CUCM의 인증서 및 인증 기관에 대한 상위 레벨 보기

목차

소개

이 문서에서는 인증서 및 인증 기관의 기본 사항에 대해 설명합니다. CUCM(Cisco Unified Communications Manager)의 암호화 또는 인증 기능을 참조하는 다른 Cisco 문서를 보완합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

인증서의 용도

인증서는 신뢰/인증 및 데이터 암호화를 구축하기 위해 엔드포인트 간에 사용됩니다. 이는 엔드포인트가 의도한 디바이스와 통신하며 두 엔드포인트 간의 데이터를 암호화하는 옵션이 있음을 확인합니다.

참고: 각 인증서의 영향을 이해하려면 Certificate Regeneration Process For Cisco Unified Communications Manager Impact by the Certificate Store 섹션을 참조하십시오

인증서의 관점에서 신뢰 정의

인증서에서 가장 중요한 부분은 엔드포인트에서 신뢰할 수 있는 엔드포인트를 정의하는 것입니다. 이 문서에서는 데이터가 암호화되고 의도한 웹 사이트, 전화, FTP 서버 등과 공유되는 방법을 알고 정의하는 데 도움이 됩니다.

시스템이 인증서를 신뢰하는 경우, 시스템에 미리 설치된 인증서가 있음을 의미합니다. 이 인증서는 올바른 엔드포인트와 정보를 공유한다는 것을 100% 확신한다는 것을 의미합니다. 그렇지 않으면 이러한 엔드포인트 간의 통신이 종료됩니다.

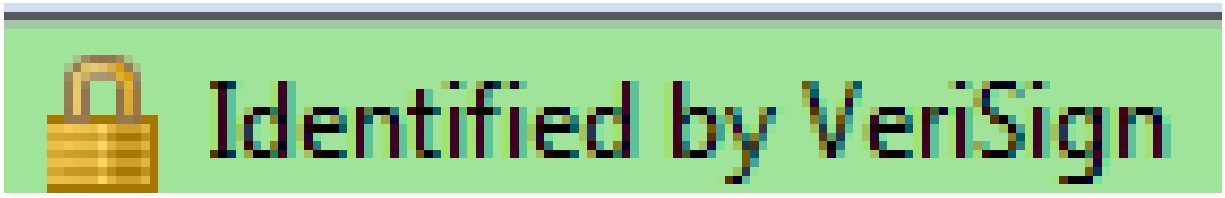
이것의 비기술적인 예는 당신의 운전면허증입니다. 이 라이센스(서버/서비스 인증서)를 사용하여 본인이 본인임을 증명합니다. 주(Certificate Authority)의 DMV(Division of Motors)에서 허가를 받은 현지 자동차 사업부(중간 인증서)에서 라이센스를 취득했습니다. 직원에게 라이센스(서버/서비스 인증서)를 보여줘야 할 때, 직원은 DMV 지점(중간 인증서) 및 자동차 사업부(인증 기관)를 신뢰할 수 있으며, 이 라이센스가 해당 기관(인증 기관)에서 발급되었음을 확인할 수 있습니다. 당신의 신원은 경찰관에게 확인되고 이제 그들은 당신이 당신이 당신이 당신이 말하는 사람이라는 것을 신뢰합니다. 그렇지 않으면 DMV(중간 인증서)에서 서명하지 않은 허위 라이센스(서버/서비스 인증서)를 제공할 경우 사용자가 누구라고 말하는지 신뢰할 수 없습니다. 이 문서의 나머지 부분에서는 인증서 계층 구조에 대한 심층적이고 기술적인 설명을 제공합니다.

브라우저에서 인증서를 사용하는 방법

1. 웹 사이트를 방문할 때 http://www.cisco.com과 같은 URL을 입력합니다.
2. DNS는 해당 사이트를 호스팅하는 서버의 IP 주소를 찾습니다.
3. 브라우저에서 해당 사이트로 이동합니다.

