High Level View of Certificaten & Autoriteiten in Nederland

Inhoud

Inleiding

In dit document worden de basisbeginselen van certificaten en certificeringsautoriteiten beschreven. Het is een aanvulling op andere Cisco-documenten die verwijzen naar codering- of verificatiefuncties in Cisco Unified Communications Manager (CUCM).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Doel van certificaten

Certificaten worden gebruikt tussen eindpunten om vertrouwen/verificatie en codering van gegevens op te bouwen. Dit bevestigt dat de eindpunten met het voorgenomen apparaat communiceren en de optie hebben om de gegevens tussen de twee eindpunten te versleutelen.

Opmerking: om de impact van elk certificaat te begrijpen, verwijst u naar het proces voor certificaatherstel voor Cisco Unified Communications Manager Impact door de sectie Certificaatopslag

---

Vertrouwen definiëren vanuit het gezichtspunt van een certificaat

Het belangrijkste deel van certificaten is de definitie van welke endpoints kunnen worden vertrouwd door uw endpoint. Dit document helpt u te weten komen en te definiëren hoe uw gegevens worden versleuteld en gedeeld met de beoogde website, telefoon, FTP-server, enzovoort.

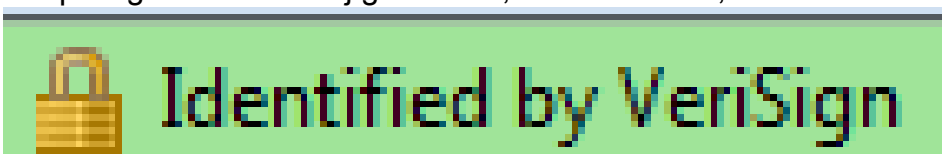
Als uw systeem op een certificaat vertrouwt, betekent dit dat er een vooraf geïnstalleerd certificaat of certificaten op uw systeem staat waarin staat dat het 100 procent zeker is dat het informatie deelt met het juiste eindpunt. Anders eindigt de communicatie tussen deze eindpunten.

Een niet-technisch voorbeeld hiervan is uw rijbewijs. U gebruikt deze licentie (server/service certificaat) om te bewijzen dat u bent wie u zegt dat u bent; u hebt uw licentie verkregen van uw lokale afdeling van Motorvoertuigen filiaal (tussencertificaat) die toestemming heeft gekregen van de Divisie Motorvoertuigen (DMV) van uw Staat (certificaatautoriteit). Wanneer u uw licentie (server/service certificaat) aan een bestuurder moet tonen, weet de functionaris dat zij het DMV-filiaal (tussencertificaat) en de afdeling Automobielvoertuigen (certificaat autoriteit) kunnen vertrouwen, en zij kunnen verifiëren dat deze licentie door hen is afgegeven (certificaatautoriteit). Je identiteit is geverifieerd aan de functionaris en nu vertrouwen ze dat jij bent wie je zegt dat je bent. Anders, als u een valse licentie (server / service certificaat) die niet is ondertekend door de DMV (tussentijds certificaat), dan zullen ze niet vertrouwen wie je zegt dat je bent. De rest van dit document geeft een diepgaande, technische uitleg van de hiërarchie van certificaten.

