

Problemumgehung für das Hochladen des Zertifikats für den Router der Serie RV32x

Zusammenfassung

Ein digitales Zertifikat bescheinigt das Eigentum an einem öffentlichen Schlüssel durch den benannten Subjekt des Zertifikats. Dadurch können sich die Parteien auf Signaturen oder Behauptungen des privaten Schlüssels verlassen, der dem öffentlichen Schlüssel entspricht, der zertifiziert ist. Ein Router kann ein selbstsigniertes Zertifikat generieren, ein Zertifikat, das von einem Netzwerkadministrator erstellt wurde. Sie kann auch Anfragen an Zertifizierungsstellen (Certificate Authority, CA) senden, um ein digitales Identitätszertifikat zu beantragen. Es ist wichtig, legitime Zertifikate von Drittanbieteranwendungen zu erhalten.

CA signiert die Zertifikate auf zwei Arten:

1. CA signiert das Zertifikat mit privaten Schlüssel.
2. CA signiert die Zertifikate mithilfe der von RV320/RV325 generierten CSR.

RV320 und RV325 unterstützen nur Zertifikate im .pem-Format. In beiden Fällen sollten Sie Zertifikate im .pem-Format von der Zertifizierungsstelle erhalten. Wenn Sie ein anderes Formatzertifikat erhalten, müssen Sie das Format selbst konvertieren oder das .pem-Zertifikat erneut von der CA anfordern.

Die meisten Anbieter von gewerblichen Zertifikaten verwenden Zwischenzertifikate. Da das Zwischenzertifikat von der Vertrauenswürdigen Stammzertifizierungsstelle ausgestellt wird, erbt jede vom Zwischenzertifikat ausgestellte Bescheinigung wie eine Vertrauenszertifizierungskette das Vertrauen der vertrauenswürdigen Stamm.

In diesem Handbuch wird beschrieben, wie die von der Zertifizierungsstelle für Zwischenzertifikate ausgestellte Bescheinigung RV320/RV325 importiert wird.

Identifiziertes Datum

24. Februar 2017

Auflösungsdatum

K/A

Betroffene Produkte

RV320/RV325	1.1.1.06 und höher

Zertifikatssignierung mit privaten Schlüsseln

In diesem Beispiel gehen wir davon aus, dass Sie eine RV320.pem von der zwischengeschalteten CA des Drittanbieters erhalten haben. Die Datei enthält folgende Inhalte: Private Key, Zertifikat, Root CA Zertifikat, Zwischenzertifikat CA Zertifikat.

Hinweis: Das Abrufen mehrerer Dateien von einer zwischengeschalteten CA anstelle nur einer Datei ist optional. Sie finden jedoch über vier Teile aus den verschiedenen Dateien.

Überprüfen Sie, ob die Zertifizierungsstellenzertifikatdatei sowohl das Stammzertifikat der Zertifizierungsstelle als auch das Zwischenzertifikat enthält. RV320/RV325 erfordert das Zwischenzertifikat und das Root-Zertifikat in einer bestimmten Reihenfolge im CA-Bündel, zuerst das Root-Zertifikat und dann das Zwischenzertifikat. Zweitens müssen Sie das RV320/RV325-Zertifikat und den privaten Schlüssel in einer Datei kombinieren.

Hinweis: Jeder Texteditor kann zum Öffnen und Bearbeiten der Dateien verwendet werden. Es ist wichtig sicherzustellen, dass zusätzliche Leerzeilen, Leerzeichen oder Wagenrücksendungen den Plan nicht wie erwartet ablaufen lassen.

Kombinieren der Zertifikate

Schritt 1: Öffnen Sie die Datei RV320.pem, kopieren Sie das zweite Zertifikat (Stammzertifikat) und das dritte Zertifikat (Zwischenzertifikat) einschließlich der Start-/Endnachricht.

