上傳RV32x系列路由器證書的解決方法

摘要

數位證書通過證書的指定主題來證明公共金鑰的所有權。這允許依賴方依賴於由與經認證的公鑰對應的私鑰進行的簽名或斷言。路由器可以生成自簽名證書，即由網路管理員建立的證書。它還可以向證書頒發機構(CA)發出申請數位身份證書的請求。必須擁有來自第三方應用程式的合法證書。

CA簽署憑證的方式有兩種：

1. CA使用私鑰簽署憑證。

2. CA使用RV320/RV325產生的CSR簽署憑證。

RV320和RV325僅支援.pem格式證書。對於這兩種情況，您都應從憑證授權單位取得.pem格式憑證。如果您取得其他格式憑證，則需要自行轉換該格式，或再次從CA要求.pem格式憑證。

大多數商業憑證供應商使用中間憑證。 由於中間證書由受信任的根CA頒發，因此由中間證書頒發的任何證書都繼承受信任的根的信任，如信任證書鏈。

本指南介紹如何匯入由中間證書頒發機構在RV320/RV325上頒發的證書。

識別日期

2017年2月24日

解決日期

不適用

受影響的產品

RV320/RV325	1.1.1.06及更高版本

使用私鑰進行證書簽名

在本範例中，我們假設您從第三方中間CA取得RV320.pem。檔案中有以下內容：私鑰、證書、根CA證書、中間CA證書。

附註：從中間CA獲取多個檔案而不是僅獲取一個檔案是可選的。但是您可以從幾個檔案中找到以上四個部分。

檢查CA憑證檔案是否同時包含根CA憑證和中間憑證。RV320/RV325要求CA套件組合中按照特定順序提供中間憑證和根憑證，先提供根憑證，再提供中間憑證。其次，您需要將

RV320/RV325證書和私鑰合併到一個檔案中。

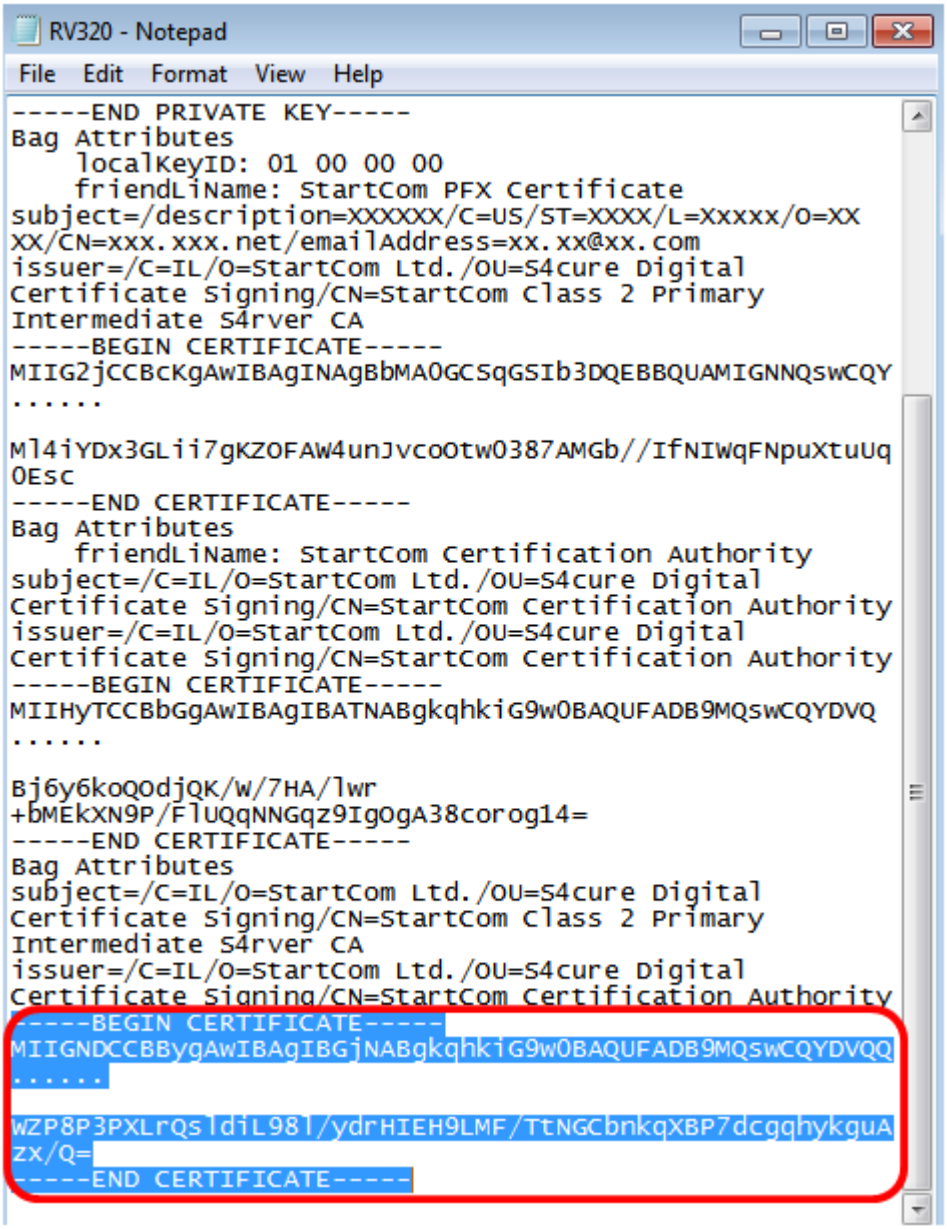
附註：任何文本編輯器都可用於開啟和編輯檔案。一定要確保任何額外的空白行、空格或回車鍵都不能使計畫按預期進行。

