

Vista ad alto livello di Certificati e Autorità in CUCM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Scopo dei certificati](#)

[Definire l'attendibilità dal punto di vista di un certificato](#)

[Utilizzo dei certificati da parte dei browser](#)

[Differenze tra i certificati PEM e i certificati DER](#)

[Gerarchia certificati](#)

[Certificati autofirmati e certificati di terze parti](#)

[Nomi comuni e nomi alternativi soggetto](#)

[Certificati jolly](#)

[Identificare i certificati](#)

[RSI e loro finalità](#)

[Utilizzo dei certificati tra endpoint e processo di handshake SSL/TLS](#)

[Utilizzo dei certificati in CUCM](#)

[La differenza tra tomcat e tomcat-trust](#)

[Conclusioni](#)

[Informazioni correlate](#)

Introduzione

In questo documento vengono descritte le nozioni di base relative ai certificati e alle autorità di certificazione. Integra altri documenti Cisco che fanno riferimento a qualsiasi funzionalità di crittografia o autenticazione di 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 attendibilità/autenticazione e crittografia dei dati. Ciò conferma che gli endpoint comunicano con il dispositivo desiderato e che è possibile crittografare i dati tra i due endpoint.

 Nota: per comprendere l'impatto di ogni certificato, fare riferimento [alla](#) sezione [Processo di rigenerazione dei certificati per l'impatto di Cisco Unified Communications Manager](#) dall'archivio certificati

Definire l'attendibilità dal punto di vista di un certificato

La parte più importante dei certificati è la definizione degli endpoint che possono essere considerati attendibili dall'endpoint. 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, termina la comunicazione tra questi endpoint.

Un esempio non tecnico è la patente di guida. Utilizzate questa licenza (certificato server/servizio) per dimostrare che siete quello che siete; avete ottenuto la licenza dalla vostra filiale locale della Divisione dei Veicoli a Motore (certificato intermedio) che ha ricevuto l'autorizzazione dalla Divisione dei Veicoli a Motore (DMV) del vostro Stato (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.