Hinweis: In diesem Beispiel ist die Hervorhebungszeichenfolge von Text das Stammzertifikat.

```
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-----
MIEVQIBADNABgkqhkiG9w0BAQEFAASCBCkCWJgSjAgEAAoIBAQCjEOq
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=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
.....

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-----
```

Hinweis: In diesem Beispiel ist die hervorgehobene Textzeichenfolge das Zwischenzertifikat.

```
RV320 - Notepad
File Edit Format View Help
-----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
.....

M14iyDX3GLii7gKZOFaw4unJvco0tw0387AMGb//IfNIWqFNpuxtuUq
OEsc
-----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/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-----
```

Schritt 2: Fügen Sie den Inhalt in eine neue Datei ein, und speichern Sie ihn 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-----
```

Schritt 3: Öffnen Sie die Datei RV320.pem, und kopieren Sie den Abschnitt für den privaten Schlüssel sowie das erste Zertifikat, einschließlich der Start-/Endnachricht.

Hinweis: Im Beispiel unten ist die hervorgehobene Zeichenfolge der private Key-Bereich.

```
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-----
MIIEVQIBADNABgkqhkiG9w0BAQEFAASCBCwJgSjAgEAAoIBAQCjEOQ
Te
.....
SV3RH/fSHuP
+NAYfgyHipxQDCobJF1Lhy0UzD/cgz7f7BdkZc0fqPTEJA90=
-----END PRIVATE KEY-----
```

Hinweis: Im Beispiel unten ist die hervorgehobene Textzeichenfolge das erste Zertifikat.

```
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-----
MIIEVQIBADNABgkqhkiG9w0BAQEFAASCBCwJgSjAgEAAoIBAQCjEOQ
Te
.....
SV3RH/fSHuP
+NAYfgyHipxQDCobJF1Lhy0UzD/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
.....
M141YDx3GL117gKZ0FAW4unJVco0tw0387AMGb//IfNIwqFNpuXtuUq
0Esc
-----END CERTIFICATE-----
```

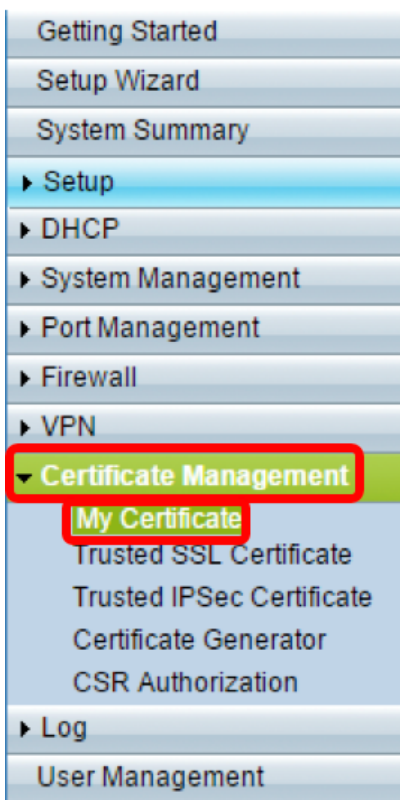
Schritt 4: Fügen Sie den Inhalt in eine neue Datei ein, und speichern Sie ihn als cer_plus_private.pem.

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBCkCWJgSjAgEAAoIBAQCjEOqTe
.....
Sv3RH/fSHuP+NAYfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNNQswCQY
.....
Ml4iYDx3GLii7gKZOFAW4unJvcoOtw0387AMGb//IfNIWqFNpuXtuUq0Esc
-----END CERTIFICATE-----
```

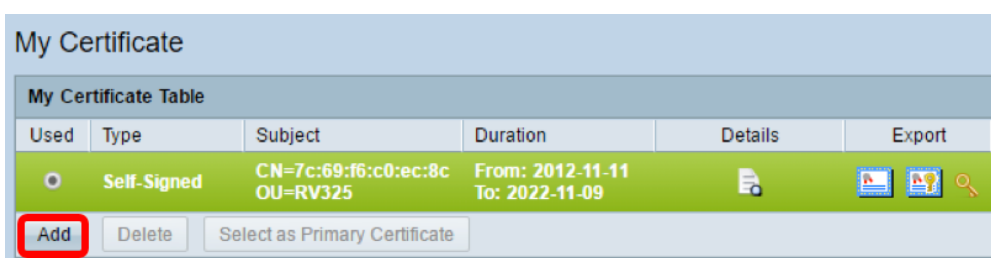
Hinweis: Wenn die Firmware-Version RV320/RV325 unter 1.1.1.06 liegt, stellen Sie sicher, dass am Ende der Datei zwei Line-Feeds vorhanden sind (cer_plus_private.pem). In der Firmware nach 1.1.1.06 müssen Sie nicht zwei weitere Line-Feeds hinzufügen. In diesem Beispiel wird eine verkürzte Version des Zertifikats nur zu Demonstrationszwecken angezeigt.

