Solução alternativa para upload do certificado do roteador RV32x Series

Summary

Um certificado digital certifica a propriedade de uma chave pública pelo assunto nomeado do certificado. Isso permite que as partes confiáveis dependam de assinaturas ou asserções feitas pela chave privada que corresponda à chave pública certificada. Um roteador pode gerar um certificado autoassinado, um certificado criado por um administrador de rede. Pode também enviar pedidos às Autoridades de Certificação (AC) para solicitarem um certificado de identidade digital. É importante ter certificados legítimos de aplicativos de terceiros.

Há duas maneiras de CA assinar os certificados:

1. CA assina o certificado com chaves privadas.

2. CA assina os certificados usando CSR gerado pelo RV320/RV325.

O RV320 e o RV325 suportam somente certificados no formato .pem. Para ambos os casos, você deve obter certificados de formato .pem da autoridade de certificação. Se você receber outro certificado de formato, precisará converter o formato sozinho ou solicitar novamente o certificado de formato .pem da CA.

A maioria dos fornecedores de certificados comerciais usa certificados intermediários. Como o certificado intermediário é emitido pela CA raiz confiável, qualquer certificado emitido pelo certificado intermediário herda a confiança da raiz confiável, como uma cadeia de certificação de confiança.

Este guia descreve como importar o certificado emitido pela Autoridade de Certificação Intermediária no RV320/RV325.

Data de identificação

24 de fevereiro de 2017

Data de resolução

N/A

Produtos afetados

RV320/RV325	1.1.1.06 e posterior

Assinatura de certificado usando chaves privadas

Neste exemplo, presumimos que você recebeu um RV320.pem da CA intermediária de terceiros. O arquivo tem esse conteúdo: chave privada, certificado, certificado CA raiz, certificado CA intermediário.

Note: A obtenção de vários arquivos da CA intermediária em vez de apenas um arquivo é opcional. Mas você pode encontrar mais de quatro partes dos vários arquivos.

Verifique se o arquivo de certificado CA contém o certificado CA raiz e o certificado intermediário. O RV320/RV325 exige o certificado intermediário e o certificado raiz em uma determinada ordem no pacote CA, primeiro o certificado raiz e depois o certificado intermediário. Em segundo lugar, você precisa combinar o certificado RV320/RV325 e a chave privada em um arquivo.

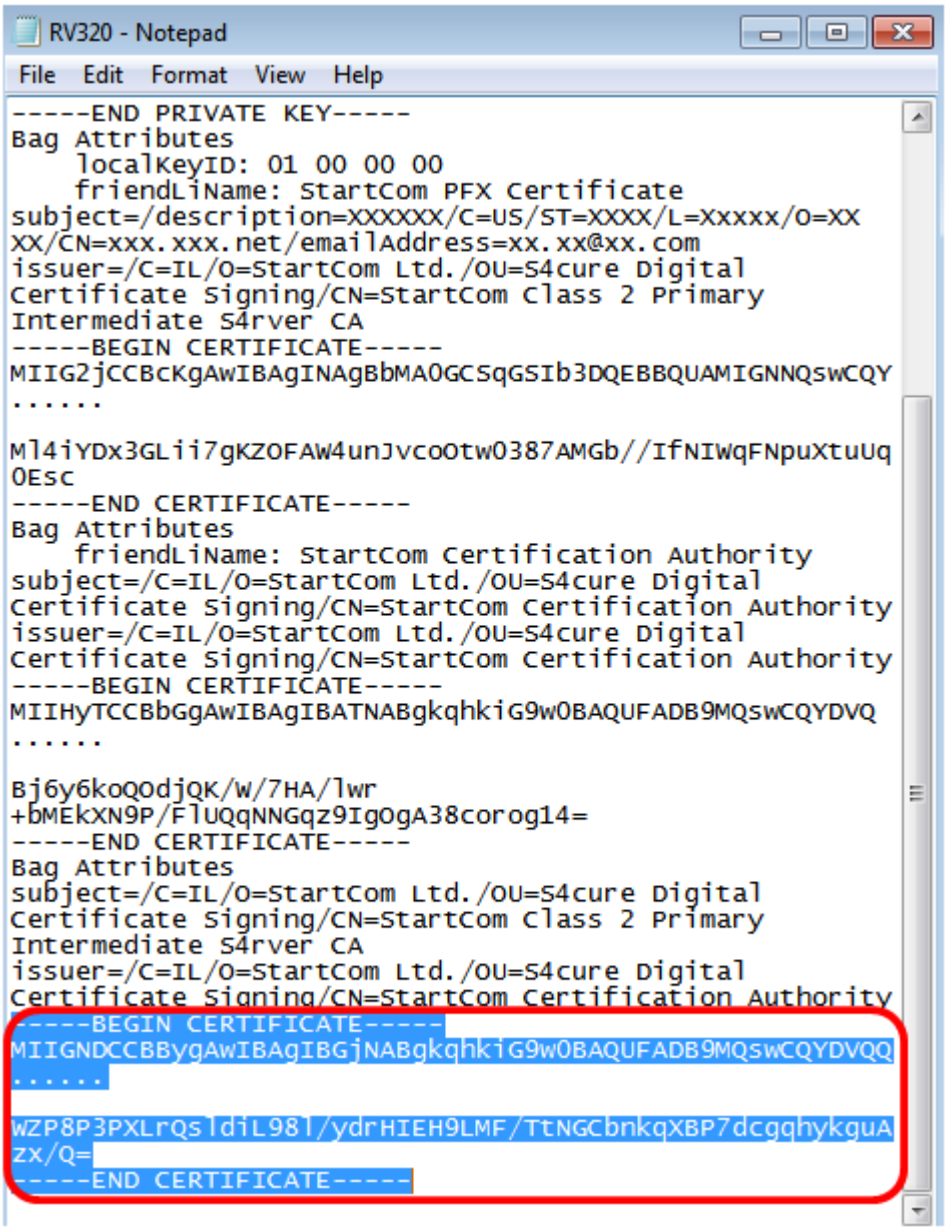
Note: Qualquer editor de texto pode ser usado para abrir e editar os arquivos. É importante certificar-se de que quaisquer linhas, espaços ou devoluções extras em branco não farão com que o plano vá conforme esperado.