Hoe browsers certificaten gebruiken

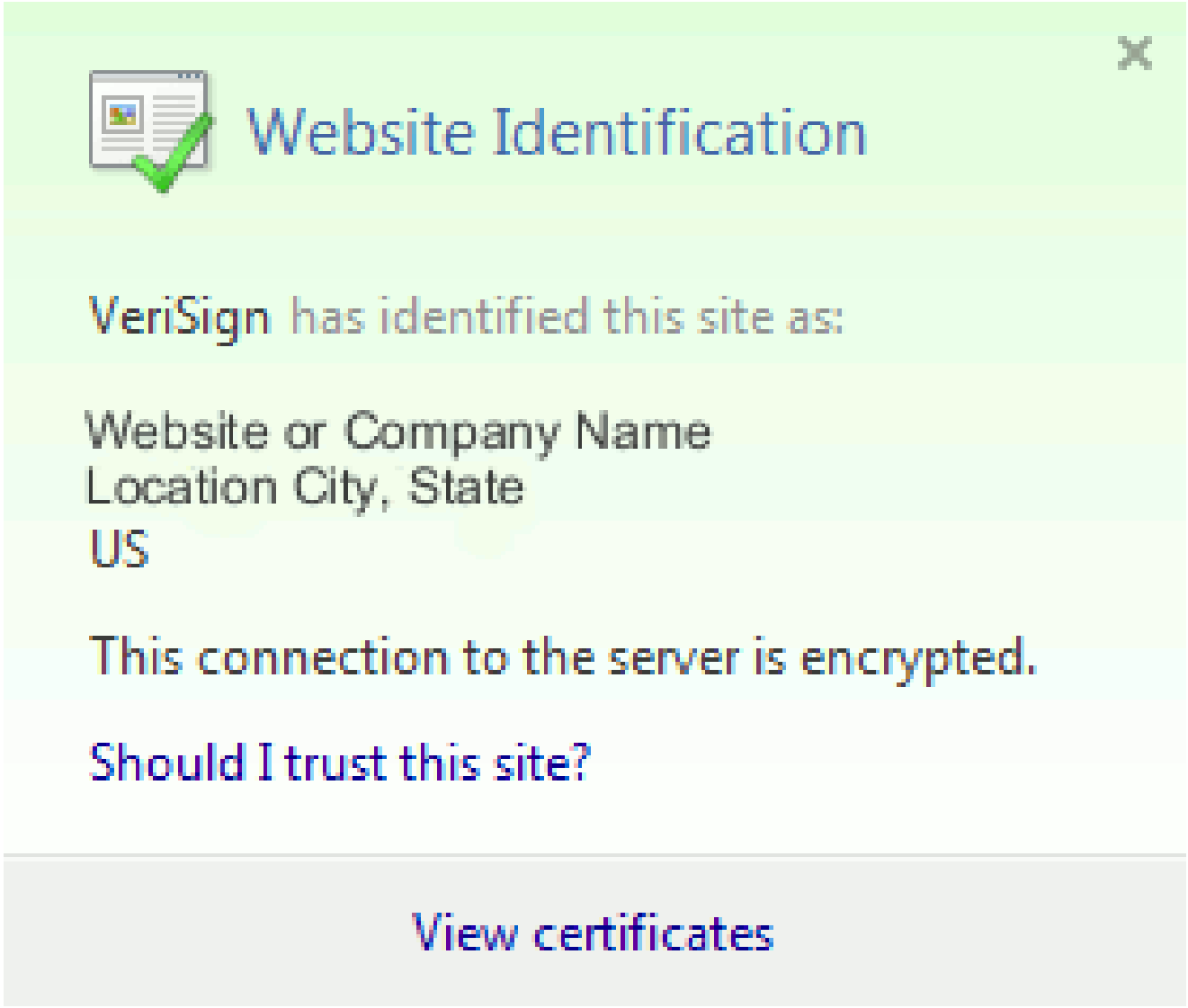
1. Wanneer u een website bezoekt, voert u de URL in, zoals http://www.cisco.com.
2. De DNS vindt het IP-adres van de server die deze site host.
3. De browser navigeert naar die site.

Zonder certificaten is het onmogelijk om te weten of een frauduleuze DNS-server is gebruikt, of of dat u naar een andere server werd