Importieren CA.pem und cer_plus_private.pem in RV320/RV325

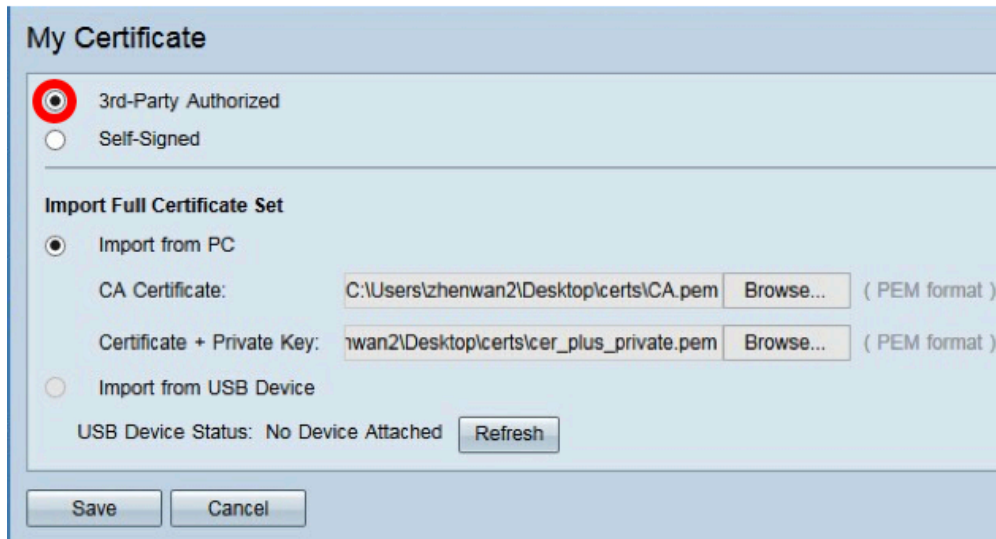
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des RV320 oder RV325 an, und wählen Sie **Certificate Management > My Certificate** aus.



Schritt 2: Klicken Sie auf **Hinzufügen**, um das Zertifikat zu importieren.



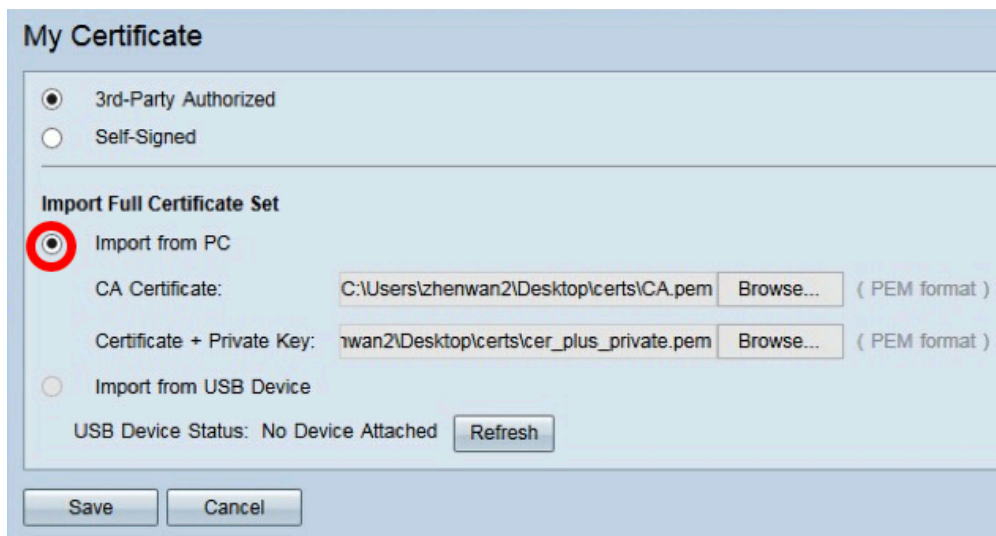
Schritt 3: Klicken Sie auf das Optionsfeld *Autorisierte Drittanbieter*, um das Zertifikat zu importieren.