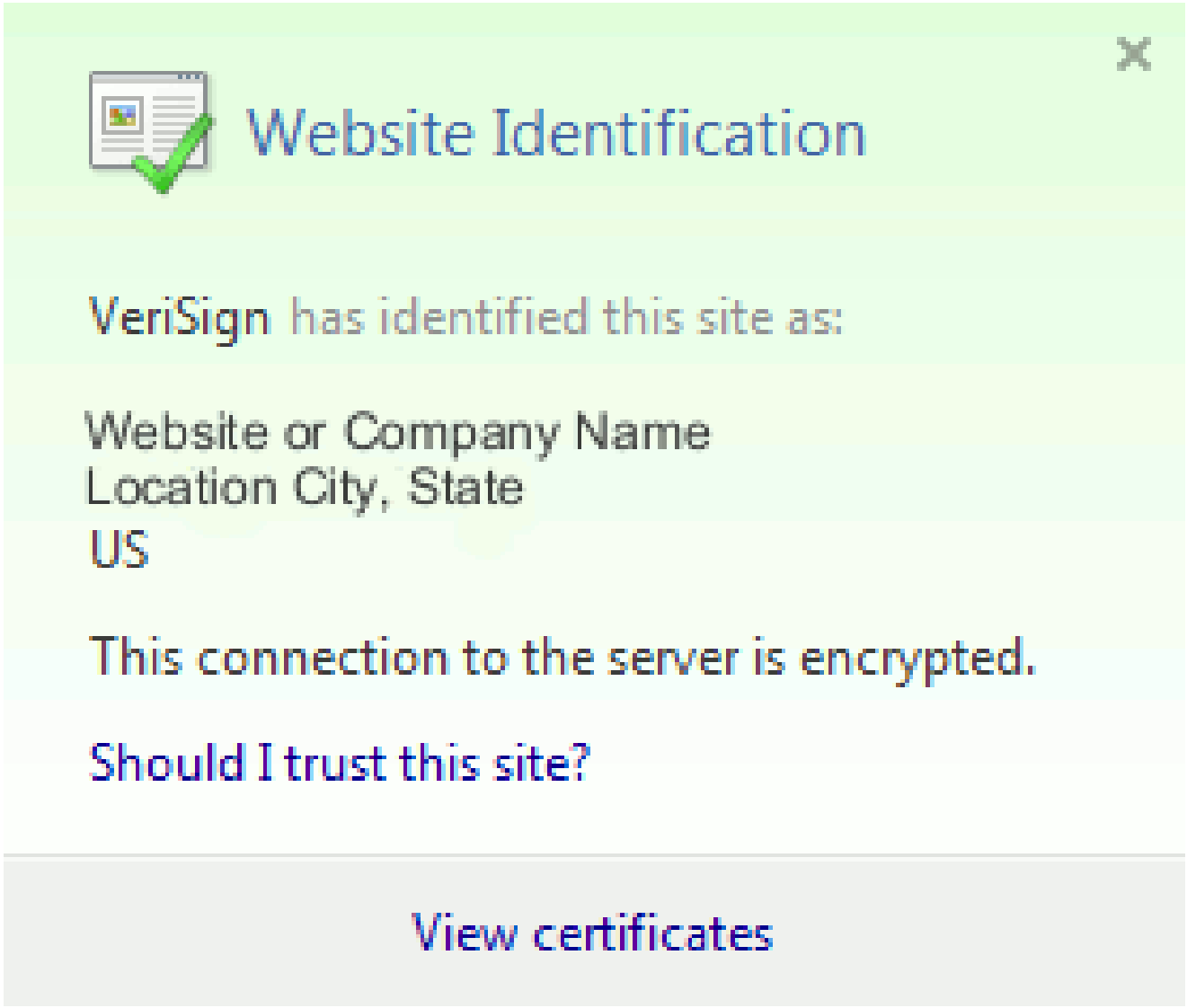
인증서가 없으면 비인가 DNS 서버가 사용되었는지 또는 다른 서버로 라우팅되었는지 알 수 없습니

다. 인증서는 사용자가 입력한 개인 정보 또는 민감한 정보가 안전한 은행 웹 사이트와 같은 의도한 웹 사이트로 올바르고 안전하게 라우팅되도록 보장합니다.

모든 브라우저에는 사용하는 아이콘이 다르지만 일반적으로 주소 표시줄에 다음과 같은 자물쇠가 표시됩니다. 

