Visualizzazione ad alto livello di certificati e autorità in CUCM

Sommario

Introduzione

Lo scopo di questo documento è comprendere le nozioni di base sui certificati e sulle autorità di certificazione. Questo documento è complementare ad altri documenti Cisco che fanno riferimento a qualsiasi funzionalità di crittografia o autenticazione in Cisco Unified Communications Manager (CUCM).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Scopo dei certificati

I certificati vengono utilizzati tra gli endpoint per creare un'attendibilità/autenticazione e la crittografia dei dati. Ciò conferma che gli endpoint comunicano con il dispositivo desiderato e che è possibile crittografare i dati tra i due endpoint.

Definisci attendibilità dal punto di vista di un certificato

La parte più importante dei certificati è la definizione di quali endpoint possono essere considerati attendibili dal punto finale. Questo documento consente di conoscere e definire in che modo i dati vengono crittografati e condivisi con il sito Web, il telefono, il server FTP e così via.

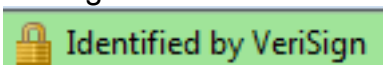
Quando il sistema considera attendibile un certificato, significa che nel sistema sono presenti uno o più certificati preinstallati che garantiscono la condivisione delle informazioni con l'endpoint corretto. In caso contrario, interrompe la comunicazione tra questi endpoint.

Un esempio non tecnico è la patente di guida. Utilizzare questa licenza (certificato server/servizio) per dimostrare di essere effettivamente l'utente corrente; Lei ha ottenuto la patente dalla sua filiale locale della Divisione dei Veicoli a Motore (certificato intermedio) che le è stata data l'autorizzazione dalla Divisione dei Veicoli a Motore (DMV) del Suo Stato (autorità di certificazione). Quando è necessario mostrare la licenza (certificato server/servizio) a un funzionario, quest'ultimo sa che può fidarsi della filiale DMV (certificato intermedio) e della divisione Veicoli a motore (autorità di certificazione) e può verificare che la licenza sia stata rilasciata da loro (autorità di certificazione). La tua identità viene verificata all'ufficiale e ora si fidano che sei quello che dici di essere. In caso contrario, se si fornisce una licenza falsa (certificato server/servizio) che non è stata firmata dal DMV (certificato intermedio), non sarà possibile considerare attendibile la propria identità. Nella parte restante di questo documento viene fornita una spiegazione tecnica approfondita della gerarchia dei certificati.

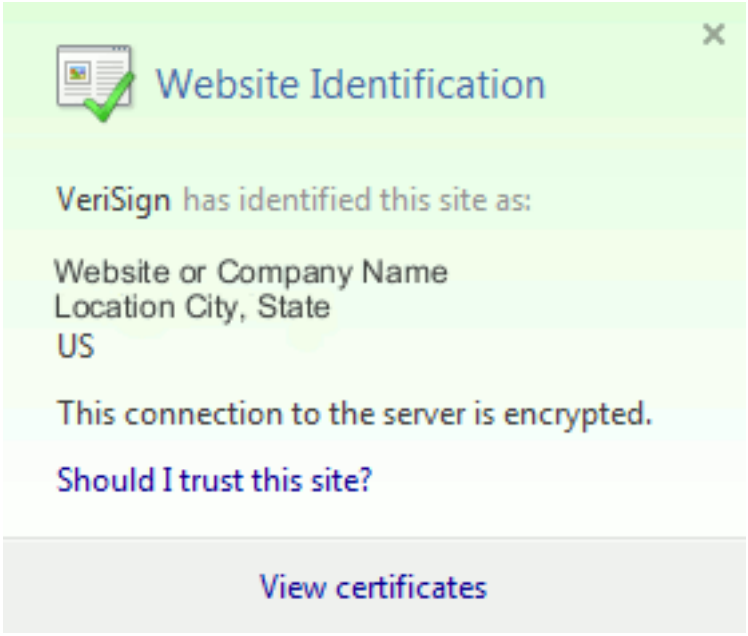
Utilizzo dei certificati da parte dei browser

1. Quando si visita un sito Web, immettere l'URL, ad esempio http://www.cisco.com.
2. Il DNS trova l'indirizzo IP del server che ospita il sito.
3. Il browser passa a tale sito.

