CUCMでの証明書および認証局の概要

内容

はじめに

このドキュメントでは、証明書と認証局の基本について説明します。Cisco Unified Communications Manager(CUCM)の暗号化機能や認証機能に関する他のシスコドキュメントを補完します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

表記法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

証明書の目的

証明書は、エンドポイント間でデータの信頼/認証および暗号化を構築するために使用されます。これにより、エンドポイントは意図したデバイスと確実に通信できるようになり、2 台のエンドポイント間でデータを暗号化するオプションが備わります。

注：各証明書の影響を理解するには、「Cisco Unified Communications Managerの証明書再生成プロセスによる証明書ストアへの影響」の項を参照してください

証明書の観点からの信頼の定義

証明書の最も重要な部分は、エンドポイントが信頼できるエンドポイントの定義です。このドキュメントは、データを暗号化する方法と、目的の Web サイト、電話、FTP サーバなどとデータを共有する方法を理解および定義するのに役立ちます。

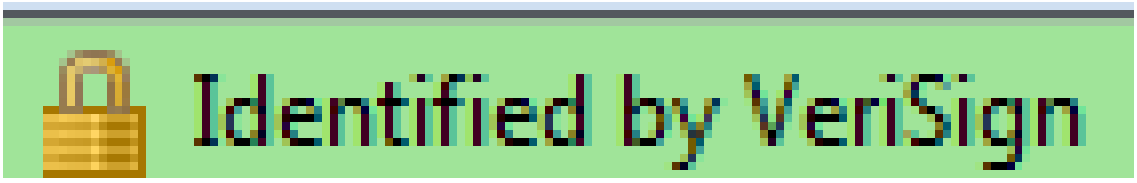
システムが証明書を信頼する場合、これは、正しいエンドポイントと情報を共有することに100%の信頼を置いていると宣言する証明書がシステムにプレインストールされていることを意味します。そうでない場合は、これらのエンドポイント間の通信を終了します。

これに関する非技術的な例は運転免許証です。このライセンス（サーバ/サービス証明書）を使用して、自分の身元を証明します。州の自動車局(DMV)から許可を受けた地域の自動車局（中間証明書）からライセンスを取得しました。職員に免許証（サーバ/サービス証明書）を提示する必要があるときには、職員は DMV 支局（中間証明書）と車両管理局（認証局）が信頼できることを知っており、この免許証がその機関（認証局）によって発行されたことを確認できます。職員は身元を確認し、自身で主張するその人の身元が正しいことを信頼します。DMV（中間証明書）によって署名されていない偽の免許証（サーバ/サービス証明書）を提示した場合、職員は、自身で主張するその人の身元を信頼しません。このドキュメントの残りの部分では、証明書階層に関する技術的な詳細な説明を提供します。

