瞭解憑證資訊，以為9800 WLC建立鏈結

目錄

簡介

本文說明如何使用眾所周知的線上工具及其說明來解碼憑證，以在9800 WLC中建立憑證鏈結。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- Cisco Catalyst 9800無線LAN控制器(WLC)
- 數位憑證、憑證簽署請求(CSR)概念。
- OpenSSL軟體。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 1.1.1w版本的OpenSSL軟體
- Windows電腦

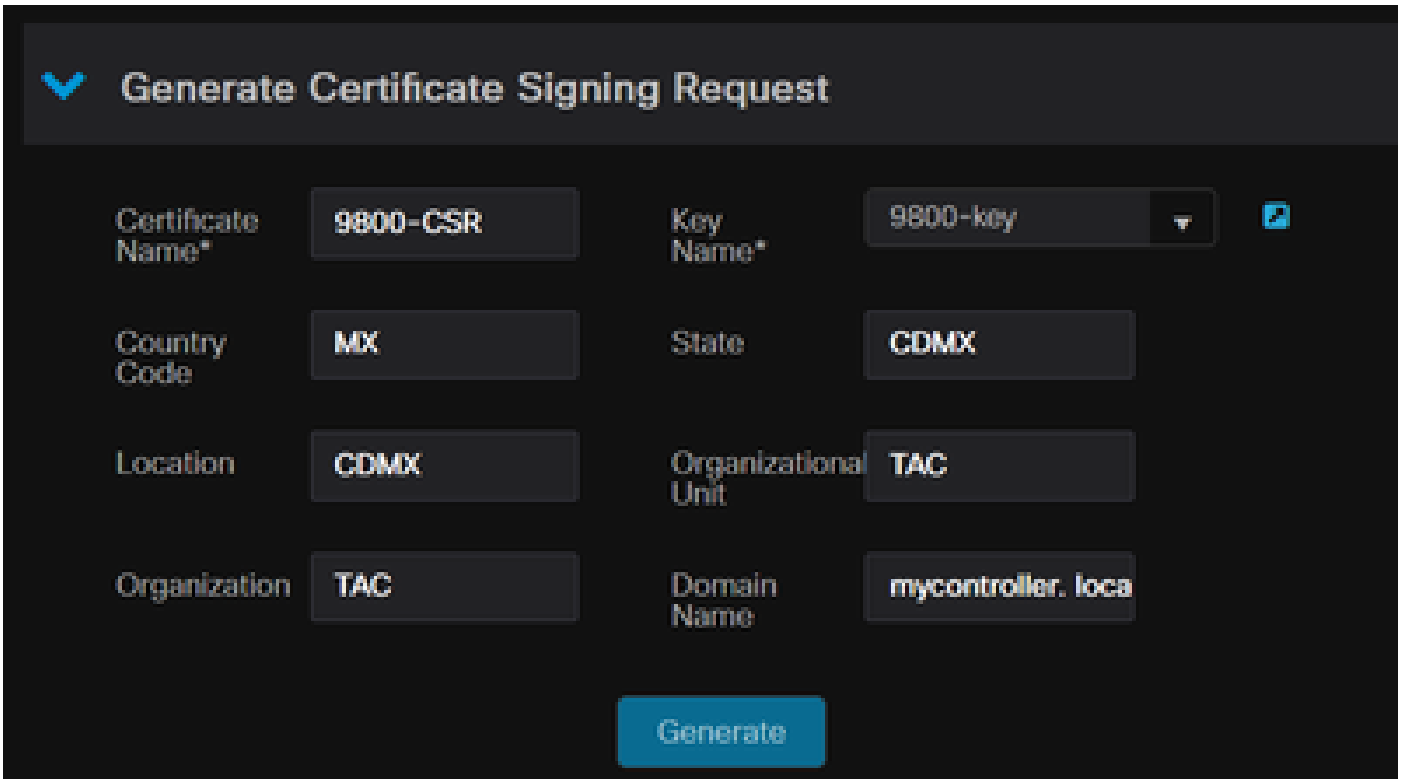
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

