

# Workround voor uploaden RV32x Series routercertificaat

## Samenvatting

Een digitaal certificaat certificeert de eigendom van een openbare sleutel door het genoemde onderwerp van het certificaat. Dit stelt betrouwbare partijen in staat om afhankelijk te zijn van handtekeningen of beweringen van de privé-sleutel die overeenkomt met de openbare sleutel die gecertificeerd is. Een router kan een zichzelf ondertekend certificaat, een certificaat produceren dat door een netwerkbeheerder wordt gemaakt. Zij kan ook verzoeken aan de certificaatinstanties (CA's) zenden om een digitaal identiteitsbewijs aan te vragen. Het is belangrijk dat er een rechtmatig certificaat is van een verzoek van derden.

Er zijn twee manieren waarop CA de certificaten tekent:

1. CA tekent het certificaat met privé-toetsen.
2. CA tekent de certificaten met CSR die door RV320/RV325 zijn gegenereerd.

RV320 en RV325 ondersteunen alleen .pem-certificaten. In beide gevallen dient u .pem-certificaten te verkrijgen van de certificaatinstantie. Als u een ander formaat certificaat krijgt, moet u het formaat zelf converteren of moet u het .pem formaat certificaat opnieuw aanvragen bij de CA.

De meeste verkopers van handelscertificaten gebruiken intermediaire certificaten. Aangezien het Intermediate Certificate is afgegeven door de Trusted Root CA, erft elk certificaat dat is afgegeven door het Intermediate Certificate het vertrouwen van de Trusted Root, zoals een certificeringsketen van vertrouwen.

In deze handleiding wordt beschreven hoe het certificaat wordt ingevoerd dat door de Intermediate certificaatinstantie is afgegeven op RV320/RV325.

## Datum geïdentificeerd

24 februari 2017

## Datum opgelost

N.v.t.

## Producten getroffen

RV320/RV325	1.1.1.06 en later

# Certificaatsignalering met behulp van privé-toetsen

In dit voorbeeld gaan we ervan uit dat je een RV320.pem van de derde tussenpersoon CA hebt. Het bestand heeft zulke inhoud: privé-toets, certificaat, basiscertificaat CA, intermediair CA-certificaat.

Opmerking: Het verkrijgen van verschillende bestanden van tussenpersoon CA in plaats van slechts één bestand is optioneel. Maar er zijn meer dan vier onderdelen te vinden uit de verschillende bestanden.

Controleer of het CA-certificaatbestand zowel het basiscertificaat als het tussentijdse certificaat bevat. RV320/RV325 vereist het tussentijdse certificaat en het basiscertificaat in een bepaalde volgorde in de CA-bundel, eerst het basiscertificaat en dan het intermediaire certificaat. Ten tweede moet u het RV320/RV325-certificaat en de privé-toets in één bestand combineren.

Opmerking: Elke teksteditor kan worden gebruikt om de bestanden te openen en te bewerken. Het is belangrijk om ervoor te zorgen dat elke extra lege regels, spaties of wagenopbrengsten het plan niet zoals verwacht laten gaan.

## De certificaten combineren

Stap 1. Open de RV320.pem-modus, kopieer het tweede certificaat (basiscertificaat) en het derde certificaat (tussencertificaat) met inbegrip van het begin-/eindbericht.

Opmerking: In dit voorbeeld is de markering van tekst het basiscertificaat.

```
RV320 - Notepad
File Edit Format View Help
Bag Attributes
  localKeyID: 01 00 00 00
  friendlyName: {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX}
  Microsoft CSP Name: Microsoft Enhanced
Cryptographic Provider v1.0
Key Attributes
  X509v3 Key Usage: 10
-----BEGIN PRIVATE KEY-----
MIEVQIBADNABgkqhkiG9w0BAQEFAASCBCkCWJgSjAgEAAoIBAQCjE0q
Te
.....

Sv3RH/fSHuP
+NayfgYHIpXQDcObJF1Lhy0uzD/cgz7f7BdkzC0fqPTEJA90=
-----END PRIVATE KEY-----
Bag Attributes
  localKeyID: 01 00 00 00
  friendlyName: StartCom PFX Certificate
subject=/description=XXXXXXXX/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
.....

M14iYDX3GLii7gKZOFaw4unJvcoOtw0387AMGb//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
.....

Bj6y6koQ0dJQK/w/7HA/lwr
+bMEkXN9P/FlUqqNNGqz9IgoA38corog14=
-----END CERTIFICATE-----
```

