Workaround for Uploading RV32x Series Router Certificate

Summary

A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows relying parties to depend upon signatures or assertions made by the private key that corresponds to the public key that is certified. A router can generate a self-signed certificate, a certificate created by a network administrator. It can also send out requests to Certificate Authorities (CAs) to apply for a digital identity certificate. It is important to have legitimate certificates from third party applications.

There are two ways that CA signs the certificates:

1. CA signs the certificate with private keys.

2. CA signs the certificates using CSR generated by RV320/RV325.

RV320 and the RV325 only support .pem format Certificates. For both cases you should get .pem format certificates from Certificate Authority. If you get other format certificate, you need to convert the format by yourself or request for the .pem format certificate again from the CA.

Most commercial certificate vendors use intermediate certificates. As the Intermediate Certificate is issued by the Trusted Root CA, any Certificates issued by the Intermediate Certificate inherits the trust of the Trusted Root, like a certification chain of trust.

This guide describes how to import certificate issued by the Intermediate Certificate Authority on RV320/RV325.

Date Identified

February 24, 2017

Date Resolved

N/A

Products Affected

RV320/RV325	1.1.1.06 and later

Certificate Signing Using Private Keys

In this example, we assume you got an RV320.pem from the third party intermediate CA. The file has such content: private key, certificate, root CA certificate, intermediate CA certificate.

Note: Obtaining several files from intermediate CA instead of only one file are optional. But you can find above four parts from the several files.

Check if the CA certificate file contains both root CA certificate and the intermediate certificate. RV320/RV325 requires the intermediate certificate and root certificate in a certain order in the CA bundle, the root certificate first and then the intermediate certificate. Secondly, you need to combine the RV320/RV325 certificate and the private key into one file.

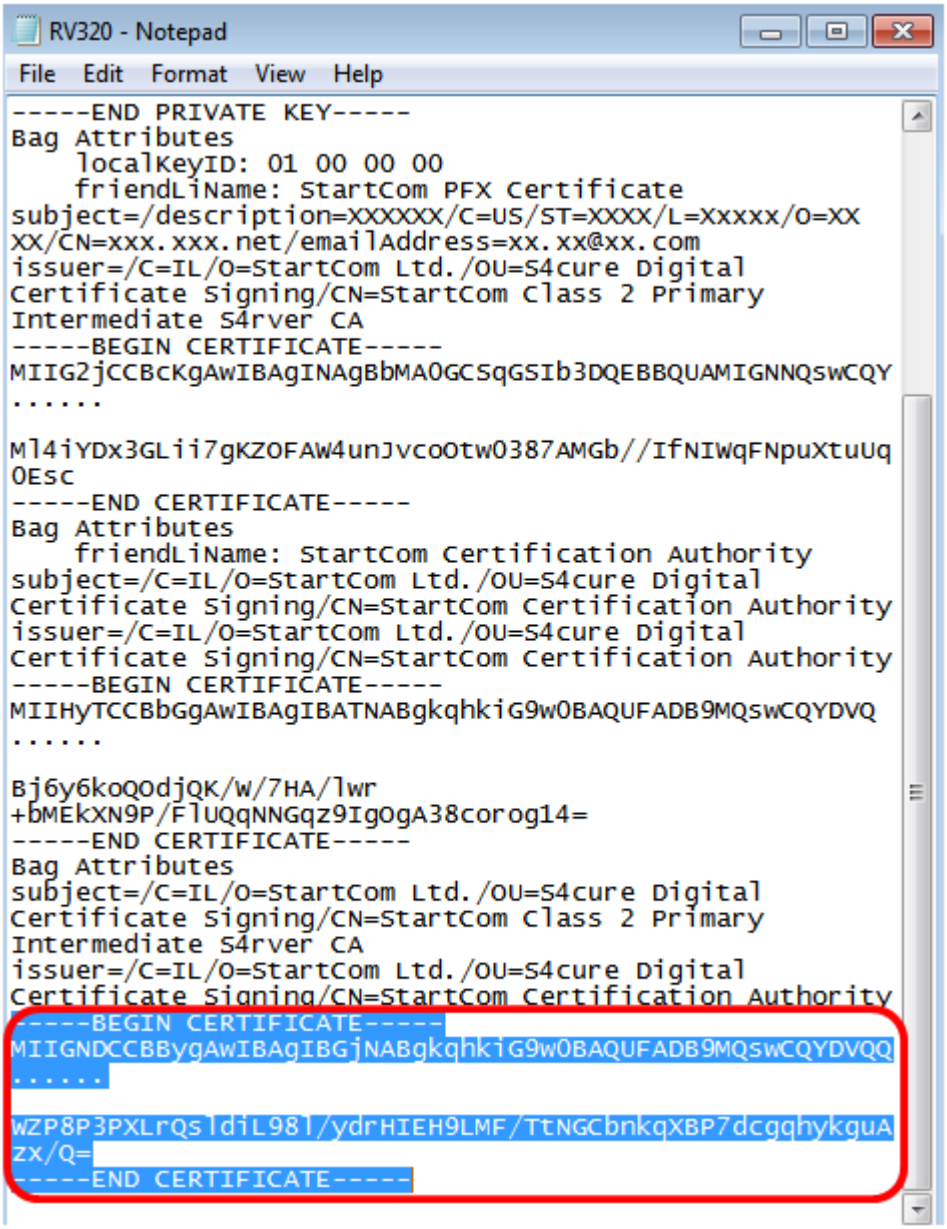
Note: Any text editor can be used to open and edit the files. It is important to make sure that any extra blank lines, spaces, or carriage returns will not make the plan go as expected.

