

# 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.

RV320 - Notepad

File Edit Format View Help

```
Bag Attributes
  localKeyID: 01 00 00 00
  friendLiName: {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx}
  Microsoft CSP Name: Microsoft EnhNaced
Cryptographic Provider v1.0
Key Attributes
  X509v3 Key Usage: 10
-----BEGIN PRIVATE KEY-----
MIIEVQIBADNABgkqhkiG9w0BAQEFAASCBKcWJgsjAgEAAoIBAQCjEOq
Te
.....
Sv3RH/fSHuP
+NaYfgYHiphQDCobJF1LhY0UzD/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
.....
M14iYDX3GLii7gKZOFAw4unJvc0tw0387AMgb//IfNIWqFNpuXtuUq
OEsc
-----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/F1uQqNNGqz9Ig0gA38corog14=
-----END CERTIFICATE-----
```

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

The screenshot shows a Windows Notepad window titled "RV320 - Notepad". The content of the window is a series of certificate snippets, each starting with "-----BEGIN CERTIFICATE-----" and ending with "-----END CERTIFICATE-----". Some sections are preceded by "Bag Attributes" and contain X.509 subject and issuer information. A red box highlights the second certificate's content, which includes a base64 encoded certificate chain. Another red box highlights the third certificate's content, which also includes a base64 encoded certificate chain.

```
-----END PRIVATE KEY-----
Bag Attributes
localKeyID: 01 00 00 00
friendlyName: StartCom PFX Certificate
subject=/description=XXXXXX/C=US/ST=XXXX/L=XXXX/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 Server CA
-----BEGIN CERTIFICATE-----
MIIG2jCCBkKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNNQswCQY
.....
M14iYDX3GLii7gKZOFw4unJvc0tw0387AMgb//IfNIWqFNpuxtuUq
0Esc
-----END CERTIFICATE-----
Bag Attributes
friendlyName: 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/FIUQQNNGqz9IgOgA38corog14=
-----END CERTIFICATE-----
Bag Attributes
subject=/C=IL/O=StartCom Ltd./OU=S4cure Digital
Certificate Signing/CN=StartCom class 2 Primary
Intermediate Server CA
issuer=/C=IL/O=StartCom Ltd./OU=S4cure Digital
Certificate Signing/CN=StartCom Certification Authority
-----BEGIN CERTIFICATE-----
MIIGNDCCBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQQ
.....
WZP8P3PXLrQsldiL981/ydrHIEH9LMF/TtNGCbnkqXBp7dcgqhykguA
zx/Q=
-----END CERTIFICATE-----
```

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

The screenshot shows a Windows Notepad window titled "CA.pem - Notepad". It contains the same certificate snippets as the previous window, but they are all enclosed within a single large red box. This indicates that the entire block of certificates has been copied from the original file and pasted into this new file.

```
-----BEGIN CERTIFICATE-----
MIIHyTCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ
.....
Bj6y6koQodjQK/W/7HA/lwr+bMEkXN9P/FIUQQNNGqz9IgOgA38corog14=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIGNDCCBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQQ
.....
WZP8P3PXLrQsldiL981/ydrHIEH9LMF/TtNGCbnkqXBp7dcgqhykguA
zx/Q=
-----END CERTIFICATE-----
```

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.

```
Bag Attributes
    localKeyID: 01 00 00 00
    friendLiName: {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx}
    Microsoft CSP Name: Microsoft EnhNaced
Cryptographic Provider v1.0
Key Attributes
    X509v3 Key Usage: 10
-----BEGIN PRIVATE KEY-----
MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBKcWJgSjAgEAAoIBAQCjEOq
Te
.....
Sv3RH/fSHuP
+NAYfgYHiphQDCobJF1LhY0UzD/cgz7f7Bdkzc0fqPTEJA90=
-----END PRIVATE KEY-----
```

