Informazioni sui certificati per creare una catena per 9800 WLC

Sommario

Introduzione

Questo documento descrive come decodificare un certificato con strumenti online conosciuti e la loro interpretazione per creare una catena di certificati nel WLC 9800.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Cisco Catalyst 9800 Wireless LAN Controller (WLC)
- Certificato digitale, concetto di richiesta di firma del certificato (CSR).
- Software OpenSSL.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software OpenSSL nella versione 1.1.1w
- computer Windows

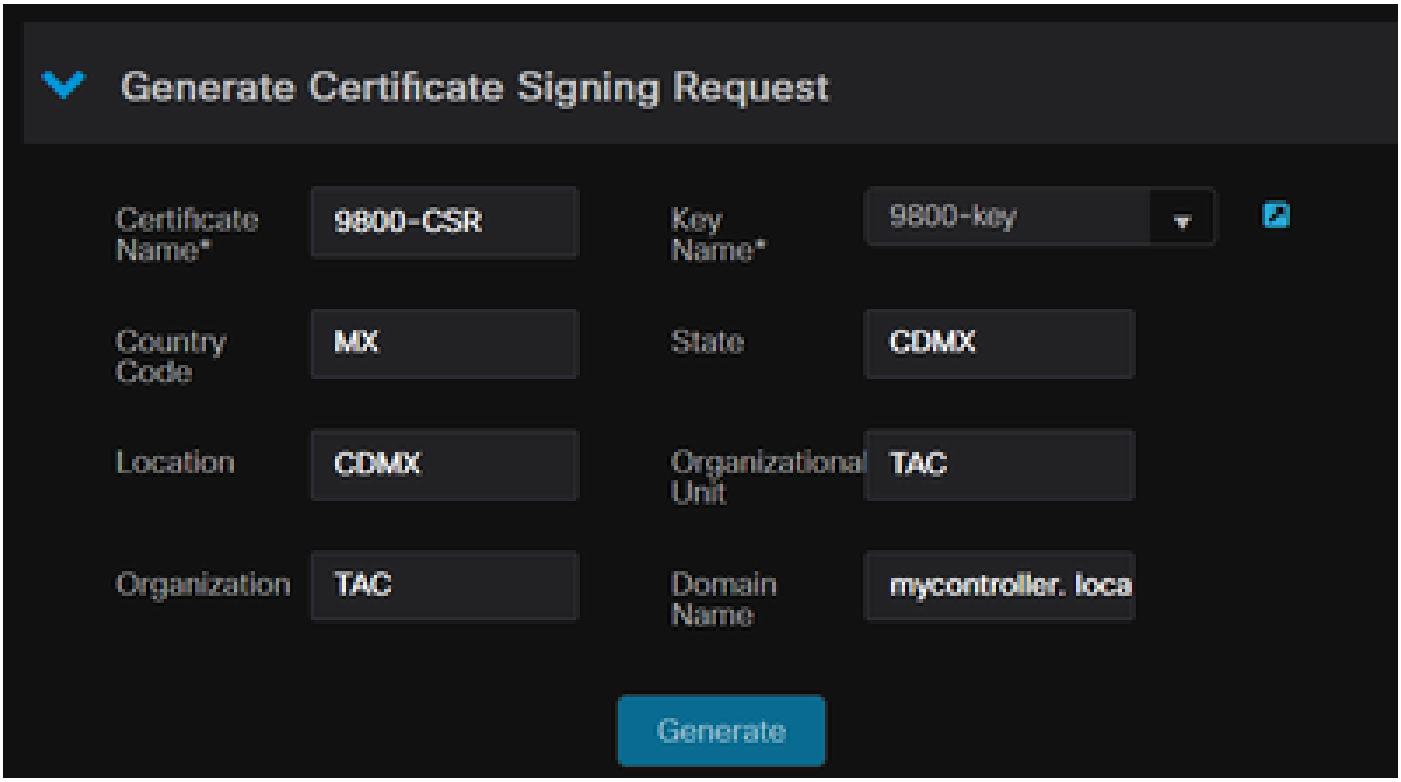
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Generazione CSR

Il CSR può essere generato nel controller o con OpenSSL.

Per generare un CSR nel WLC 9800, selezionare Configurazione > Sicurezza > Gestione PKI > Aggiungi certificato > Genera richiesta di firma certificato.

Quando viene generata una richiesta di firma del certificato, sono necessarie informazioni quali una chiave privata, un nome comune (CN), un codice di paese, uno stato, un'ubicazione, un'organizzazione e un'unità organizzativa.