CSR 產生

可以在控制器中或使用OpenSSL產生CSR。

要在9800 WLC中生成CSR，請導航到配置>安全> PKI管理>增加證書>生成證書簽名請求。

生成證書簽名請求時，需要提供私鑰、公用名(CN)、國家/地區代碼、狀態、位置、組織和組織單位等資訊。

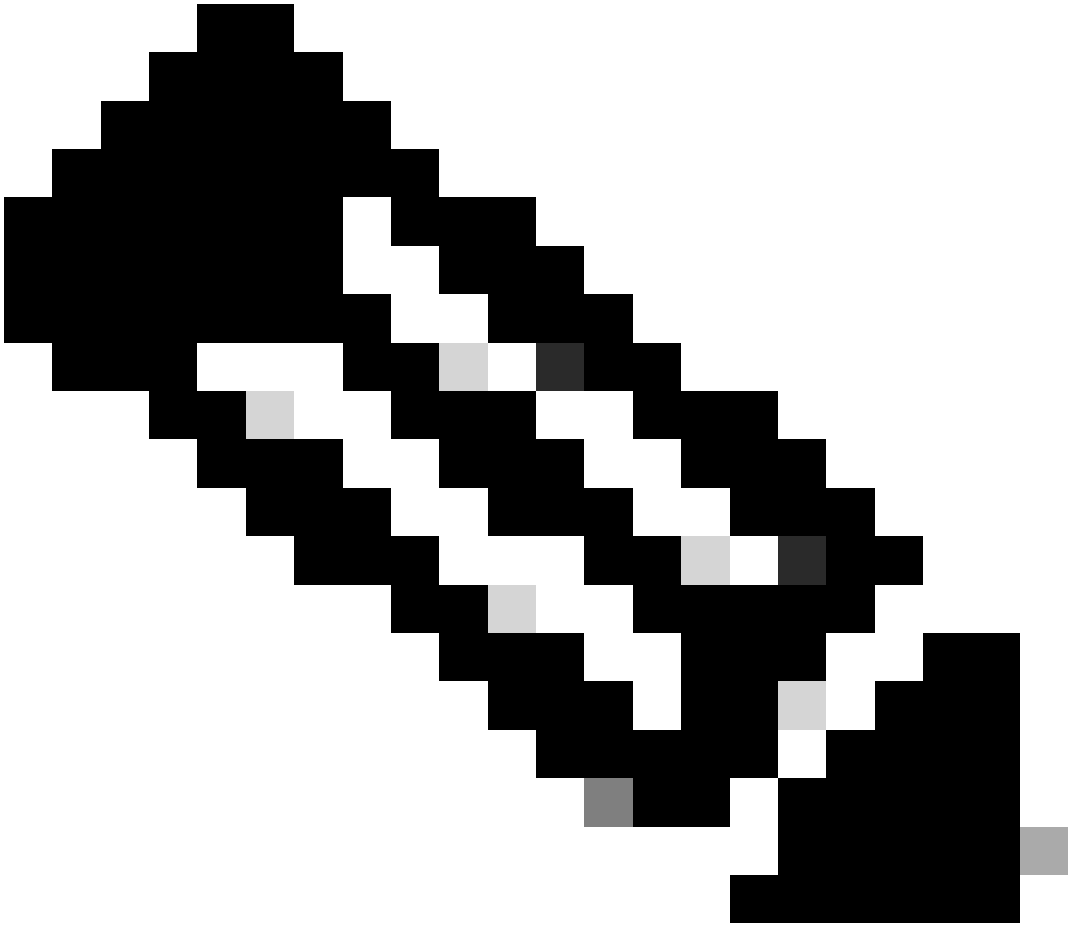


在WLC中生成CSR

在請求中填充的所有CSR資訊都會顯示在解碼中。

OpenSSL軟體是憑證解碼時的單一事實來源。它會顯示它的所有資訊。

要對安裝了OpenSSL的Windows或MacBook電腦中的證書進行解碼，請以管理員身份打開命令提示符並運行命令openssl x509 -in <certificate.crt> -text -noout。輸出將顯示為控制檯資訊。