組合證書

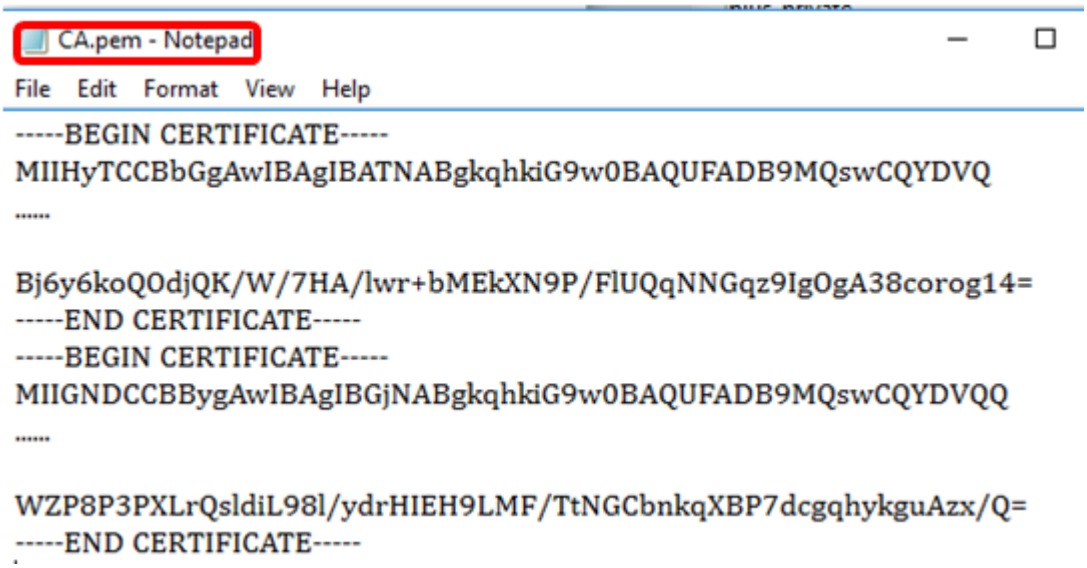
步驟1。開啟RV320.pem，複製第二個憑證（根憑證）和第三個憑證（中間憑證），包括開始/結束訊息。