ブラウザによる証明書の使用法

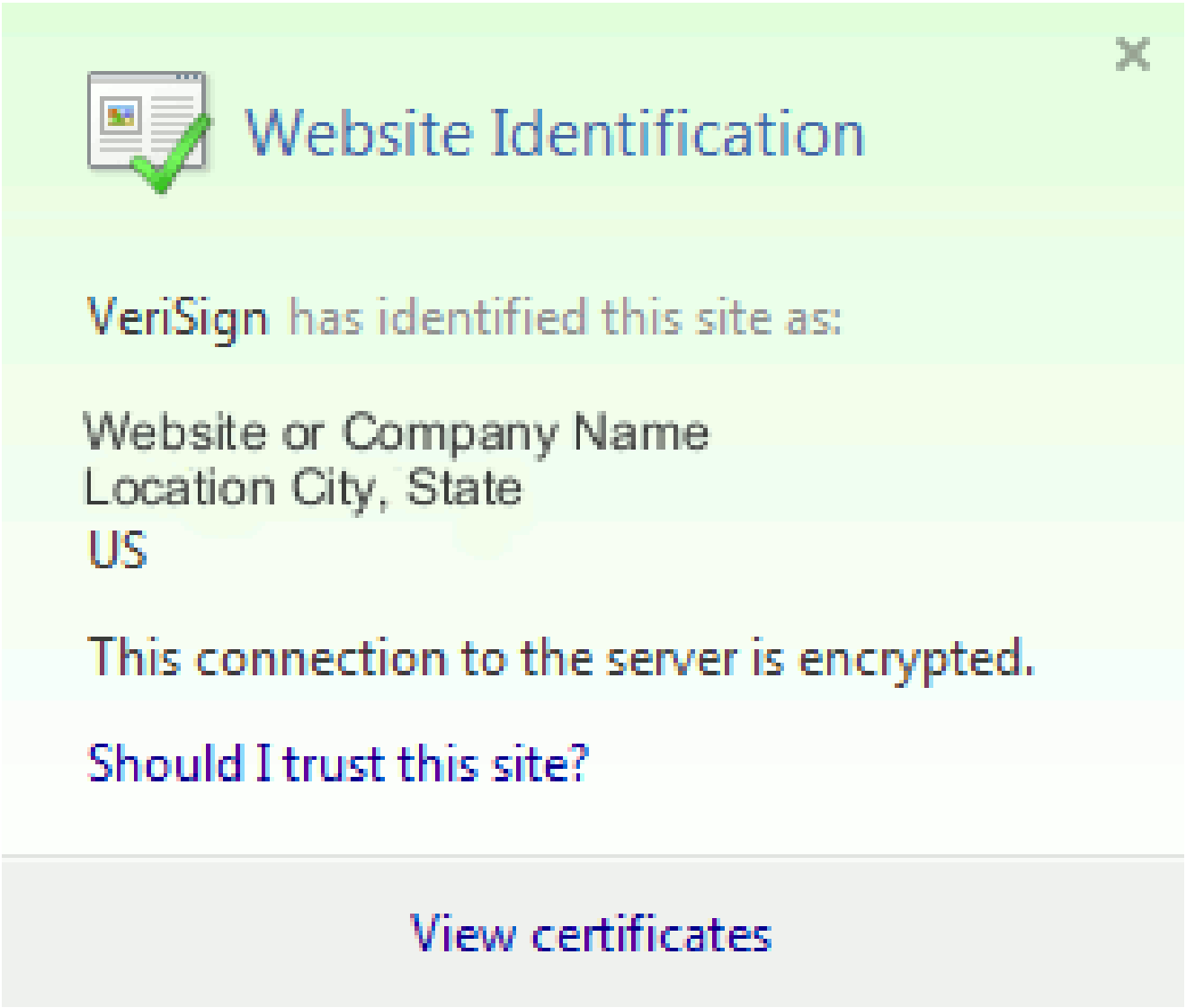
1. Web サイトにアクセスするときは、http://www.cisco.com などの URL を入力します。
2. DNS がそのサイトをホストするサーバの IP アドレスを見つけます。
3. ブラウザがそのサイトに移動します。

証明書がなければ、不正な DNS サーバが使用されていないか、または別のサーバにルーティングされていないかを知ることはできません。証明書を使用することで、銀行の Web サイトなどの目的の Web サイトに適切かつ安全にルーティングされ、そこで入力する個人情報または機密情報が保護されることが保証されます。