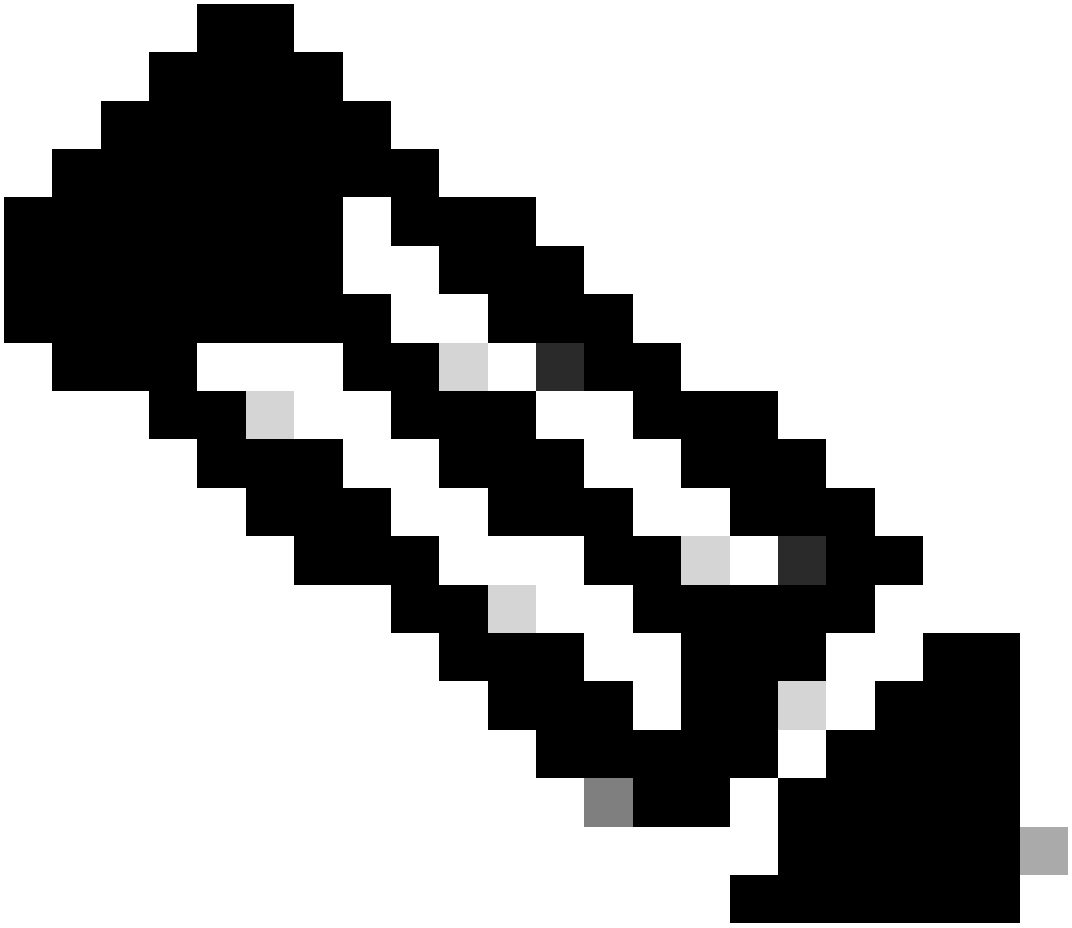


Generazione di CSR in WLC

Tutte le informazioni CSR inserite nella richiesta vengono visualizzate nella decodifica.

Il software OpenSSL è l'unica fonte di verità quando un certificato viene decodificato. Mostra tutte le informazioni a riguardo.

Per decodificare un certificato in un computer Windows o MacBook in cui è installato OpenSSL, aprire il prompt dei comandi come amministratore ed eseguire il comando openssl x509 -in <certificate.crt> -text -noout. L'output viene visualizzato come informazioni della console.



Nota: non tutte le versioni openSSL sono supportate in 9800 WLC. Le versioni suggerite sono 0.9.8 e 1.1.1w

Esistono altri strumenti in linea per decodificare i certificati che mostrano l'output in modo più semplice, ad esempio CertLogik e SSL Shopper, che non sono presentati in questo documento.

Tenere presente che utilizzano lo stesso comando OpenSSL già indicato per decodificare i certificati.

Certificato di terze parti

Il CSR viene inviato all'Autorità di certificazione (CA) per la firma e la restituzione. Scarica tutta la catena di certificati in modo da poterla caricare sul WLC.