附註：在本示例中，文本的高亮字串是根證書。

附註：在本示例中，突出顯示的文本字串是中間證書。

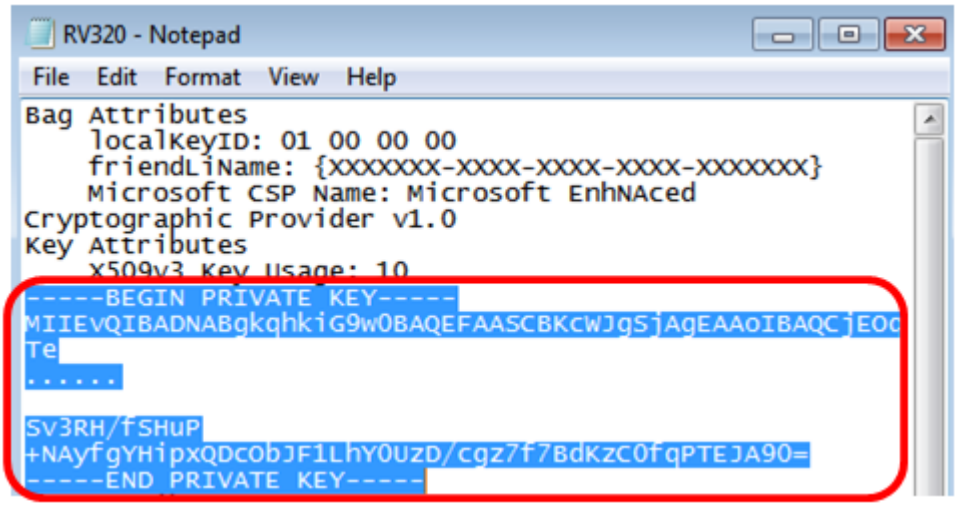


步驟2.將內容貼上到新檔案中並將其另存為CA.pem。

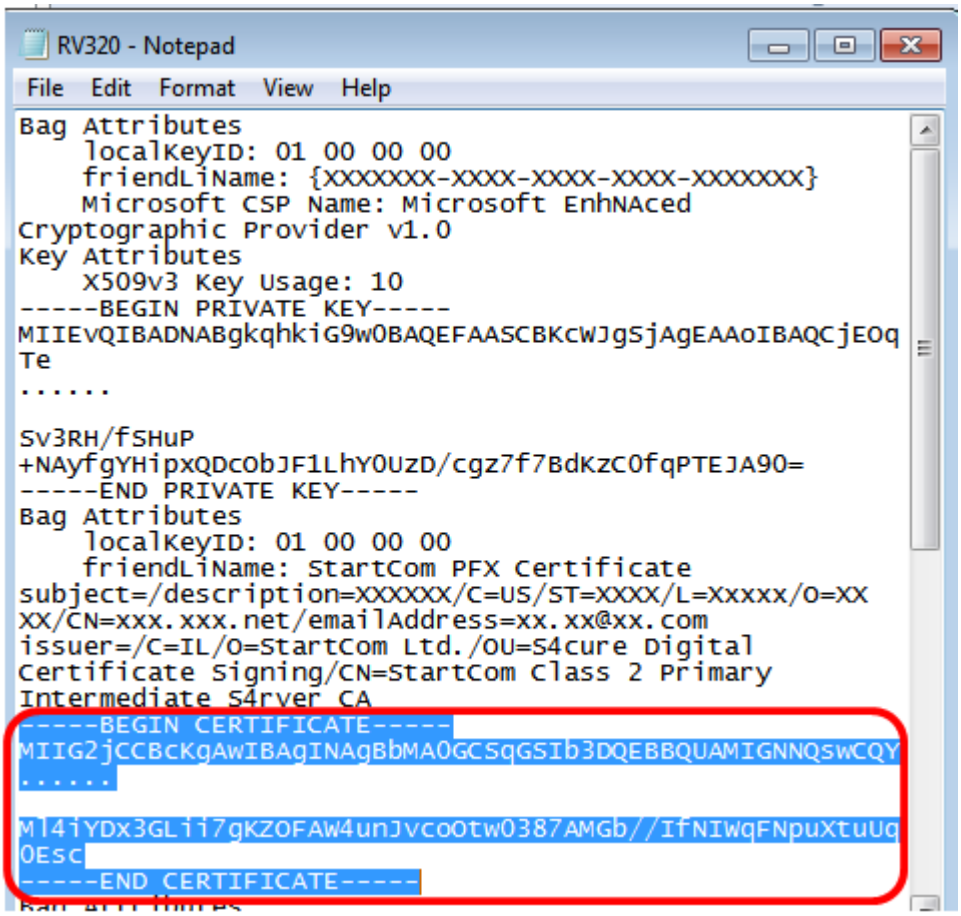


步驟3.開啟RV320.pem，複製私鑰部分和第一個證書，包括開始/結束消息。

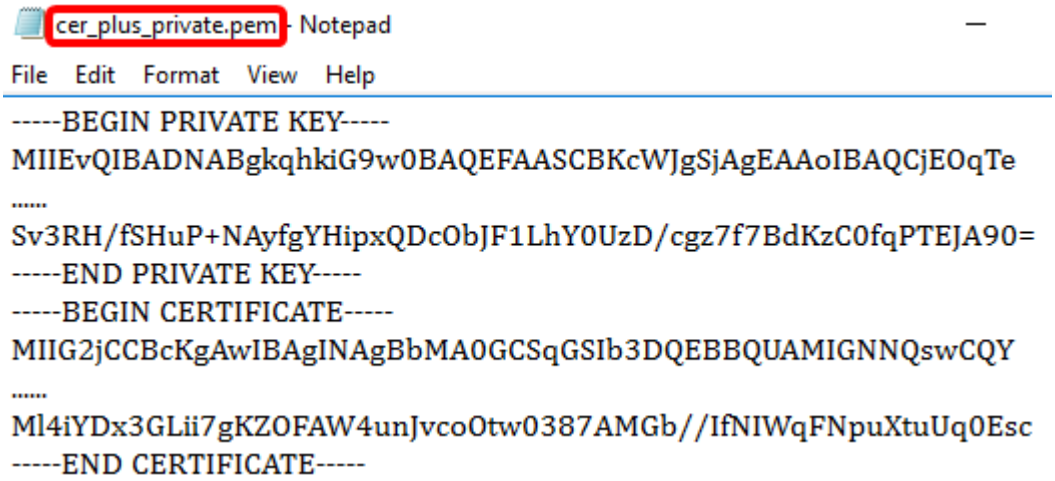
附註：在下面的示例中，突出顯示的文本字串是私鑰部分。