Combining the Certificates

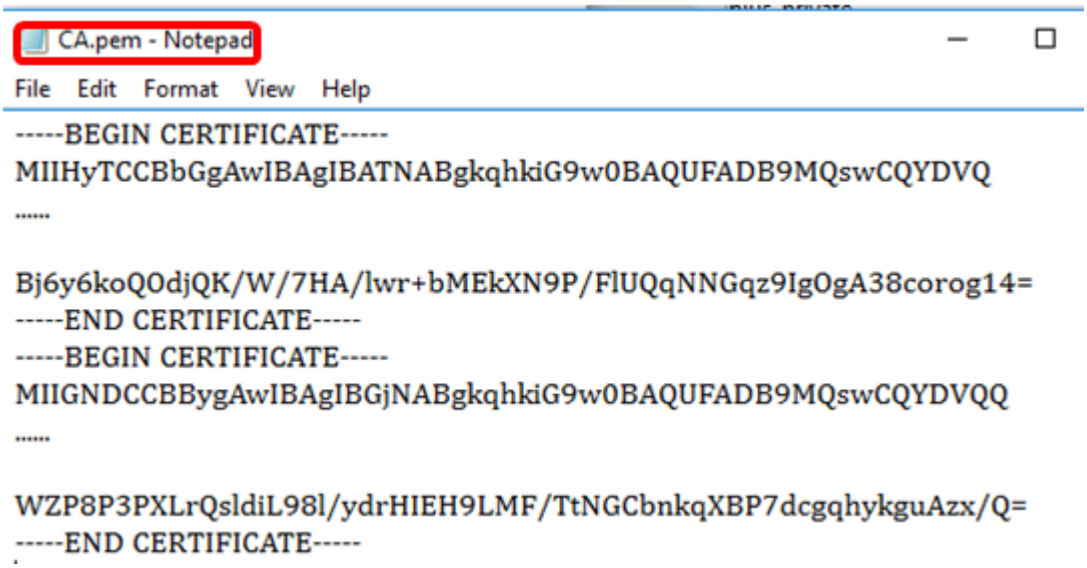
Step 1. Open the RV320.pem, copy the second certificate (root certificate) and the third certificate (intermediate certificate) including the begin/end message.

Note: In this example, the highlight string of text is the root certificate.

Note: In this example, the highlighted string of text is the intermediate certificate.