Per comprendere la catena di un certificato, è possibile decodificare tutti i file ricevuti dalla CA. Assicurarsi che siano in formato Base64.

È possibile ricevere più file dalla CA. Dipende dal numero di file CA intermedi.

Per identificare ogni file, è necessario decodificarlo.

Quando un certificato firmato viene decodificato, viene aggiunta la sezione Issuer. Si riferisce alla CA che ha firmato il certificato.

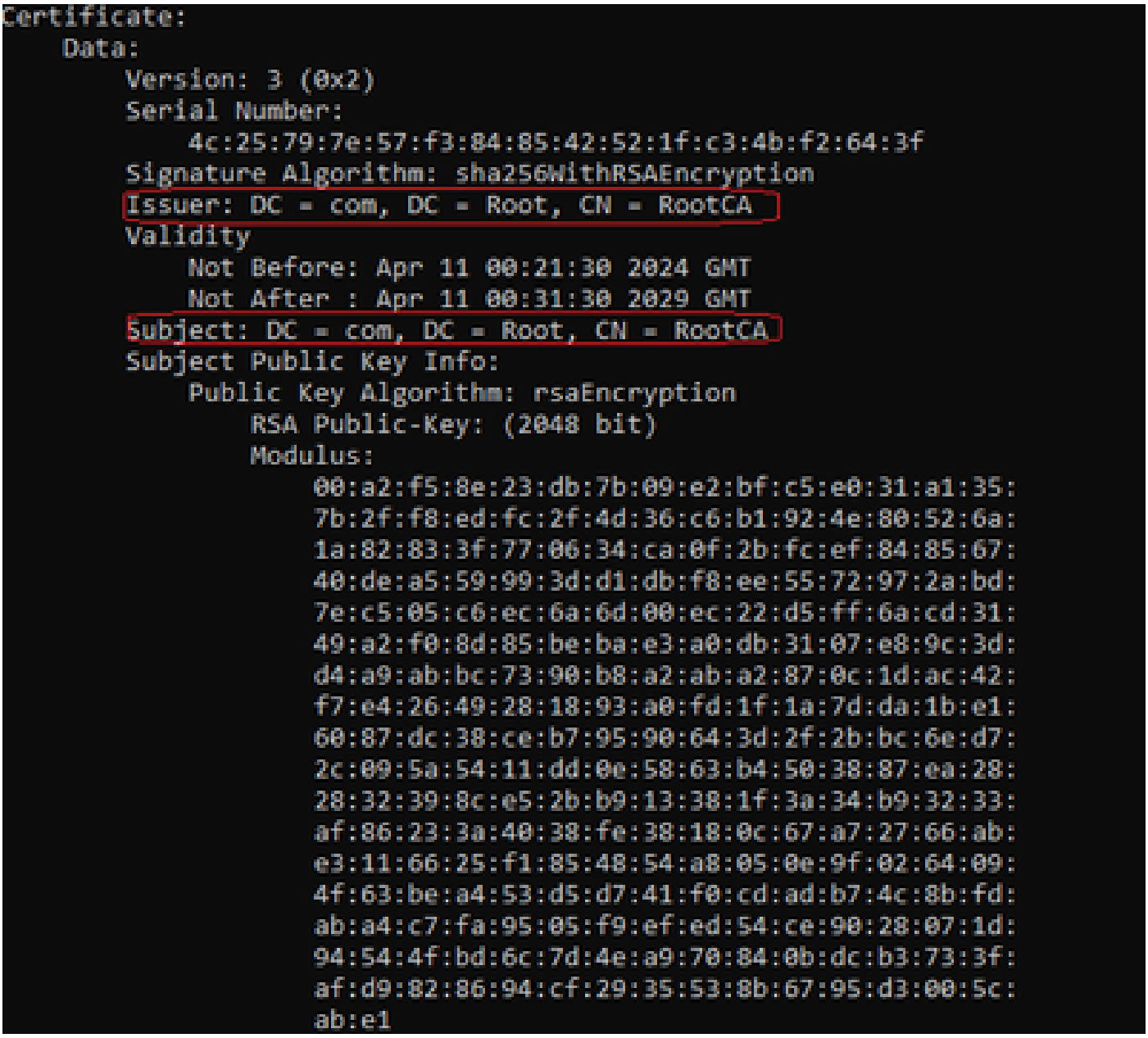
Se si decodifica un file CSR non firmato, la sezione Issuer non esiste perché non è ancora stato firmato.