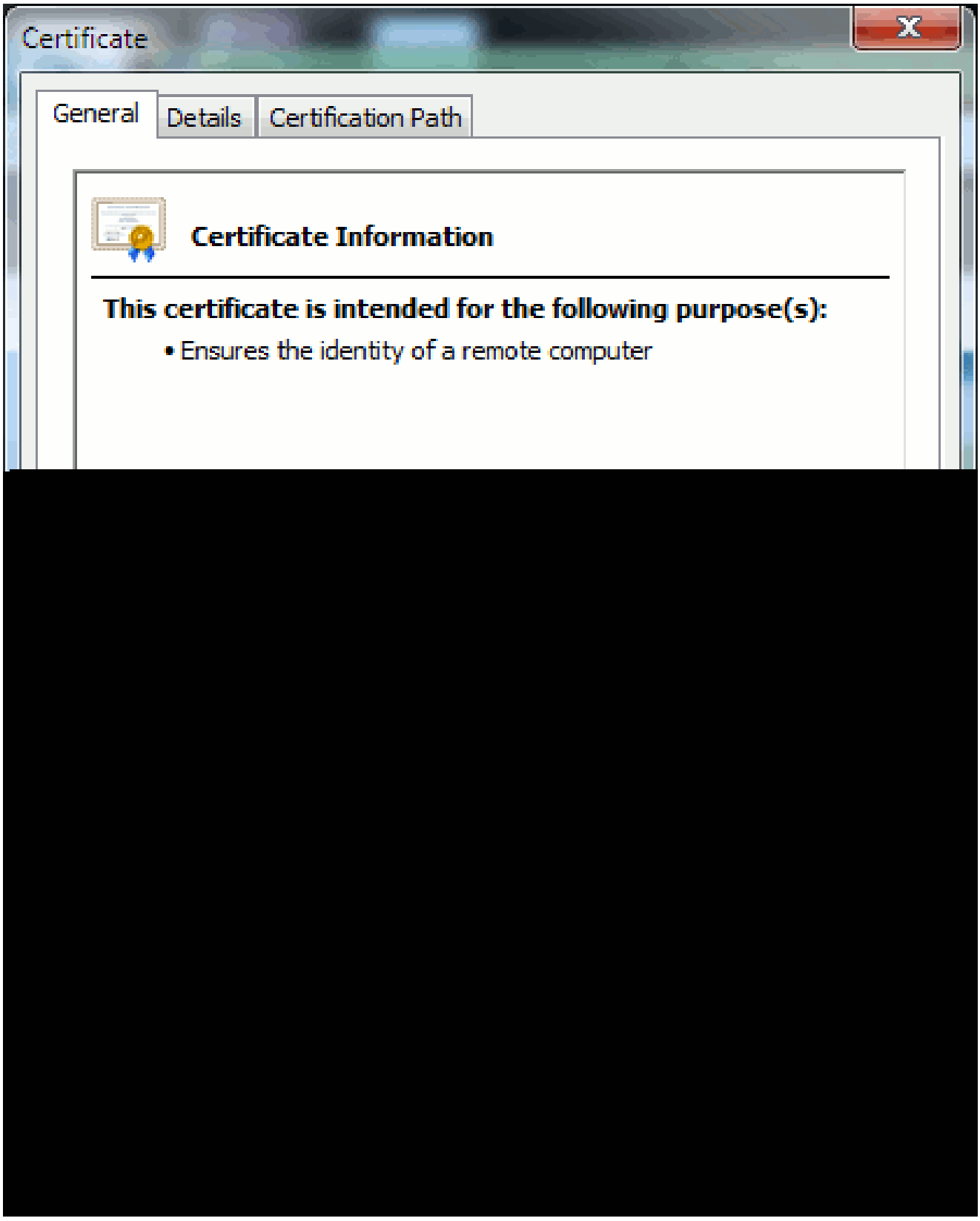
1. 자물쇠를 클릭하면 다음과 같은 창이 표시됩니다.

   그림 1: 웹 사이트 식별



2. 다음 예에 나와 있는 것처럼 사이트의 인증서를 보려면 View Certificates(인증서 보기)를 클릭합니다.

   그림 2: Certificate Information, General(일반) 탭



강조 표시된 정보는 중요합니다.

- 발급자는 시스템에서 이미 신뢰하는 회사 또는 CA(Certificate Authority)입니다.
- Valid from/to는 이 인증서를 사용할 수 있는 날짜 범위입니다. CA를 신뢰하는 인증서를 볼 수 있지만 인증서가 유효하지 않은 경우도 있습니다. 만료되었는지 여부를 알 수 있도록 항상 날짜를 확인합니다.)

팁: 모범 사례는 만료되기 전에 달력에 인증서를 갱신하라는 알림을 만드는 것입니다. 이렇게 하면 향후 문제가 발생하지 않습니다.

PEM과 DER 인증서의 차이점

PEM은 ASCII이고 DER는 이진입니다. 그림 3은 PEM 인증서 형식을 보여줍니다.