使用されるアイコンはブラウザによって異なりますが、通常は次のような南京錠がアドレス バーに表示されます。 

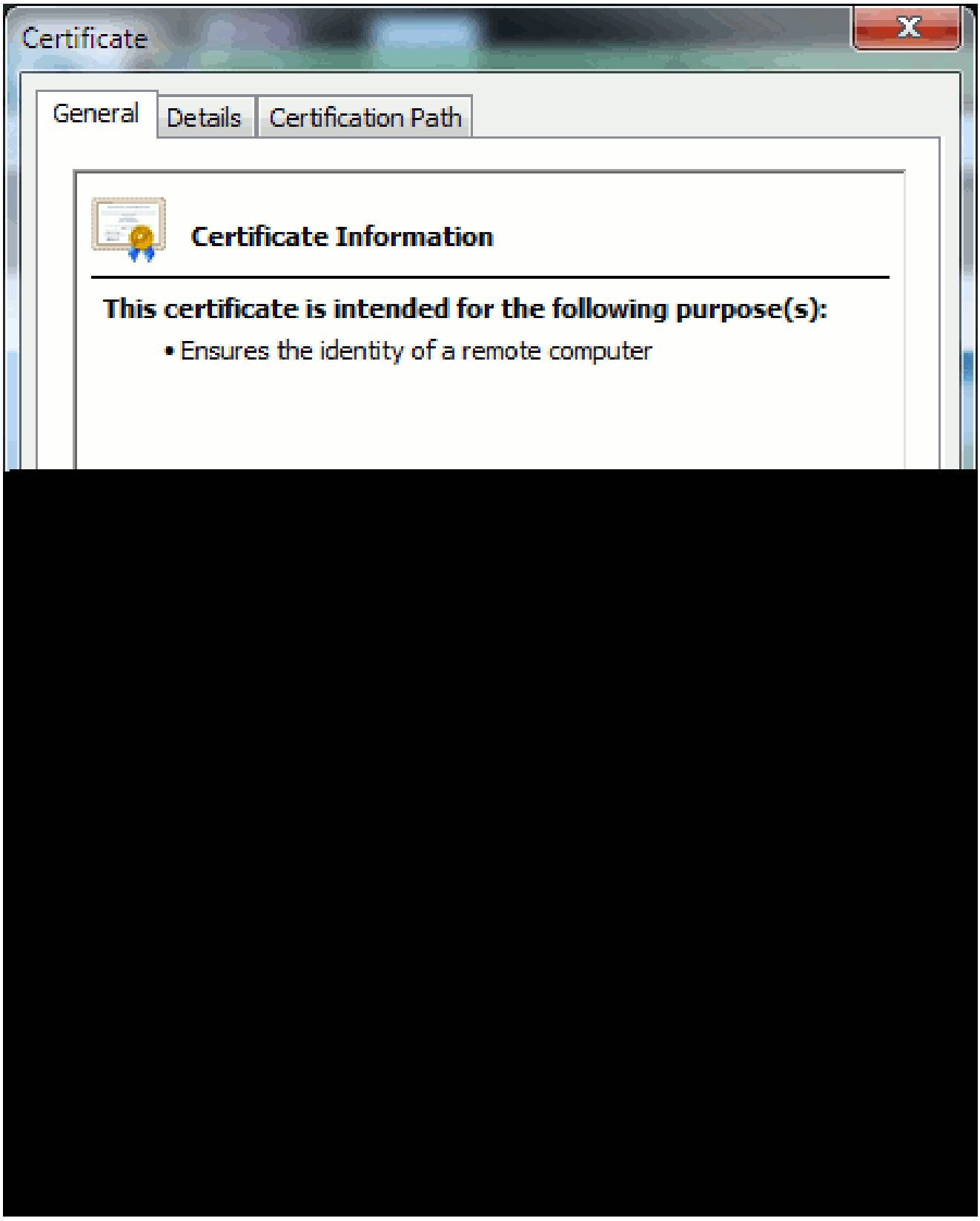
1. 南京錠をクリックすると、次のウィンドウが表示されます。

   図1: Webサイトの特定



2. 次の例に示すように、[View Certificates] をクリックしてサイトの証明書を表示します。

   図2：証明書情報の[全般]タブ



強調表示されている情報が重要です。

- [Issued by]：システムがすでに信頼している会社または認証局（CA）です。
- [Valid from/to]：この証明書が使用可能な日付範囲です（証明書の CA を信頼していることがわかっているにもかかわらず、その証明書が無効になっていることがあります。必ず日付を調べて、証明書の有効期限が切れていないかどうかを確認してください