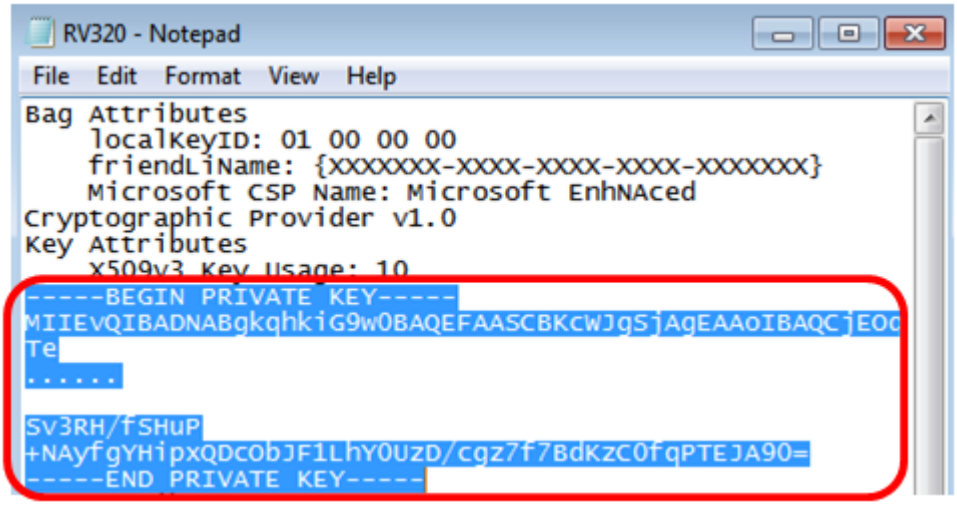


Step 2. Paste the content into a new file and save it as CA.pem.

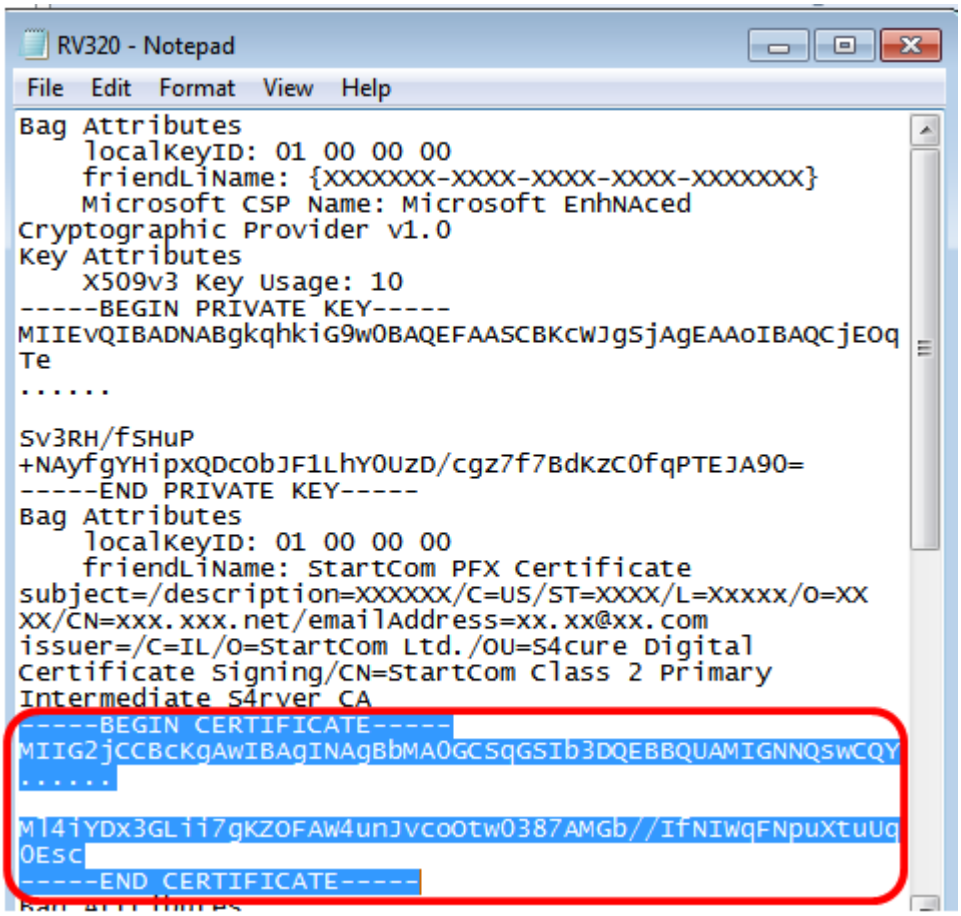


Step 3. Open the RV320.pem, and copy the private key section and the first certificate, including the begin/end message.