gerouteerd. Certificaten zorgen ervoor dat u correct en veilig wordt doorgestuurd naar de beoogde website, zoals uw bankwebsite, waar de persoonlijke of gevoelige informatie die u invoert, veilig is.

Alle browsers hebben verschillende pictogrammen die zij gebruiken, maar normaal, ziet u een hangslot in de adresbalk als dit: 

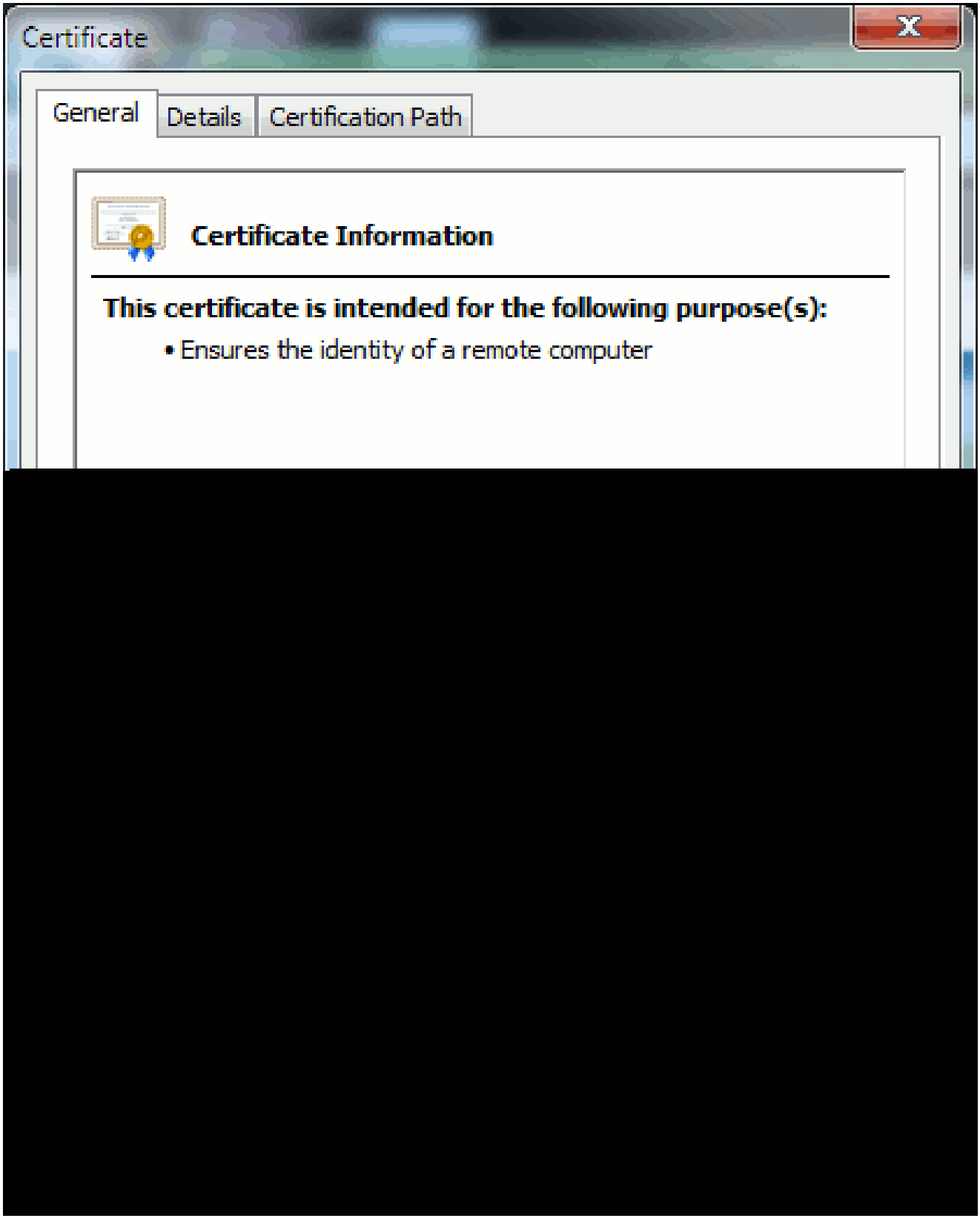
1. Klik op het hangslot en het venster toont:

   Afbeelding 1: Website Identificatie



2. Klik op Certificaten bekijken om het certificaat van de site te zien zoals in dit voorbeeld:

Afbeelding 2: Tabblad Certificaatinformatie, Algemeen



De benadrukte informatie is belangrijk.

- Afgegeven door is de Company of Certificate Authority (CA) die uw systeem al vertrouwt.

- Geldig van/naar is het datumbereik dat dit certificaat bruikbaar is. (Soms zie je een certificaat waarin je weet dat je de CA vertrouwt, maar je ziet dat het certificaat ongeldig is. Controleer altijd de datum zodat u weet of deze verlopen is.)

Tip: Een best practice is om een herinnering te maken in uw agenda om het certificaat te vernieuwen voordat het vervalt. Dit voorkomt toekomstige problemen.

De verschillen tussen PEM- en DER-certificaten

PEM is ASCII; DER is binair. Afbeelding 3 toont het formaat van het PEM-certificaat.

Figuur 3: Voorbeeld van het PEM-certificaat

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
BQcDAgYIKwYBBQUHAwUwKQYDVR0RBCIwIIIOODUxUHViLmtqbC5jb22CDnBob25l
cy5ramwuY29tMB0GA1UdDgQWBBTbWvEUfpl7hvrsTJpQfmcoNpB4LzANBgkqhkiG
9w0BAQUFAAOCAQEArZWeqarg4tagW0O0rQElZj6UJ9S8ZAcp9XDT4Iz1QwRaaiBr
EBhfulaMjmtMKXFV5eCU9QcPbPG8XmiRZiEg9Q8Wtn0OZpuPGlkwxmFYRz40aY4T
5lw+d0wVb9sPChNQEGccjjqwtstElYWDo/A4RoqdH0ALceP8a4bovK/CpmRGdb5C
+hqP4zIJs4P+YKmzrJeq7H8xCCqqkYXcRLkmG6mif78txFQ5lr8rJEoU1VlL8znc
fJvSfEsCfwnSqPaGcQTnxMOZOIyM0OjXvvhWIezrpk8cyj3vSTgXSTwO53flZX4L
tu28d5H3AHo8U6cfHRIJ1f6Yv2ClGBShXwFp6Q==
-----END CERTIFICATE-----
```

Afbeelding 4 toont het DER-certificaat.

Afbeelding 4: Voorbeeld van het DER-certificaat

De meeste bedrijven van CA zoals VeriSign of Thawt gebruiken PEM formaat om de certificaten naar klanten te verzenden, omdat het e-mailvriendelijk is. De klant moet de gehele string kopiëren en -----BEGIN CERTIFICAAT— en -----END CERTIFICAAT— opnemen, het in een tekstbestand plakken en opslaan met de extensie .PEM of .CER.

Windows kan DER- en CER-formaten lezen met zijn eigen certificaatbeheerapplicatie en toont het certificaat zoals in afbeelding 5.

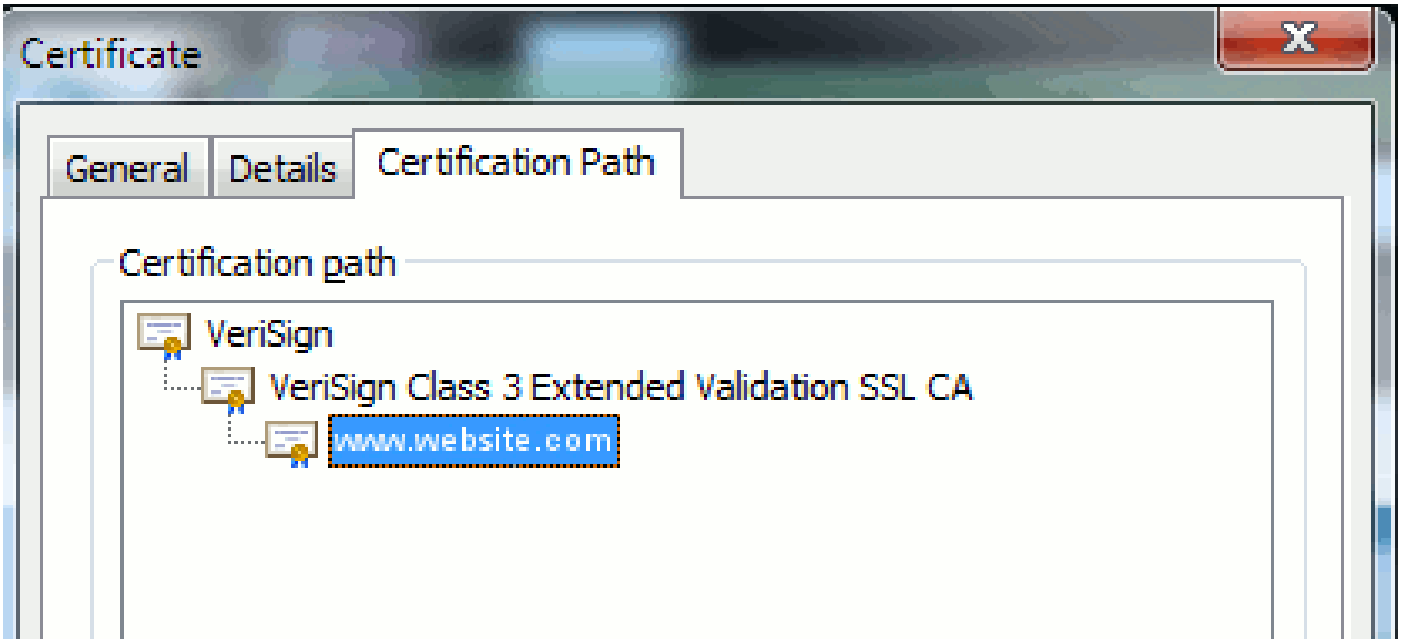
Afbeelding 5: Informatie over certificaten

In sommige gevallen vereist een apparaat een specifiek formaat (ASCII of binair). Om dit te veranderen, download het certificaat van CA in het vereiste formaat of gebruik een SSL converter tool, zoals https://www.sslshopper.com/ssl-converter.html.