그림 3: PEM 인증서 예

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
BQcDAgYIKwYBBQUHAwUwKQYDVR0RBCIwIIIOODUxUHViLmtqbC5jb22CDnBob251
cy5ramwuY29tMB0GA1UdDgQWBBTbWvEUfpl7hvrsTJpQfmcoNpB4LzANBgkqhkiG
9w0BAQUFAAOCAQEArZWeqarg4tagW0O0rQElZj6UJ9S8ZAcp9XDT4Iz1QwRaaiBr
EBhfulaMjmtMKXFV5eCU9QcPbPG8XmiRZiEg9Q8Wtn0OZpuPGlkwxmFYRz40aY4T
5lw+d0wVb9sPChNQEGccjjqwtstElYWDo/A4RoqdH0ALceP8a4bovK/CpmRGdb5C
+hqP4zIJs4P+YKmzrJeq7H8xCCqqkYXcRLkmG6mif78txFQ5lr8rJEoU1VlL8znc
fJvSfEsCfwnSqPaGcQTnxMOZOIyM0OjXvvhWIezrpk8cyj3vSTgXSTwO53flZX4L
tu28d5H3AHo8U6cfHRIJ1f6Yv2ClGBShXwFp6Q==
-----END CERTIFICATE-----
```

그림 4는 DER 인증서를 보여줍니다.

그림 4: DER 인증서 예

VeriSign이나 Thawt와 같은 대부분의 CA 회사는 이메일로 사용이 가능하므로 PEM 형식을 사용하여 고객에게 인증서를 보냅니다. 고객은 전체 문자열을 복사하고 -----BEGIN CERTIFICATE 및 -----END CERTIFICATE를 포함하여 텍스트 파일에 붙여 넣은 다음 확장자 .PEM 또는 .CER로 저장해야 합니다.

Windows는 자체 Certificate Management Applet으로 DER 및 CER 형식을 읽을 수 있으며 그림 5와 같이 인증서를 표시합니다.

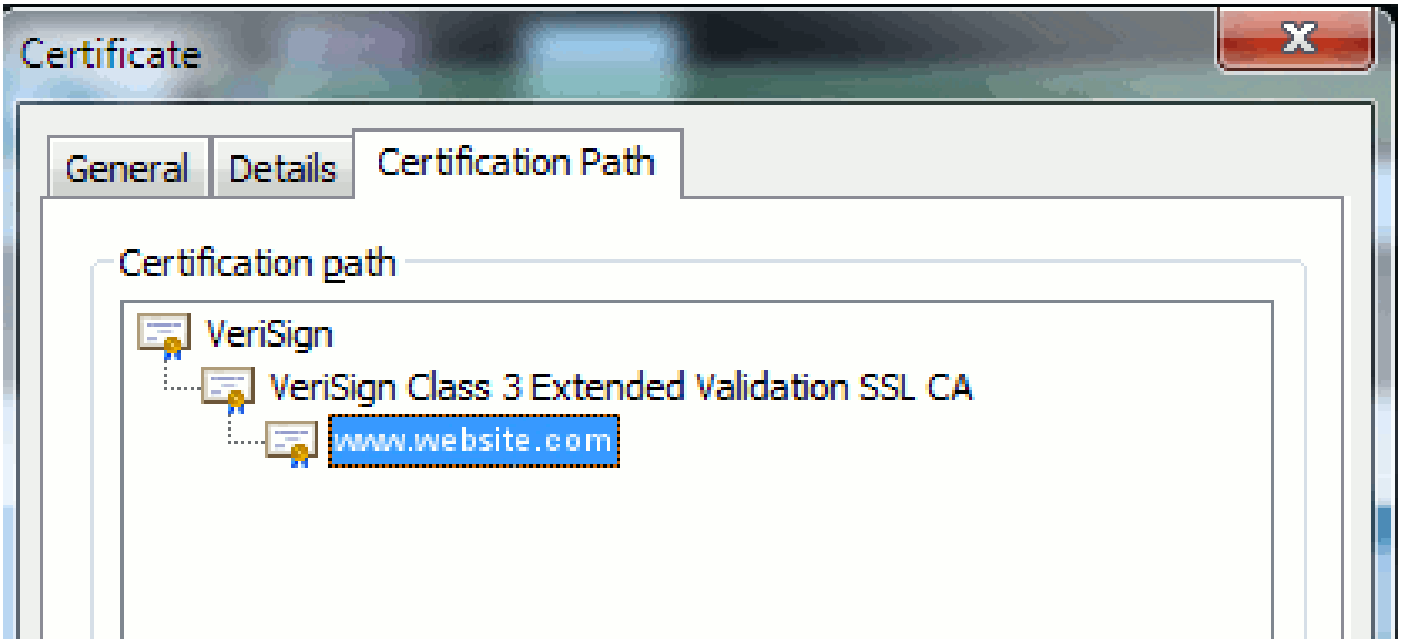
그림 5: 인증서 정보

장치에 특정 형식(ASCII 또는 이진)이 필요한 경우도 있습니다. 이를 변경하려면 CA에서 필요한 형식으로 인증서를 다운로드하거나 https://www.sslshopper.com/ssl-converter.html과 같은 SSL 변환기 도구를 사용합니다.

인증서 계층 구조

엔드포인트에서 인증서를 신뢰하려면 서드파티 CA와 이미 설정된 신뢰가 있어야 합니다. 예를 들어, 그림 6에는 3개의 인증서로 구성된 계층이 나와 있습니다.

그림 6: 인증서 계층 구조



- Verisign은 CA입니다.
