RV32xシリーズルータ証明書のアップロードの 回避策

要約

デジタル証明書は、証明書の名前付きサブジェクトによって公開キーの所有権を証明します 。これにより、証明書利用者は、認証された公開キーに対応する秘密キーによる署名やアサ ーションに依存できます。ルータは、自己署名証明書、つまりネットワーク管理者によって 作成された証明書を生成できます。また、認証局(CA)に要求を送信して、デジタルID証明書 を申請することもできます。サードパーティアプリケーションから正当な証明書を取得する ことが重要です。

CAが証明書に署名する方法は2つあります。

1. CAは秘密キーを使用して証明書に署名します。

2. CAは、RV320/RV325によって生成されたCSRを使用して証明書に署名します。

RV320およびRV325は、.pem形式の証明書のみをサポートします。どちらの場合も、認証 局から.pem形式の証明書を取得する必要があります。他の形式の証明書を取得した場合は 、自分で形式を変換するか、CAから.pem形式の証明書を再度要求する必要があります。

ほとんどの商用の証明書ベンダーは中間証明書を使用します。 中間証明書が信頼ルート CAによって発行されると、中間証明書によって発行された証明書は、信頼の証明書チェー ンのように、信頼ルートの信頼を継承します。

このガイドでは、RV320/RV325の中間認証局(CA)によって発行された証明書をインポート する方法について説明します。

指定日

2017年2月24日

解決日

N/A

影響を受ける製品

RV320/RV325	1.1.1.06 以降

秘密キーを使用した証明書署名

この例では、サードパーティ中間CAからRV320.pemを取得したと仮定します。ファイルに は次のような内容が含まれています。秘密キー、証明書、ルートCA証明書、中間CA証明書 。

注:1つのファイルではなく、中間CAから複数のファイルを取得することはオプションです 。しかし、複数のファイルから上の4つの部分を見つけることができます。

CA証明書ファイルにルートCA証明書と中間証明書の両方が含まれているかどうかを確認し ます。RV320/RV325では、CAバンドル内の特定の順序で中間証明書とルート証明書が必要 です。ルート証明書が最初に、中間証明書が次に必要です。次に、RV320/RV325証明書と 秘密キーを1つのファイルに結合する必要があります。

注:任意のテキストエディタを使用して、ファイルを開いて編集できます。余分な空白行、 スペース、またはキャリッジリターンが計画を期待どおりに実行しないようにすることが重 要です。

証明書の結合

ステップ1:RV320.pemを開き、2番目の証明書(ルート証明書)と3番目の証明書(中間証 明書)をコピーし、開始/終了メッセージを含めます。

注:この例では、強調表示されているテキスト文字列がルート証明書です。



注:この例では、強調表示されているテキスト文字列が中間証明書です。



ステップ2:コンテンツを新しいファイルに貼り付け、CA.pemとして保存します。

	IDUIT DEBUTO		
CA.pem - Notepad File Edit Format View H	łelp	-	
BEGIN CERTIFICATE MIIHyTCCBbGgAwIBAgI 	g IBATNABgkqhkiG9w0BAQUFADB9MQsw0	QYDVQ	
Bj6y6koQOdjQK/W/7H END CERTIFICATE BEGIN CERTIFICATE	A/lwr+bMEkXN9P/FlUQqNNGqz9IgOgA3 }	8corog14	=
MIIGNDCCBBygAwIBAg	IBGjNABgkqhkiG9w0BAQUFADB9MQsw0	QYDVQQ	
WZP8P3PXLrQsldiL98l/	/ydrHIEH9LMF/TtNGCbnkqXBP7dcgqhyl 	kguAzx/Q	=

ステップ3:RV320.pemを開き、秘密キーセクションと最初の証明書(開始/終了メッセージを含む)をコピーします。

注:次の例では、強調表示されているテキスト文字列が秘密キーのセクションです。

RV320 - Notepad	
File Edit Format View Help	
Bag Attributes localKeyID: 01 00 00 00 friendLiName: {XXXXXX-XXXX-XXXX-XXXX-XXXX Microsoft CSP Name: Microsoft EnhNAced Cryptographic Provider v1.0 Key Attributes X509V3 Key Usage: 10	xxxx}
BEGIN PRIVATE KEY MIIEVQIBADNABgkqhkiG9w0BAQEFAASCBKcWJgSjAgEAA Te 	DIBAQCJEOC
Sv3RH/fSHuP +NAyfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJ END PRIVATE KEY	490=