Certificaathiërarchie

Om op een certificaat van een eindpunt te kunnen vertrouwen, moet er een vertrouwen zijn dat al met een derde CA is aangegaan. Afbeelding 6 laat bijvoorbeeld zien dat er een hiërarchie van drie certificaten bestaat.

Afbeelding 6: Certificaathiërarchie



- Verisign is een CA.
- Verisign Class 3 Extended Validation SSL CA is een tussenpersoon of een ondertekeningsservercertificaat (een server die door CA is geautoriseerd om certificaten in zijn naam af te geven).
- www.website.com is een server- of servicecertificaat.

Uw eindpunt moet weten dat het zowel de CA- als tussentijdse certificaten eerst kan vertrouwen voordat het weet dat het het servercertificaat kan vertrouwen dat door de SSL Handshake wordt voorgesteld (hieronder details). Om beter te begrijpen hoe dit vertrouwen werkt, verwijzen we naar de sectie in dit document: Definieer "Vertrouwen" vanuit het gezichtspunt van een certificaat.

Zelfondertekende certificaten versus certificaten van derden

De belangrijkste verschillen tussen zelfondertekende en derdencertificaten zijn wie het certificaat ondertekende, of u ze nu vertrouwt.

Een zelfondertekend certificaat is een certificaat dat is ondertekend door de server die het voorlegt; daarom zijn het server/service certificaat en het CA certificaat hetzelfde.

Een CA van derden is een service die wordt geleverd door een openbare CA (zoals Verisign, Entrust, Digicert) of een server (zoals Windows 2003, Linux, Unix, IOS) die de geldigheid van het server-/servicecertificaat controleert.

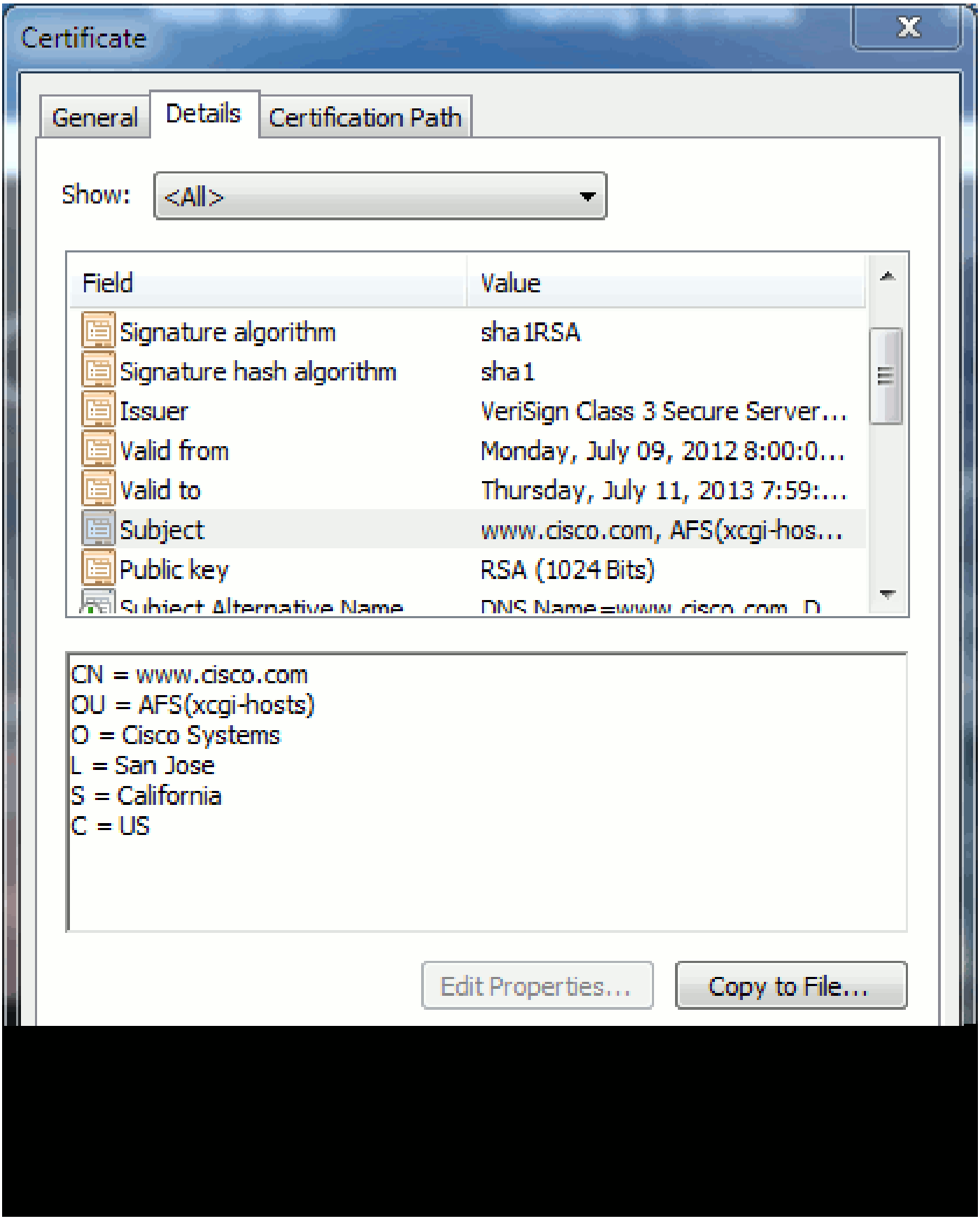
Elke kan een CA zijn. Of uw systeem dat CA al dan niet vertrouwt, is het belangrijkste.

Gemeenschappelijke en alternatieve namen

Common Names (CN) en Onderwerp Alternative Names (SAN) zijn verwijzingen naar het IP-adres of Fully Qualified Domain Name (FQDN) van het gevraagde adres. Als u bijvoorbeeld https://www.cisco.com invoert, moet de CN of SAN www.cisco.com in de header hebben.

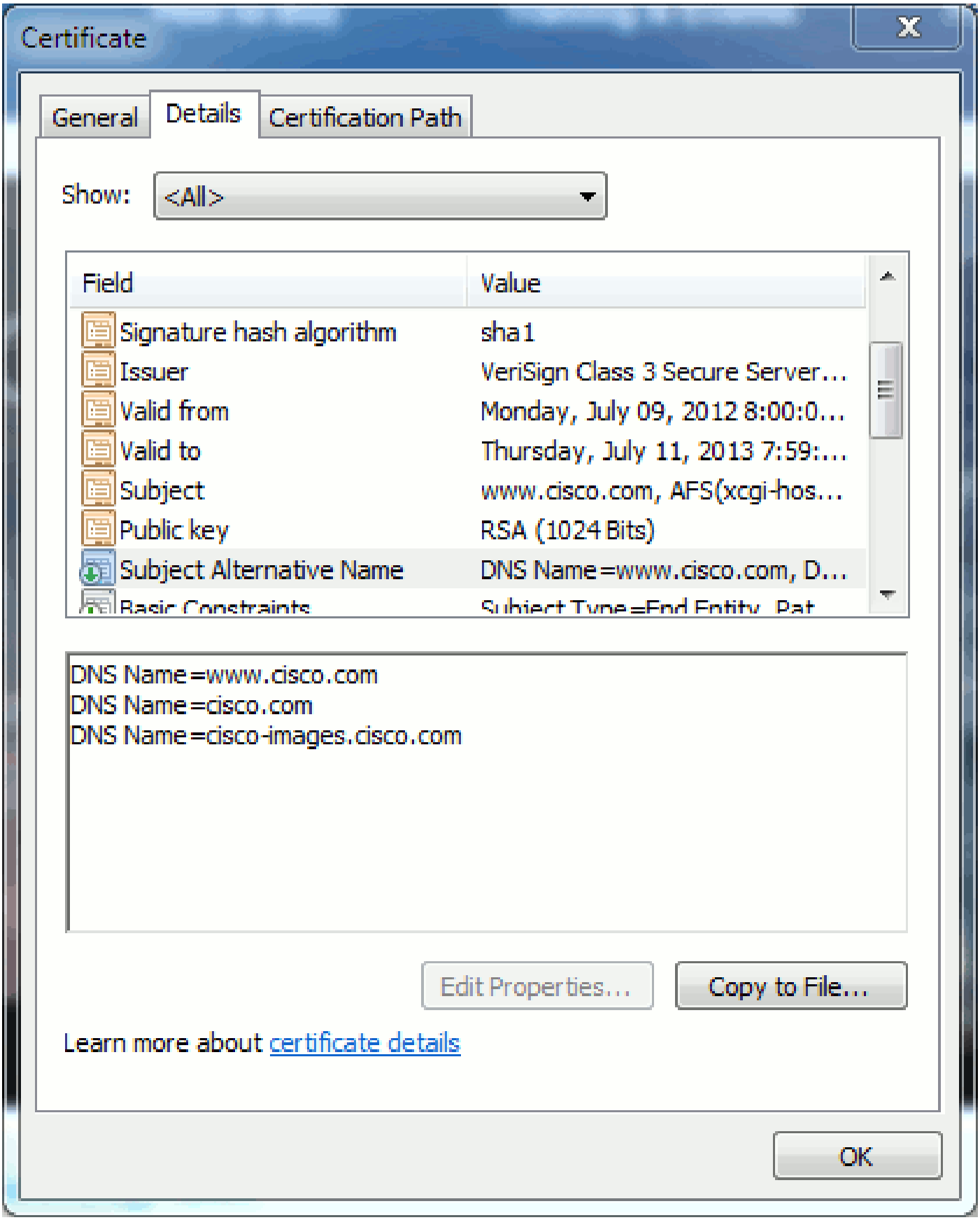
In het voorbeeld in figuur 7 heeft het certificaat de GN als www.cisco.com. Het URL-verzoek om www.cisco.com van de browser controleert de URL FQDN aan de hand van de informatie in het certificaat. In dit geval passen ze aan, en het toont dat de SSL handdruk succesvol is. Deze website is geverifieerd als de juiste website en communicatie wordt nu versleuteld tussen het bureaublad en de website.