Combinando os certificados

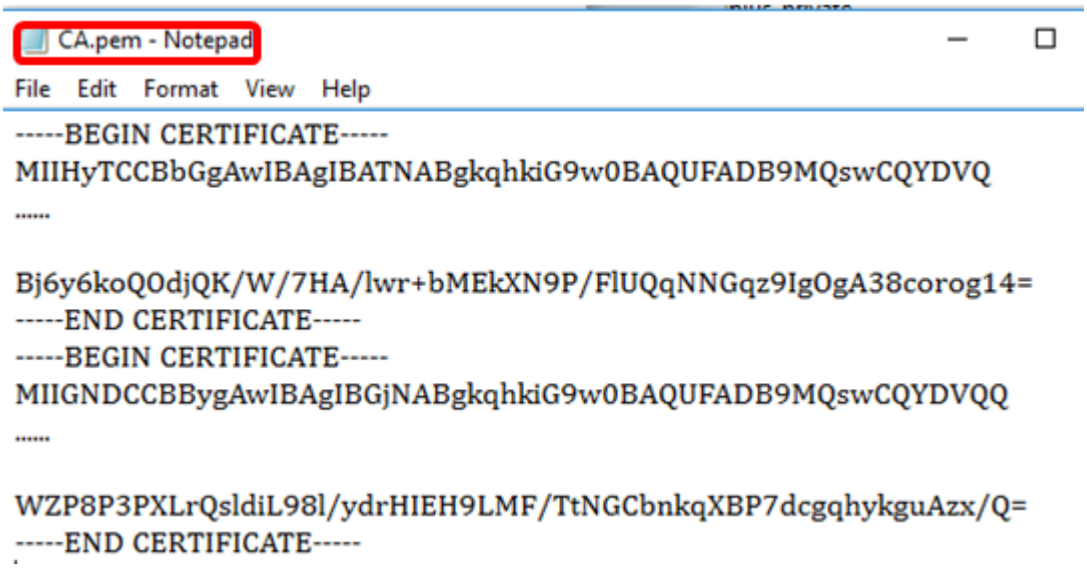
Etapa 1. Abra o RV320.pem, copie o segundo certificado (certificado raiz) e o terceiro certificado (certificado intermediário) incluindo a mensagem de início/fim.

Note: Neste exemplo, a sequência de caracteres de texto realçada é o certificado raiz.

Note: Neste exemplo, a cadeia de texto realçada é o certificado intermediário.