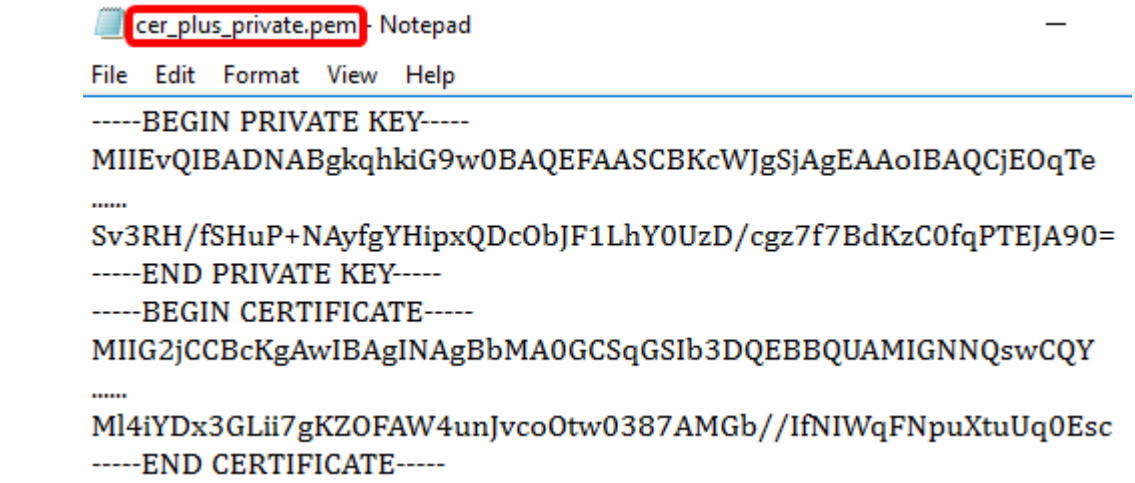
Note: In the example below, the highlighted string of text is the private key section.



Note: In the example below, the highlighted string of text is the first certificate.



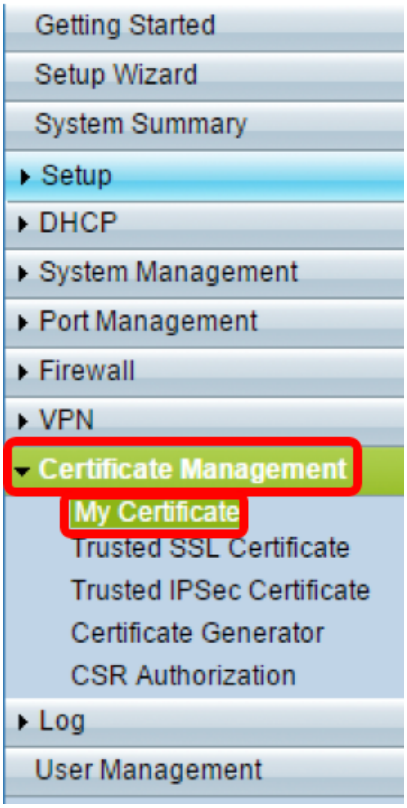
Step 4. Paste the content into a new file and save it as cer_plus_private.pem



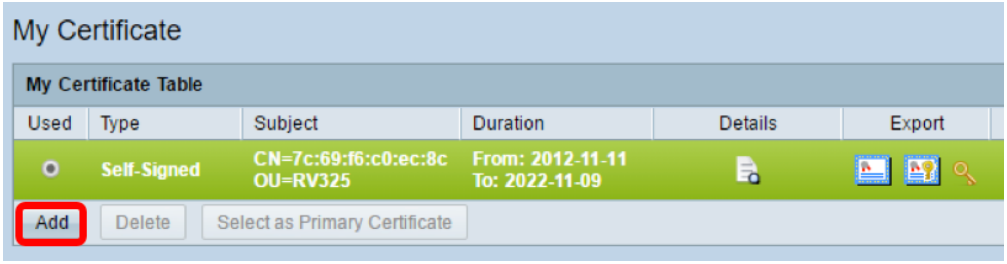
Note: If RV320/RV325 Firmware version is below 1.1.1.06, make sure there are two line feeds at the end of the file (cer_plus_private.pem). In the firmware after 1.1.1.06, you do not need to add two more line feeds. In this example, a shortened version of the certificate is displayed for demonstration purposes only.

