Weergave op hoog niveau van certificaten en autoriteiten in CUCM

Inhoud

Inleiding

Dit document heeft tot doel inzicht te krijgen in de basisbeginselen van de autoriteiten van certificaten en certificaten. Dit document vult andere Cisco-documenten aan die verwijzen naar alle 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 de certificaten

Certificaten worden tussen eindpunten gebruikt om een vertrouwen/authenticatie en encryptie van gegevens op te bouwen. Dit bevestigt dat de eindpunten met het beoogde apparaat communiceren en de optie hebben om de gegevens tussen de twee eindpunten te versleutelen.

Definieer het vertrouwen vanuit het standpunt van een certificaat

Het belangrijkste deel van certificaten is de definitie van welke eindpunten aan uw eind kunnen worden vertrouwd. Dit document helpt u te weten en te definiëren hoe uw gegevens versleuteld en gedeeld worden met de geplande website, telefoon, FTP server enzovoort.

Wanneer uw systeem een certificaat vertrouwt, betekent dit dat er een voorgeïnstalleerd certificaat of certificaten op uw systeem is, waarin staat dat het 100% ervan overtuigd is dat het de informatie met het juiste eindpunt deelt. Anders stopt het de communicatie tussen deze eindpunten.

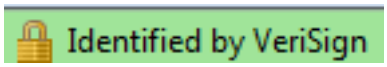
Een niet-technisch voorbeeld hiervan is je rijbewijs. U gebruikt deze licentie (server-/servicecertificaat) om aan te tonen dat u bent wie u zegt dat u bent; u heeft uw rijbewijs verkregen van uw plaatselijke afdeling motorvoertuigen (tussentijds certificaat), die toestemming heeft gekregen van de afdeling motorvoertuigen (DMV) van uw staat (certificaatinstantie). Wanneer u uw rijbewijs (server/service certificaat) aan een ambtenaar moet tonen, weet de ambtenaar dat zij vertrouwen kunnen hebben in de DMV-afdeling (tussencertificaat) en de afdeling motorvoertuigen (certificatie-instantie) en dat zij kunnen controleren of deze vergunning door hen is afgegeven (certificaatinstantie). Je identiteit wordt gecontroleerd aan de agent en nu vertrouwen ze erop dat jij bent wie je zegt dat je bent. Als u anders een valse licentie (server/service certificaat) geeft die niet is getekend door de DMV (tussentijds certificaat), dan vertrouwen ze niet op wie u zegt dat u bent. De rest van dit document geeft een diepgaande technische uitleg van de hiërarchie van certificaten.

Hoe browsers certificaten gebruiken

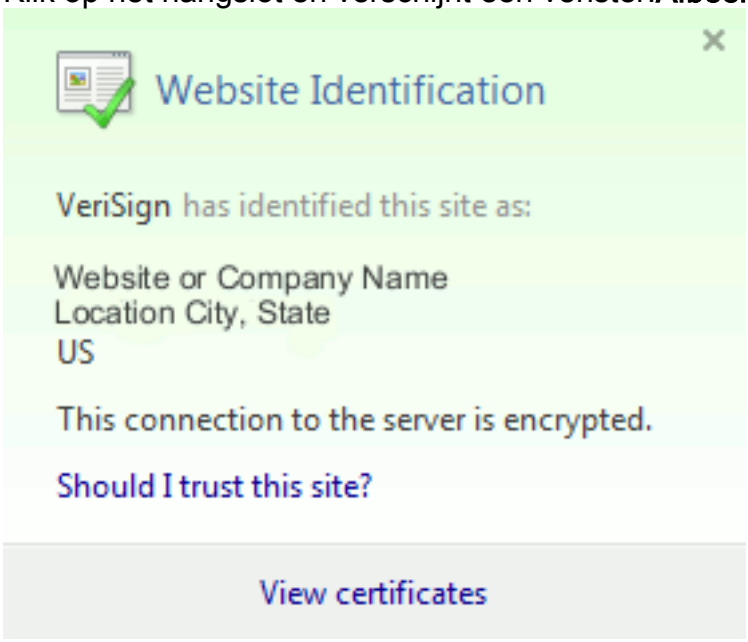
1. Wanneer u een website bezoekt, voer u de URL in, zoals http://www.cisco.com.
2. De DNS vindt het IP adres van de server die die op die plaats is gevestigd.
3. De browser navigeert naar die site.

Zonder certificaten is het onmogelijk om te weten of een sterk DNS server gebruikt werd of of dat u naar een andere server gestuurd werd. Certificaten verzekeren dat u correct en veilig naar de bedoelde website, zoals uw bankwebsite, wordt verstuurd, waar de persoonlijke of gevoelige informatie die u ingeeft, veilig is.