Questo è un esempio di un'autorizzazione multilivello o di uno scenario con certificati concatenati:

- CA radice
- Certificato CA intermedio
- Certificato dispositivo

CA radice decodificata

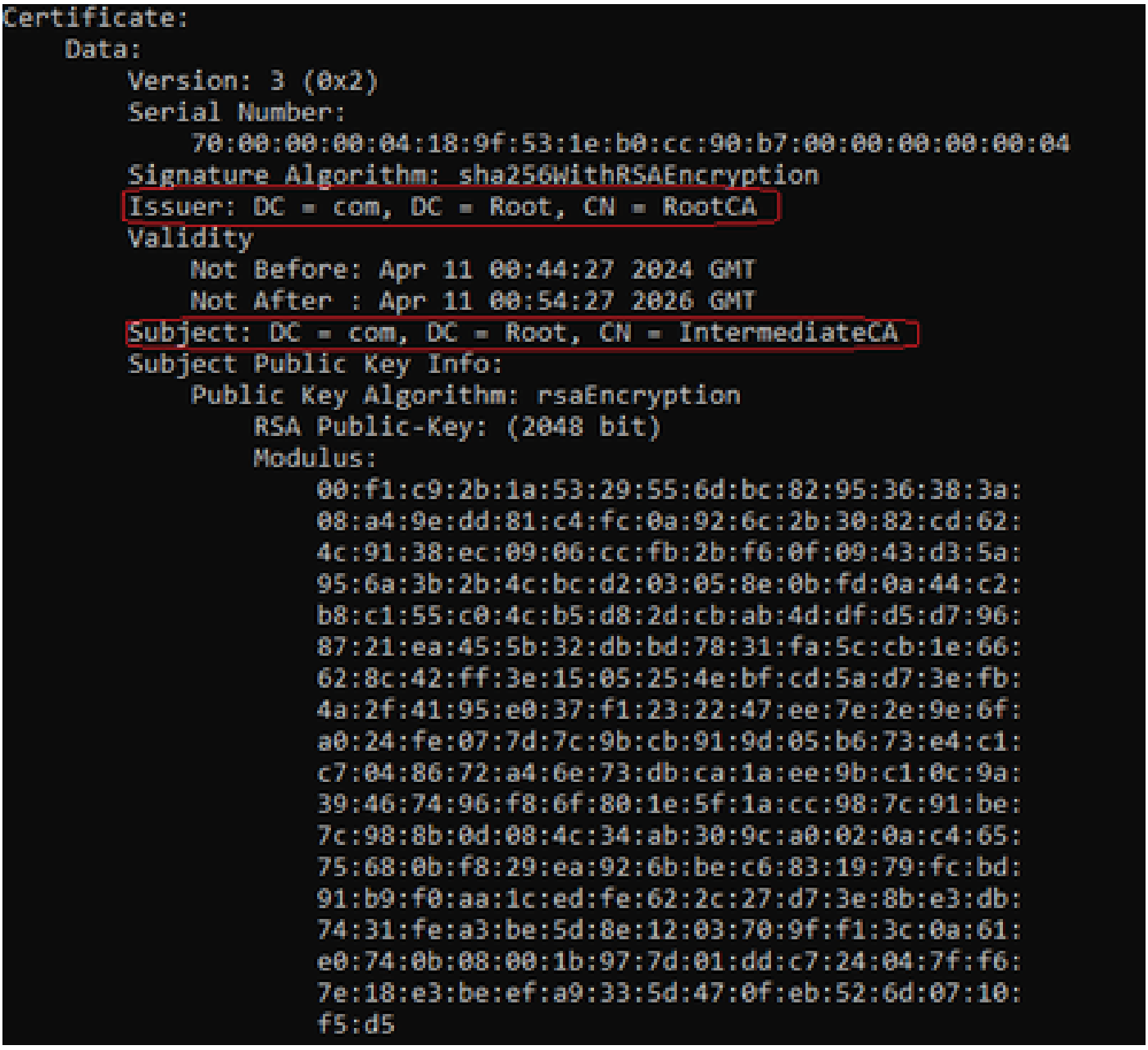
Per una CA radice, poiché è la massima autorità della catena, Issuer e Subject devono essere gli stessi.