Afbeelding 7: Website Verificatie



In hetzelfde certificaat is er een SAN-header voor drie FQDN/DNS-adressen:

Afbeelding 8: SAN-header



Met dit certificaat kan www.cisco.com (ook gedefinieerd in de GN), cisco.com en cisco-images.cisco.com worden geverifieerd. Dit betekent dat u ook cisco.com kunt typen, en dit zelfde certificaat kan worden gebruikt om deze website te verifiëren en te versleutelen.

CUCM kan SAN-headers maken. Raadpleeg het document van Jason Burn, CUCM Upload

CCMAdmin Web GUI-certificaten op de ondersteuningscommunity voor meer informatie over SAN-headers.

Wild Card-certificaten

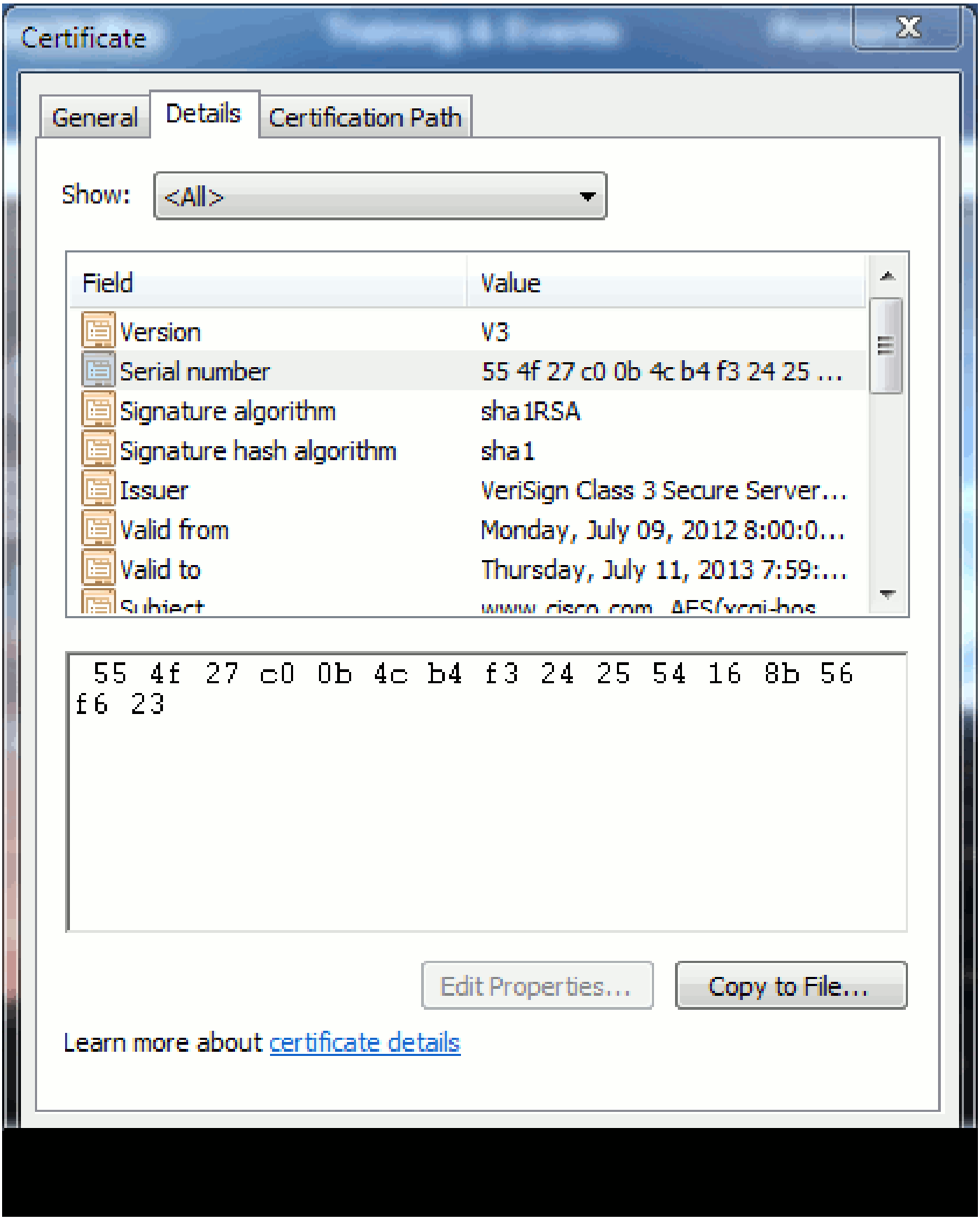
Wildcard-certificaten zijn certificaten die een sterretje (*) gebruiken om een tekenreeks in een deel van een URL te vertegenwoordigen. Als een beheerder bijvoorbeeld een certificaat voor www.cisco.com, ftp.cisco.com, ssh.cisco.com enzovoort wil hebben, hoeft hij alleen een certificaat voor *.cisco.com aan te maken. Om geld te besparen hoeft de beheerder slechts één certificaat te kopen en hoeft hij geen meerdere certificaten te kopen.

Deze optie wordt momenteel niet ondersteund door Cisco Unified Communications Manager (CUCM). U kunt echter wel bijhouden van deze verbetering: CSCta14114: Verzoek om ondersteuning van wildcard certificaat in CUCM en private key import.

Identificeer de certificaten

Wanneer certificaten dezelfde informatie bevatten, kunt u zien of het hetzelfde certificaat is. Alle certificaten hebben een uniek serienummer. U kunt dit gebruiken om te vergelijken als de certificaten dezelfde, geregenereerde of vervalste certificaten zijn. Afbeelding 9 geeft een voorbeeld:

Afbeelding 9: Serienummer van het certificaat



MVO's en hun doel

CSR staat voor certificaatondertekeningsaanvraag. Als u een certificaat van derden wilt aanmaken voor een CUCM-server, hebt u een CSR nodig om aan de CA te presenteren. Dit CSR lijkt veel op

een PEM (ASCII) certificaat.

Opmerking: dit is geen certificaat en kan niet als één certificaat worden gebruikt.

\

CUCM maakt automatisch CSR's via web GUI: Cisco Unified Operating System Administration > Security > Certificate Management > Generate CSR, kies de service die u wilt maken van het certificaat SNF en Generate CSR. Elke keer dat deze optie wordt gebruikt, wordt er een nieuwe privésleutel en MVO gegenereerd.