Import CA.pem and cer_plus_private.pem into RV320/RV325

Step 1. Log in to the web-based utility of the RV320 or RV325 and choose **Certificate Management > My Certificate**.



Step 2. Click **Add** to import the certificate.



Step 3. Click the *3rd-Party Authorized* radio button to import the certificate.

Step 4. In the *Import Full Certificate Set* area, click a radio button to choose the source of the saved certificates. The options are:

- *Import from PC* - Choose this if the files are found on the computer.
- *Import from USB* - Choose this to import the files from a flash drive.

Note: In this example, **Import from PC** is chosen.

Step 5. In the *CA Certificate* area, click **Browse…** and locate the CA.pem. file.

Note: If you are running firmware later than 1.1.0.6, click the choose button and locate the necessary file.

Step 6. In the *Certificate + Private Key* area, click **Browse…**and locate thecer_plus_private.pem file.

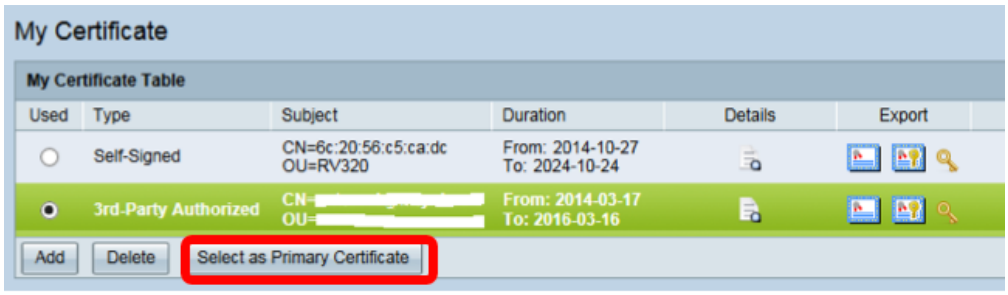
Note: If you are running firmware later than 1.1.0.6, click the choose button and locate the necessary file.

Step 7. Click **Save**.

The certificates are imported successfully. It can now be used for HTTPS access, SSL VPN,

or IPSec VPN.

Step 8. (Optional) To use the certificate for HTTPS or SSL VPN, click the radio button of the certificate and click the **Select as Primary Certificate** button.

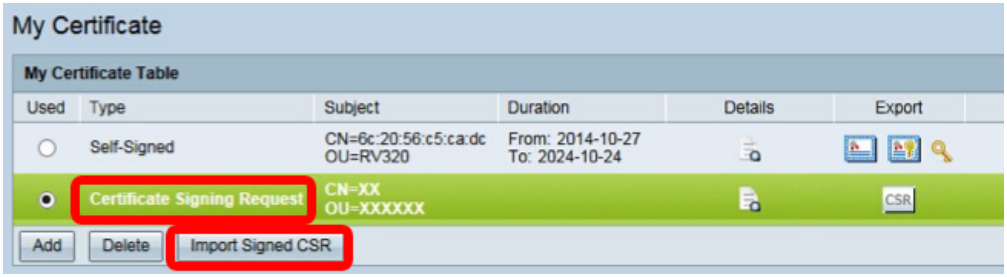


You should now have successfully imported a certificate.