Schritt 4: Klicken Sie im Bereich *Vollständigen Zertifikatssatz importieren* auf ein Optionsfeld, um die Quelle der gespeicherten Zertifikate auszuwählen. Folgende Optionen stehen zur Verfügung:

- *Importieren von PC*: Wählen Sie diese Option aus, wenn die Dateien auf dem Computer gefunden werden.
- *Importieren aus USB* - Wählen Sie diese Option, um die Dateien von einem Flash-Laufwerk zu importieren.

Hinweis: In diesem Beispiel wird **Import von PC** ausgewählt.



Schritt 5: Klicken Sie im Bereich *CA Certificate* auf **Browse...** und suchen Sie die Datei CA.pem. Datei.

Hinweis: Wenn Sie die Firmware nach 1.1.0.6 ausführen, klicken Sie auf die Schaltfläche *Auswählen*, und suchen Sie die gewünschte Datei.

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**

Schritt 6: Klicken Sie im Bereich *Zertifikat + Privater Schlüssel* auf **Durchsuchen...** und suchen Sie die Datei "er_plus_private.pem".

Hinweis: Wenn Sie die Firmware nach 1.1.0.6 ausführen, klicken Sie auf die Schaltfläche **Auswählen**, und suchen Sie die gewünschte Datei.

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**

Schritt 7: Klicken Sie auf **Speichern**.

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

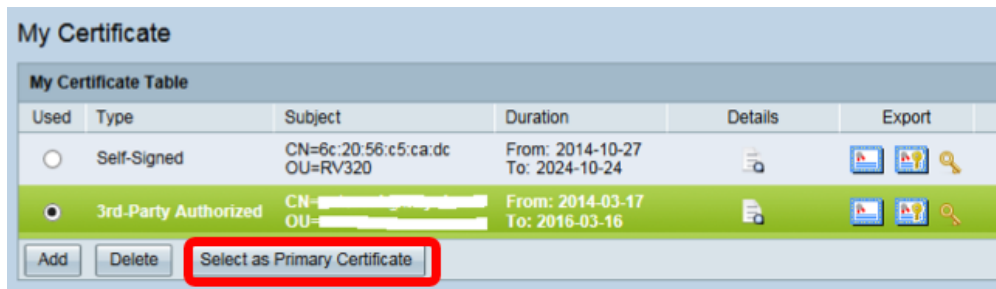
USB Device Status: No Device Attached **Refresh**

Save **Cancel**

Die Zertifikate werden erfolgreich importiert. Sie kann jetzt für HTTPS-Zugriff, SSL VPN oder

IPSec VPN verwendet werden.

Schritt 8: (Optional) Um das Zertifikat für HTTPS oder SSL VPN zu verwenden, klicken Sie auf das Optionsfeld des Zertifikats, und klicken Sie auf die Schaltfläche **Als primäres Zertifikat auswählen**.

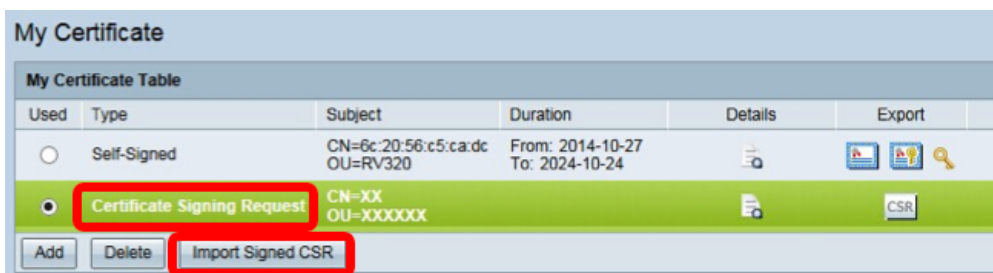


Sie sollten jetzt ein Zertifikat erfolgreich importiert haben.