Opmerking: Een privé-sleutel is een bestand dat uniek is voor deze server en service. Dit mag nooit aan iemand worden gegeven! Als u een privé-sleutel aan iemand verstrekt, compromitteert het de veiligheid die het certificaat verstrekt. Ook, regenereer geen nieuwe CSR voor de zelfde dienst als u oude CSR gebruikt om een certificaat te creëren. De CUCM verwijdert de oude MVO en de persoonlijke sleutel en vervangt deze beide, wat de oude MVO nutteloos maakt.

Raadpleeg de documentatie van Jason Burn op de Support Community: CUCM Upload CCMAdmin Web GUI Certificates voor informatie over het maken van CSR's.

Gebruik van certificaten tussen eindpunt en SSL/TLS-handschuddingsproces

Het handshake-protocol is een serie gerangschikte berichten die over de veiligheidsparameters van een gegevensoverdrachtsessie onderhandelen. Raadpleeg SSL/TLS in detail , waarin de berichtvolgorde in het handshake-protocol wordt gedocumenteerd. Deze zijn te zien in packet capture (PCAP). De details omvatten de eerste, verdere, en definitieve berichten die tussen de cliënt en de server worden verzonden en worden ontvangen.

Hoe CUCM certificaten gebruikt

Het verschil tussen tomcat en tomcat-trust

Wanneer certificaten naar CUCM worden geüpload, zijn er twee opties voor elke service via Cisco Unified Operating System Administration > Security > Certificate Management > Find.

De vijf diensten die u toestaan om certificaten in CUCM te beheren zijn:

- kater
- ipsec

- callmanager
- capf
- tv's (in CUCM release 8.0 en hoger)

Hier zijn de diensten die u toestaan om certificaten aan CUCM te uploaden:

- kater
- kater-trust
- ipsec
- ipsec-trust
- callmanager
- CallManager-trust
- capf
- Kapitaalfonds

Dit zijn de services die beschikbaar zijn in CUCM release 8.0 en hoger:

- tv
- Tv-trust
- telefoontrust
- phone-VPN-trust
- phone-sast-trust
- phone-ctl-trust

Raadpleeg de CUCM Security Guides door Release voor meer informatie over deze typen certificaten. In deze sectie wordt alleen het verschil tussen een servicecertificaat en een vertrouwenscertificaat toegelicht.