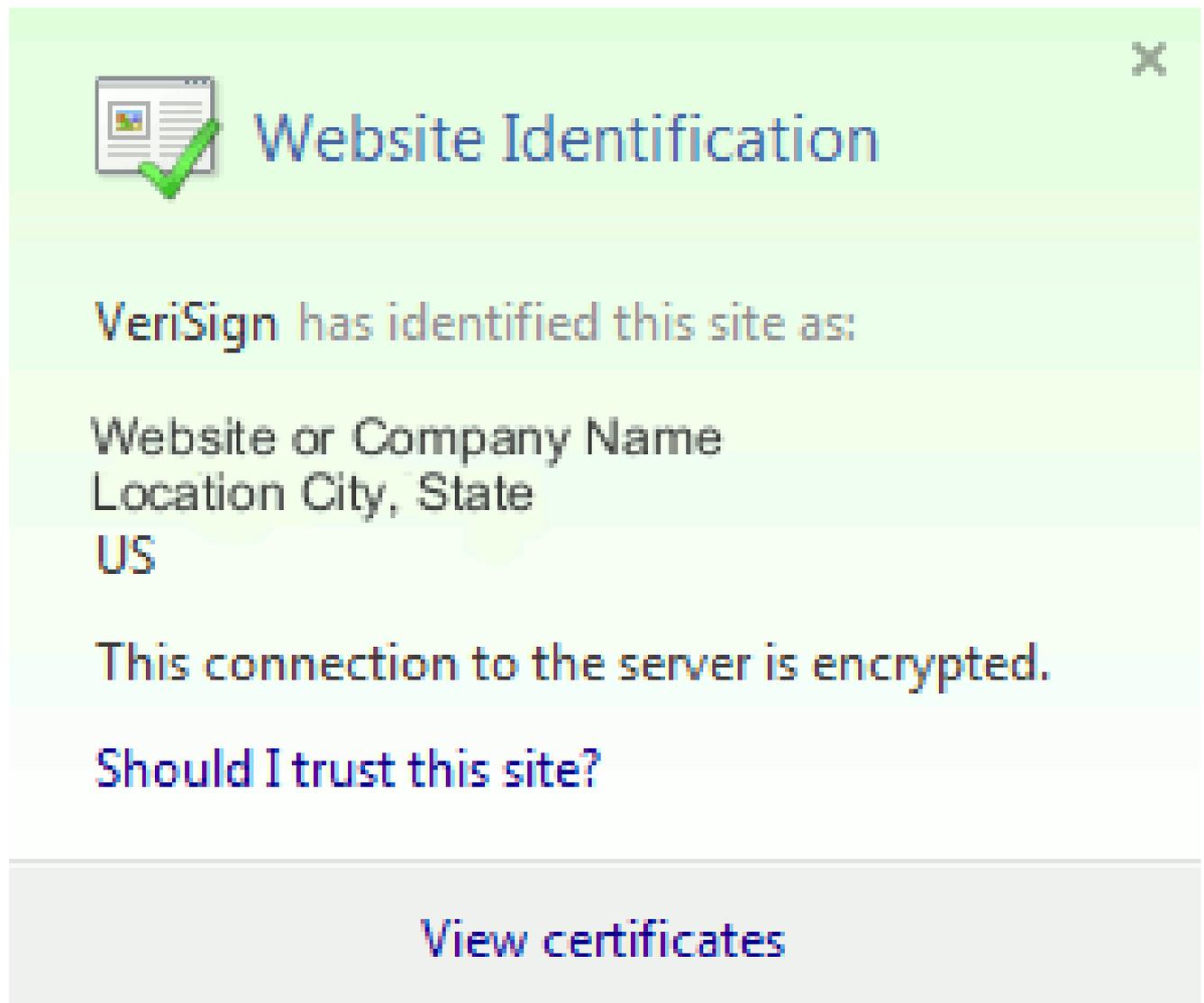
Senza certificati è impossibile sapere se è stato utilizzato un server DNS non autorizzato o se è stato eseguito il routing a un altro server. I certificati garantiscono che l'utente venga indirizzato in modo corretto e sicuro al sito Web desiderato, ad esempio il sito Web della banca, in cui le informazioni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