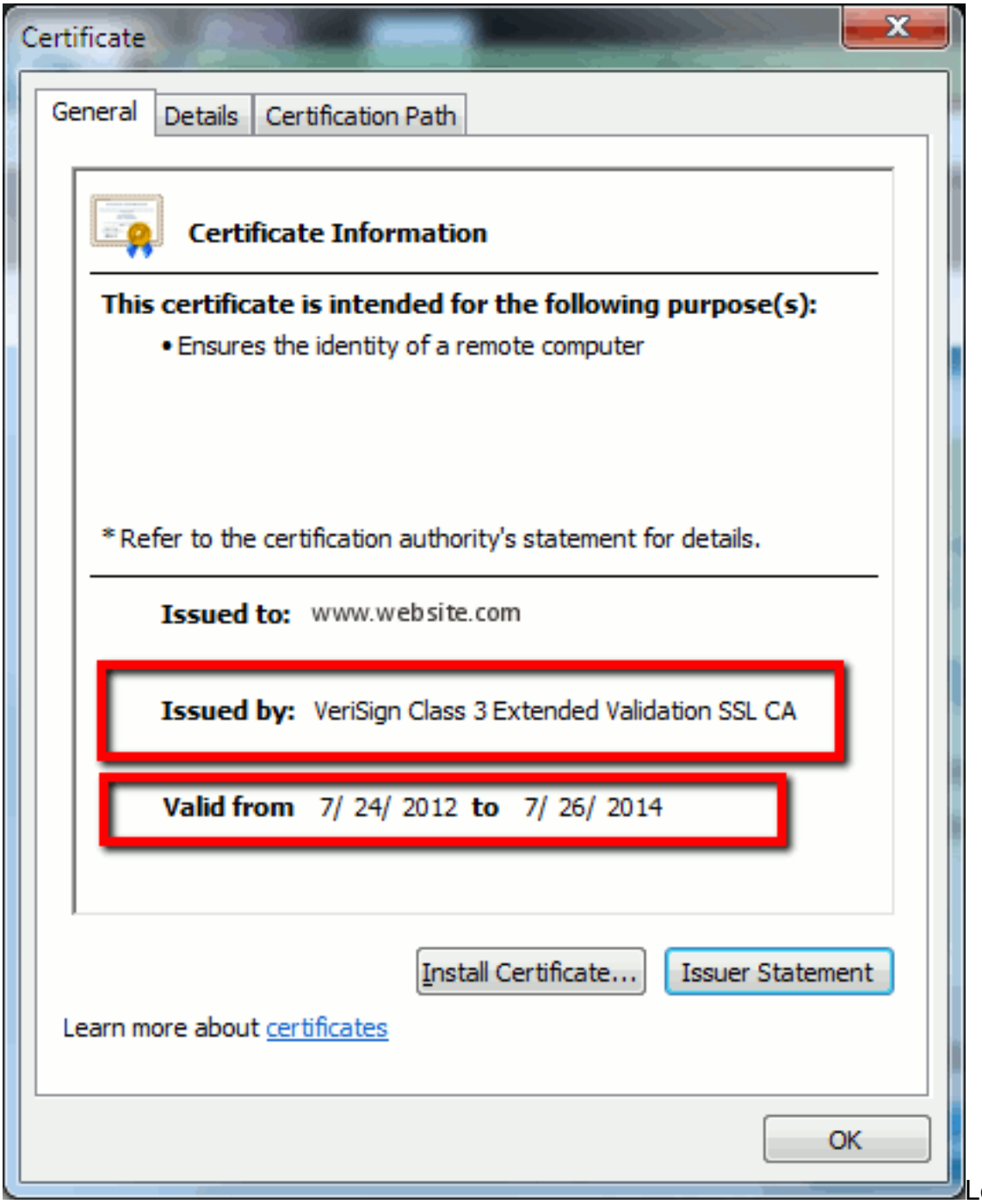
Senza certificati è impossibile sapere se è stato utilizzato un server DNS non autorizzato o se è stato eseguito il routing a un altro server. I certificati garantiscono che l'utente venga indirizzato in modo corretto e sicuro al sito Web desiderato, ad esempio il sito Web della banca, in cui le informazioni personali o riservate immesse sono protette.

Tutti i browser dispongono di icone diverse, ma in genere nella barra degli indirizzi viene visualizzato un lucchetto simile al seguente: 

1. Fare clic sul lucchetto e viene visualizzata una finestra:**Figura 1: Identificazione sito Web**



2. Fare clic su **View Certificates** (Visualizza certificati) per visualizzare il certificato del sito come mostrato nell'esempio seguente:**Figura 2: Informazioni sul certificato, scheda Generale**



Le informazioni evidenziate sono importanti.**Emesso da** è la società o l'autorità di certificazione (CA) già considerata attendibile dal sistema.**Valido - Da/A** è l'intervallo di date in cui il certificato è utilizzabile. Talvolta è possibile che venga visualizzato un certificato in cui si è certi dell'attendibilità della CA, ma il certificato non è valido. Controllare sempre la data per sapere se è scaduta o meno.)**SUGGERIMENTO:** È consigliabile creare un promemoria nel calendario per rinnovare il certificato prima della scadenza. In questo modo si evitano problemi futuri.

Differenze tra i certificati PEM e i certificati DER

PEM è ASCII; DER è binario. Nella figura 3 è illustrato il formato del certificato PEM.