附註：在下面的示例中，突出顯示的文本字串是第一個證書。



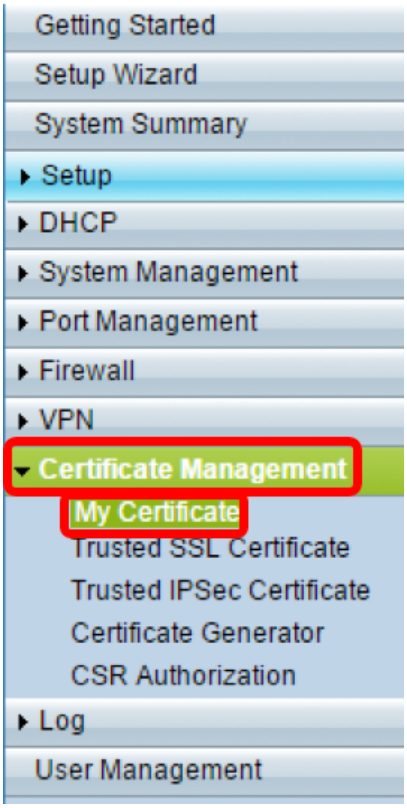
步驟4.將內容貼上到新檔案中並將其另存為cer_plus_private.pem



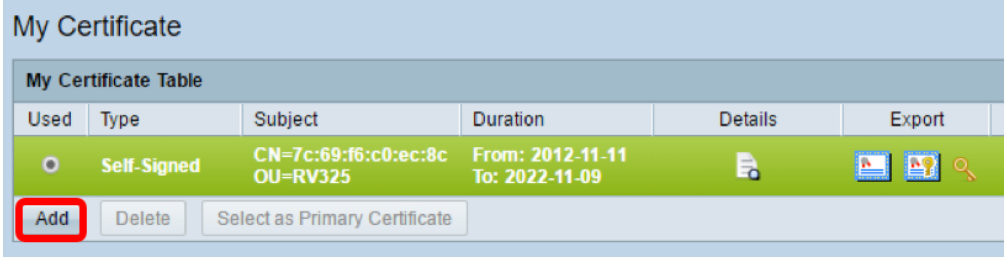
附註：如果RV320/RV325韌體版本低於1.1.1.06，請確保檔案末尾有兩個行饋送(cer_plus_private.pem)。 在1.1.1.06之後的韌體中，無需再新增兩個線路饋送。在此範例中，系統只會顯示縮短版本的憑證，以供演示之用。