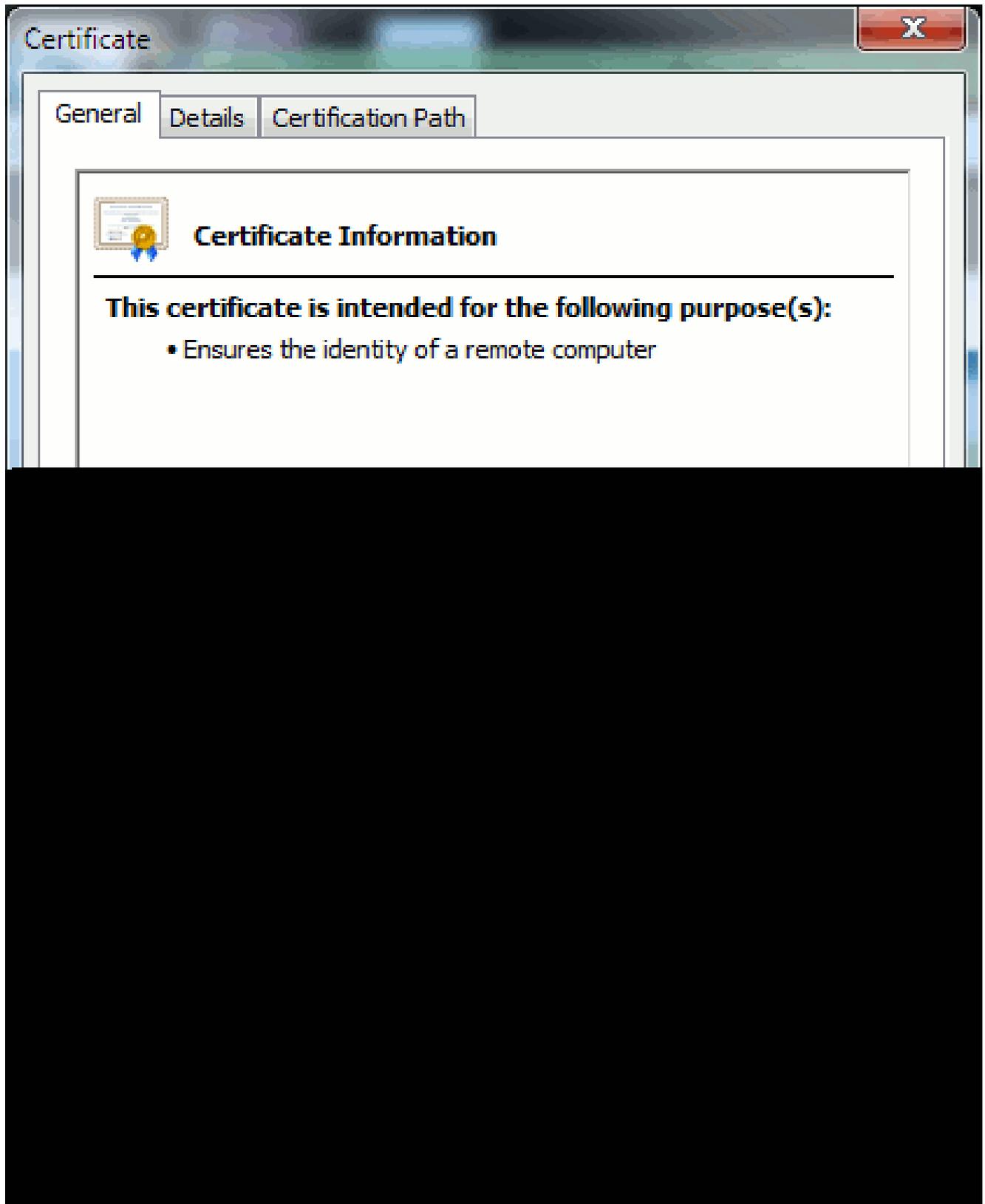
1. Fare clic sul lucchetto e viene visualizzata una finestra:

Figura 1: Identificazione del 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

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.