Opmerking: In dit voorbeeld is de gemarkeerde string tekst het intermediaire certificaat.

```
RV320 - Notepad
File Edit Format View Help
-----END PRIVATE KEY-----
Bag Attributes
    localkeyID: 01 00 00 00
    friendLiName: 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 S4rver CA
-----BEGIN CERTIFICATE-----
MIIG2jCCBCKgAwIBAgINAgBbMA0GCSqGSIB3DQEBBQUAMIGNNQswCQY
.....

M14iyDX3GLii7gKZOFaw4unJvco0tw0387AMGb//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
.....

Bj6y6koQ0djQK/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-----
MIIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ
.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dCgqhykquA
zx/Q=
-----END CERTIFICATE-----
```

Stap 2. Plakt de inhoud in een nieuw bestand en slaat deze op als CA.pem.

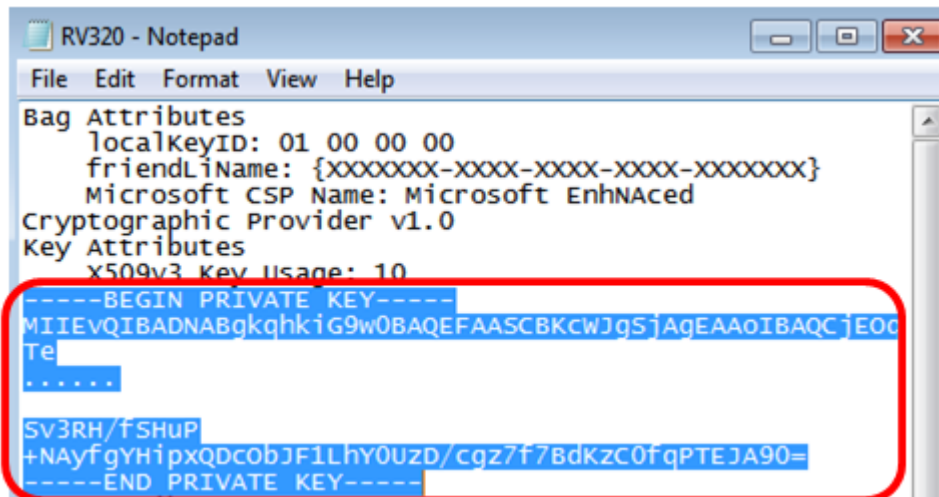
```
CA.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIHytCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ
.....

Bj6y6koQ0djQK/W/7HA/lwr+bMEkXN9P/FlUQqNNGqz9IgOgA38corog14=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ
.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dCgqhykquA
zx/Q=
-----END CERTIFICATE-----
```

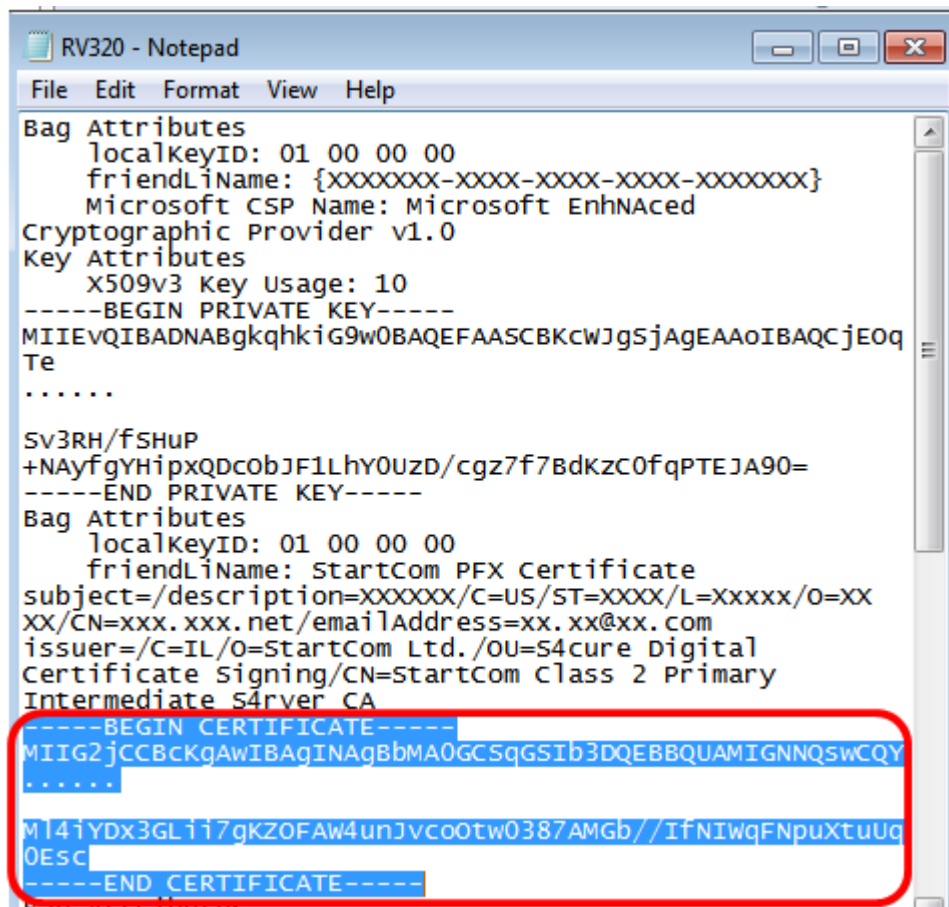
Stap 3. Open de RV320.pem-modus en kopieer de privé-sleutelsectie en het eerste certificaat, inclusief het begin-/eindbericht.