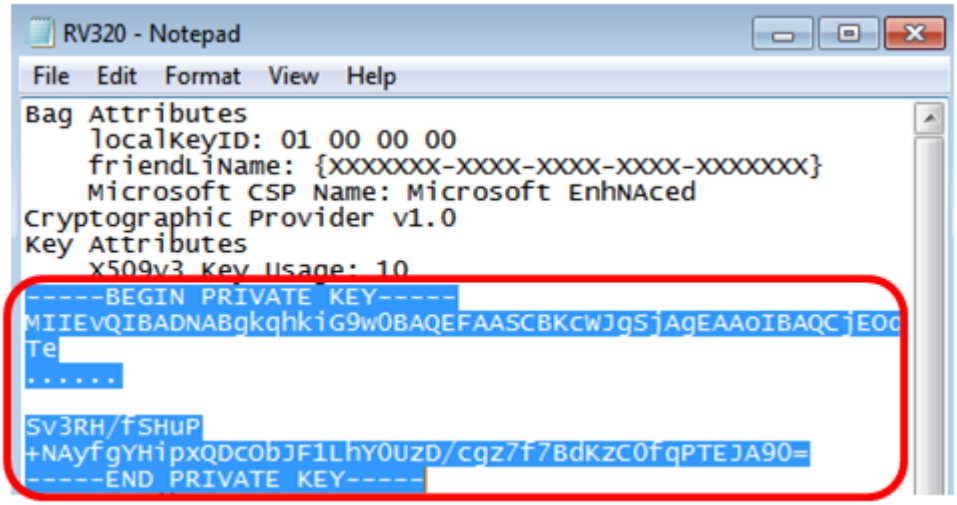


Etapa 2. Cole o conteúdo em um novo arquivo e salve-o como CA.pem.

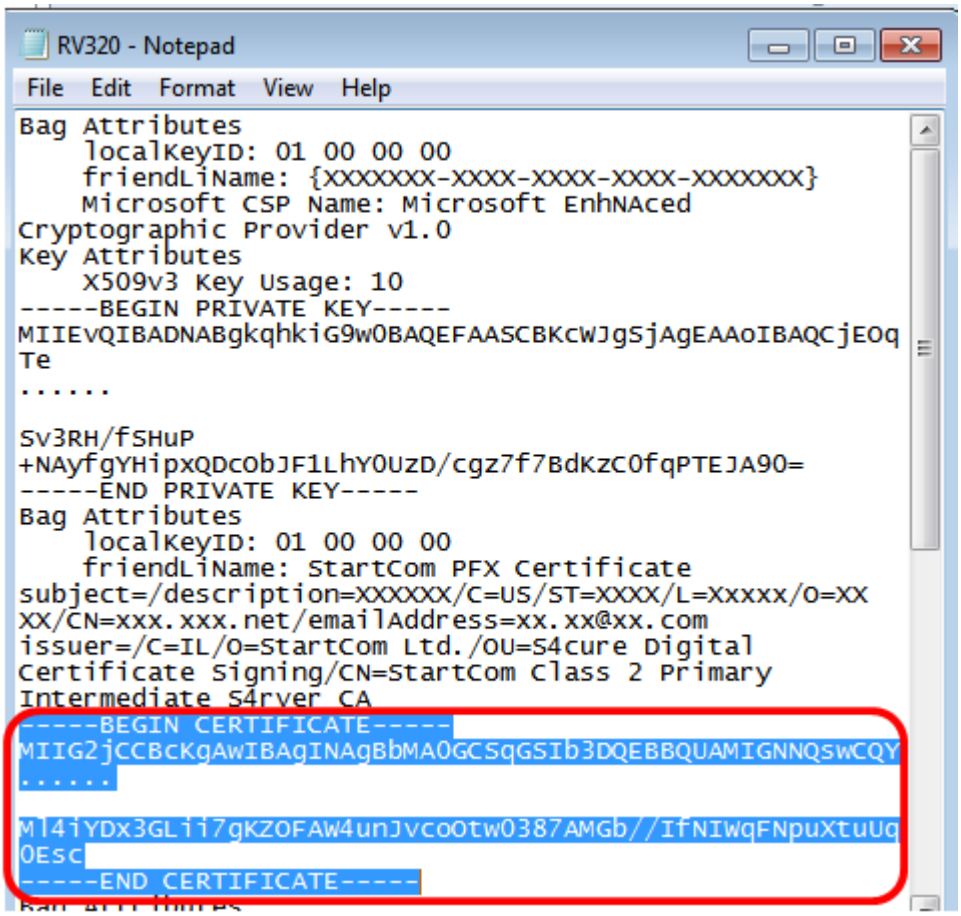


Etapa 3. Abra o RV320.pem e copie a seção chave privada e o primeiro certificado, incluindo a mensagem de início/fim.