- Verisign Class 3 Extended Validation SSL CA는 중간 또는 서명 서버 인증서(CA가 인증하여 이름으로 인증서를 발급할 수 있는 서버)입니다.
- www.website.com는 서버 또는 서비스 인증서입니다.

엔드 포인트는 SSL 핸드셰이크가 제공하는 서버 인증서를 신뢰할 수 있음을 알기 전에 먼저 CA 및 중간 인증서를 신뢰할 수 있음을 알아야 합니다(아래 세부 정보). 이 트러스트의 작동 방식을 더 잘 이해하려면 이 문서의 섹션 인증서 관점에서 "트러스트"를 정의하십시오.

자체 서명 인증서와 타사 인증서 비교

자체 서명 인증서와 타사 인증서의 주요 차이점은 인증서를 누가 서명했는지, 신뢰하는지 여부입니다.

자체 서명 인증서는 해당 인증서를 제공하는 서버에서 서명한 인증서이므로 서버/서비스 인증서와 CA 인증서가 동일합니다.

서드파티 CA는 공용 CA(예: Verisign, Entrust, Digicert) 또는 서버(예: Windows 2003, Linux, Unix, IOS)에서 서버/서비스 인증서의 유효성을 제어하는 서비스입니다.

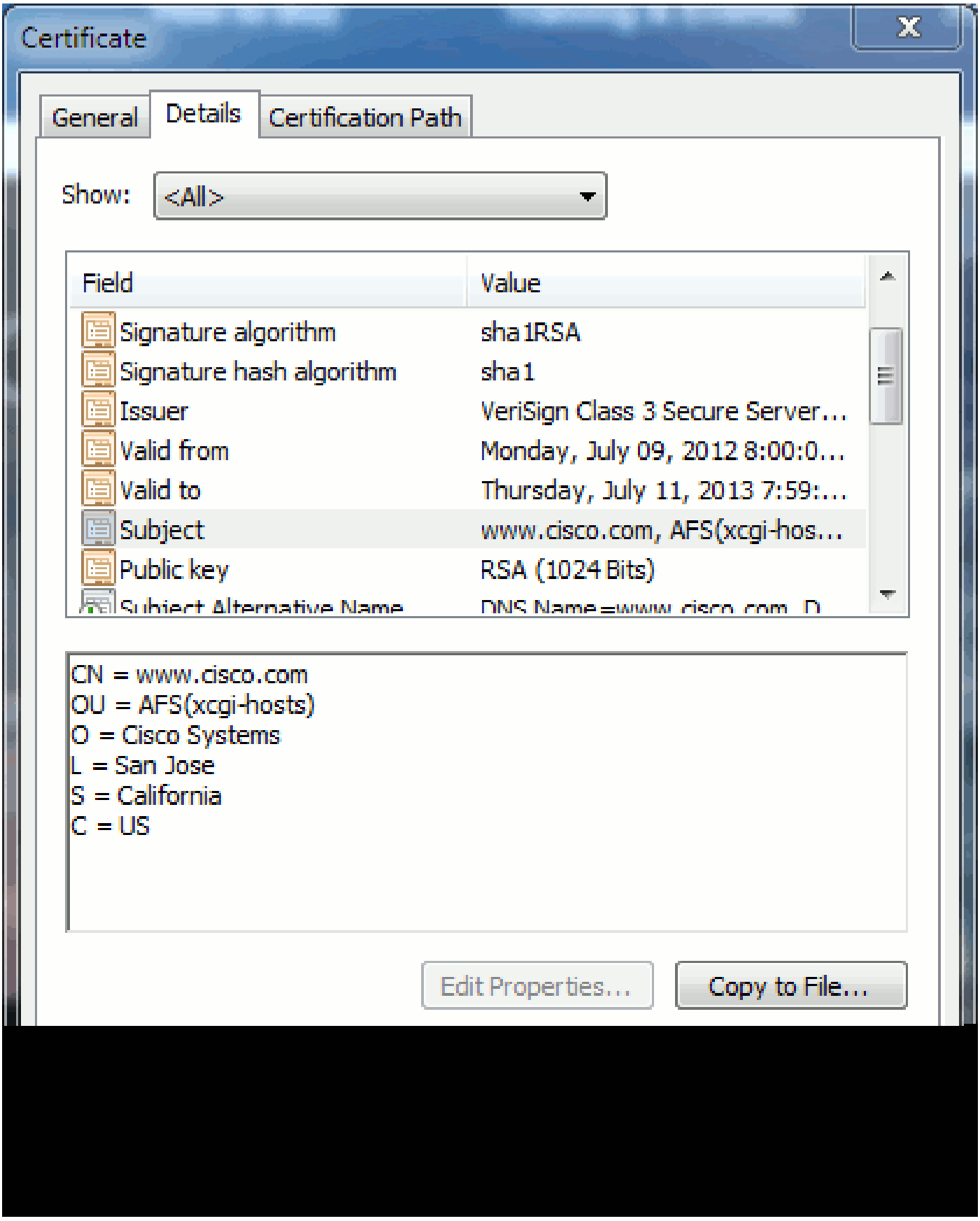
각각 CA가 될 수 있습니다. 시스템에서 그 CA를 신뢰하는지 여부가 가장 중요한 부분입니다.

일반 이름 및 제목 대체 이름

CN(Common Names) 및 SAN(Subject Alternative Names)은 요청된 주소의 IP 주소 또는 FQDN(Fully Qualified Domain Name)을 참조합니다. 예를 들어, https://www.cisco.com을 입력할 경우 CN 또는 SAN은 헤더에 www.cisco.com를 포함해야 합니다.

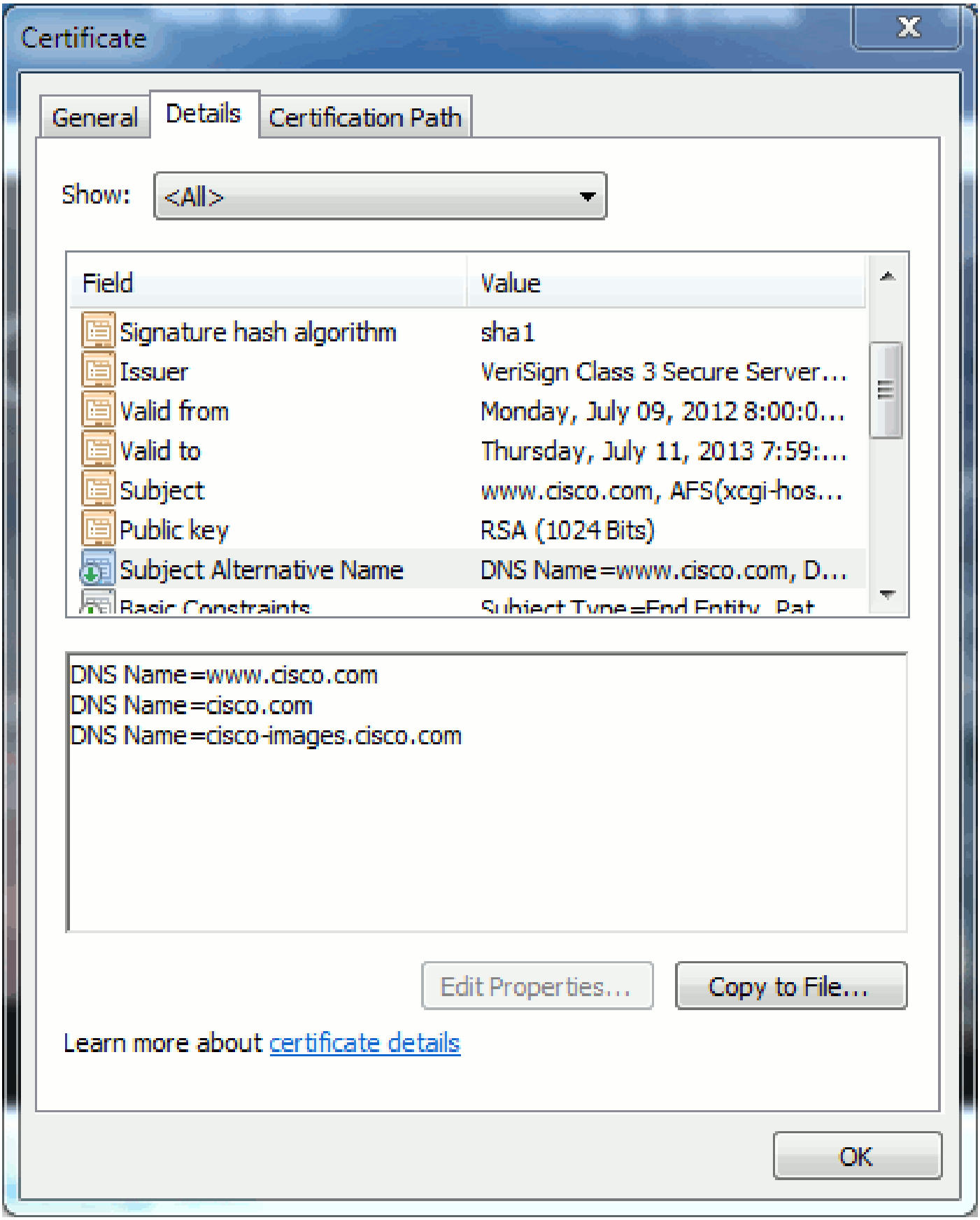
그림 7의 예에서는 인증서의 CN이 www.cisco.com입니다. 브라우저에서 www.cisco.com에 대한 URL 요청은 인증서가 제공하는 정보에 대해 URL FQDN을 확인합니다. 이 경우 일치하며 SSL 핸드셰이크가 성공했음을 보여줍니다. 이 웹 사이트는 올바른 웹 사이트로 확인되었으며 이제 데스크톱과 웹 사이트 간에 통신이 암호화됩니다.

그림 7: 웹 사이트 확인



동일한 인증서에는 3개의 FQDN/DNS 주소에 대한 SAN 헤더가 있습니다.

그림 8: SAN 헤더



이 인증서는 www.cisco.com(CN에도 정의됨), cisco.com 및 cisco-images.cisco.com을 인증/확인할 수 있습니다. 즉, cisco.com을 입력할 수도 있으며, 이 인증서를 사용하여 이 웹 사이트를 인증하고 암호화할 수 있습니다.