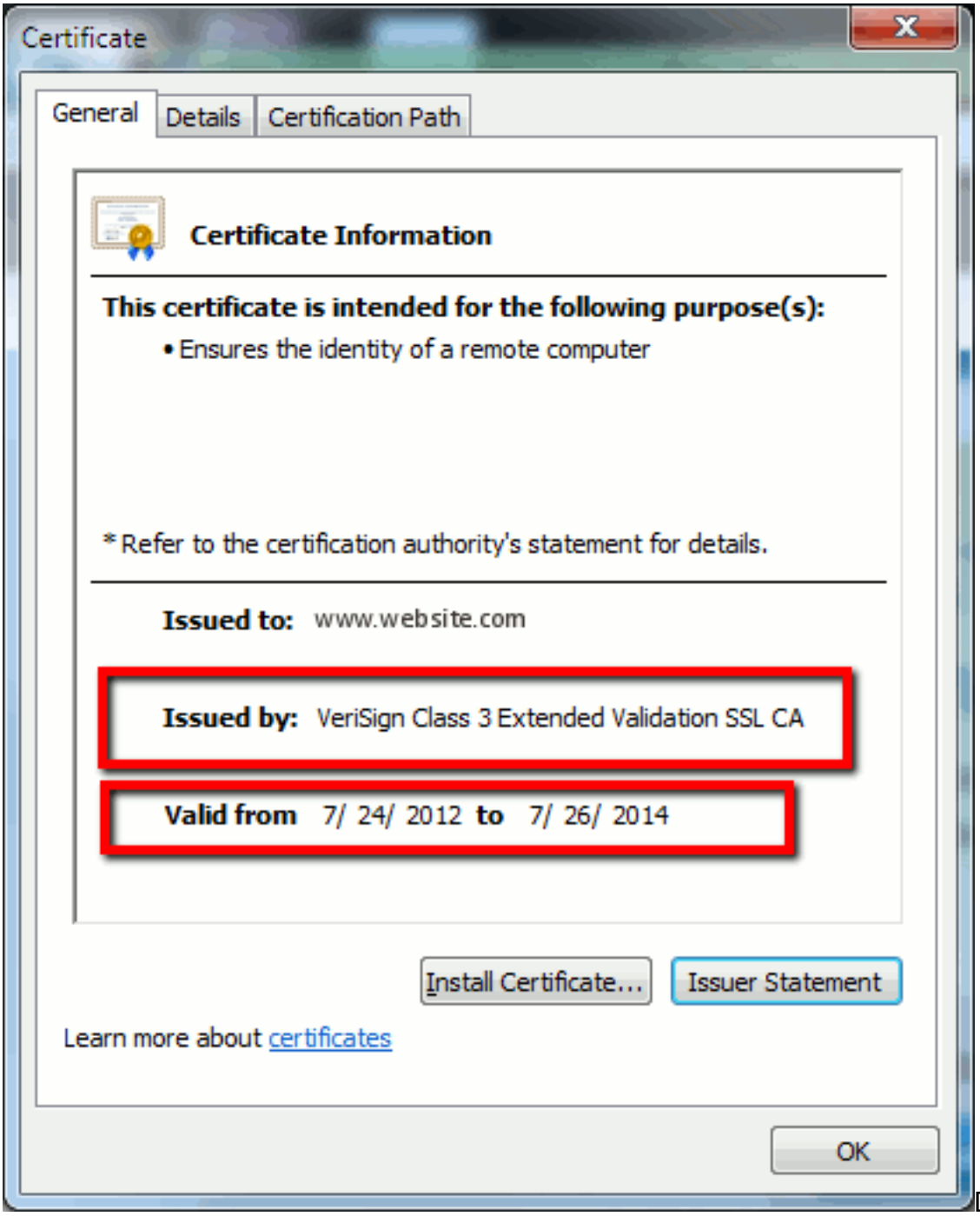
Alle browsers hebben verschillende pictogrammen die ze gebruiken, maar normaal zie je een

hangslot in de adresbalk zoals deze: 

1. Klik op het hangslot en verschijnt een venster:**Afbeelding 1: Identificatie van website**



2. Klik op **Certificaten bekijken** om het certificaat van de site te zien zoals in dit voorbeeld:**Afbeelding 2: certificaatinformatie, tabblad Algemeen**



De gemarkeerde informatie is belangrijk.**Afgegeven door** is de Company of de certificaatinstantie (CA) die uw systeem al beheerst.**Geldig van/tot** is het datumbereik dat dit certificaat bruikbaar is. (Soms ziet u een certificaat waarvan u weet dat u de CA vertrouwt, maar u ziet dat het certificaat ongeldig is. Controleer altijd de datum zodat u weet of deze al dan niet is verlopen.)**TIP:** Een goede praktijk is om in uw kalender een herinnering te maken om het certificaat te vernieuwen voordat het verstrijkt. Dit voorkomt toekomstige problemen.

De verschillen tussen PEM- en DER-certificaten

PEM is ASCII; DER is binair. Afbeelding 3 toont het PEM-certificaatformaat.

