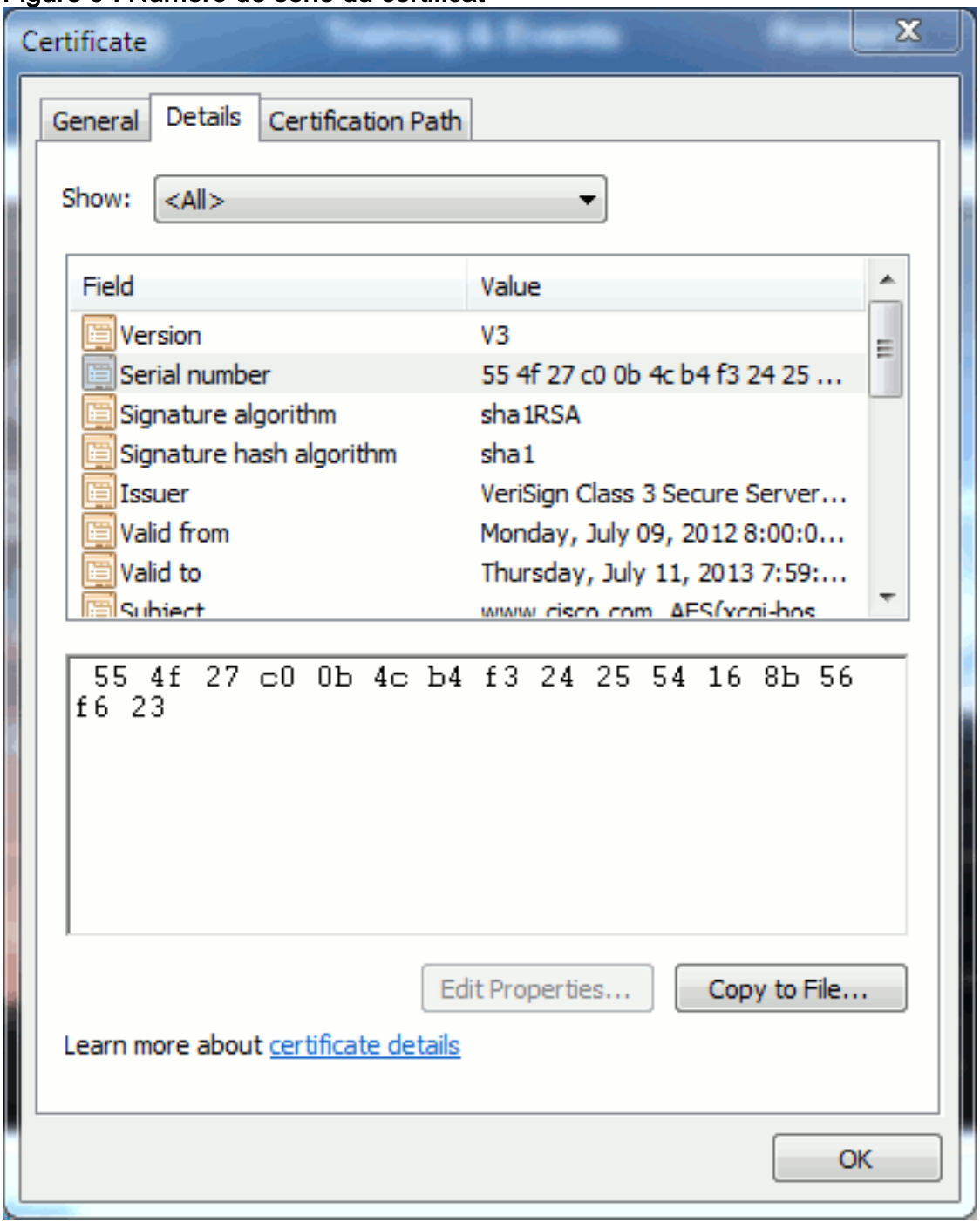
Les certificats génériques sont des certificats qui utilisent un astérisque (*) pour représenter n'importe quelle chaîne dans une section d'une URL. Par exemple, pour disposer d'un certificat pour www.cisco.com, ftp.cisco.com, ssh.cisco.com, etc., un administrateur doit uniquement créer un certificat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

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

Identification des 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 utiliser cette option 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 leurs objectifs

CSR signifie Demande de signature de certificat. Si vous voulez créer un certificat tiers pour un

serveur CUCM, vous devez présenter un CSR à l'autorité de certification. Cette CSR ressemble beaucoup à un certificat PEM (ASCII).

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

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

Remarque : Une clé privée est un fichier unique à ce serveur et à ce service. Ça 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 Téléchargement des certificats de l'interface utilisateur graphique Web CCMAdmin pour plus d'informations sur la création de CSR.

Utilisation de certificats entre le point de terminaison et le processus de connexion SSL/TLS

Le protocole d'échange de données est une série de messages séquencés qui négocient les paramètres de sécurité d'une session de transfert de données. Reportez-vous à SSL/TLS in Detail , qui documente la séquence de messages dans le protocole de connexion. Elles peuvent être vues dans une 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 les suivants :

- tomcat
- ipsec
- callmanager
- capf
- tvs (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
- tvs-trust
- phone-trust
- phone-vpn-trust
- phone-sast-trust
- phone-ctl-trust

Reportez-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 de confiance.

Par exemple, avec **tomcat**, les **tomcat-trust** téléchargent les certificats CA et intermédiaires pour que ce noeud CUCM sache qu'il peut faire confiance à tout certificat signé par l'autorité de certification et le serveur intermédiaire. Le certificat tomcat est le certificat qui est présenté par le service tomcat sur ce serveur, si un point d'extrémité fait une requête HTTP à ce serveur. Afin de permettre la présentation des 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 CA et intermédiaires avant le téléchargement du certificat tomcat (service).

Reportez-vous à Jason Burn's CUCM Uploading CCMAdmin Web GUI Certificates on the Support Community pour obtenir des informations qui vous aideront à comprendre comment télécharger des certificats dans CUCM.

Chaque service possède son propre certificat de service et ses propres certificats de confiance. Ils ne travaillent pas entre eux. 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 de CUCM sont établis par 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 sur chaque serveur et noeud avant CUCM version 8.5. Dans CUCM version 8.5 et ultérieure, il existe un service qui répliquera 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 pour 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 aide et développe un niveau élevé de connaissances sur les certificats. Ce sujet peut devenir plus approfondi, mais ce document vous familiarise assez pour travailler avec les

certificats. Si vous avez des questions sur les fonctionnalités de sécurité de CUCM, reportez-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 de l'interface utilisateur Web CCMAdmin
- Bogue CSCta14114 : Demande de support du certificat générique dans CUCM et importation de clé privée
- Réponse d'urgence Cisco (CER) expliquée
- Support et documentation techniques - Cisco Systems