）。

ヒント：ベストプラクティスは、カレンダーにリマインダを作成して、証明書の有効期限が切れる前に更新することです。こうすることで、今後の問題を回避できます。

PEM 証明書と DER 証明書の違い

PEMはASCII、DERは2進数です。図 3 に、PEM 証明書の形式を示します。

図3:PEM証明書の例

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
BQcDAgYIKwYBBQUHAwUwKQYDVR0RBCIwIIIOODUxUHViLmtqbC5jb22CDnBob251
cy5ramwuY29tMB0GA1UdDgQWBBTbWvEUfpl7hvrsTJpQfmcoNpB4LzANBgkqhkiG
9w0BAQUFAAOCAQEAr2Weqarg4tagW0O0rQElZj6UJ9S8ZAcp9XDT4Iz1QwRaaiBr
EBhfulaMjmtMKXFV5eCU9QcPbPG8XmiRZiEg9Q8Wtn0OZpuPGlkwxmFYRz40aY4T
5lw+d0wVb9sPChNQEGccjjqwtstElYWDo/A4RoqdH0ALceP8a4bovK/CpmRGdb5C
+hqP4zIJs4P+YKmzrJeq7H8xCCqqkYXcRLkmG6mif78txFQ5lr8rJEoU1VlL8znc
fJvSfEsCfwnSqPaGcQTnxMOZOIyM0OjXvvhWIezrpk8cyj3vSTgXSTwO53flZX4L
tu28d5H3AHo8U6cfHRIJ1f6Yv2ClGBShXwFp6Q==
-----END CERTIFICATE-----
```

図 4 に、DER 証明書を示します。

図4:DER証明書の例

PEM 形式は電子メールで扱いやすいため、VeriSign や Thawt などのほとんどの CA 企業は、顧客への証明書の送信にこの PEM 形式を使用します。文字列全体をコピーし、-----BEGIN CERTIFICATE—および-----END CERTIFICATE—を含め、それをテキストファイルにペーストして、拡張子.PEMまたは.CERを付けて保存します。

Windows は、独自の証明書管理アプレットで DER 形式と CER 形式を読み取り、図 5 で示しているような証明書を表示します。

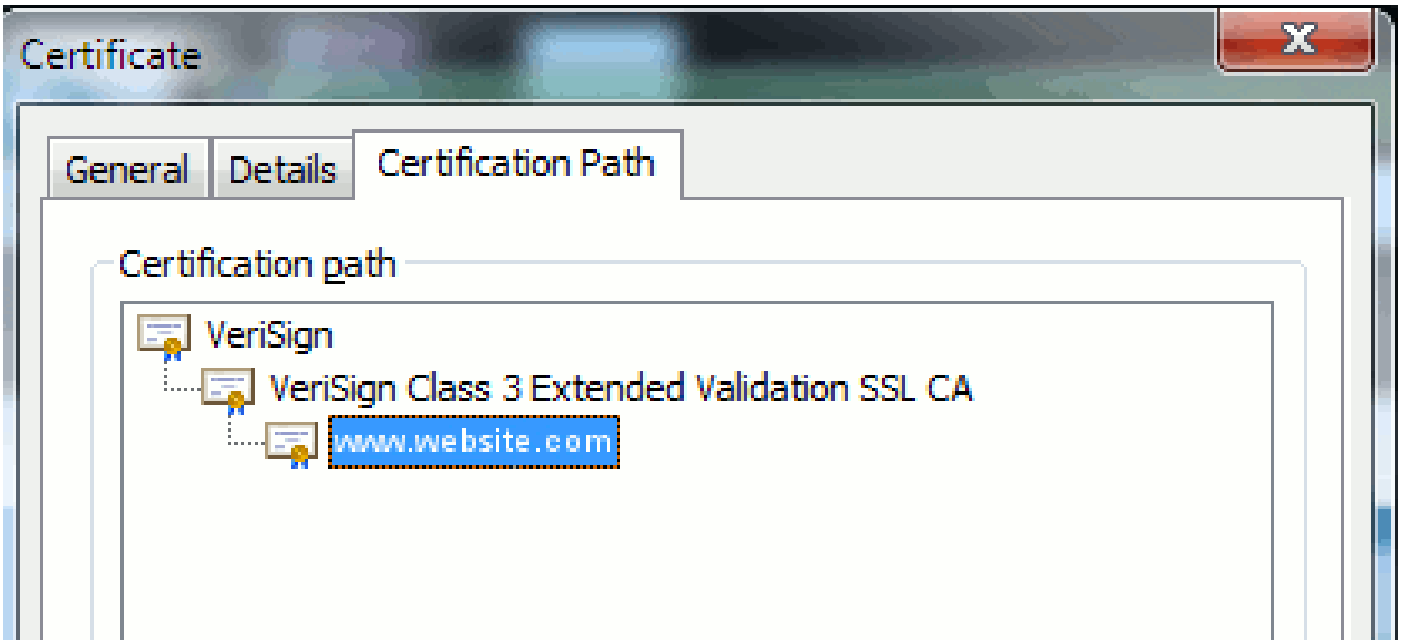
図5：証明書情報

場合によっては、デバイスで特定の形式（ASCII またはバイナリ）が必要になります。これを変更するには、CA から必要な形式の証明書をダウンロードするか、https://www.sslshopper.com/ssl-converter.html などの SSL コンバータ ツールを使用します。

証明書階層