Afbeelding 3: PEM-certificaatvoorbeeld

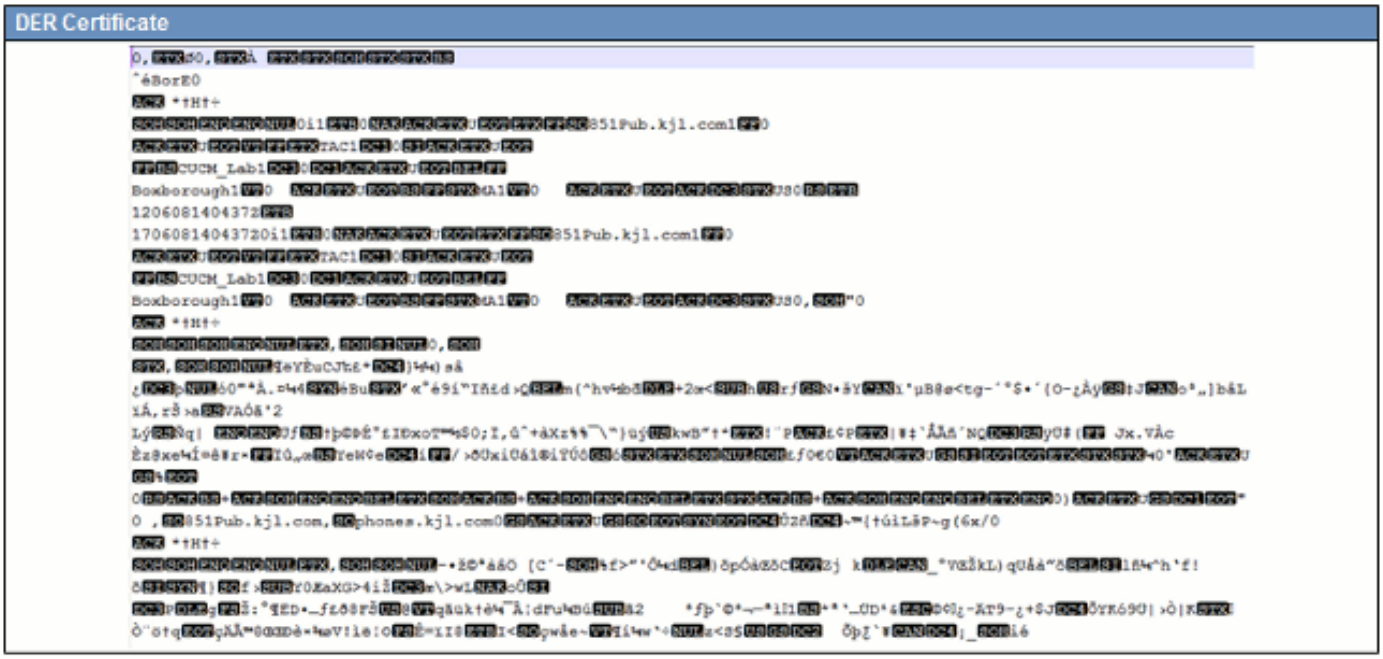
PEM Certificate

```
-----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-----
```

Afbeelding 4 toont het DER-certificaat.