Opmerking: In het onderstaande voorbeeld is de gemarkeerde string tekst de private key Section.



```
RV320 - Notepad
File Edit Format View Help
Bag Attributes
  localKeyID: 01 00 00 00
  friendlyName: {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
+NAYfgyH1pxQDcobJF1Lhy0Uzd/cgz7f7BdkZc0fqPTEJA90=
-----END PRIVATE KEY-----
```

Opmerking: In het onderstaande voorbeeld is de gemarkeerde string tekst het eerste certificaat.



```
RV320 - Notepad
File Edit Format View Help
Bag Attributes
  localKeyID: 01 00 00 00
  friendlyName: {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
+NAYfgyH1pxQDcobJF1Lhy0Uzd/cgz7f7BdkZc0fqPTEJA90=
-----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 S4rver CA
-----BEGIN CERTIFICATE-----
MIIG2jCCBCKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNNQswCQY
.....
M141YDx3GLi17gKZ0FAW4unJvco0tw0387AMGb//IfNIwqFNpuXtuUq
0Esc
-----END CERTIFICATE-----
```

Stap 4. Plakt de inhoud in een nieuw bestand en slaat deze op als cer\_plus\_private.pem

```

cer_plus_private.pem - Notepad
File Edit Format View Help
-----BEGIN PRIVATE KEY-----
MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBCkCWJgSjAgEAAoIBAQCjEOqTe
.....
Sv3RH/fSHuP+NAYfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNNQswCQY
.....
Ml4iYDx3GLii7gKZ0FAW4unJvcoOtw0387AMGb//IfNIWqFNpuXtuUq0Esc
-----END CERTIFICATE-----

```

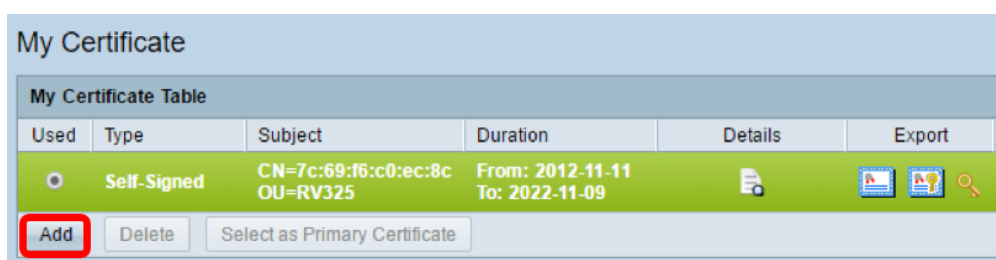
Opmerking: Als de versie van RV320/RV325-firmware lager is dan 1.1.1.06, zorg er dan voor dat er aan het einde van het bestand twee regelfeeds zijn (cer\_plus\_private.pem). In de firmware na 1.1.1.06 hoeft u niet nog twee lijnvelden toe te voegen. In dit voorbeeld wordt een verkorte versie van het certificaat alleen voor demonstratiedoeleinden weergegeven.