Certificate Signing Using CSR

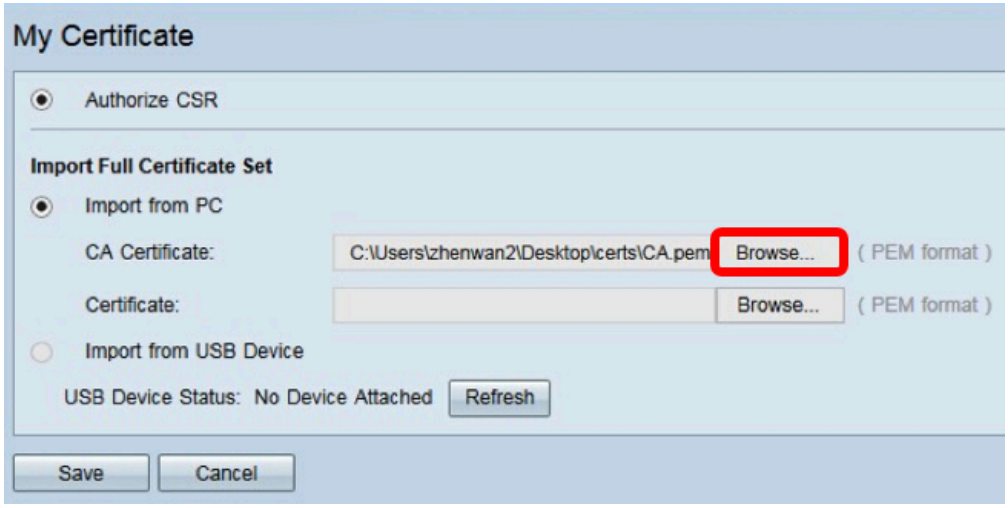
Step 1. Generate a Certificate Signing Request (CSR) on RV320/RV325. To learn how to generate a CSR, click here.

Step 2. To import the certificate, choose **Certificate Signing Request** and click **Import Signed CSR**.

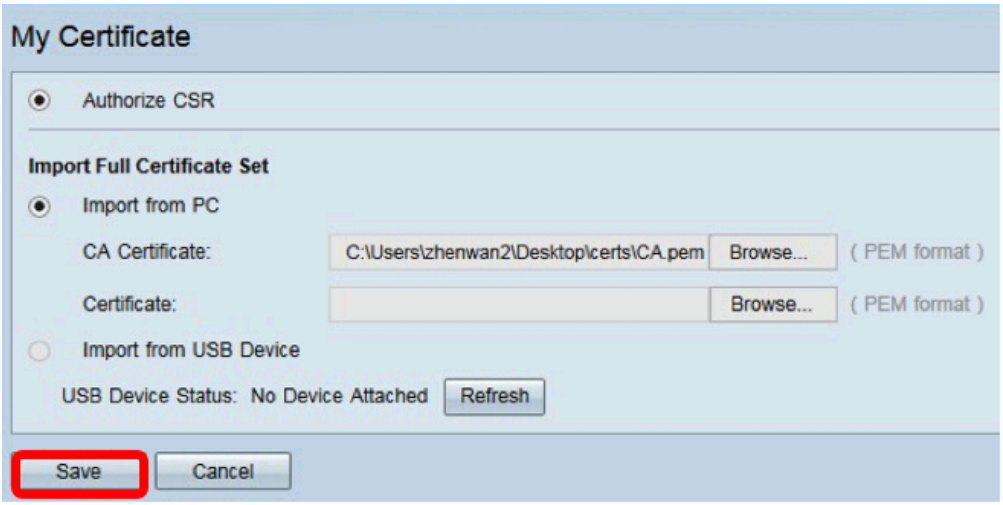


Step 3. Click **Browse…** and choose the CA certificate file. This contains the root CA + intermediate CA certificate.

Note: In this example, private key is not required since the certificate is generated using CSR.



Step 4. Click **Save**.



You should now have successfully uploaded a certificate using the CSR.

Appendix:

Content of RV320.pem

Bag Attributes

localKeyID: 01 00 00 00

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

Microsoft CSP Name: Microsoft EnhNAced Cryptographic Provider v1.0

Key Attributes

X509v3 Key Usage: 10

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

MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBKcWJgSjAgEAAoIBAQCjEOqTe

.....

Sv3RH/fSHuP+NAyfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=

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

Bag Attributes

localKeyID: 01 00 00 00

friendLiName: StartCom PFX Certificate

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-----

MIIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNNQswCQY

.....

Ml4iYDx3GLii7gKZOFAW4unJvcoOtw0387AMGb//IfNIWqFNpuXtuUq0Esc

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

Bag Attributes

friendLiName: StartCom Certification Authority

subject=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signing/CN=StartCom Certification Authority

issuer=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signing/CN=StartCom Certification Authority

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

MIIHyTCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

.....

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

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

Bag Attributes

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 Digital Certificate Signing/CN=StartCom Certification Authority

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

MIIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQQ

.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dcgqhykguAzx/Q=

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