匯入 CA.pem 和 思er_plus_private.pem 到RV320中/RV325

步驟1.登入到RV320或RV325的基於Web的實用程式，然後選擇**Certificate Management > My Certificate**。



步驟2.按一下**Add**以匯入憑證。



步驟3.按一下*Third-Party Authorized*單選按鈕匯入證書。

步驟4.在*Import Full Certificate Set*區域中，按一下單選按鈕以選擇已儲存憑證的來源。選項包括：

- *從PC匯入* — 如果在電腦上找到了檔案，請選擇此選項。
- *從USB匯入* — 選擇此項可從快閃記憶體驅動器匯入檔案。

附註：在本例中，選擇了Import from PC。

步驟5.在*CA Certificate*區域中，按一下**Browse**...，然後找到CA.pem。檔案。

附註：如果運行韌體版本高於1.1.0.6，請按一下「選擇」按鈕並找到所需的檔案。

步驟6.在*Certificate + Private Key*區域中，按一下**Browse...**，然後找到er_plus_private.pem檔案。

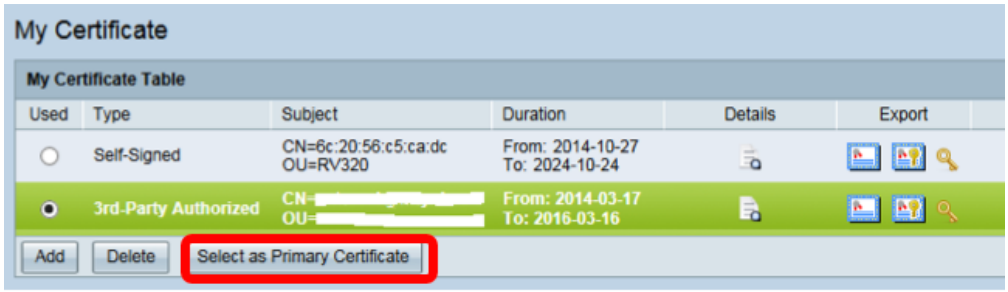
附註：如果運行韌體版本高於1.1.0.6，請按一下「選擇」按鈕並找到所需的檔案。

步驟7.按一下「**Save**」。

已成功匯入證書。現在可用於HTTPS訪問、SSL VPN或IPSec VPN。

步驟8.（可選）若要將憑證用於HTTPS或SSL VPN，請按一下憑證的單選按鈕，然後按一下

「Select as Primary Certificate」按鈕。

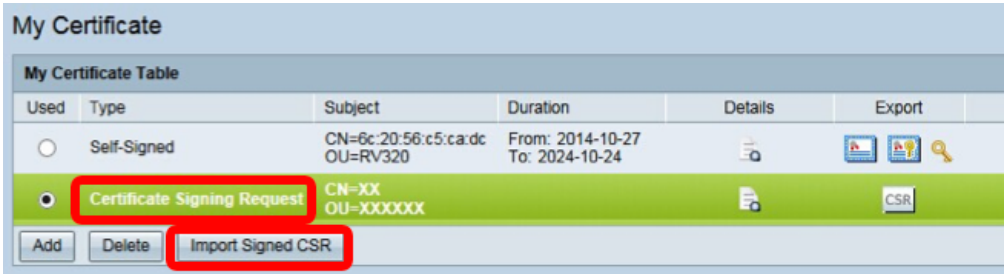


您現在應該已成功匯入證書。

使用CSR的證書簽名

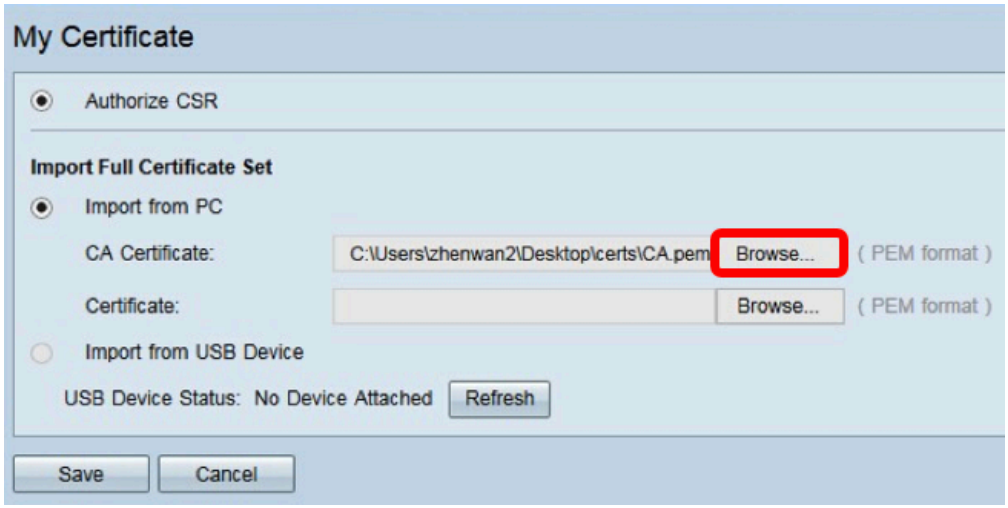
步驟1.在RV320/RV325上產生憑證簽署請求(CSR)。若要瞭解如何產生CSR，請按一下此處。