### Importeren CA.pem en cer\_plus\_private.pem naar RV320LEAVING /RV325

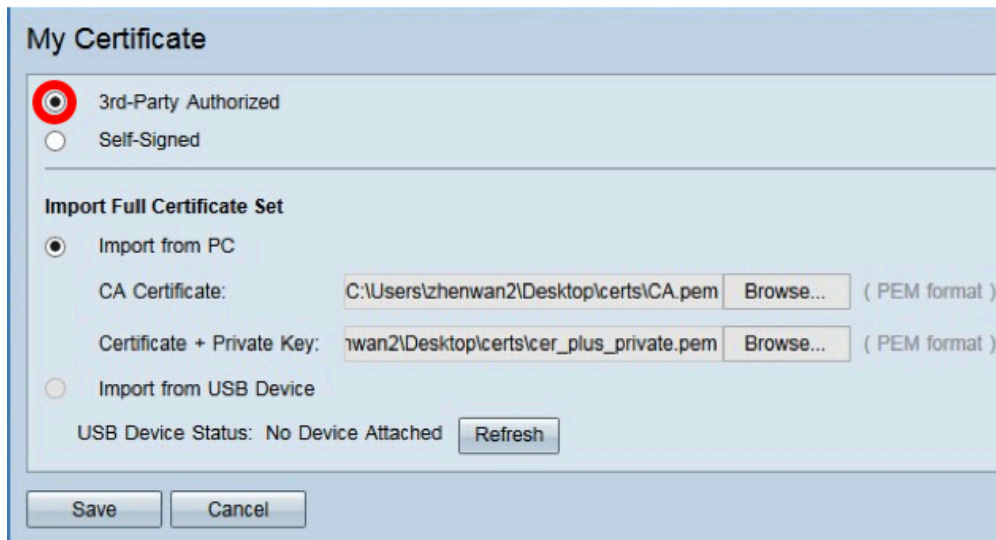
Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van RV320 of RV325 en kies **certificaatbeheer > Mijn certificaat**.



Stap 2. Klik op **Add** om het certificaat te importeren.



Stap 3. Klik op het radioknop *van de derde partij* om het certificaat te importeren.



Stap 4. *Klik* in het gebied dat *het* gehele *certificaat* invoert op een radioknop om de bron van de opgeslagen certificaten te kiezen. De opties zijn:

- *Importeren vanaf een pc* - Kies deze optie als de bestanden op de computer aanwezig zijn.
- *Importeren op USB* - Kies dit om de bestanden te importeren vanuit een flitsstation.

Opmerking: In dit voorbeeld wordt **Importeren vanaf een pc** geselecteerd.



Stap 5. *Klik* in het gebied *CA-certificaat* op **Bladeren...** en plaats de optie CA.pem. bestand.

Opmerking: Als u firmware later dan 1.1.0.6 gebruikt, klikt u op de knop kiezen en zoekt u het gewenste bestand.

**My Certificate**

3rd-Party Authorized  
 Self-Signed

---

**Import Full Certificate Set**

Import from PC

CA Certificate: C:\Users\zhenwan2\Desktop\certs\CA.pem **Browse...** ( PEM format )

Certificate + Private Key: zhenwan2\Desktop\certs\cer\_plus\_private.pem **Browse...** ( PEM format )

Import from USB Device

USB Device Status: No Device Attached **Refresh**

**Save** **Cancel**

Stap 6. Klik in het gebied *Certificaat + Private Key*, op **Bladeren...** en plaats het bestand *cer\_plus\_private.pem*.

Opmerking: Als u firmware later dan 1.1.0.6 gebruikt, klikt u op de knop **kies** en zoekt u het gewenste bestand.

**My Certificate**

3rd-Party Authorized  
 Self-Signed

---

**Import Full Certificate Set**

Import from PC

CA Certificate: C:\Users\zhenwan2\Desktop\certs\CA.pem **Browse...** ( PEM format )

Certificate + Private Key: zhenwan2\Desktop\certs\cer\_plus\_private.pem **Browse...** ( PEM format )

Import from USB Device

USB Device Status: No Device Attached **Refresh**

**Save** **Cancel**

Stap 7. Klik op **Opslaan**.