Figura 3: Esempio di certificato PEM

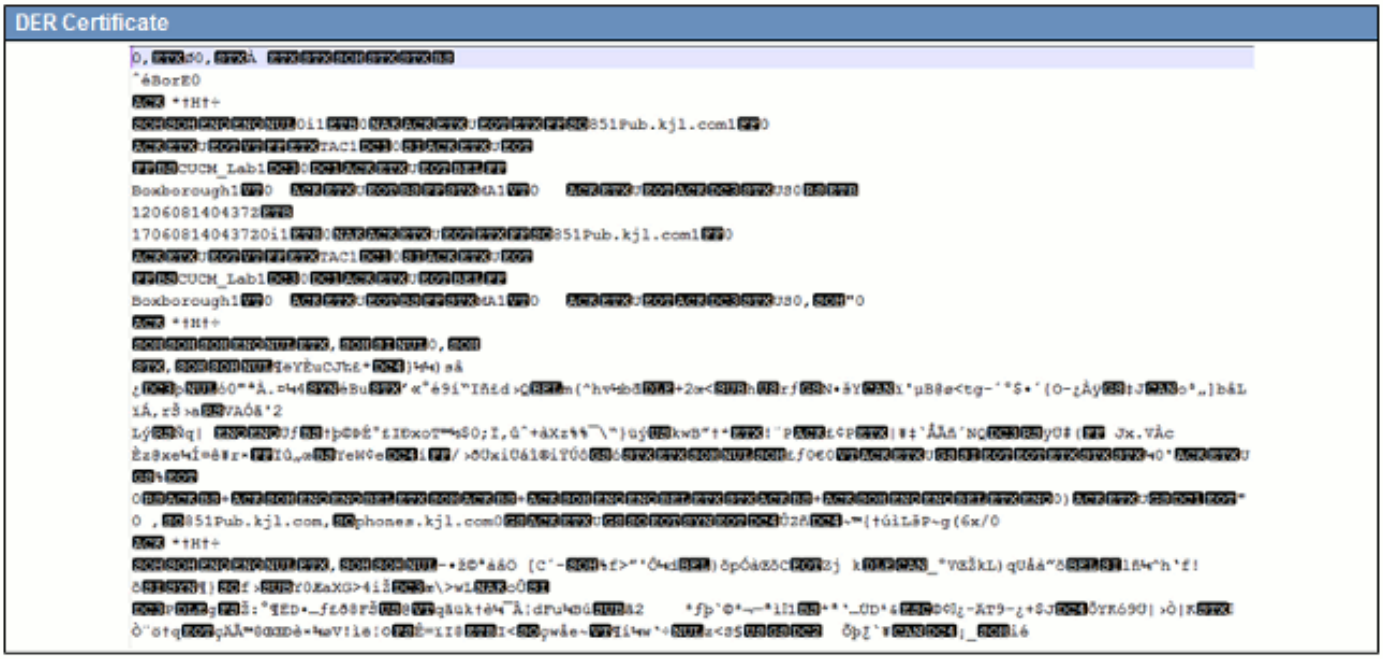
PEM Certificate

```
-----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 Figura 4 mostra il certificato DER.

Figura 4: Esempio di certificato DER

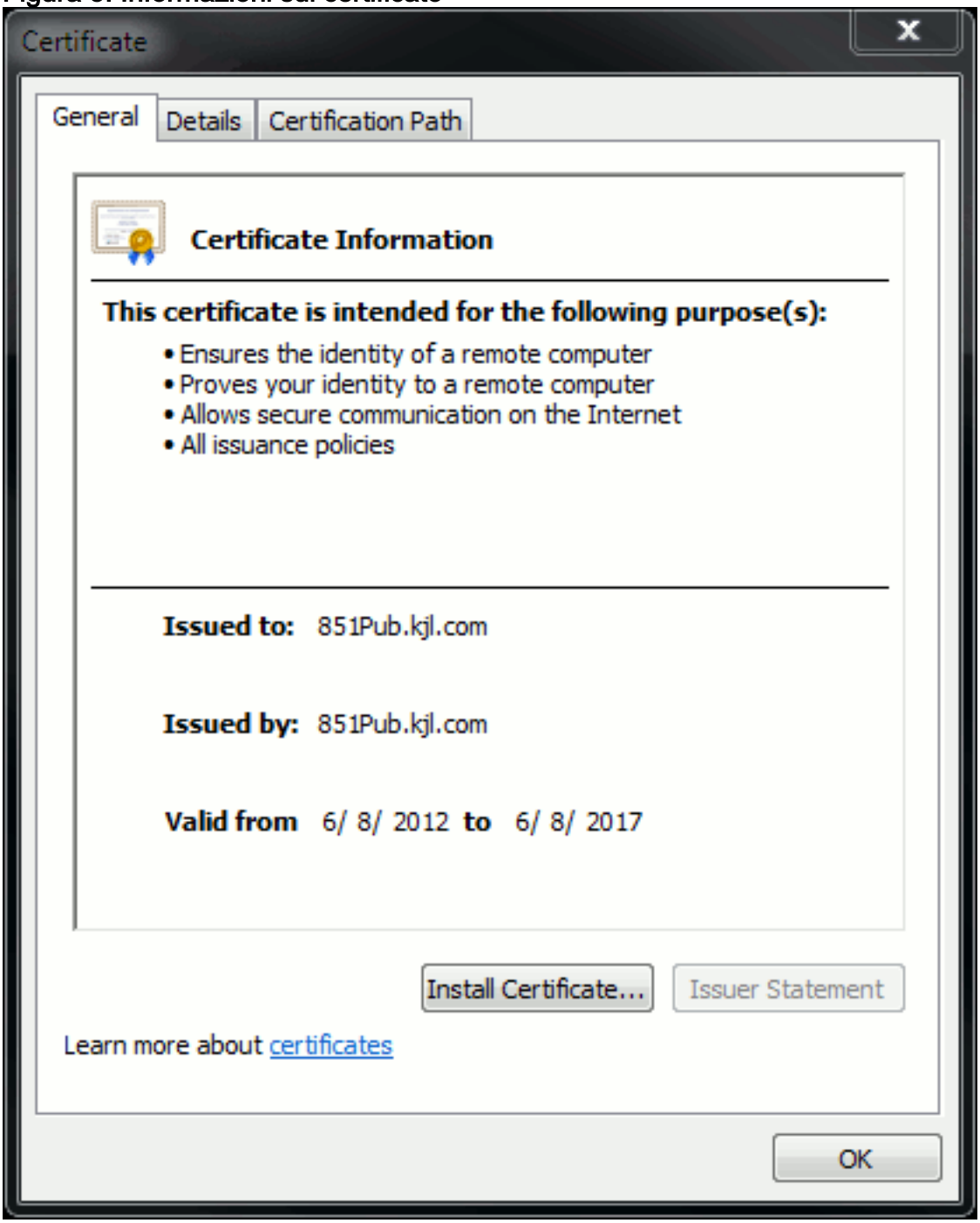
DER Certificate



La maggior parte delle società CA, ad esempio VeriSign o Thawt, utilizza il formato PEM per inviare i certificati ai clienti, in quanto è compatibile con la posta elettronica. Il cliente deve copiare l'intera stringa e includere **—BEGIN CERTIFICATE—** e **—END CERTIFICATE—**, incollarla in un file di testo e salvarla con l'estensione .PEM o .CER.

Windows è in grado di leggere i formati DER e CER con una propria applicazione di gestione dei certificati e visualizza il certificato come mostrato nella Figura 5.

Figura 5: Informazioni sul certificato

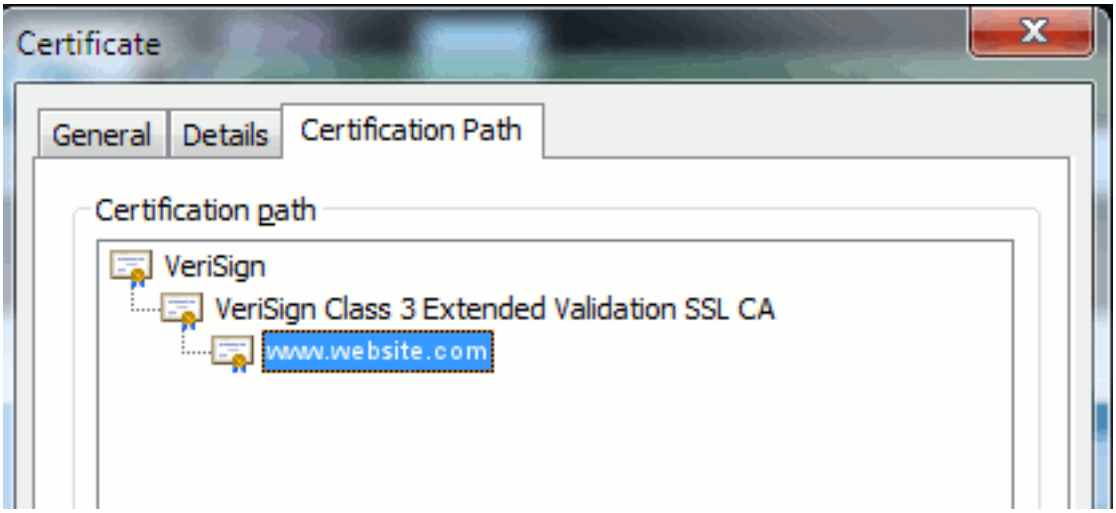


In alcuni casi, un dispositivo richiede un formato specifico (ASCII o binario). Per modificare questa impostazione, scaricare il certificato dalla CA nel formato richiesto o utilizzare uno strumento di conversione SSL, ad esempio https://www.sslshopper.com/ssl-converter.html.

Gerarchia certificati

Per considerare attendibile un certificato da un endpoint, è necessario che sia già stata stabilita una relazione di trust con un'autorità di certificazione di terze parti. Nella Figura 6, ad esempio, è illustrata la gerarchia di tre certificati.

Figura 6: Gerarchia certificati



- **Verisign** è una CA.
- **La CA SSL di convalida estesa di classe 3** è un certificato server intermedio o di firma (un server autorizzato dalla CA a rilasciare certificati con il proprio nome).
- **www.website.com** è un certificato server o di servizio.