Afbeelding 4: certificaatvoorbeeld voor DER

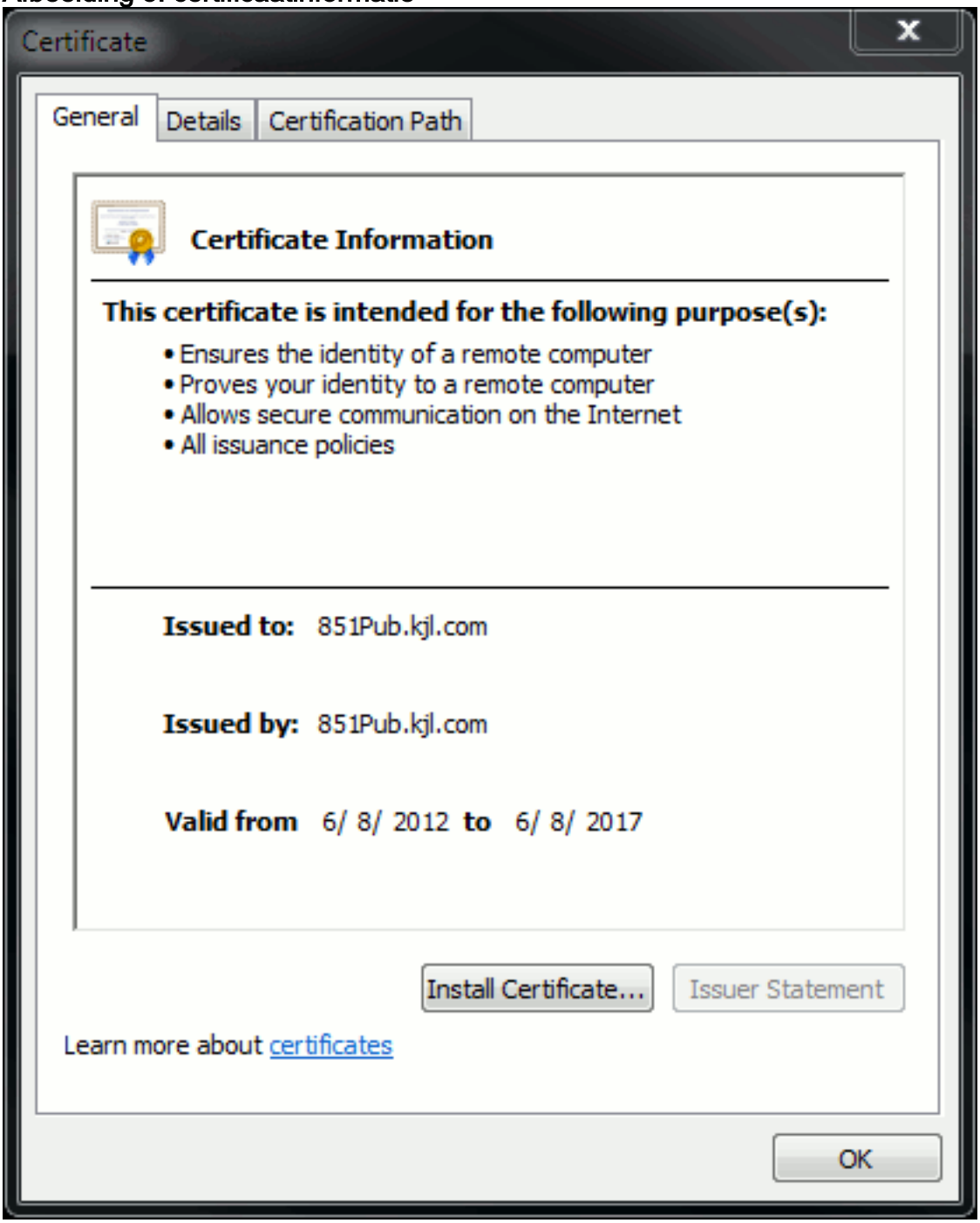
DER Certificate



De meeste CA-bedrijven zoals VeriSign of Thawt gebruiken PEM-indeling om de certificaten naar klanten te sturen, omdat het e-mailvriendelijk is. De klant dient de gehele string te kopiëren en op te nemen **—BEGIN CERTIFICAAT—** en **—EINDCERTIFICAAT—**, het in een tekstbestand te plakken en het op te slaan met de extensie .PEM of .CER.

Windows kan de bestandsindelingen DER en CER met hun eigen certificaatapplicatie lezen en het certificaat weergeven zoals in afbeelding 5.

Afbeelding 5: certificaatinformatie

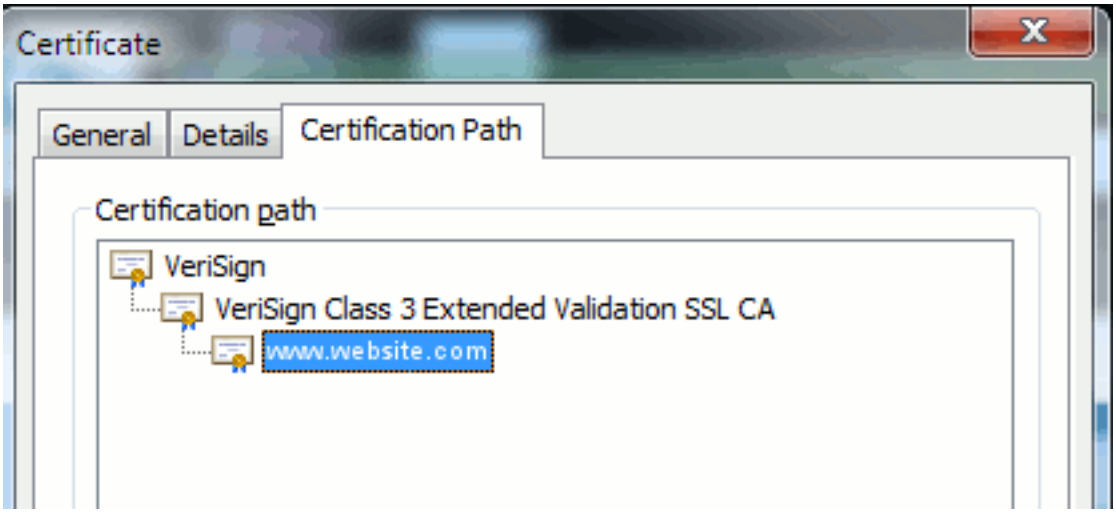


In sommige gevallen vereist een apparaat een specifiek formaat (ASCII of binair). Om dit te wijzigen, kunt u het certificaat van de CA in de gewenste indeling downloaden of een SSL-conversiegereedschap gebruiken, zoals https://www.sslshopper.com/ssl-converter.html.

certificaathiërarchie

Om een certificaat vanaf een eindpunt te kunnen vertrouwen, moet er een reeds met een derde partij opgericht vertrouwen zijn. Afbeelding 6 toont bijvoorbeeld een hiërarchie van drie certificaten.