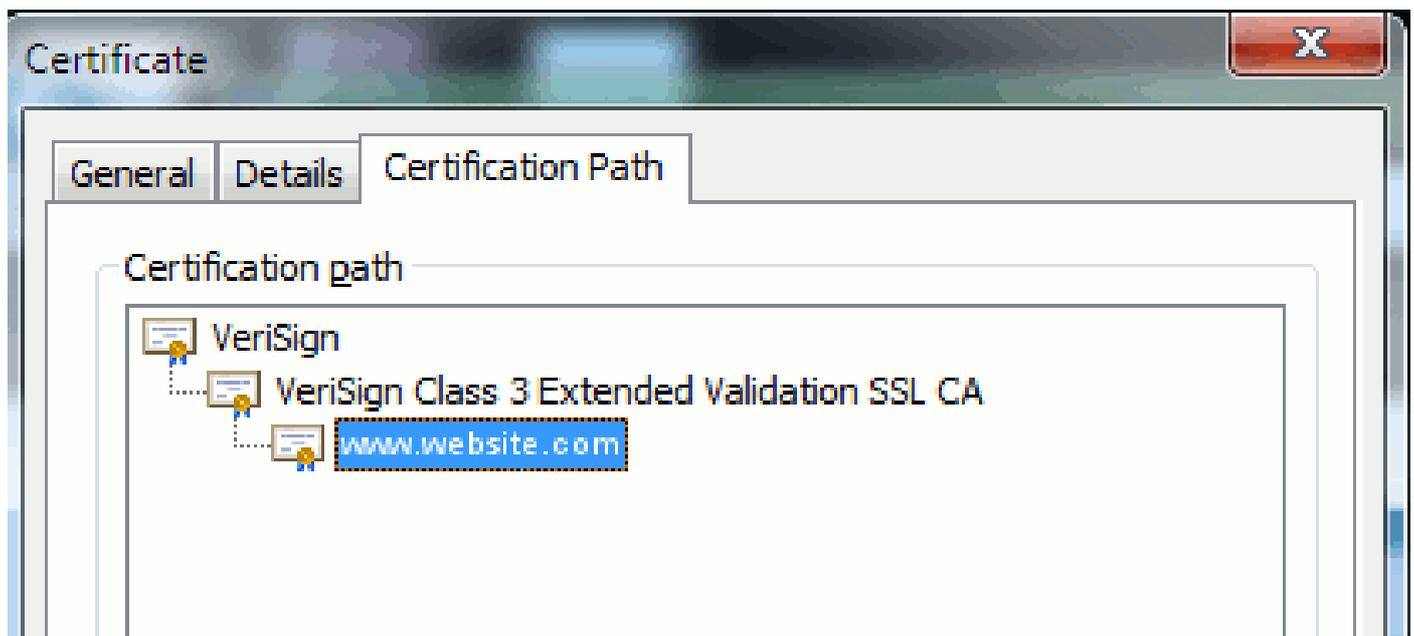
Figura 5: Informazioni sul certificato

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 di server o di servizio.

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