**My Certificate**

3rd-Party Authorized  
 Self-Signed

---

**Import Full Certificate Set**

Import from PC

CA Certificate: C:\Users\zhenwan2\Desktop\certs\CA.pem **Browse...** ( PEM format )

Certificate + Private Key: zhenwan2\Desktop\certs\cer\_plus\_private.pem **Browse...** ( PEM format )

Import from USB Device

USB Device Status: No Device Attached **Refresh**

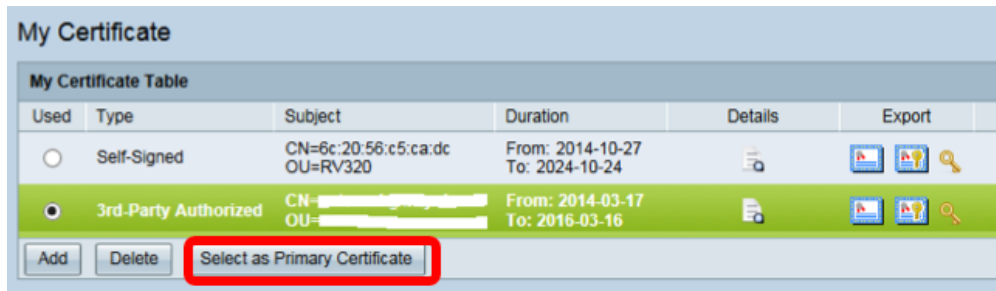
**Save** **Cancel**

De certificaten worden met succes ingevoerd. Het kan nu worden gebruikt voor HTTPS-



toegang, SSL VPN of IPsec VPN.

Stap 8. (optioneel) Klik om het certificaat voor HTTPS of SSL VPN te gebruiken op de radioknop van het certificaat en klik op de knop **Selecteren als Primair certificaat**.

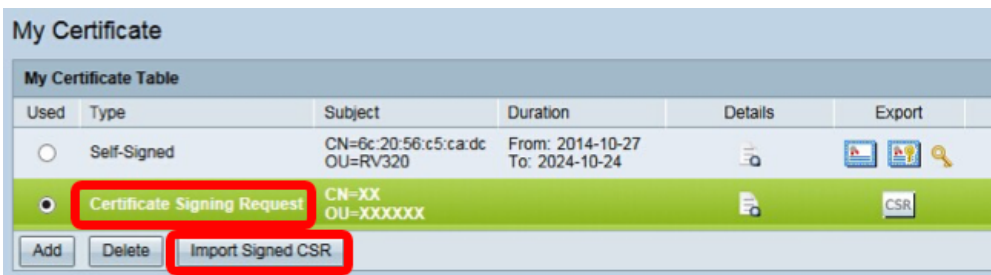


U hebt nu een certificaat geïmporteerd.

## Certificaatsignalering met CSR

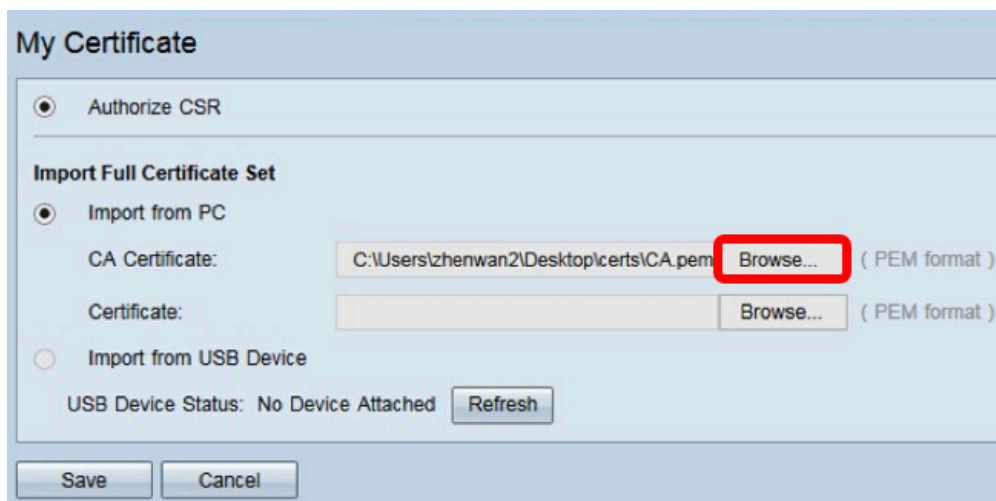
Stap 1. Generate een certificaataanvraag (CSR) op RV320/RV325. Klik [hier](#) om te leren hoe een CSR te genereren.

Stap 2. Als u het certificaat wilt importeren, kiest u **certificaataanvraag** en vervolgens klikt u op **Ondertekend CSR**.