Afbeelding 6: certificaathiërarchie



- **Versiering** is een CA.
- **Vertrouwend Klasse 3 Extended Validation SSL CA** is een intermediair of het ondertekenen van een servercertificaat (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 de intermediaire certificaten eerst kan vertrouwen vooraleer het weet dat het het servercertificaat kan vertrouwen dat door de SSL Handshake wordt aangeboden (details hieronder). Om beter te begrijpen hoe dit vertrouwen werkt, raadpleegt u de sectie in dit document: **Defineer "vertrouwen" vanuit het gezichtspunt van een certificaat**.

Zelfgetekende certificaten versus certificaten van derden

De belangrijkste verschillen tussen zelfgetekende en derdencertificaten zijn wie het certificaat heeft ondertekend, of je ze nu vertrouwt.

Een zichzelf ondertekend certificaat is een certificaat dat is ondertekend door de server die het presenteert; Daarom zijn het server/service certificaat en het CA-certificaat hetzelfde.

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

Elke kan een CA zijn. Of je systeem dat wel of niet vertrouwt op CA, is wat er het meest toe doet.

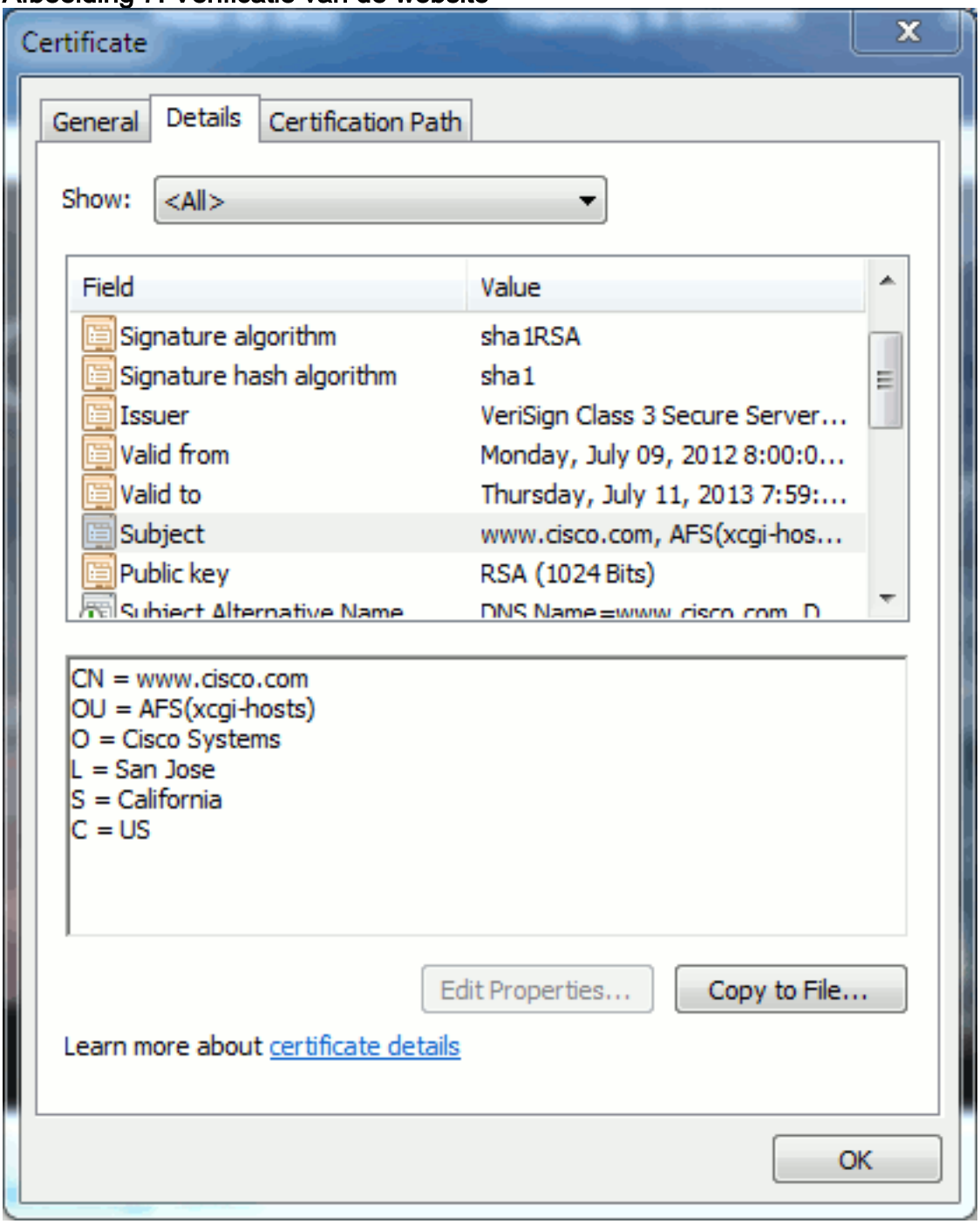
Gemeenschappelijke namen en alternatieve namen voor onderwerp

Gemeenschappelijke namen (CN) en Onderwerp Alternative Names (SAN) zijn verwijzingen naar het IP-adres of Full Qualified Domain Name (FQDN) van het gevraagde adres. Bijvoorbeeld, als u https://www.cisco.com ingaat, dan moeten de GN of SAN www.cisco.com in de header hebben.