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

```
Bag Attributes
    localKeyID: 01 00 00 00
    friendLiName: {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx}
    Microsoft CSP Name: Microsoft EnhNaced
Cryptographic Provider v1.0
Key Attributes
    X509v3 Key Usage: 10
-----BEGIN PRIVATE KEY-----
MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBKcWJgSjAgEAAoIBAQCjEOq
Te
.....
Sv3RH/fSHuP
+NAYfgYHiphQDCobJF1LhY0UzD/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 Server CA
-----BEGIN CERTIFICATE-----
MIIG2jCCBcKgAwIBAgINAqBbMA0GCSqGSIb3DQEBBQUAMIGNNQSwCQY
.....
M14iYDX3GLi7gKZOFAw4unJvc0tw0387AMGb//IfNIwqFNpuXtuUc
0ESC
-----END CERTIFICATE-----
```

Step 4. Paste the content into a new file and save it as cer\_plus\_private.pem

**cer\_plus\_private.pem** - Notepad

File Edit Format View Help

-----BEGIN PRIVATE KEY-----  
MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBKcWJgSjAgEAAoIBAQCjEOqTe  
.....  
Sv3RH/fSHuP+NAyfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzCOfqPTEJA90=

-----END PRIVATE KEY-----  
-----BEGIN CERTIFICATE-----  
MIIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNNQswCQY  
.....  
MI4iYDx3GLii7gKZOFW4unJvco0tw0387AMGb//IfNIWqFNpuXtuUq0Esc  
-----END CERTIFICATE-----

**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**.

Getting Started

Setup Wizard

System Summary

► Setup

► DHCP

► System Management

► Port Management

► Firewall

► VPN

▼ Certificate Management

My Certificate

- Trusted SSL Certificate
- Trusted IPsec Certificate
- Certificate Generator
- CSR Authorization

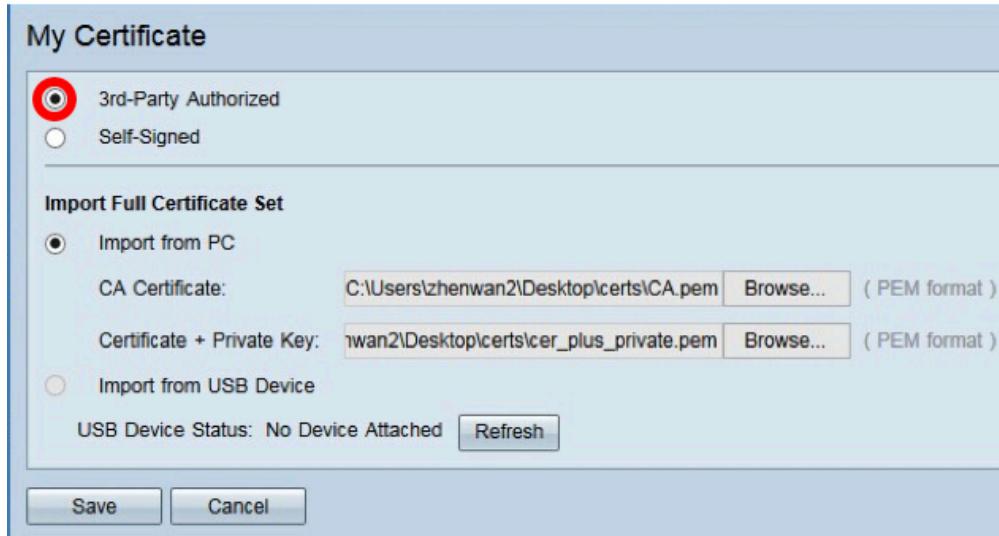
► Log

User Management

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

My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=7c:69:f6:c0:ec:8c OU=RV325	From: 2012-11-11 To: 2022-11-09		
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Select as Primary 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.