エンドポイントからの証明書を信頼するには、サードパーティCAとの信頼がすでに確立されている必要があります。たとえば、図6は、3つの証明書の階層があることを示しています。

図6：証明書階層



- Verisign は CA です。
- Verisign Class 3 Extended Validation SSL CA は、中間証明書または署名サーバ証明書（自身の名前で証明書を発行することが CA から許可されているサーバ）です。
- www.website.com はサーバ証明書またはサービス証明書です。

エンドポイントは、SSL ハンドシェイク（詳細は下記を参照）によって提供されるサーバ証明書が信頼できることを確認する前に、まず CA と中間証明書の両方が信頼できることを確認する必要があります。この信頼の仕組みをより深く理解するには、このドキュメントの「証明書の観点からの「信頼」の定義」セクションを参照してください。

自己署名証明書とサード パーティ証明書

自己署名証明書とサードパーティ証明書の主な違いは、誰が証明書に署名したか、その署名者を信頼するかどうかです。

自己署名証明書とは、証明書を提示するサーバによって署名された証明書です。したがって、サーバ/サービス証明書とCA証明書は同じです。

サードパーティ CA は、パブリック CA（VeriSign、Entrust、Digicert など）、またはサーバ/サービス証明書の有効性を管理するサーバ（Windows 2003、Linux、UNIX、IOS など）のいずれかによって提供されるサービスです。

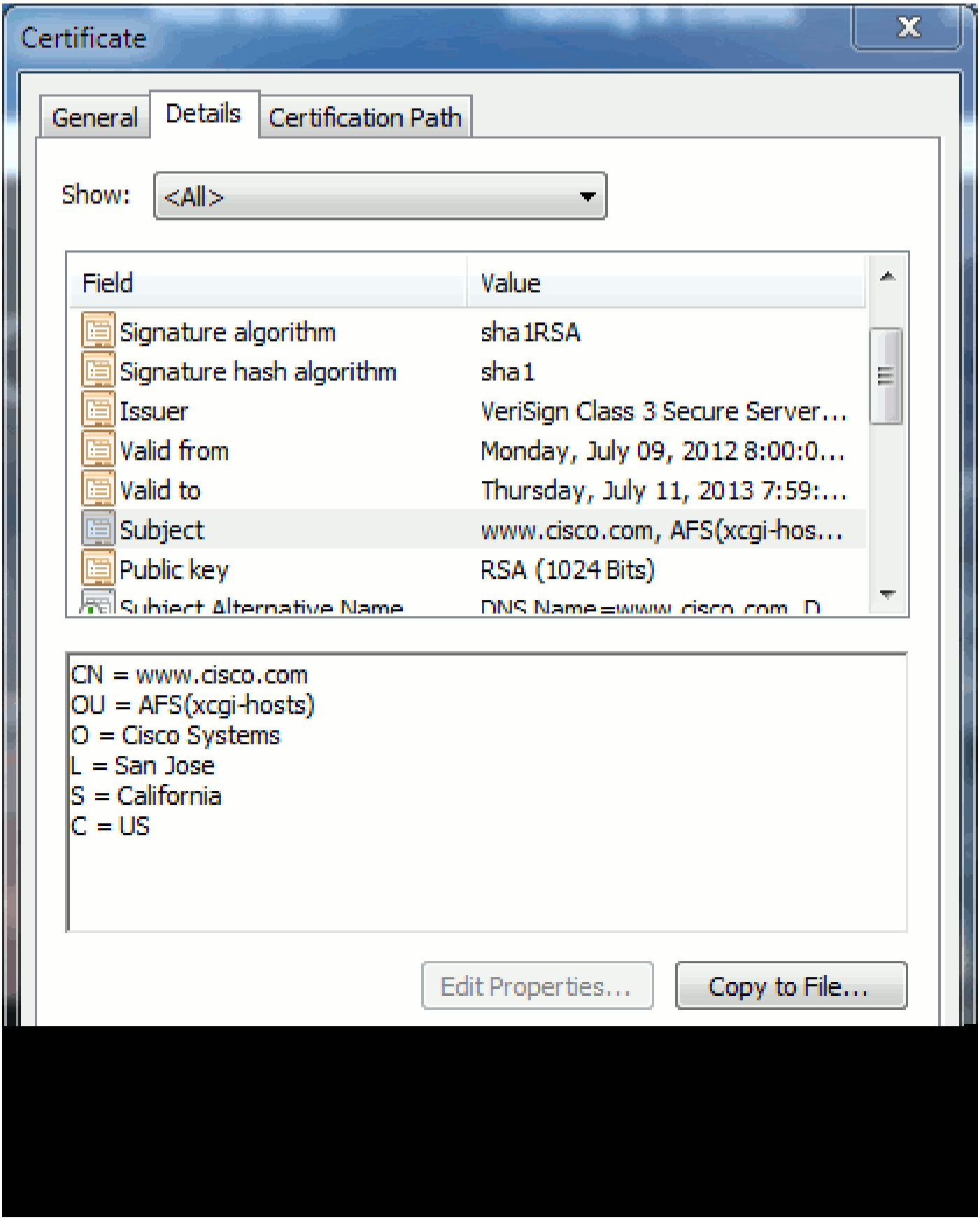
それぞれがCAになることができます。システムがそのCAを信頼するかどうかが最も重要です。

共通名とサブジェクトの別名

共通名（CN）とサブジェクトの別名（SAN）は、IP アドレス、または要求されるアドレスの完全修飾ドメイン名（FQDN）への参照です。たとえば、https://www.cisco.com と入力すると、CN または SAN のヘッダーに www.cisco.com が含まれている必要があります。

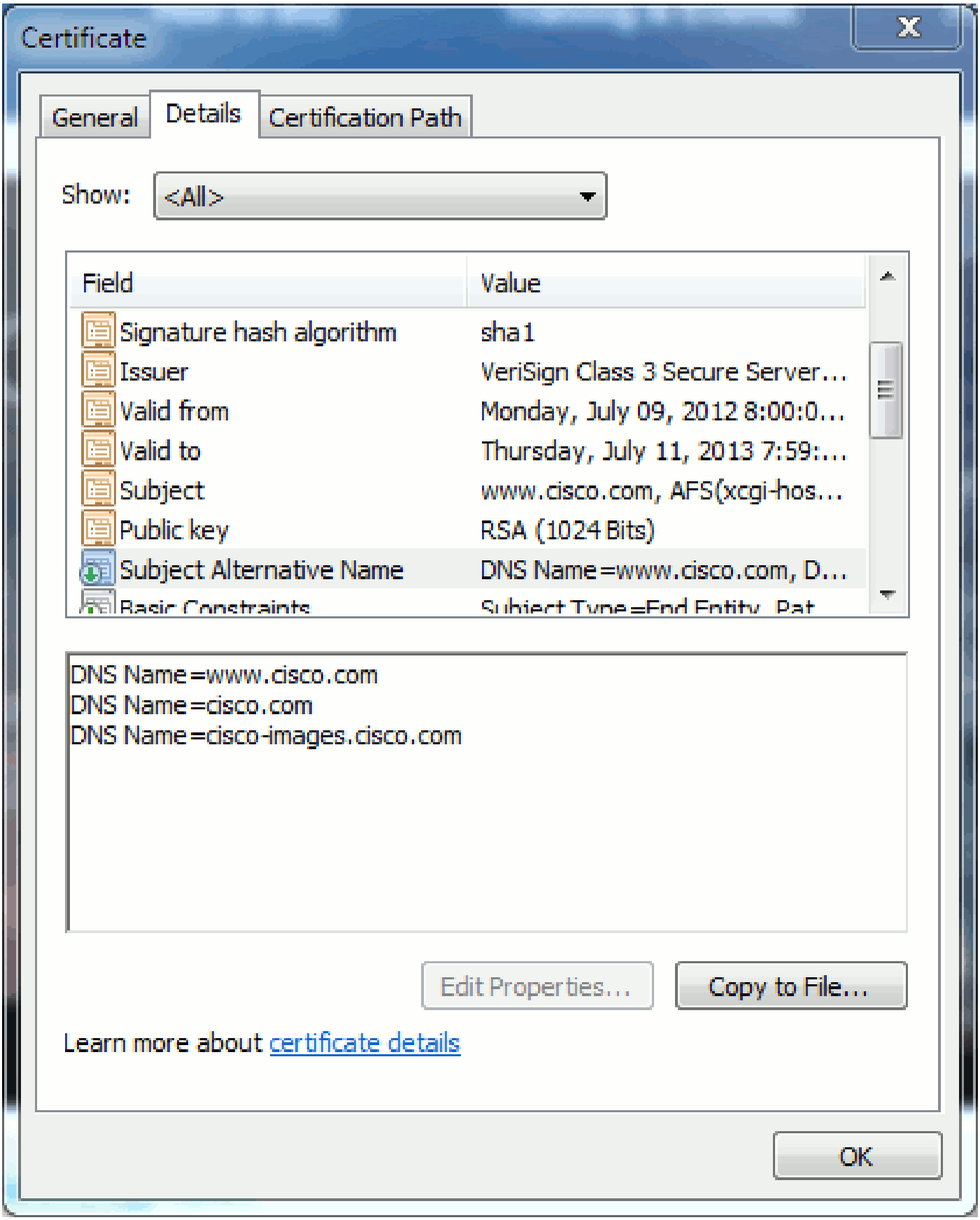
図 7 に示している例では、証明書に www.cisco.com という CN があります。ブラウザからの www.cisco.com への URL 要求では、URL FQDN と証明書が提供する情報が照合されます。この場合、これらは一致し、SSL ハンドシェイクに成功したことが表示されます。この Web サイトは正しい Web サイトであることが確認され、デスクトップと Web サイト間の通信が暗号化されます。

図7:Webサイトの確認



同じ証明書に、3 つの FQDN/DNS アドレスに対応する SAN ヘッダーがあります。

図8:SANヘッダー