步驟2。若要匯入憑證，請選擇**憑證簽署請求**，然後按一下**Import Signed CSR**。

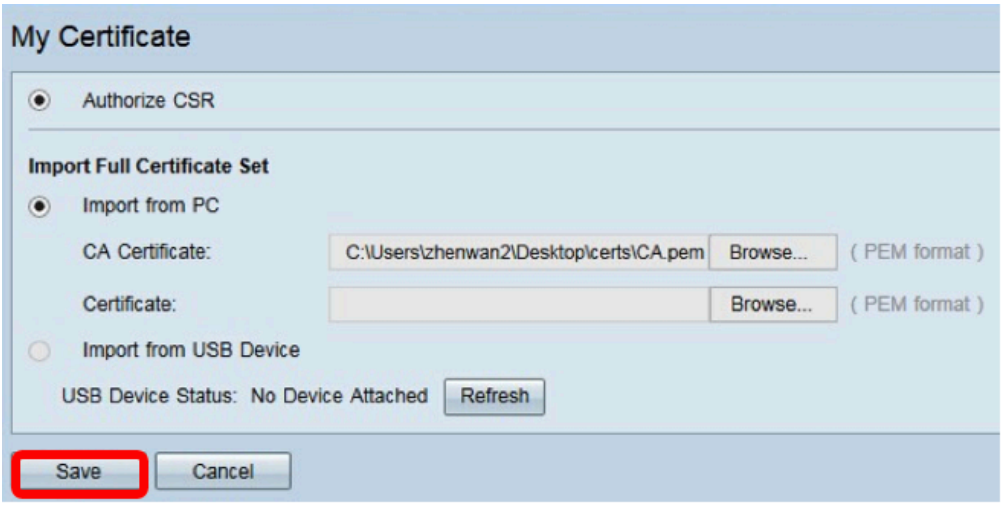


步驟3.按一下**Browse...**，然後選擇CA憑證檔案。這包含根CA +中間CA證書。

附註：在本範例中，由於憑證是使用CSR產生的，因此不需要私鑰。



步驟4.按一下「Save」。



您現在應該已經使用CSR成功上傳了證書。

附錄:

RV320.pem的內容

包屬性

localKeyID:01 00 00 00

friendLiName:{{XXXXXXX-XXXX-XXXX-XXXX-XXXXXXX}}

Microsoft CSP名稱：Microsoft Enhanced加密提供程式v1.0

關鍵屬性

X509v3金鑰用法：10

-----BEGIN PRIVATE KEY-----

MIIEvQIBADNABgkqhkiG9w0BAQEFAAASCBKcWJgSjAgEAAoIBAQCjEOqTe

.....

Sv3RH/fSHuP+NAyfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=

-----END PRIVATE KEY-----

包屬性

localKeyID:01 00 00 00

friendLiName:StartCom PFX證書

subject=/description=XXXXXX/C=US/ST=XXXX/L=Xxxxx/O=XX XX/CN=xxx.xxx.net/emailAddress=xx.xx@xx.com

issuer=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signing/CN=StartCom Class 2 Primary Intermediate S4rver CA

-----BEGIN CERTIFICATE-----

MIIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNQswCQY

.....

Ml4iYDx3GLii7gKZOFAW4unJvcoOtw0387AMGb//IfNIWqFNpuXtuUq0Esc

-----END CERTIFICATE-----

包屬性

friendLiName:StartCom證書頒發機構

subject=/C=IL/O=StartCom Ltd./OU=S4cure數位證書簽名/CN=StartCom證書頒發機構

issuer=/C=IL/O=StartCom Ltd./OU=S4cure數位證書簽名/CN=StartCom證書頒發機構

-----BEGIN CERTIFICATE-----

MIIHyTCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

.....

Bj6y6koQOdjQK/W/7HA/lwr+bMEkXN9P/FlUQqNNGqz9IgOgA38corog14=

-----END CERTIFICATE-----

包屬性

subject=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signing/CN=StartCom Class 2 Primary Intermediate S4rver CA

issuer=/C=IL/O=StartCom Ltd./OU=S4cure數位證書簽名/CN=StartCom證書頒發機構

-----BEGIN CERTIFICATE-----

MIIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQQ

.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dcgqhykguAzx/Q=

-----END CERTIFICATE-----