L'endpoint deve essere in grado di considerare attendibili sia la CA che i certificati intermedi prima di poter considerare attendibile il certificato del server presentato dall'handshake SSL (dettagli seguenti). Per ulteriori informazioni sul funzionamento del trust, fare riferimento alla sezione seguente del documento: **Definire "Attendibilità" dal punto di vista di un certificato**.

Certificati autofirmati e certificati di terze parti

Le differenze principali tra i certificati autofirmati e i certificati di terze parti sono rappresentate dalla firma del certificato, indipendentemente dall'attendibilità.

Un certificato autofirmato è un certificato firmato dal server che lo presenta. pertanto, il certificato server/servizio e il certificato CA coincidono.

Un'autorità di certificazione di terze parti è un servizio fornito da un'autorità di certificazione pubblica (come Verisign, Entrust, Digicert) o da un server (come Windows 2003, Linux, Unix, IOS) che controlla la validità del certificato server/servizio.

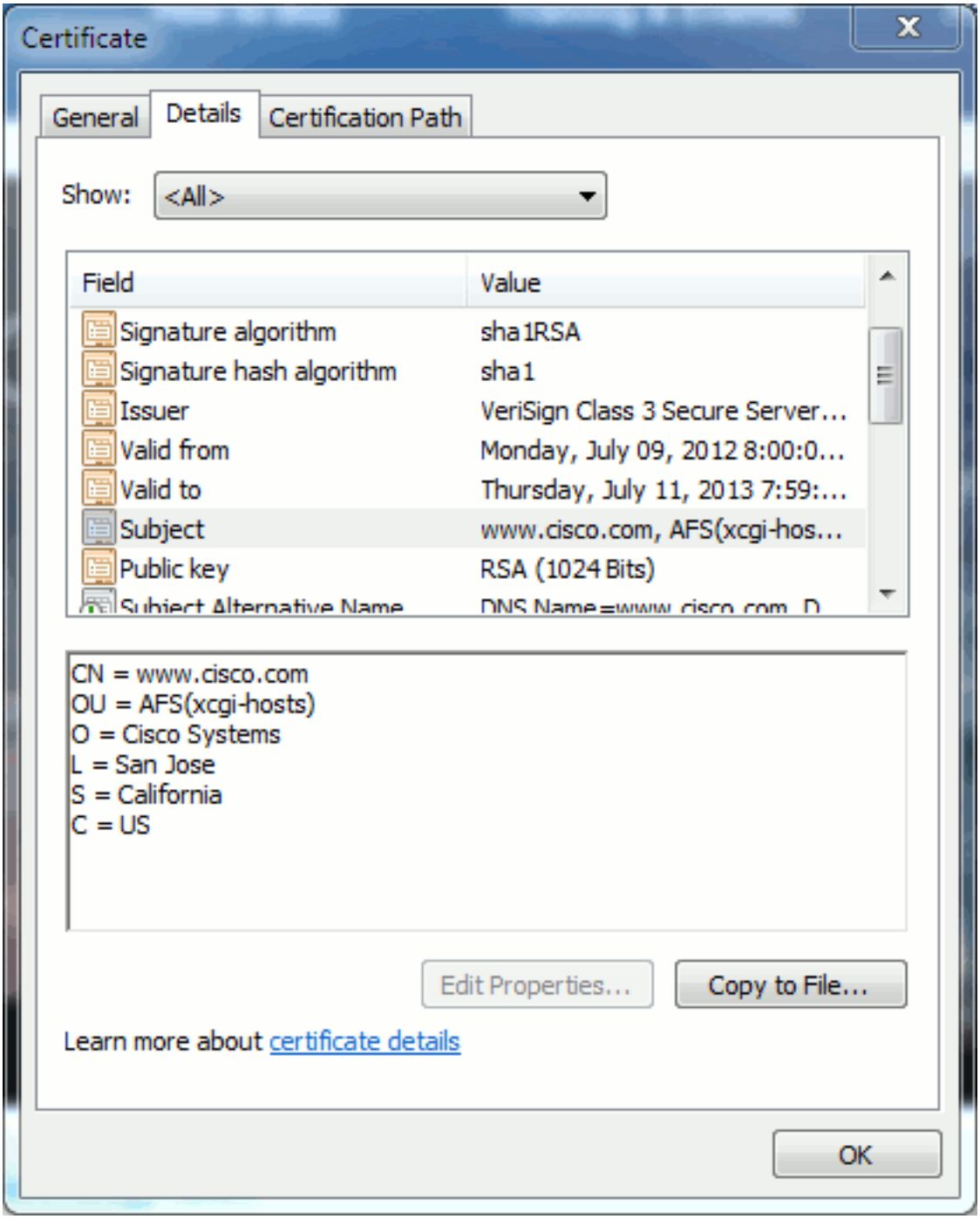
Ognuna può essere una CA. Ciò che conta di più è se il sistema considera attendibile o meno tale CA.

Nomi comuni e nomi alternativi soggetto

I nomi comuni (CN) e i nomi alternativi soggetto (SAN) sono riferimenti all'indirizzo IP o al nome di dominio completo (FQDN) dell'indirizzo richiesto. Ad esempio, se si immette https://www.cisco.com, la CN o SAN deve avere www.cisco.com nell'intestazione.

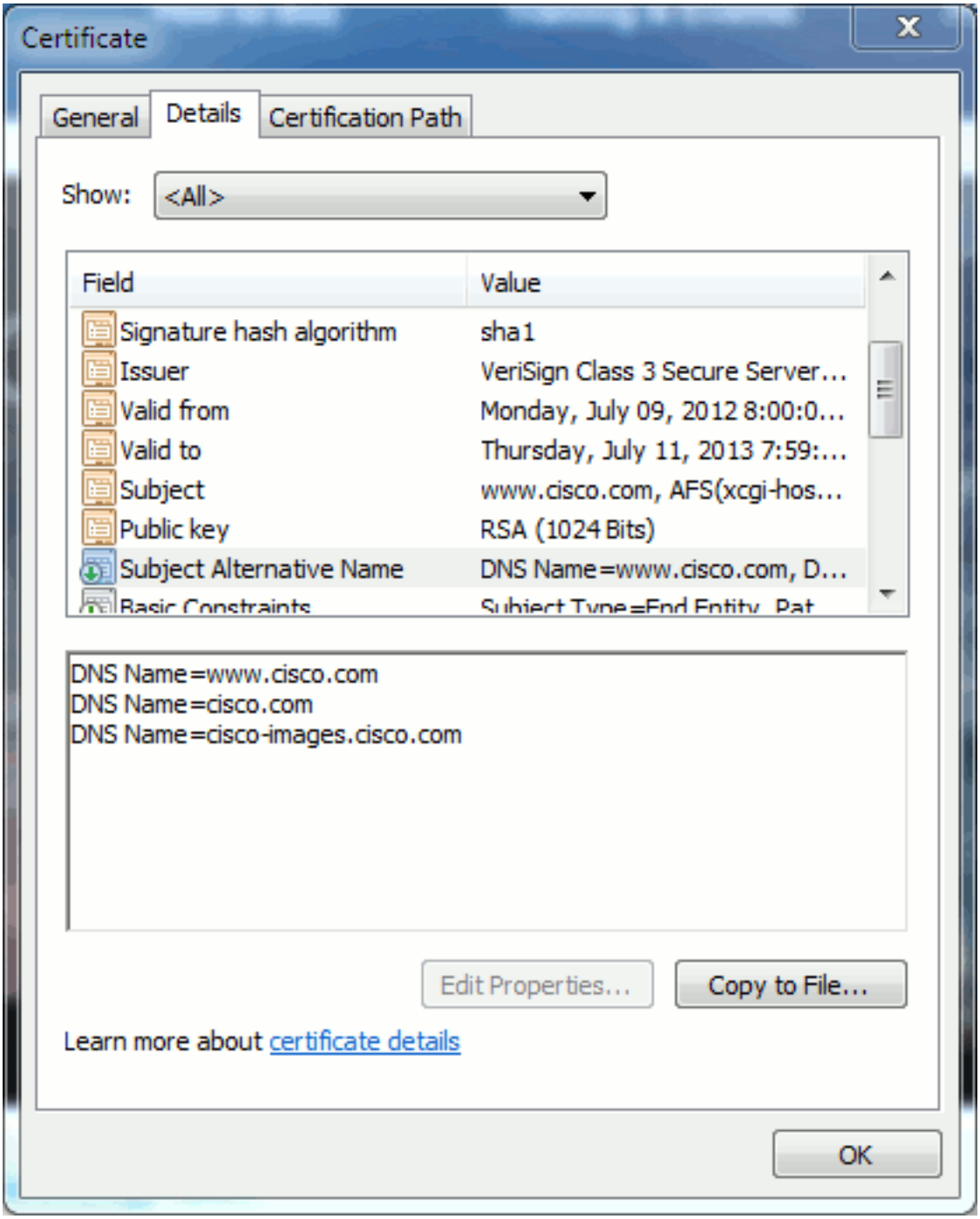
Nell'esempio riportato nella Figura 7, la CN del certificato è www.cisco.com. L'URL richiesto per www.cisco.com dal browser controlla l'FQDN dell'URL in base alle informazioni presentate dal certificato. In questo caso, corrispondono e viene indicato che l'handshake SSL ha esito positivo. Questo sito Web è stato verificato come corretto e le comunicazioni sono ora crittografate tra il desktop e il sito Web.