注:次の例では、強調表示されたテキスト文字列が最初の証明書です。



ステップ4:コンテンツを新しいファイルに貼り付け、cer_plus_private.pemという名前で保存します

cer_plus_private.pem - Notepad

File Edit Format View Help

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

MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBKcWJgSjAgEAAoIBAQCjEOqTeprotection and the second statement of the

•••••

Sv3RH/fSHuP+NAyfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90= -----END PRIVATE KEY-----

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

MIIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNNQswCQY

Ml4iYDx3GLii7gKZ0FAW4unJvco0tw0387AMGb//IfNIWqFNpuXtuUq0Esc

注:RV320/RV325ファームウェアのバージョンが1.1.1.06より前の場合は、ファイルの末尾 に2行のフィード(cer_plus_private.pem)があることを確認してください。 1.1.1.06以降のフ ァームウェアでは、さらに2つの回線フィードを追加する必要はありません。この例では、 証明書の短縮バージョンがデモ目的でのみ表示されます。

インポート CA.pem と cer_plus_private.pem RV320に接続/RV325

ステップ1:RV320またはRV325のWebベースのユーティリティにログインし、[**Certificate Management] > [My Certificate]を選択します**。



ステップ2:[Add]をクリックして証明書をインポートします。

My Ce	ertificate				
My Cer	rtificate Table				
Used	Туре	Subject	Duration	Details	Export
•	Self-Signed	CN=7c:69:f6:c0:ec:8c OU=RV325	From: 2012-11-11 To: 2022-11-09	2	<u> </u>
Add	Delete Se	lect as Primary Certificate			

ステップ3:[*Rd-Party Authorized*]オプションボタンをクリックして、証明書をインポートし

ます。

1	Му С	Certificate			
	0	3rd-Party Authorized Self-Signed			
	Imp	ort Full Certificate Set			
	۲	Import from PC			
		CA Certificate:	C:\Users\zhenwan2\Desktop\certs\CA.pem	Browse] (PEM format)
		Certificate + Private Key:	wan2\Desktop\certs\cer_plus_private.pem	Browse	(PEM format)
		Import from USB Device			
	ι	USB Device Status: No Dev	ice Attached Refresh		
	S	Cancel			

ステップ4:[Import Full Certificate Set(完全な証明書セットのインポート)]領域で、オプショ ンボタンをクリックして、保存した証明書のソースを選択します。次のオプションがありま す。

- ●*PCからインポート*:ファイルがコンピュータで見つかった場合は、これを選択します。
- Import from USB: フラッシュドライブからファイルをインポートする場合に選択します。
 - 注:この例では、[Import from PC]が選択されています。

My C	Certificate			
۲	3rd-Party Authorized			
	Self-Signed			
Imp	ort Full Certificate Set			
0	Import from PC			
	CA Certificate:	C:\Users\zhenwan2\Desktop\certs\CA.pem	Browse] (PEM format)
	Certificate + Private Key:	nwan2\Desktop\certs\cer_plus_private.pem	Browse	(PEM format)
0	Import from USB Device			
L	USB Device Status: No Dev	ice Attached Refresh		
S	Cancel			

ステップ5:[CA Certificate]領*域で[***Browse**...]をクリックして、CA.pemを探します。出力を提供してください。

注:1.1.0.6以降のファームウェアを実行している場合は、選択ボタンをクリックして必要な ファイルを探します。

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:	nwan2\Desktop\certs\cer_plus_private.pem	Browse (PEM format)
Import from USB Device USB Device Status: No Dev	ice Attached Refresh	
Save Cancel		

ステップ6:[*Certificate + Private Key*]領*域で、[***Browse...]をクリック**し、 er_plus_private.pemファイルを見つけます。

注:1.1.0.6以降のファームウェアを実行している場合は、選択ボタンをクリックして必要なファイルを探します。

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: <a href="http://www.www.www.www.www.www.www.www.www.w</td>
Save Cancel	