In het voorbeeld in afbeelding 7 heeft het certificaat de GN als www.cisco.com. Het URL verzoek om www.cisco.com van de browser controleert de URL FQDN tegen de informatie die het certificaat presenteert. In dit geval passen ze elkaar aan, en het laat zien dat de SSL handdruk succesvol is. Deze website blijkt de juiste website te zijn en de communicatie is nu versleuteld

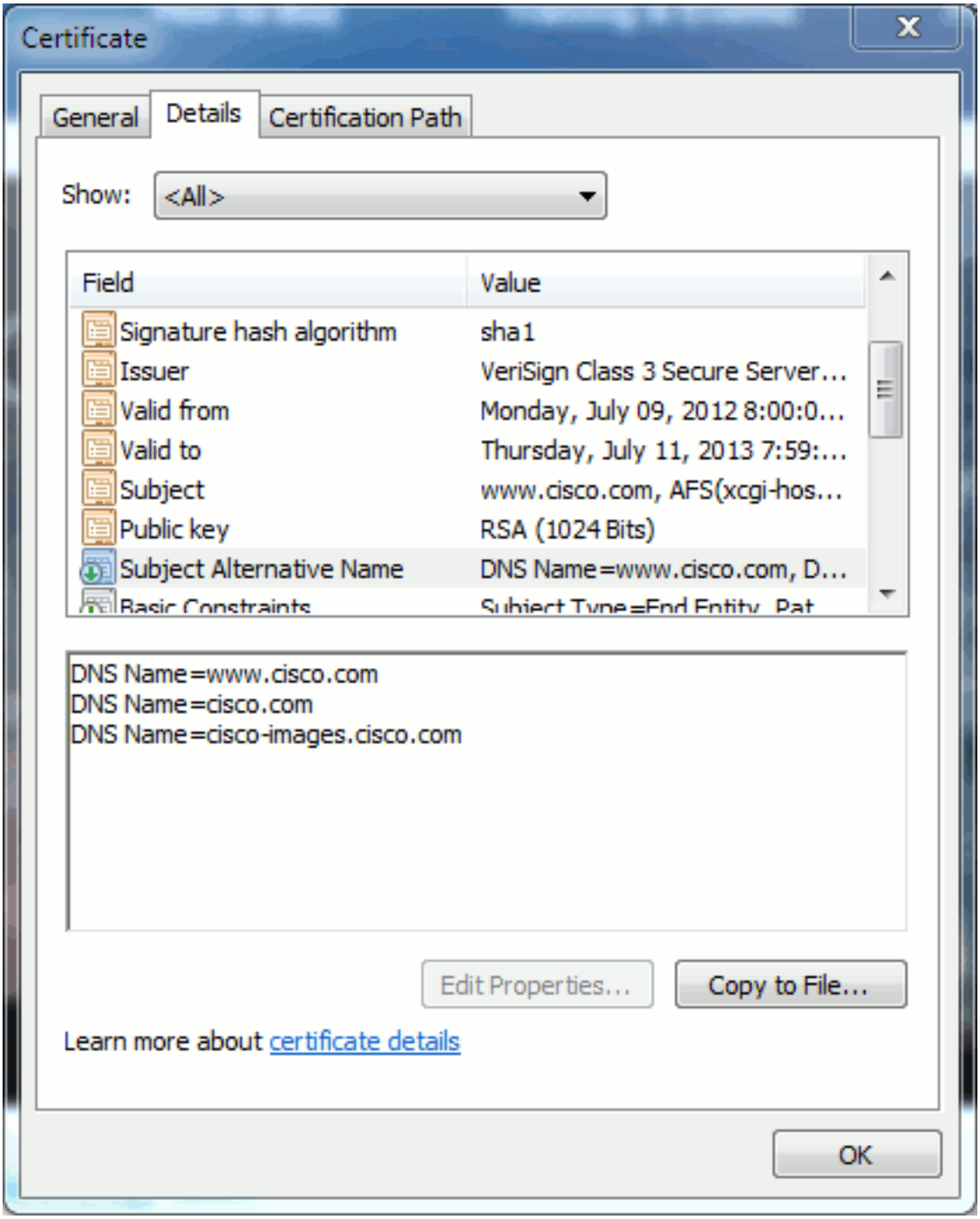
tussen het bureaublad en de website.

Afbeelding 7: Verificatie van de website



In hetzelfde certificaat heeft u een SAN-header voor drie FQDN/DNS-adressen:

Afbeelding 8: SAN-kop



Dit certificaat kan worden gewaarmerkt op www.cisco.com (ook gedefinieerd in de GN), cisco.com en cisco-Image.cisco.com. Dit betekent dat u ook cisco.com kunt typen en dit certificaat kan worden gebruikt om deze website te authentiseren en te versleutelen.

CUCM kan SAN-headers maken. Raadpleeg het document van Jason Burn, CUCM Upload CCMAdmin Web GUI Certificaten op de Support Community voor meer informatie over SAN-headers.