CUCM은 SAN 헤더를 생성할 수 있습니다. SAN 헤더에 대한 자세한 내용은 Jason Burn의 문서,

CUCM Uploading CCMAdmin Web GUI Certificates on the Support Community를 참조하십시오.

와일드카드 인증서

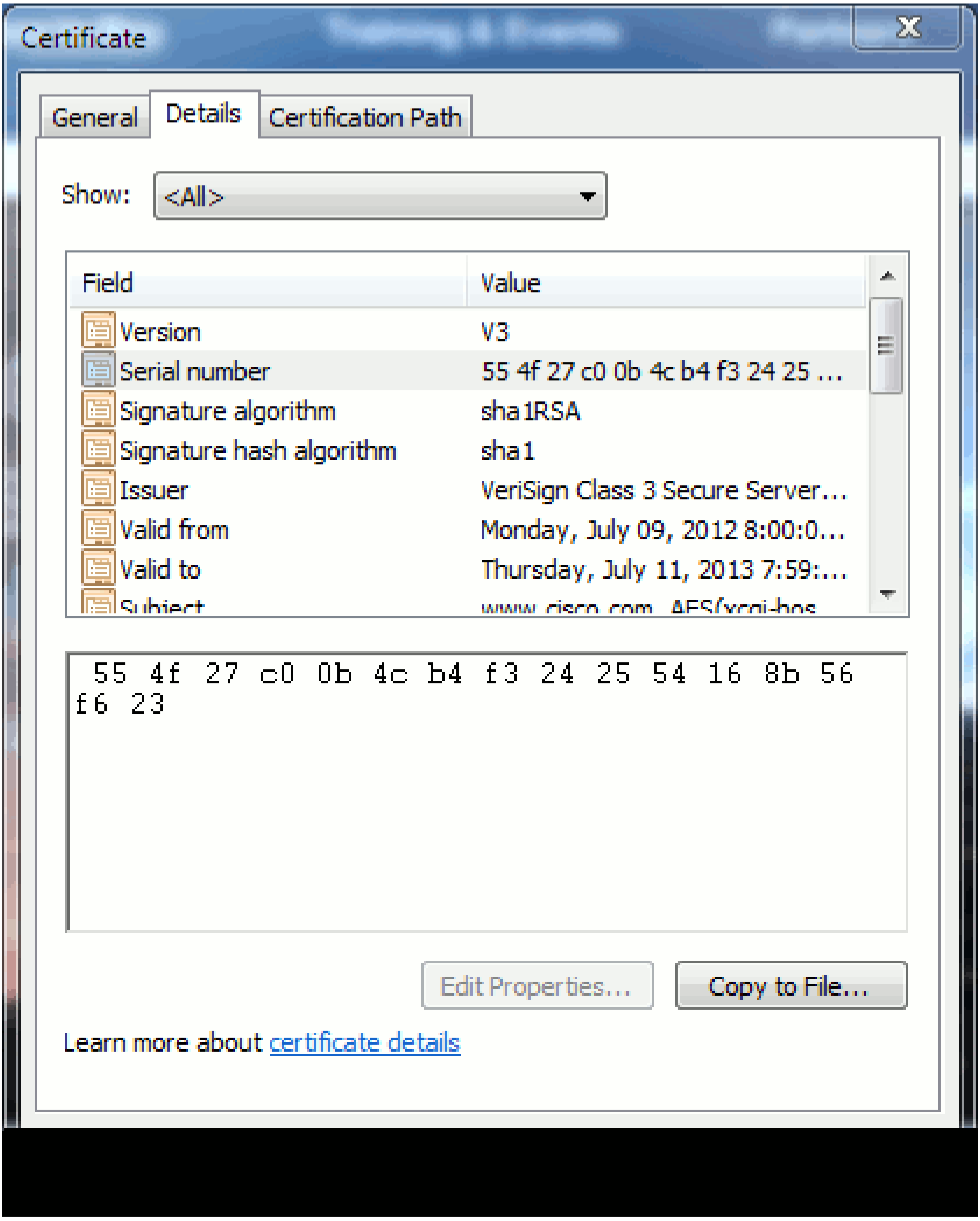
와일드카드 인증서는 URL 섹션의 문자열을 나타내기 위해 별표(*)를 사용하는 인증서입니다. 예를 들어, www.cisco.com, ftp.cisco.com, ssh.cisco.com 등에 대한 인증서를 보유하려면 관리자가 *.cisco.com에 대한 인증서만 생성하면 됩니다. 비용을 절약하기 위해 관리자는 단일 인증서만 구매하면 되고 여러 인증서를 구매하지 않아도 됩니다.

이 기능은 현재 CUCM(Cisco Unified Communications Manager)에서 지원되지 않습니다. 그러나 CSCta14114: CUCM 및 개인 키 가져오기에서 와일드카드 인증서 지원 요청을 추적할 수 있습니다 .

인증서 식별

인증서에 동일한 정보가 있는 경우 동일한 인증서인지 확인할 수 있습니다. 모든 인증서에는 고유한 일련 번호가 있습니다. 이를 사용하여 인증서가 동일한 인증서, 재생성 또는 위조인지 비교할 수 있습니다. 그림 9는 예를 보여줍니다.

그림 9: 인증서 일련 번호



CSR 및 목적

CSR은 Certificate Signing Request의 약자입니다. CUCM 서버에 대한 서드파티 인증서를 생성하려면 CA에 제공할 CSR이 필요합니다. 이 CSR은 PEM(ASCII) 인증서와 매우 유사합니다.

참고: 이는 인증서가 아니며 인증서로 사용할 수 없습니다.

\

CUCM은 웹 GUI를 통해 자동으로 CSR을 생성합니다. Cisco Unified Operating System Administration(Cisco Unified Operating System 관리) > Security(보안) > Certificate Management(인증서 관리) > Generate CSR(CSR 생성), 인증서 SNF를 생성할 서비스를 선택한 다음 CSR을 생성합니다.입니다.CSR을 선택합니다. 이 옵션을 사용할 때마다 새 개인 키와 CSR이 생성됩니다.