Figura 7: Verifica sito Web



Nello stesso certificato è presente un'intestazione SAN per tre indirizzi FQDN/DNS:

Figura 8: Intestazione SAN



Questo certificato può autenticare/verificare www.cisco.com (definito anche nel CN), cisco.com e cisco-images.cisco.com. È quindi possibile digitare anche cisco.com e lo stesso certificato può essere utilizzato per autenticare e crittografare il sito Web.

CUCM consente di creare intestazioni SAN. Per ulteriori informazioni sulle intestazioni SAN, fare riferimento al documento di Jason Burn, CUCM Uploading CCMAdmin Web GUI Certificates sulla Support Community.

Certificati jolly

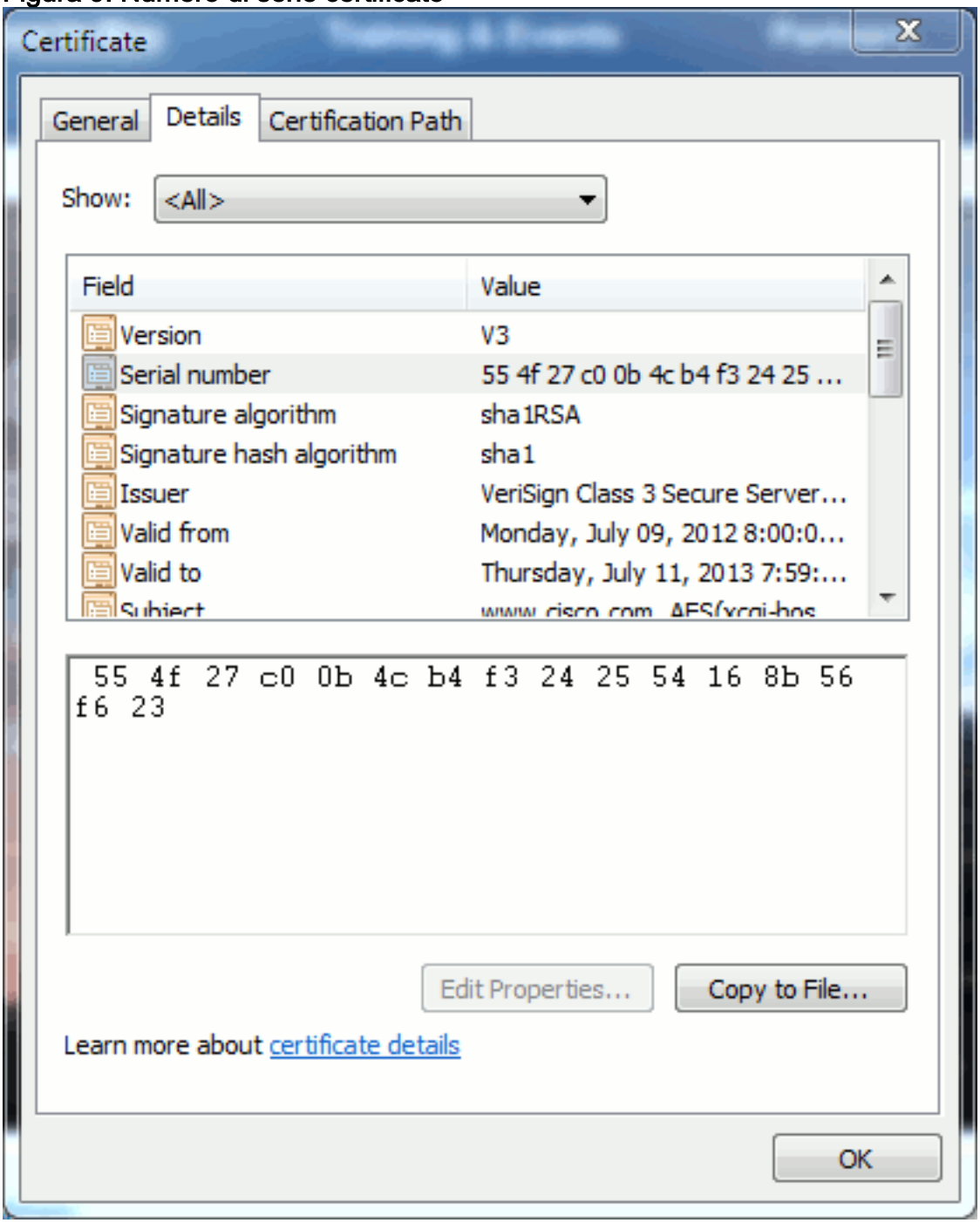
I certificati con caratteri jolly sono certificati che utilizzano un asterisco (*) per rappresentare qualsiasi stringa in una sezione di un URL. Ad esempio, per avere un certificato per www.cisco.com, ftp.cisco.com, ssh.cisco.com e così via, un amministratore deve solo creare un certificato per *.cisco.com. Per risparmiare, l'amministratore deve acquistare un solo certificato e non deve acquistare più certificati.

Questa funzionalità non è attualmente supportata da Cisco Unified Communications Manager (CUCM). È tuttavia possibile tenere traccia di questo miglioramento: CSCta14114: Richiesta di supporto per il certificato con caratteri jolly in CUCM e l'importazione della chiave privata.

Identificare i certificati

Quando i certificati contengono le stesse informazioni, è possibile verificare se si tratta dello stesso certificato. Tutti i certificati hanno un numero di serie univoco. È possibile utilizzare questa opzione per confrontare se i certificati sono gli stessi certificati, sono stati rigenerati o sono contraffatti. La Figura 9 fornisce un esempio:

Figura 9: Numero di serie certificato