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.

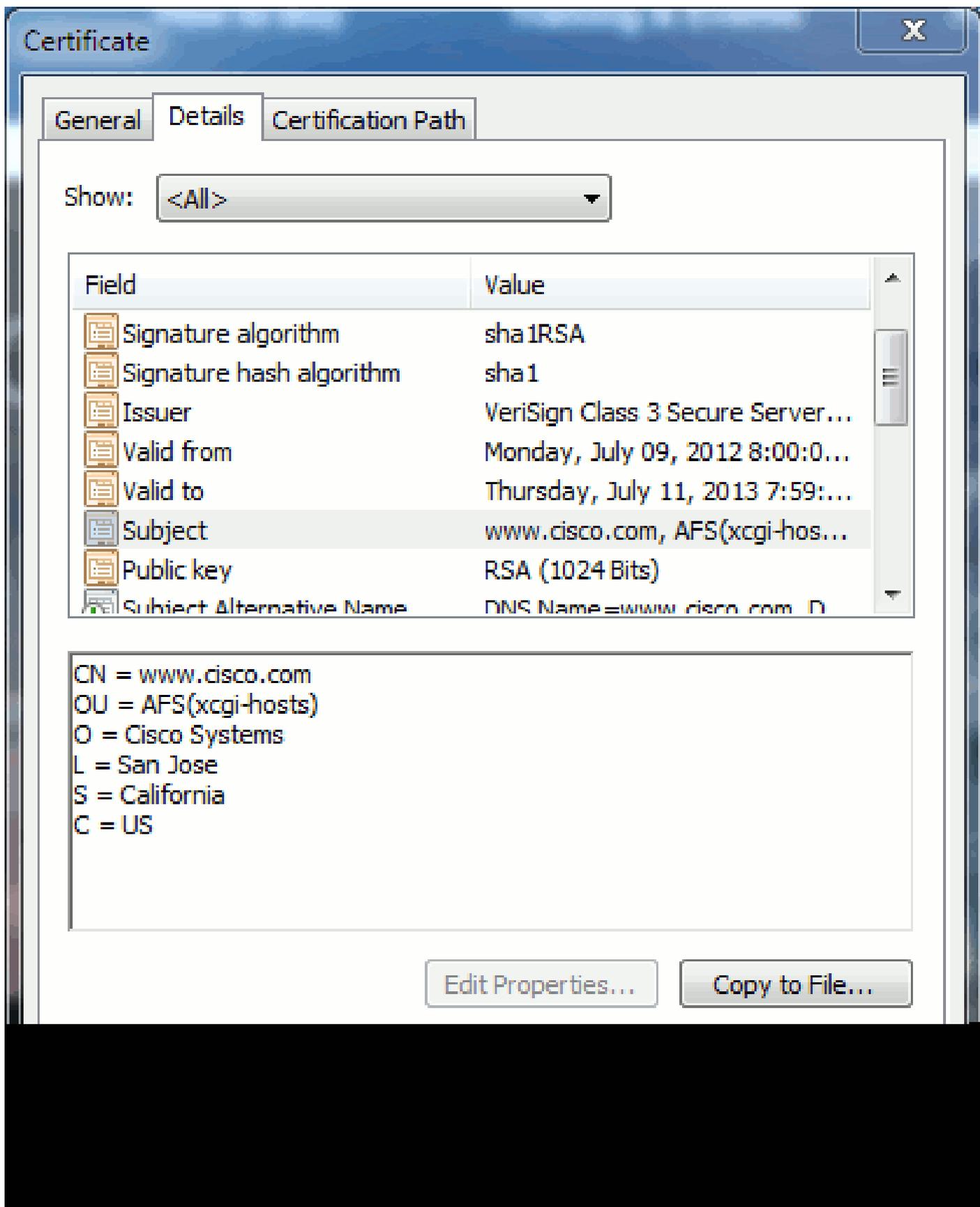
Ognuna può essere una CA. Ciò che conta di più è se il sistema considera attendibile o meno tale CA.