この証明書では、www.cisco.com (CN でも定義されています) 、cisco.com、および cisco-images.cisco.com を認証および確認できます。つまり、cisco.com と入力しても、同じ証明書を使用してこの Web サイトを認証および暗号化することができます。

CUCM は SAN ヘッダーを作成できます。SAN ヘッダーの詳細については、サポート コミュニテ

ィにある Jason Burn のドキュメント『CCMAdmin Web GUI 証明書の CUCM へのアップロード』を参照してください。

ワイルド カード証明書

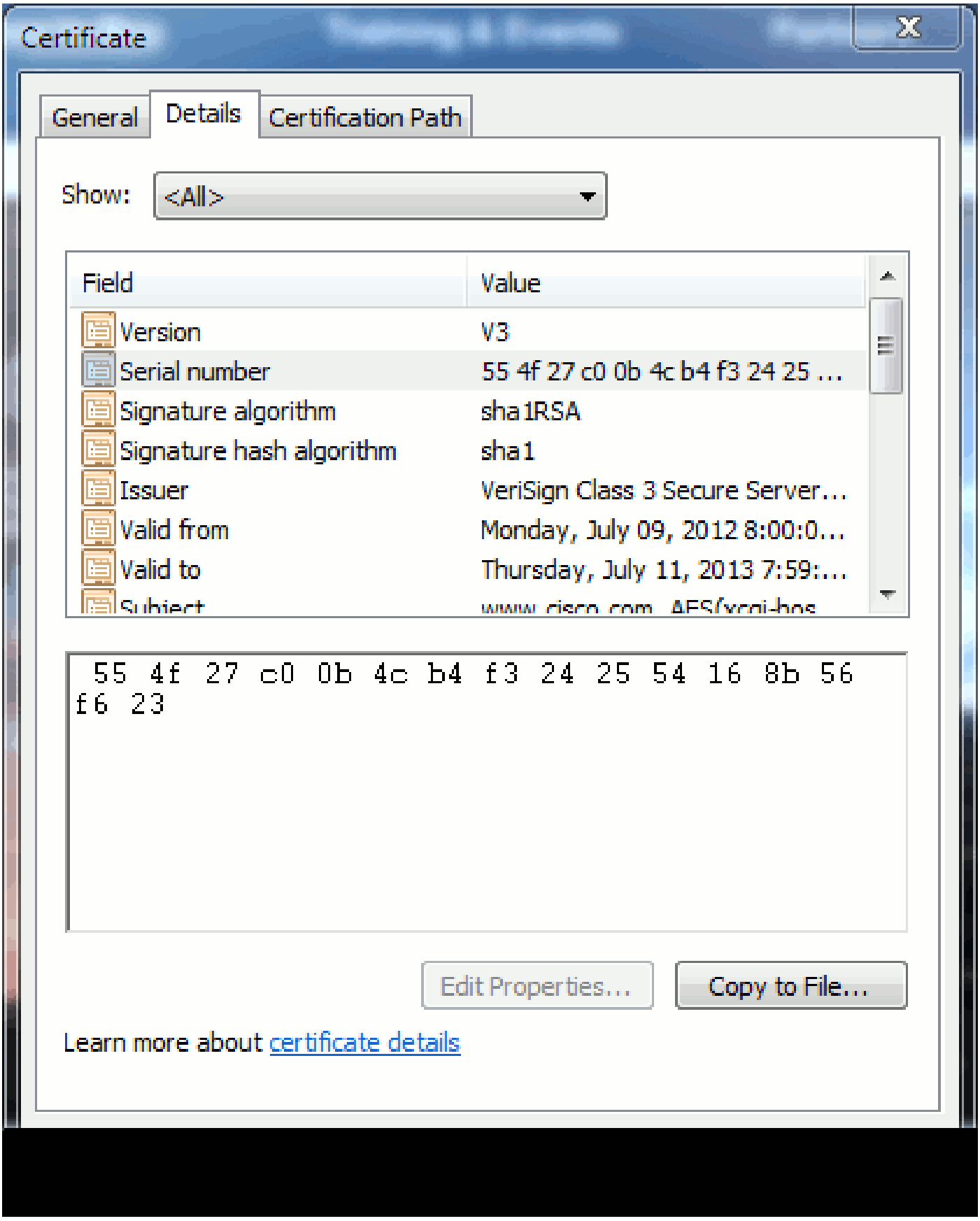
ワイルドカード証明書は、アスタリスク (*) を使用して URL セクションの任意の文字列を表す証明書です。たとえば、www.cisco.com、ftp.cisco.com、ssh.cisco.com などに対応する証明書が必要な場合、管理者は *.cisco.com の証明書を作成するだけで済みます。コストを節約するために、管理者が購入する必要がある証明書は 1 つだけです。複数の証明書を購入する必要はありません。

この機能は、Cisco Unified Communications Manager （CUCM）では現在サポートされていません。ただし、この機能拡張は追跡できます。CSCta14114:CUCMと秘密キーのインポートでのワイルドカード証明書のサポートの要求。

証明書の識別

複数の証明書に同じ情報が含まれている場合は、それらが同じ証明書かどうかを確認できます。すべての証明書には一意のシリアル番号があります。このシリアル番号を使用して比較し、証明書が同じ証明書であるか、再生成されたものであるか、または偽造されたものであるかを確認できます。図 9 に例を示します。

図9：証明書シリアル番号



CSR とその目的

CSR は証明書署名要求のことです。CUCM サーバ用のサードパーティ証明書を作成する場合は、CA に提示する CSR が必要です。この CSR は PEM (ASCII) 証明書によく似ています。

注：これは証明書ではないため、証明書として使用することはできません。

\

CUCMはWeb GUIを介して自動的にCSRを作成します。Cisco Unified Operating System Administration > Security > Certificate Management > Generate CSRを選択し、証明書を作成するサービスをsnf、次にGenerate CSRを選択します。このオプションを使用するたびに、新しい秘密キーと CSR が生成されます。