RSI e loro finalità

CSR è l'acronimo di Certificate Signing Request. Se si desidera creare un certificato di terze parti

per un server CUCM, è necessario un CSR da presentare alla CA. Questo CSR ha l'aspetto di un certificato PEM (ASCII).

Nota: non si tratta di un certificato e non può essere utilizzato come tale.

CUCM crea automaticamente i CSR tramite GUI Web: **Cisco Unified Operating System Administration > Security > Certificate Management > Generate CSR >** scegliere il servizio per cui si desidera creare il certificato **>** quindi **Generate CSR**. Ogni volta che si utilizza questa opzione, vengono generati una nuova chiave privata e un nuovo CSR.

Nota: una chiave privata è un file univoco per questo server e servizio. Questo non dovrebbe mai essere dato a nessuno! Se si fornisce una chiave privata a un utente, la protezione fornita dal certificato verrà compromessa. Inoltre, non rigenerare un nuovo CSR per lo stesso servizio se si utilizza il CSR precedente per creare un certificato. Il comando CUCM elimina la vecchia CSR e la chiave privata e li sostituisce entrambi, rendendo la vecchia CSR inutile.

Per ulteriori informazioni, fare riferimento alla documentazione di Jason Burn sulla Support Community: Caricamento dei certificati CUCMdmin Web GUI per informazioni su come creare i CSR.

Utilizzo dei certificati tra endpoint e processo di handshake SSL/TLS

Il protocollo handshake è una serie di messaggi in sequenza che negoziano i parametri di sicurezza di una sessione di trasferimento dati. Fare riferimento a SSL/TLS in Detail , che documenta la sequenza di messaggi nel protocollo di handshake. Queste funzioni possono essere rilevate in una funzione di acquisizione dei pacchetti (PCAP). I dettagli includono i messaggi iniziali, successivi e finali inviati e ricevuti tra il client e il server.