Zertifikatssignierung mit CSR

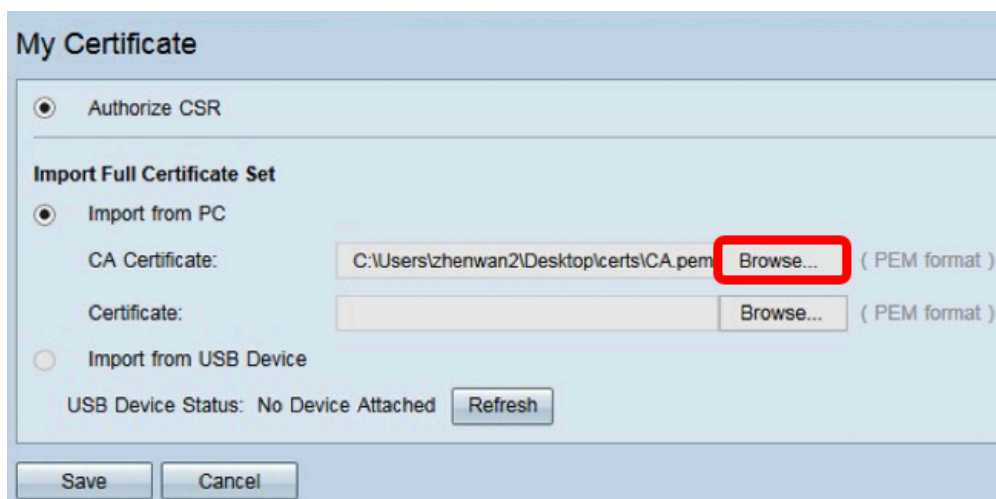
Schritt 1: Erstellen Sie eine CSR-Anfrage (Certificate Signing Request) für RV320/RV325. Um zu erfahren, wie Sie eine CSR-Anfrage erstellen, klicken Sie [hier](#).

Schritt 2: Um das Zertifikat zu importieren, wählen Sie **Zertifikatssignierungsanfrage** und klicken Sie auf **Signierten CSR importieren**.



Schritt 3: Klicken Sie auf **Durchsuchen..** und wählen Sie die Zertifizierungsstellen-Zertifikatsdatei aus. Diese enthält das Stammzertifikat der CA + Zwischenzertifikat der Zertifizierungsstelle.

Hinweis: In diesem Beispiel ist kein privater Schlüssel erforderlich, da das Zertifikat mit CSR generiert wird.



Schritt 4: Klicken Sie auf **Speichern**.

My Certificate

Authorize CSR

Import Full Certificate Set

Import from PC

CA Certificate: (PEM format)

Certificate: (PEM format)

Import from USB Device

USB Device Status: No Device Attached

Sie sollten jetzt ein Zertifikat erfolgreich mithilfe der CSR hochgeladen haben.

Anhang:

Inhalt von RV320.pem

Bag-Attribute

localKeyID: 01 00 00 00

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

Microsoft CSP-Name: Microsoft Enhanced Cryptographic Provider v1.0

Wichtigste Attribute

X509v3-Schlüsselverwendung: 10

—PRIVATER SCHLÜSSEL BEGINNEN—

MIIEvQIBADNABGkqhkiG9w0BAQEFAASCBCkCWJgSjAgEoIBAQCjEOqTe

.....

Sv3RH/fSHuP+NAYfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=

—PRIVATER ENDSCHLÜSSEL—

Bag-Attribute

localKeyID: 01 00 00 00

friendlyName: StartCom PFX-Zertifikat

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

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

—BEGINNUNGSBESCHEINIGUNG—

MIIG2jCCBcKgAwIBAgINAqBbMA0GCSqGSIb3DQEEBQUAMIGNQswCQY

.....

MI4iYDx3GLii7gKZOF4W4unJvcoOtw0387AMGb/IfNIWqFNpuXtuUq0ESC

—ENDBESCHEINIGUNG—

Bag-Attribute

friendLiName: Zertifizierungsstelle StartCom

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

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

—BEGINNUNGSBESCHEINIGUNG—

MIHyTCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

.....

Bj6y6koQOdjQK/W/7HA/lwr+bMEkXN9P/FIUQNGqz9lgOgA38corog14=

—ENDBESCHEINIGUNG—

Bag-Attribute

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

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

—BEGINNUNGSBESCHEINIGUNG—

MIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dcdgqhykguAzx/Q=

—ENDBESCHEINIGUNG—