Wilde kaartcertificaten

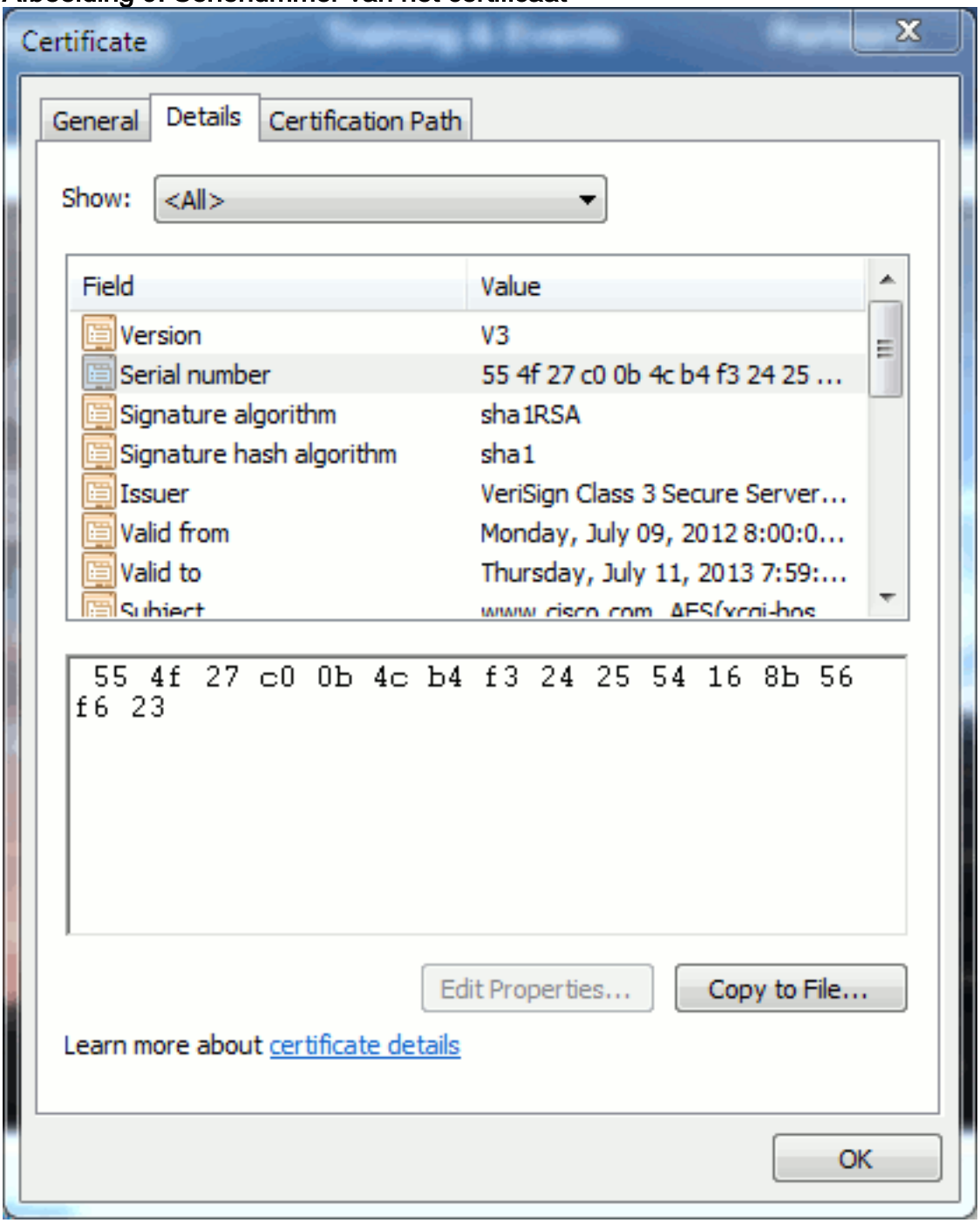
Wildcard certificaten zijn certificaten die een sterretje (*) gebruiken om een string in een sectie van een URL weer te geven. Om bijvoorbeeld een certificaat te hebben voor www.cisco.com, ftp.cisco.com, ssh.cisco.com, enzovoort, hoeft een beheerder alleen een certificaat voor *.cisco.com te maken. Om geld te besparen hoeft de beheerder slechts één certificaat te kopen en geen meerdere certificaten aan te schaffen.

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

De certificaten identificeren

Als de certificaten dezelfde informatie in hen hebben, kunt u zien of het hetzelfde certificaat is. Alle certificaten hebben een uniek serienummer. U kunt deze optie gebruiken om te vergelijken of de certificaten dezelfde certificaten, regeneraties of vervalsingen zijn. Afbeelding 9 geeft een voorbeeld:

Afbeelding 9: Serienummer van het certificaat



MVO's en hun doel

CSR staat voor certificaataanvraag. Als u een certificaat van derden voor een CUCM server wilt

maken, hebt u een CSR nodig om aan CA te presenteren. Dit CSR lijkt erg op een PEM (ASCII)-certificaat.