Utilizzo dei certificati in CUCM

La differenza tra tomcat e tomcat-trust

Quando i certificati vengono caricati in CUCM, sono disponibili due opzioni per ogni servizio tramite **Cisco Unified Operating System Administration > Security > Certificate Management > Find**.

I cinque servizi che consentono di **gestire** i certificati in CUCM sono:

- gatto
- ipsec
- callmanager
- capf
- televisori (in CUCM release 8.0 e successive)

Di seguito sono elencati i servizi che consentono di **caricare** certificati in CUCM:

- gatto
- tomcat-trust
- ipsec

- ipsec-trust
- callmanager
- callmanager-trust
- capf
- capf-trust

Questi sono i servizi disponibili in CUCM release 8.0 e successive:

- televisori
- tvs-trust
- trust telefonico
- phone-vpn-trust
- phone-sast-trust
- phone-ctl-trust

Per ulteriori informazioni su questi tipi di certificati, consultare le guide alla sicurezza di CUCM per versione. In questa sezione viene illustrata solo la differenza tra un certificato di servizio e un certificato di attendibilità.

Ad esempio, con **tomcat**, **tomcat-trusts** carica la CA e i certificati intermedi in modo che il nodo CUCM sia consapevole di poter considerare attendibili tutti i certificati firmati dalla CA e dal server intermedio. Il certificato tomcat è il certificato presentato dal servizio tomcat su questo server, se un endpoint effettua una richiesta HTTP a questo server. Per consentire la presentazione di certificati di terze parti da parte di tomcat, il nodo CUCM deve sapere che può considerare attendibili la CA e il server intermedio. È pertanto necessario caricare i certificati CA e intermedi prima di caricare il certificato tomcat (servizio).

Fare riferimento a Jason Burn's CUCM Uploading CCMAdmin Web GUI Certificates on the Support Community per informazioni su come caricare i certificati in CUCM.