Bijvoorbeeld, met tomcat, de tomcat-trusts uploaden van de CA en de tussenliggende certificaten zodat deze CUCM-knooppunt weet dat het elk certificaat kan vertrouwen dat is ondertekend door de CA en de tussenserver. Het tomcat-certificaat is het certificaat dat door de tomcat-service op deze server wordt aangeboden als een eindpunt een HTTP-verzoek aan deze server doet. Om de presentatie van certificaten van derden per tomcat mogelijk te maken, moet het CUCM-knooppunt weten dat het de CA en de tussenserver kan vertrouwen. Daarom is het een vereiste om CA en de tussentijdse certificaten te uploaden alvorens het tomcat (dienst) certificaat wordt geüpload.

Raadpleeg de CCMAdmin Web GUI-certificaten op de ondersteuningscommunity van Jason

Burn's CUCM voor informatie die u zal helpen te begrijpen hoe u certificaten naar CUCM kunt uploaden.

Elke dienst heeft zijn eigen servicecertificaat en vertrouwenscertificaten. Ze werken niet van elkaar af. Met andere woorden, een CA- en tussentijds certificaat dat als tomcat-trust-service is geüpload, kan niet door de CallManager-service worden gebruikt.

Opmerking: certificaten in CUCM zijn per knooppunt. Als u dus certificaten moet uploaden naar de uitgever, en u de abonnees nodig hebt om dezelfde certificaten te hebben, moet u ze uploaden naar elke individuele server en knooppunt voorafgaand aan CUCM release 8.5. In CUCM release 8.5 en hoger is er een service die geüploade certificaten repliceert naar de rest van de knooppunten in het cluster.

Opmerking: elk knooppunt heeft een andere GN. Daarom moet er door elk knooppunt een MVO worden gecreëerd, zodat de dienst zijn eigen certificaten kan presenteren.

Als u extra specifieke vragen hebt over een van de beveiligingsfuncties van de CUCM, raadpleegt u de beveiligingsdocumentatie.

Conclusie

Dit document ondersteunt en bouwt een hoog kennisniveau op het gebied van certificaten. Dit onderwerp kan van belang worden meer diepgaand, maar dit document maakt u voldoende vertrouwd om met certificaten te werken. Als u vragen hebt over de beveiligingsfuncties van CUCM, raadpleegt u de beveiligingshandleidingen van CUCM door release voor meer informatie.

Gerelateerde informatie

- Onderhouds- en beveiligingshandleidingen voor Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- Cisco-ondersteuningscommunity: CUCM-uploadcertificaten voor CCMdmin Web GUI
- Bug CSCta14114: Verzoek om ondersteuning van wildcard certificaat in CUCM en private key import
- Cisco Emergency Responder (CER) toegelicht
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.