注：秘密キーは、このサーバとサービスに固有のファイルです。秘密キーは誰にも渡さないでください。秘密キーを誰かに渡すと、証明書のセキュリティが損なわれます。また、古い CSR を使用して証明書を作成する場合は、同じサービス用の新しい CSR を再生成しないでください。CUCM によって古い CSR と秘密キーが削除され、両方とも置き換えられます。その結果、古い CSR が使用できなくなります。

CSRを作成する方法については、サポートコミュニティにあるJason Burnのドキュメント『CCMAdmin Web GUI証明書のCUCMへのアップロード』を参照してください。

エンドポイントと SSL/TLS ハンドシェイク プロセス間での証明書の使用

ハンドシェイク プロトコルは、データ転送セッションのセキュリティ パラメータをネゴシエートする一連の順序付けられたメッセージです。
「SSL/TLSの詳細」を参照してください。このドキュメントには、ハンドシェイクプロトコルのメッセージシーケンスが記載されています。これはパケットキャプチャ(PCAP)で確認できます。詳細には、クライアントとサーバ間で送受信される初期メッセージ、後続のメッセージ、最終メッセージが含まれます。

CUCM による証明書の使用法

tomcat と tomcat-trust との違い

証明書を CUCM にアップロードするときには、Cisco Unified Operating System Administration > [Security] > [Certificate Management] > [Find] でサービスごとに 2 つのオプションを使用できます

。

次に、CUCM での証明書の管理に使用できる 5 つのサービスを示します。

- Tomcat
- IPSec
- callmanager
- capf
- tvs（CUCM リリース 8.0 以降）

次に、CUCM に証明書をアップロードできるサービスを示します。

- Tomcat
- Tomcatの信頼性
- IPSec
- Ipsecの信頼性
- callmanager
- callmanager-trust
- capf
- capf-trust

これらは、CUCM リリース 8.0 以降で使用できるサービスです。

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

これらのタイプの証明書の詳細については、『リリース別 CUCM セキュリティ ガイド』を参照してください。このセクションでは、サービス証明書と信頼証明書の違いについてのみ説明します。

たとえば、tomcat では、tomcat-trusts で CA と中間証明書をアップロードします。その結果、この CUCM ノードは、CA および中間サーバによって署名されたすべての証明書が信頼できること