CA radice decodificata

CA intermedia decodificata

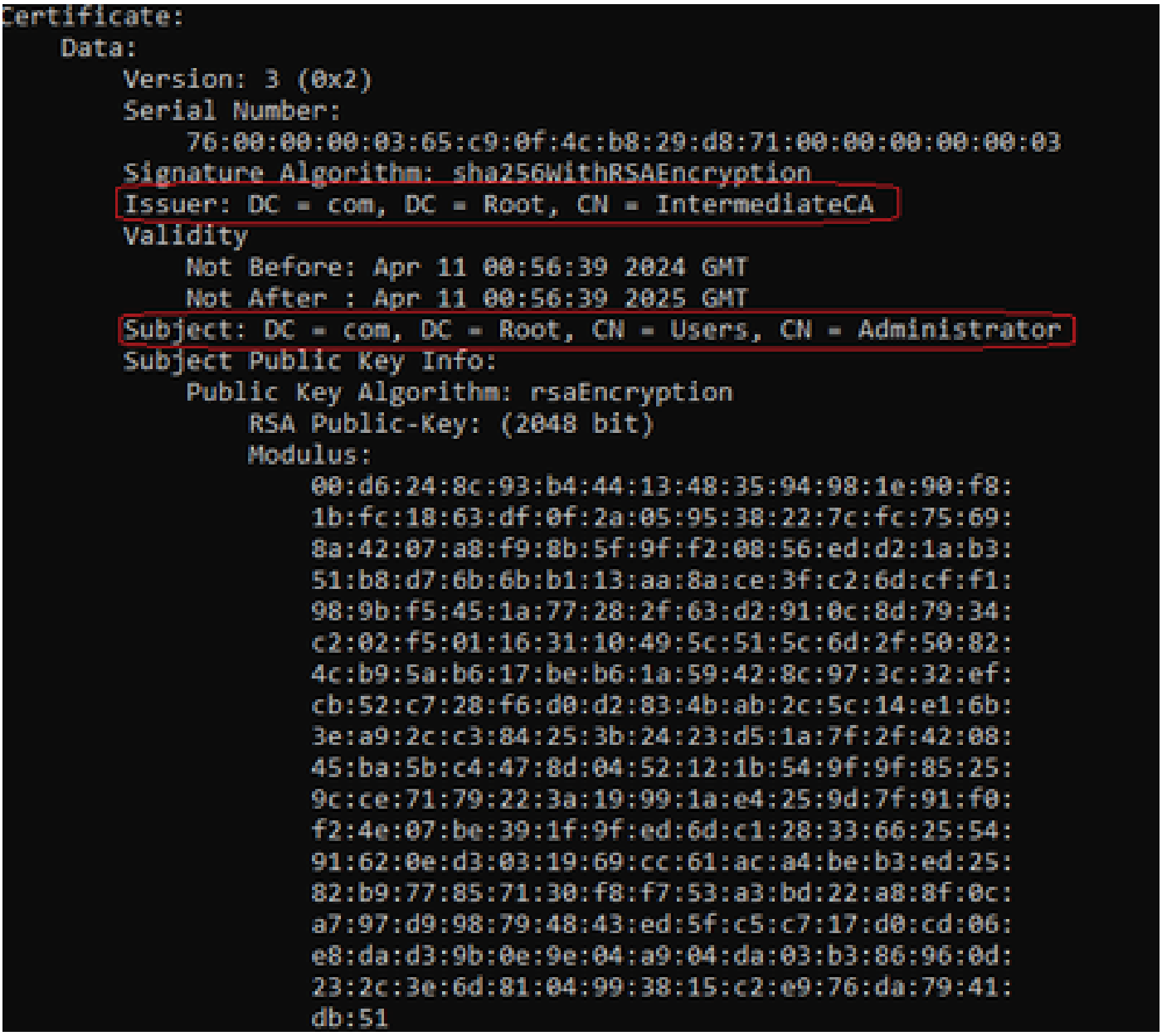
Per la CA intermedia, poiché è firmata dalla CA radice, l'autorità emittente deve corrispondere al CN della CA radice.



CA intermedia decodificata

Certificato dispositivo decodificato

Per il certificato del dispositivo, poiché è firmato dalla CA intermedia, l'autorità emittente deve corrispondere al CN della CA intermedia



Certificato dispositivo decodificato

In uno scenario in cui vengono utilizzate più CA intermedie, utilizzare lo stesso processo di decodifica.

Una volta identificato, l'ordine a catena può essere caricato sul controller.

Il WLC 9800 richiede l'intera catena nell'ordine corretto, in modo che il certificato possa funzionare correttamente.

Per i passaggi successivi per caricare un certificato sul controller, consultare il documento sulla generazione e il download dei certificati CSR sui WLC di Catalyst 9800.

Prima di continuare, accertarsi di aver compreso a fondo il processo di decodifica. In tal caso, è necessario completare i passaggi successivi per caricare un certificato Web Auth, Web Admin o Management in un WLC 9800.

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).