Ogni servizio dispone di certificati di servizio e certificati di attendibilità specifici. Non si interagiscono. In altre parole, una CA e un certificato intermedio caricati come servizio tomcat-trust non possono essere utilizzati dal servizio callmanager.

Nota: i certificati CUCM sono una base per nodo. Pertanto, se è necessario caricare i certificati nel server di pubblicazione e i sottoscrittori devono disporre degli stessi certificati, è necessario caricarli in ogni singolo server e nodo prima di CUCM Release 8.5. In CUCM Release 8.5 e versioni successive è disponibile un servizio che replica i certificati caricati negli altri nodi del cluster.

Nota: ogni nodo ha un CN diverso. Per consentire al servizio di presentare i propri certificati, è pertanto necessario creare un CSR da ogni nodo.

Per ulteriori domande specifiche sulle funzioni di sicurezza di CUCM, consultare la documentazione relativa alla sicurezza.

Conclusioni

Questo documento supporta e rafforza un livello elevato di conoscenza dei certificati. L'argomento può diventare più approfondito, ma in questo documento viene acquisita sufficiente familiarità per l'utilizzo dei certificati. In caso di domande sulle funzioni di sicurezza di CUCM, consultare le Guide alla sicurezza di CUCM per versione per ulteriori informazioni.

Informazioni correlate

- Guide alla manutenzione e alla sicurezza di Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- Cisco Support Community: Caricamento CUCM in corso CMAdmin Web GUI Certificates
- Bug CSCta14114: Richiesta di supporto per il certificato con caratteri jolly in CUCM e l'importazione della chiave privata
- Spiegazione di Cisco Emergency Responder (CER)
- Documentazione e supporto tecnico – Cisco Systems