참고: 개인 키는 이 서버 및 서비스에 고유한 파일입니다. 이것은 누구에게도 주어져서는 안 됩니다! 누군가에게 개인 키를 제공하면 인증서가 제공하는 보안을 침해하게 됩니다. 또한 이전 CSR을 사용하여 인증서를 생성하는 경우 동일한 서비스에 대해 새 CSR을 재생성하지 마십시오. CUCM은 기존 CSR 및 개인 키를 삭제하고 두 키를 모두 교체하므로 기존 CSR을 사용할 수 없습니다.

CSR을 생성하는 방법에 대한 자세한 내용은 Support Community: CUCM Uploading CCMAdmin 웹 GUI Certificates에서 Jason Burn의 설명서를 참조하십시오.

엔드포인트와 SSL/TLS 핸드셰이크 프로세스 간의 인증서 사용

핸드셰이크 프로토콜은 데이터 전송 세션의 보안 매개변수를 협상하는 일련의 순차적 메시지입니다. 핸드셰이크 프로토콜의 메시지 시퀀스를 문서화하는 SSL/TLS를 자세히 참조하십시오. 이러한 내용은 PCAP(패킷 캡처)에서 확인할 수 있습니다. 세부 정보에는 클라이언트와 서버 간에 주고받은 초기, 후속 및 최종 메시지가 포함됩니다.

CUCM에서 인증서를 사용하는 방법

tomcat과 tomcat-trust의 차이

인증서를 CUCM에 업로드하면 Cisco Unified Operating System Administration(Cisco Unified Operating System 관리) > Security(보안) > Certificate Management(인증서 관리) > Find(찾기)를 통해 각 서비스에 대해 두 가지 옵션이 있습니다.

CUCM에서 인증서를 관리할 수 있는 5가지 서비스는 다음과 같습니다.

- 수고양이
- ipsec
- 통화 관리자

- capf
- tv(CUCM 릴리스 8.0 이상)

다음은 CUCM에 인증서를 업로드할 수 있는 서비스입니다.

- 수고양이
- tomcat-트러스트
- ipsec
- ipsec 트러스트
- 통화 관리자
- callmanager-trust
- capf
- CAPF 트러스트

다음은 CUCM Release 8.0 이상에서 사용할 수 있는 서비스입니다.

- tv
- tv-트러스트
- 전화 신뢰
- phone-vpn-trust
- 전화 금고
- phone-ctl-trust

이러한 인증서 유형에 대한 자세한 내용은 릴리스별 CUCM 보안 가이드를 참조하십시오. 이 절에서는 서비스 인증서와 신뢰 인증서의 차이점만 설명합니다.