注意：9800 WLC並不支援所有openSSL版本。建議版本為0.9.8和1.1.1w

還有其他一些線上工具可以解碼憑證，這些憑證會以較方便使用的方式顯示輸出，例如CertLogik和SSL Shopper，但本檔案並未提供這些工具。

請注意，它們使用之前提及的相同OpenSSL命令來解碼憑證。

第三方證書

CSR會傳送給憑證授權單位(CA)，以便簽署並傳回。下載所有憑證鏈結，以便您可以將其上傳到WLC。

要瞭解證書鏈，可以對CA接收的所有檔案進行解碼。請確定它們是Base64格式。

您可以從CA接收多個檔案。這取決於中間CA檔案的數量。

要辨識每個檔案，您需要將其解碼。

簽名證書解碼時，增加頒發者部分。這是指簽署憑證的CA。

如果您解碼未簽名的CSR檔案，則Issuer部分不存在，因為它尚未簽名。

以下是多層級授權或鏈結憑證案例的範例：

- 根CA
- 中間CA憑證
- 裝置證書

已解碼根CA

對於根CA，因為它是鏈的最高優先順序，所以Issuer和Subject必須相同。

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4c:25:79:7e:57:f3:84:85:42:52:1f:c3:4b:f2:64:3f
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = com, DC = Root, CN = RootCA
        Validity
            Not Before: Apr 11 00:21:30 2024 GMT
            Not After : Apr 11 00:31:30 2029 GMT
        Subject: DC = com, DC = Root, CN = RootCA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:a2:f5:8e:23:db:7b:09:e2:bf:c5:e0:31:a1:35:
                    7b:2f:f8:ed:fc:2f:4d:36:c6:b1:92:4e:80:52:6a:
                    1a:82:83:3f:77:06:34:ca:0f:2b:fc:ef:84:85:67:
                    40:de:a5:59:99:3d:d1:db:f8:ee:55:72:97:2a:bd:
                    7e:c5:05:c6:ec:6a:6d:00:ec:22:d5:ff:6a:cd:31:
                    49:a2:f0:8d:85:be:ba:e3:a0:db:31:07:e8:9c:3d:
                    d4:a9:ab:bc:73:90:b8:a2:ab:a2:87:0c:1d:ac:42:
                    f7:e4:26:49:28:18:93:a0:fd:1f:1a:7d:da:1b:e1:
                    60:87:dc:38:ce:b7:95:90:64:3d:2f:2b:bc:6e:d7:
                    2c:09:5a:54:11:dd:0e:58:63:b4:50:38:87:ea:28:
                    28:32:39:8c:e5:2b:b9:13:38:1f:3a:34:b9:32:33:
                    af:86:23:3a:40:38:fe:38:18:0c:67:a7:27:66:ab:
                    e3:11:66:25:f1:85:48:54:a8:05:0e:9f:02:64:09:
                    4f:63:be:a4:53:d5:d7:41:f0:cd:ad:b7:4c:8b:fd:
                    ab:a4:c7:fa:95:05:f9:ef:ed:54:ce:90:28:07:1d:
                    94:54:4f:bd:6c:7d:4e:a9:70:84:0b:dc:b3:73:3f:
                    af:d9:82:86:94:cf:29:35:53:8b:67:95:d3:00:5c:
                    ab:e1