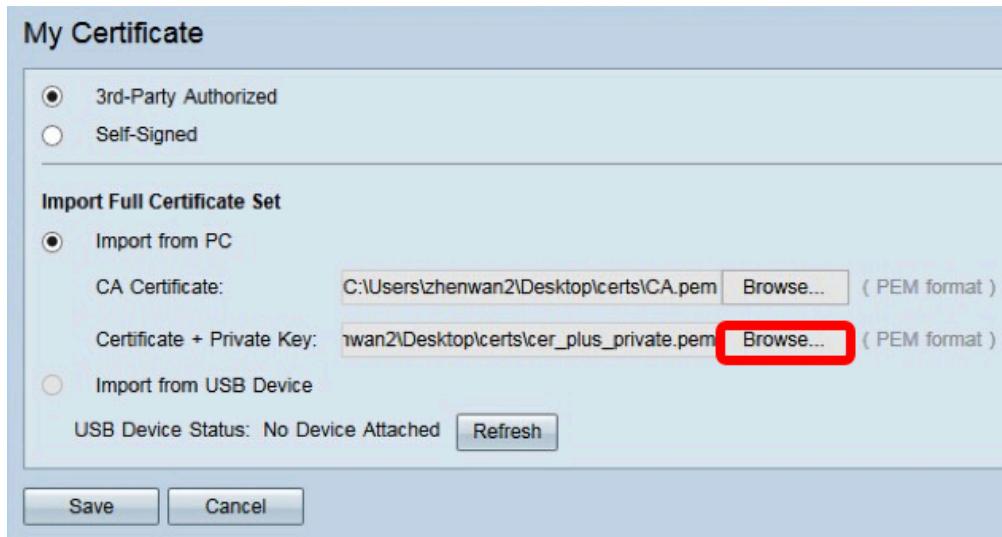
Step 5. In the CA Certificate area, click **Browse...** and locate the CA.pem file.

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

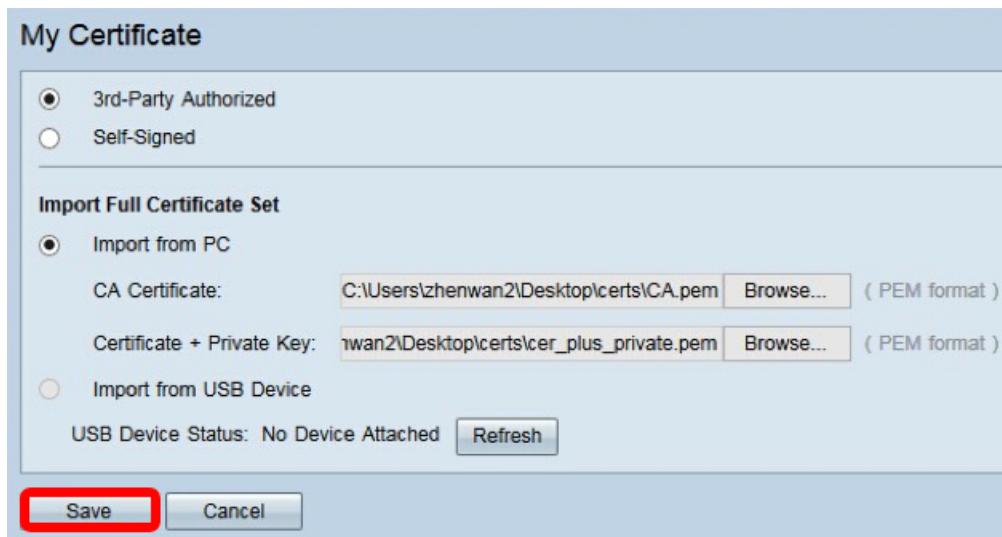


Step 6. In the *Certificate + Private Key* area, click **Browse...** and locate thecer\_plus\_private.pem file.

**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.

The screenshot shows a 'My Certificate' interface with a 'My Certificate Table'. The table has columns: Used, Type, Subject, Duration, Details, and Export. There are two entries:

- Self-Signed: CN=6c:20:56:c5:ca:dc, OU=RV320. Duration: From: 2014-10-27 To: 2024-10-24. Buttons: Details, Export, Search.
- 3rd-Party Authorized: CN=[REDACTED], OU=[REDACTED]. Duration: From: 2014-03-17 To: 2016-03-16. Buttons: Details, Export, Search.