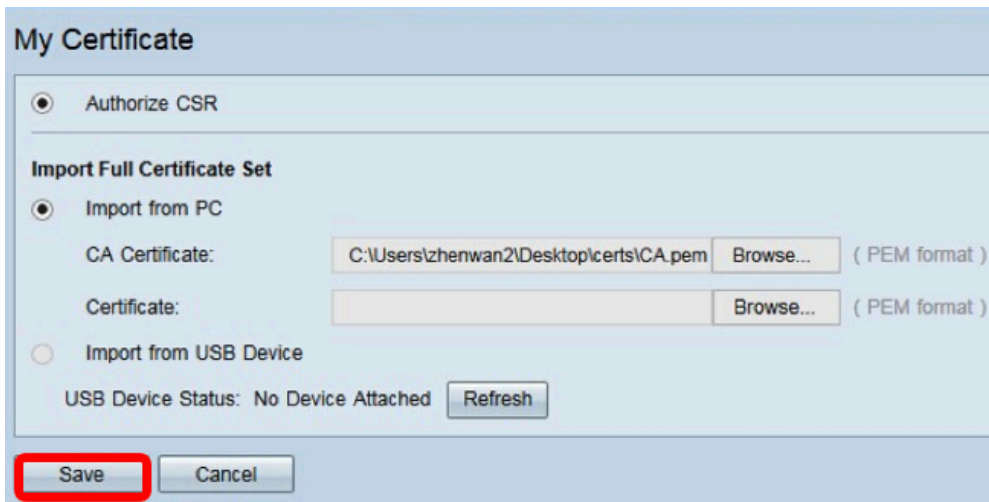


Stap 3. Klik op **Bladeren...** en kies het CA-certificaatbestand. Dit bevat de basis CA + tussenpersoon CA certificaat.

Opmerking: In dit voorbeeld is geen privé-toets vereist aangezien het certificaat gegenereerd wordt met CSR.



Stap 4. Klik op **Opslaan**.



U moet nu met succes een certificaat hebben geüpload met behulp van de CSR.

### Bijlage:

Inhoud van RV320.pem

Bag-kenmerken

LocalKeyID: 01 00 00 00

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

Microsoft CSP-naam: Microsoft EnhNA-technologie voor cryptografische providers v1.0

Belangrijkste kenmerken

Gebruik van de X509v3-toets: 10

—BEGIN PARTICULIERE SLEUTEL—

MIIEvQIBADNABGkqhkiG9w0BAQEFAASCBCcWJgSjAgEAAIBAQCjEOQTe

.....

Sv3RH/fSHuP+NAYfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=

—EINDPRIVÉ-SLEUTEL—

Bag-kenmerken

LocalKeyID: 01 00 00 00

vriendLiName: StartCom PFX-certificaat

onderwerp=/beschrijving=XXXX/C=US/ST=XXXX/L=Xxxxx/O=XX/CN=xxx.xxx.net/emailAddress=xx.xx@xx.com

emittent=/c=IL/O=StartCom Ltd./OU=S4genezing Digitaal certificaat Signing/CN=StartCom Klasse 2 Primair Intermediate S4rver CA

—BEGIN CERTIFICAAT—

MIIG2JCBcKgAwIBAgINAgBbMA0GCSqGSIlb3DQEBBQUAMIGNQswCQY

.....

MI4iYDx3GLii7gKZOF4W4unJvcoOtw0387AMGb/ifNIWqFNpuXtuUQ0ESC

—EINDCERTIFICAAT—

Bag-kenmerken

vriendLiName: StartCom-certificeringsinstantie

onderwerp=/C=IL/O=StartCom Ltd./OU=S4genezing Digitaal certificaat  
Signalering/CN=StartCom Certificeringsinstantie

emittent=/c=IL/O=StartCom Ltd./OU=S4genezing Digitaal certificaat  
Signalering/CN=StartCom Certificeringsinstantie

—BEGIN CERTIFICAAT—

MIIHyTCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

.....

Bj6y6koQOdjQK/W/7HA/lwr+bMEkXN9P/FIUQQNNGqz9lgOgA38corog14=

—EINDCERTIFICAAT—

Bag-kenmerken

onderwerp=/C=IL/O=StartCom Ltd./OU=S4genezing Digitaal certificaat  
Signing/CN=StartCom Klasse 2 Primair Intermediate S4rver CA

emittent=/c=IL/O=StartCom Ltd./OU=S4genezing Digitaal certificaat  
Signalering/CN=StartCom Certificeringsinstantie

—BEGIN CERTIFICAAT—

MIIGNDygAwIBAgIBGNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dgcgqhykg uAzx/Q=

—EINDCERTIFICAAT—