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.

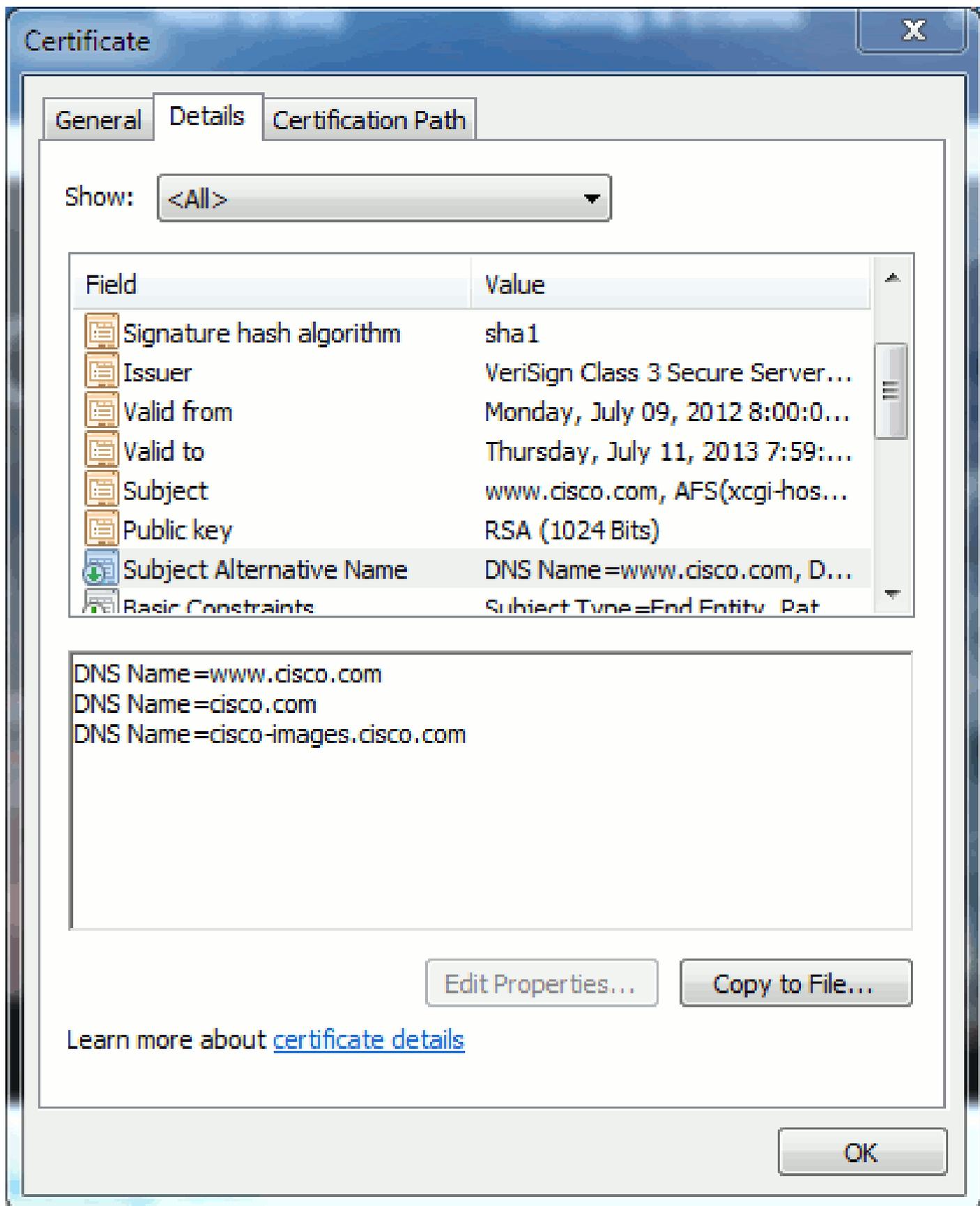
Nell'esempio mostrato nella Figura 7, la CN del certificato è www.cisco.com. L'URL richiesto per www.cisco.com dal browser controlla l'FQDN dell'URL in base alle informazioni presentate dal certificato. In questo caso, corrispondono e viene indicato che l'handshake SSL ha esito positivo. Questo sito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