Below the table are buttons: Add, Delete, and Select as Primary Certificate. The 'Select as Primary Certificate' button is highlighted with a red box.

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**.

The screenshot shows a 'My Certificate' interface with a 'My Certificate Table'. The table has columns: Used, Type, Subject, Duration, Details, and Export. There are two entries:

- Self-Signed: CN=6c:20:56:c5:ca:dc, OU=RV320. Duration: From: 2014-10-27 To: 2024-10-24. Buttons: Details, Export, Search.
- Certificate Signing Request: CN=XX, OU=XXXXXX. Duration: [REDACTED]. Buttons: Details, CSR.

Below the table are buttons: Add, Delete, and Import Signed CSR. The 'Import Signed CSR' button is highlighted with a red box.

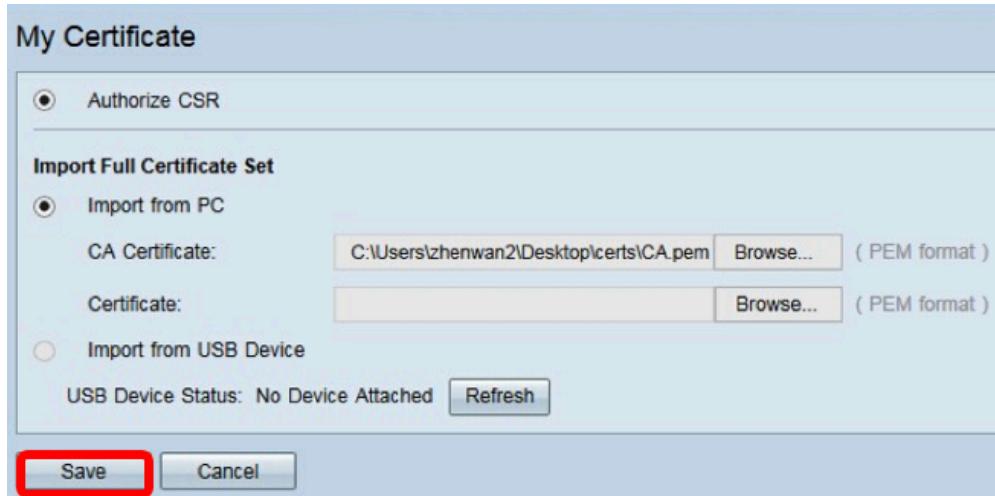
Step 3. Click **Browse...** and choose the CA certificate file. This contains the root CA + intermediate CA certificate.

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

The screenshot shows a 'My Certificate' interface with the following sections:

- Authorize CSR** (radio button selected)
- Import Full Certificate Set**
  - Import from PC** (radio button selected)
    - CA Certificate: C:\Users\zhenwan2\Desktop\certs\CA.pem (PEM format). **Browse...** button highlighted with a red box.
    - Certificate: [REDACTED] (PEM format). **Browse...** button.
  - Import from USB Device**
    - USB Device Status: No Device Attached. **Refresh** button.
- Save** and **Cancel** buttons at the bottom.

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: {{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX}}

Microsoft CSP Name: Microsoft Enhanced 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-----

MIIG2jCCBcKgAwIBAgINAjBbMA0GCSqGSIb3DQEBCUAMIGNNQswCQY

.....

MI4iYDx3GLii7gKZOFW4unJvcoOtw0387AMGb//IfNIWqFNpuXtuUq0Esc

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

Bag Attributes

friendlyName: 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/FIUQqNNGqz9lgOgA38corog14=

-----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-----

MIIGNDCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQQ

.....

WZP8P3PXLrQsldiL98I/ydrHIEH9LMF/TtNGCbnkqXBP7dcgqhykguAzx/Q=

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