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

CUCM maakt CSR's automatisch via web GUI: **Cisco Unified Operating System Management > Security > certificaatbeheer > Generate CSR >** kiest de service die u het certificaat wilt maken **> Generate CSR**. Elke keer dat deze optie wordt gebruikt, wordt er een nieuwe privé-sleutel en CSR gegenereerd.

Opmerking: Een privé-toets is een bestand dat uniek is voor deze server en service. Dit mag nooit aan iemand gegeven worden! Als u iemand een privésleutel geeft, komt de beveiliging in het gedrang die het certificaat biedt. Reinig ook geen nieuwe CSR voor dezelfde service als u de oude CSR gebruikt om een certificaat te maken. CUCM verwijdert de oude CSR- en privé-toets en vervangt beide, waardoor de oude CSR nutteloos wordt.

Raadpleeg de documentatie van Jason Burn over de ondersteuningscommunity: CUCM Upload CCMAdmin Web GUI Certificaten voor informatie over hoe u CSRs kunt maken.

Gebruik van certificaten tussen eindpunt en SSL/TLS-handdrukproces

Het handshake protocol is een reeks van gesequentieerde berichten die onderhandelen over de veiligheidsparameters van een gegevensoverdrachtsessie. Raadpleeg SSL/TLS in Detail , die de berichtvolgorde in het handshake-protocol documenteert. Deze kunnen worden gezien in een pakketvastlegging (PCAP). De details omvatten de eerste, volgende en laatste berichten die tussen de client en de server worden verzonden en 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 Management > Security > certificaatbeheer > Find**.

De vijf services die u in staat stellen certificaten in CUCM te **beheren** zijn:

- tomcat
- ipsec
- callmanager
- hoofd
- vs (in CUCM release 8.0 en later)

Hier zijn de services die het mogelijk maken certificaten **te uploaden** naar CUCM:

- tomcat
- kat-trust
- ipsec
- ipsec-trust
- callmanager

- callmanager
- hoofd
- trust

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

- vs
- tvs-trust
- telefoonvertrouwen
- telefoonvertrouwen
- telefoonvertrouwen
- telefooncel

Raadpleeg de CUCM Security Guides door release voor meer informatie over deze typen certificaten. In deze sectie wordt alleen het verschil uitgelegd tussen een servicecertificaat en een trust certificaat.

Bijvoorbeeld, met **tomcat**, de **tomcat-trusts** uploaden de CA en intermediaire certificaten zodat dit CUCM knooppunt weet dat het elk certificaat kan vertrouwen dat door de CA en de intermediaire server wordt ondertekend. Het certificaat van The Tomcat is het certificaat dat door de tomcat service op deze server wordt voorgesteld, als een eindpunt een HTTP aanvraag aan deze server indient. Om de presentatie van derdencertificaten door tomcat toe te staan, moet het CUCM-knooppunt weten dat het de CA- en intermediaire server kan vertrouwen. Daarom is het noodzakelijk de CA- en de tussentijdse certificaten te uploaden voordat het certificaat van de tomcat (service) wordt geüpload.

Raadpleeg de CUCM van Jason Burn om CCMAdmin Web GUI-certificaten te uploaden op de ondersteuningscommunity voor informatie die u helpt te begrijpen hoe u certificaten aan CUCM kunt uploaden.

Elke dienst heeft zijn eigen servicecertificaten en vertrouwenscertificaten. Ze werken niet van elkaar. Met andere woorden, een CA en een tussencertificaat dat als een trustdienst is geüpload kan niet door de dienst van de callmanager worden gebruikt.

Opmerking: Certificaten in CUCM zijn per knooppunt. Daarom, als u certificaten nodig hebt die aan de uitgever worden geüpload, en u de abonnees nodig hebt om de zelfde certificaten te hebben, moet u deze aan elke individuele server en knooppunt vóór CUCM release 8.5 uploaden. In CUCM release 8.5 en later is er een service die certificaten aan de rest van de knooppunten in het cluster uploadt.

Opmerking: Elk knooppunt heeft een andere GN. Daarom moet er door elk knooppunt een CSR worden gemaakt, zodat de dienst zijn eigen certificaten kan aanbieden.

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

Conclusie

Dit document helpt en bouwt een hoog niveau van kennis over certificaten op. Dit onderwerp kan dieper worden, maar dit document vertrouwt u genoeg om met certificaten te werken. Als u vragen hebt over alle CUCM-beveiligingsfuncties, raadpleegt u de CUCM Security Guides door release voor meer informatie.

Gerelateerde informatie

- Cisco Unified Communications Manager (CallManager) onderhouds- en beveiligingshandleidingen
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- Cisco-ondersteuningscommunity: CUCM Upload CCMAdmin Web GUI-certificaten
- CSCta14114: Verzoek om ondersteuning van een certificaat met jokerteken in CUCM en de invoer van een particuliere sleutel
- Cisco Response (CER) uitgelegd
- Technische ondersteuning en documentatie – Cisco Systems