Figura 7: verifica del 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 CCMAAdmin Web GUI Certificates](#) on the Support Community ([Caricamento di certificati CUCMadmin Web GUI](#) sulla community di supporto).

Certificati jolly

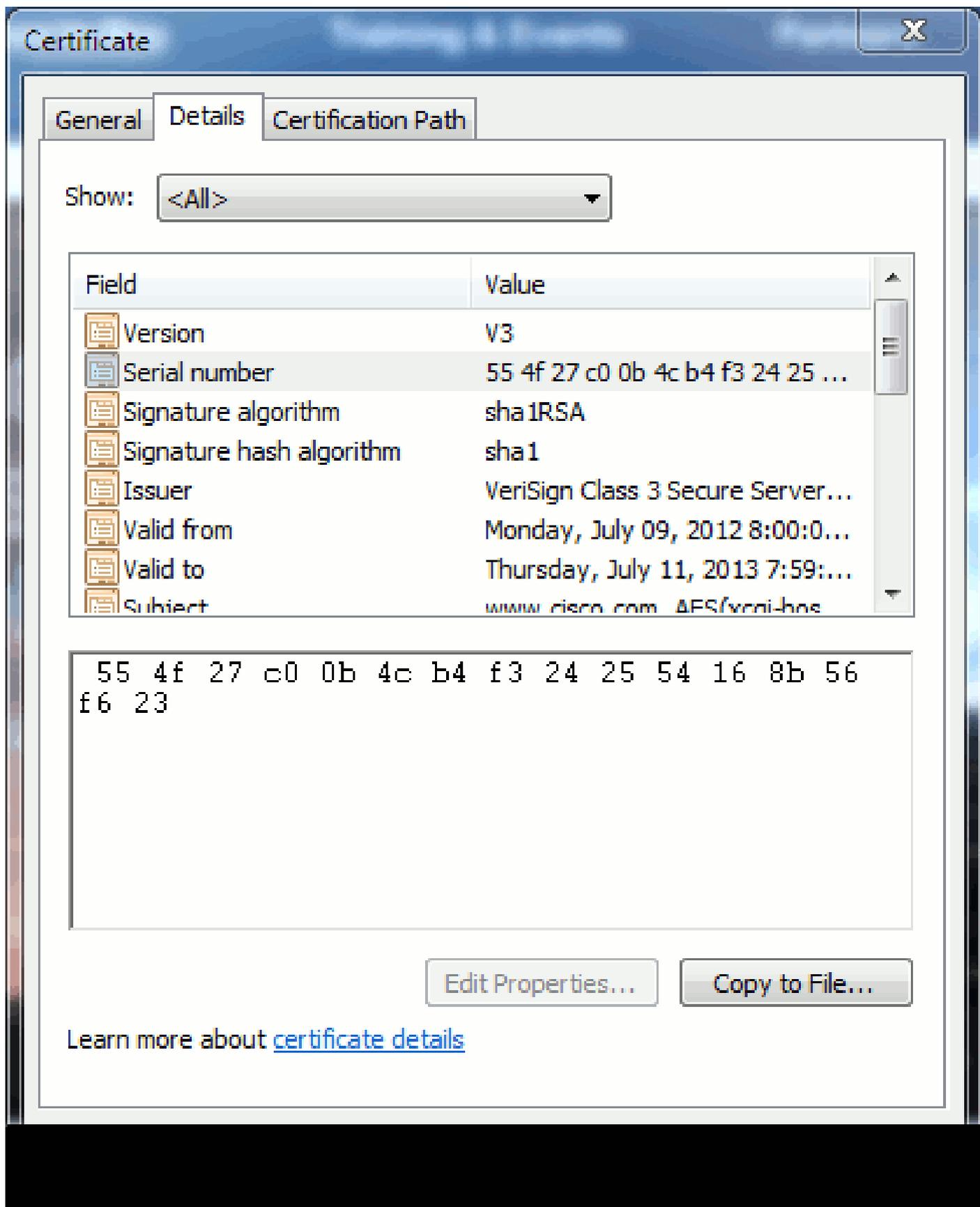
I certificati jolly sono certificati che utilizzano un asterisco (*) per rappresentare qualsiasi stringa in una sezione di un URL. Ad esempio, per ottenere un certificato per [www.cisco.com](#), ftp.cisco.com, ssh.cisco.com e così via, un amministratore deve solo creare un certificato per *.cisco.com. 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). Tuttavia, è possibile tenere traccia di questo miglioramento: [CSCta14114: Richiesta di supporto del certificato jolly in CUCM e 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, se sono stati rigenerati o se sono contraffatti. La Figura 9 fornisce un esempio:

Figura 9: numero di serie del certificato



RSI e loro finalità

CSR (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 che si desidera creare il snf del certificato, quindi Generate CSR. Ogni volta che si utilizza questa opzione, viene generata 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 altro 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 informazioni su come creare i CSR, consultare [la documentazione di Jason Burn sulla Support Community: CUCM Uploading CCMAdmin Web GUI Certificates](#).

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. Questi effetti possono essere rilevati in Packet Capture (PCAP). I dettagli includono i messaggi iniziali, successivi e finali inviati e ricevuti tra client e 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:

- tomcat
- ipsec

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

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

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

Di seguito sono elencati i servizi disponibili in CUCM release 8.0 e successive:

- tvs
- tvs-trust
- phone-trust
- 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, i tomcat-trusts caricano 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 lavorano l'uno con l'altro. In altre parole, una CA e un certificato intermedio caricati come servizio tomcat-trust non possono essere utilizzati dal servizio CallManager.

 Nota: i certificati in CUCM sono una base per nodo. Pertanto, se è necessario caricare i certificati nell'editore 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 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 dei certificati CMAAdmin Web GUI](#)
- [Bug CSCta14114: Richiesta di supporto del certificato con caratteri jolly in CUCM e nell'importazione della chiave privata](#)
- [Spiegazione di Cisco Emergency Responder \(CER\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).