예를 들어 tomcat을 사용하면 tomcat-trust는 CA 및 중간 인증서를 업로드하여 이 CUCM 노드가 CA 및 중간 서버에서 서명한 모든 인증서를 신뢰할 수 있음을 알도록 합니다. tomcat 인증서는 엔드포인트가 이 서버에 HTTP 요청을 하는 경우 이 서버의 tomcat 서비스에서 제공하는 인증서입니다. tomcat에서 서드파티 인증서를 표시할 수 있도록 하려면 CUCM 노드가 CA 및 중간 서버를 신뢰할 수 있음을 알아야 합니다. 따라서 tomcat(서비스) 인증서를 업로드하기 전에 CA 및 중간 인증서를 업로드해야 합니다.

CUCM에 인증서를 업로드하는 방법에 대한 자세한 내용은 지원 커뮤니티에서 Jason Burn의 CUCM Uploading CCMAdmin 웹 GUI Certificates를 참조하십시오.

각 서비스에는 고유한 서비스 인증서 및 신뢰 인증서가 있습니다. 그들은 서로 잘 어울리지 않는다. 즉, tomcat-trust 서비스로 업로드된 CA 및 중간 인증서는 CallManager 서비스에서 사용할 수 없습

니다.

> 참고: CUCM의 인증서는 노드별로 다릅니다. 따라서 게시자에 업로드된 인증서가 필요하고 가입자가 동일한 인증서를 보유해야 하는 경우 CUCM 릴리스 8.5 이전에 각 개별 서버 및 노드에 인증서를 업로드해야 합니다. CUCM Release 8.5 이상에서는 업로드된 인증서를 클러스터의 나머지 노드에 복제하는 서비스가 있습니다.

> 참고: 각 노드에는 서로 다른 CN이 있습니다. 따라서 서비스가 자체 인증서를 제공하려면 각 노드에 의해 CSR이 생성되어야 합니다.

CUCM 보안 기능에 대한 추가 질문이 있는 경우 보안 문서를 참조하십시오.

결론

이 문서는 인증서에 대한 높은 수준의 지식을 제공하고 구축합니다. 이 주제는 더 심층적인 내용이 될 수 있지만, 이 문서에서는 인증서를 다룰 수 있을 만큼 충분히 익혀 줍니다. CUCM 보안 기능에 대한 자세한 내용은 CUCM Security Guides by Release를 참조하십시오.

관련 정보

- Cisco Unified Communications Manager(CallManager) 유지 관리 및 보안 가이드
- Cisco Unified Communications Manager(CallManager)
- Cisco Unified Communications Manager Express
- Cisco Support Community: CUCM 업로드 CCMAdmin 웹 GUI 인증서
- Bug CSCta14114: CUCM 및 개인 키 가져오기에서 와일드카드 인증서 지원 요청
- Cisco CER(Emergency Responder) 설명
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.