ステップ7:[Save]をクリ**ックします**。

۲	3rd-Party Authorized			
0	Self-Signed			
Imp	ort Full Certificate Set			
۲	Import from PC			
	CA Certificate:	C:\Users\zhenwan2\Desktop\certs\CA.pem	Browse	(PEM format)
	Certificate + Private Key:	wan2\Desktop\certs\cer_plus_private.pem	Browse	(PEM format)
	Import from USB Device			
	ISB Device Status: No Dev	ice Attached Refresh		

証明書が正常にインポートされます。HTTPSアクセス、SSL VPN、またはIPSec VPNに使

用できるようになりました。

ステップ8:(オプション)HTTPSまたはSSL VPN用の証明書を使用するには、証明書のオ プションボタンをクリックし、[Select as Primary Certificate]ボタンをクリックします。

My Certificate							
My Cer	My Certificate Table						
Used	Туре	Subject	Duration	Details	Export		
0	Self-Signed	CN=6c:20:56:c5:ca:dc OU=RV320	From: 2014-10-27 To: 2024-10-24		🖭 🔮 🔍		
•	3rd-Party Authorized	CN-	From: 2014-03-17 To: 2016-03-16	B	P P 9		
Add	Add Delete Select as Primary Certificate						

これで、証明書が正常にインポートされました。

CSRを使用した証明書署名

ステップ1:RV320/RV325で証明書署名要求(CSR)を生成します。CSRの生成方法について は、ここをクリックし<u>てください</u>。

ステップ2:証明書をインポートするには、[Certificate Signing Request]を選択**し、[Import** Signed CSR]をクリ**ックします**。

My Ce	y Certificate				
My Cer	tificate Table				
Used	Туре	Subject	Duration	Details	Export
0	Self-Signed	CN=6c:20:56:c5:ca:dc OU=RV320	From: 2014-10-27 To: 2024-10-24		P 19 9
•	Certificate Signing Request	CN=XX OU=XXXXXXX		6	CSR
Add	Delete Import Signed CS	SR			

ステップ3:[**Browse...]をクリック**し、CA証明書ファイルを選択します。これには、ルート CA +中間CA証明書が含まれます。

注:この例では、CSRを使用して証明書が生成されるため、秘密キーは必要ありません。

Authorize CSR			
Import Full Certificate Set			
Import from PC			
CA Certificate:	C:\Users\zhenwan2\Desktop\certs\CA.pem	Browse	(PEM format
Certificate:		Browse	(PEM format
Import from USB Dev	vice		
USB Device Status: No	Device Attached Refresh		
oob bevice claus. In			

ステップ4:[Save]をクリ**ックします**。

My Certificate				
۲	Authorize CSR			
Imp	ort Full Certificate Set			
۲	Import from PC			
	CA Certificate:	C:\Users\zhenwan2\Desktop\certs\CA.pem	Browse] (PEM format)
	Certificate:		Browse	(PEM format)
Import from USB Device				
1	USB Device Status: No Device	ce Attached Refresh		
S	Save Cancel			

これで、CSRを使用して証明書を正常にアップロードできました。

付録:

RV320.pemの内容

バッグの属性

localKeyID:01 00 00 00

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

Microsoft CSP名: Microsoft Enhanced Cryptographic Provider v1.0

キー属性

X509v3キーの使用法:10

-BEGIN PRIVATE KEY-

MIIEvQIBADNABgkqhkiG9w0BAQEFAASBKcWJgSjAgEAAoIBAQCjEOqTe

••••

Sv3RH/fSHuP+NAyfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0PTEJA90=

- 秘密キーの終了 -

バッグの属性

localKeyID:01 00 00 00

friendLiName:StartCom PFX証明書

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-----

MIIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBBQUAMIGNQswCQY

....

MI4iYDx3GLii7gKZOFAW4unJvcoOtw0387AMGb//IfNIWqFNpuXtuUq0Esc

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

バッグの属性

friendLiName:StartCom認証局

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-----

MIIHyTCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

....

Bj6y6koQOdjQK/W/7HA/lwr+bMEkXN9P/FIUQqNNGqz9IgOgA38corog14=

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

バッグの属性

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 Digital Certificate Signing/CN=StartCom Certification Authority

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

MIIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQQ

....

WZP8P3PXLrQsIdiL98I/ydrHIEH9LMF/TtNGCbnkqXBP7dcgqhykguAzx/Q=

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