```

已解碼根CA

解碼的中間CA

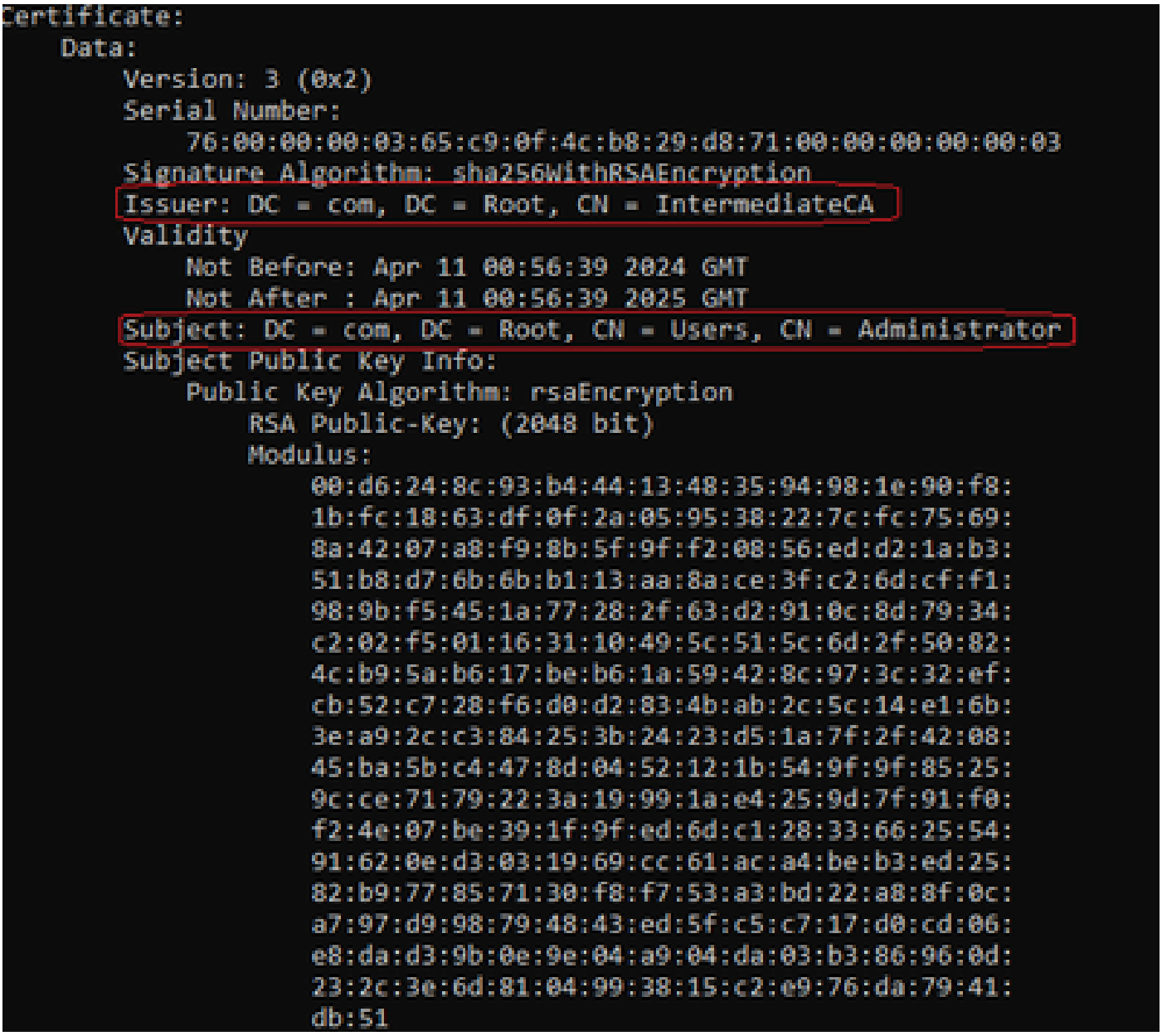
對於中間CA，因為它由根CA簽署，所以Issuer必須與根CA CN匹配。

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            70:00:00:00:04:18:9f:53:1e:b0:cc:90:b7:00:00:00:00:00:04
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = com, DC = Root, CN = RootCA
        Validity
            Not Before: Apr 11 00:44:27 2024 GMT
            Not After : Apr 11 00:54:27 2026 GMT
        Subject: DC = com, DC = Root, CN = IntermediateCA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:f1:c9:2b:1a:53:29:55:6d:bc:82:95:36:38:3a:
                    08:a4:9e:dd:81:c4:fc:0a:92:6c:2b:30:82:cd:62:
                    4c:91:38:ec:09:06:cc:fb:2b:f6:0f:09:43:d3:5a:
                    95:6a:3b:2b:4c:bc:d2:03:05:8e:0b:fd:0a:44:c2:
                    b8:c1:55:c0:4c:b5:d8:2d:cb:ab:4d:df:d5:d7:96:
                    87:21:ea:45:5b:32:db:bd:78:31:fa:5c:cb:1e:66:
                    62:8c:42:ff:3e:15:05:25:4e:bf:cd:5a:d7:3e:fb:
                    4a:2f:41:95:e0:37:f1:23:22:47:ee:7e:2e:9e:6f:
                    a0:24:fe:07:7d:7c:9b:cb:91:9d:05:b6:73:e4:c1:
                    c7:04:86:72:a4:6e:73:db:ca:1a:ee:9b:c1:0c:9a:
                    39:46:74:96:f8:6f:80:1e:5f:1a:cc:98:7c:91:be:
                    7c:98:8b:0d:08:4c:34:ab:30:9c:a0:02:0a:c4:65:
                    75:68:0b:f8:29:ea:92:6b:be:c6:83:19:79:fc:bd:
                    91:b9:f0:aa:1c:ed:fe:62:2c:27:d7:3e:8b:e3:db:
                    74:31:fe:a3:be:5d:8e:12:03:70:9f:f1:3c:0a:61:
                    e0:74:0b:08:00:1b:97:7d:01:dd:c7:24:04:7f:f6:
                    7e:18:e3:be:ef:a9:33:5d:47:0f:eb:52:6d:07:10:
                    f5:d5
```

解碼的中間CA

解碼的裝置證書

對於裝置證書，由於它是由中間CA簽署的，因此Issuer必須與中間CA CN匹配



解碼的裝置證書

在使用1個以上中間CA的場景中，請使用相同的解碼過程。

一旦辨識鏈結順序，就可以將其上傳到控制器。

9800 WLC需要整個鏈結的順序正確，才能讓憑證正確運作。

有關將證書上傳到控制器的後續步驟，請參閱在Catalyst 9800 WLC上生成和下載CSR證書。

繼續進行之前，請確認您已瞭解解碼程式。如果是，需要完成以下步驟，才能在9800 WLC中上傳Web驗證、Web管理或管理憑證。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。