を確認できます。tomcat証明書は、エンドポイントがこのサーバにHTTP要求を行った場合に、このサーバのtomcatサービスによって提示される証明書です。tomcatでサードパーティ証明書を表示できるようにするには、CUCMノードがCAと中間サーバを信頼できることを知っている必要があります。したがって、tomcat（サービス）証明書をアップロードする前に、CA と中間証明書をアップロードする必要があります。

CUCM に証明書をアップロードする方法を理解するのに役立つ情報については、サポート コミュニティにある Jason Burn の『CCMAdmin Web GUI 証明書の CUCM へのアップロード』を参照してください。

各サービスには固有のサービス証明書と信頼証明書があります。それらが別々に機能するようになることはありません。つまり、tomcat-trust サービスとしてアップロードされた CA および中間証明書は、callmanager サービスでは使用できません。

注:CUCMの証明書はノード単位です。したがって、パブリッシャにアップロードされた証明書と、同じ証明書を利用するサブスクライバが必要な場合、CUCM リリース 8.5 より前のリリースでは、証明書を各サーバと各ノードにアップロードする必要があります。CUCM リリース 8.5 以降では、アップロードされた証明書をクラスタ内の残りのノードに複製するサービスがあります。

注：各ノードのCNは異なります。したがって、サービスが独自の証明書を提示するためには、各ノードでCSRを作成する必要があります。

CUCM セキュリティ機能についてその他の具体的な疑問がある場合は、セキュリティ ドキュメントを参照してください。

結論

このドキュメントは、証明書に関する高レベルの知識を身に付けるのに役立ちます。このテーマは重要であり、より詳しく説明することもできますが、このドキュメントでは証明書の扱いに十分慣れ親しんでいただくだけにとどめます。CUCM のセキュリティ機能について疑問がある場合は、『リリース別 CUCM セキュリティ ガイド』で詳細を参照してください。

関連情報

- Cisco Unified Communications Manager（CallManager）のメンテナンスおよびセキュリティ ガイド
- Cisco Unified Communications Manager（CallManager）
- Cisco Unified Communications Manager Express
- シスコサポートコミュニティ：CCMAdmin Web GUI証明書のCUCMへのアップロード
- バグCSCta14114:CUCMと秘密キーのインポートでのワイルドカード証明書のサポートの要求
- Cisco Emergency Responder（CER）の説明
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。