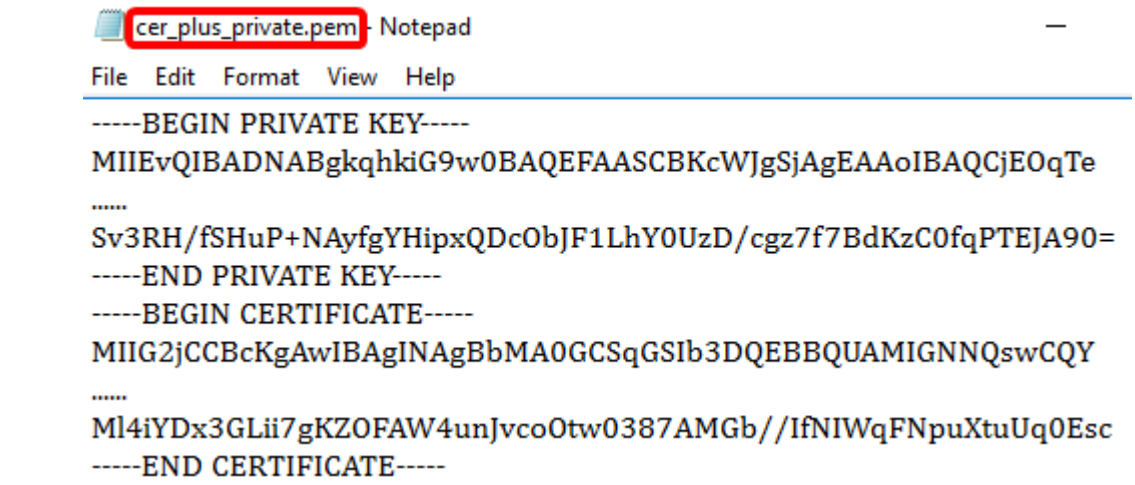
Note: No exemplo abaixo, a string destacada de texto é a seção chave privada.



Note: No exemplo abaixo, a string de texto realçada é o primeiro certificado.



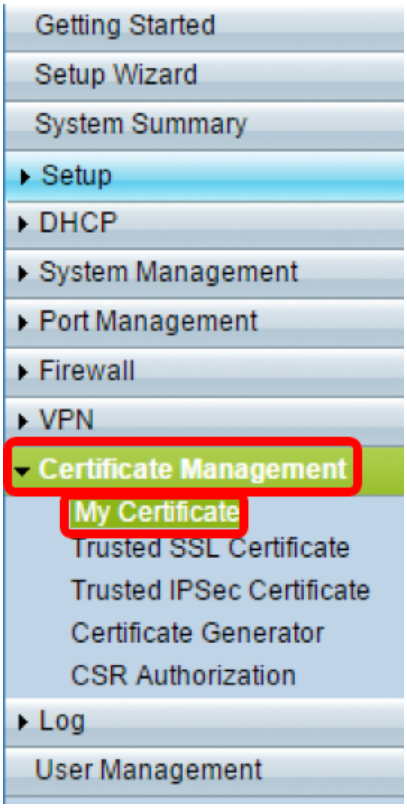
Etapa 4. Cole o conteúdo em um novo arquivo e salve-o como cer_plus_private.pem



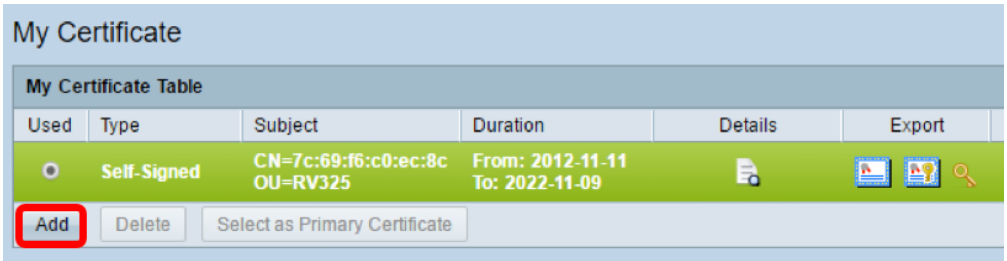
Note: Se a versão do firmware RV320/RV325 estiver abaixo de 1.1.1.06, verifique se há dois feeds de linha no final do arquivo (cer_plus_private.pem). No firmware após 1.1.1.06, você não precisa adicionar mais dois feeds de linha. Neste exemplo, uma versão abreviada do certificado é exibida somente para fins de demonstração.

Importar CA.pem e cer_plus_private.pem no RV320/RV325

Etapa 1. Efetue login no utilitário baseado na Web do RV320 ou RV325 e escolha **Certificate Management > My Certificate**.



Etapa 2. Clique em **Adicionar** para importar o certificado.



Etapa 3. Clique no botão de opção *Autorizado de terceiros* para importar o certificado.

Etapa 4. Na área *Importar conjunto completo de certificados*, clique em um botão de opção para escolher a origem dos certificados salvos. As opções são:

- *Import from PC* - (Importar do PC) - Escolha esta opção se os arquivos forem encontrados no computador.
- *Import from USB (Importar do USB*) - Escolha esta opção para importar os arquivos de uma unidade flash.

Note: Neste exemplo, **Importar do PC** é escolhido.

Etapa 5. Na área *Certificado CA*, clique em **Procurar...** e localize o CA.pem. arquivo.

Note: Se você estiver executando um firmware posterior à versão 1.1.0.6, clique no botão escolher e localize o arquivo necessário.

Etapa 6. Na área *Certificado + chave privada*, clique em **Procurar...**e localize o arquivo th_plus_private.pem.

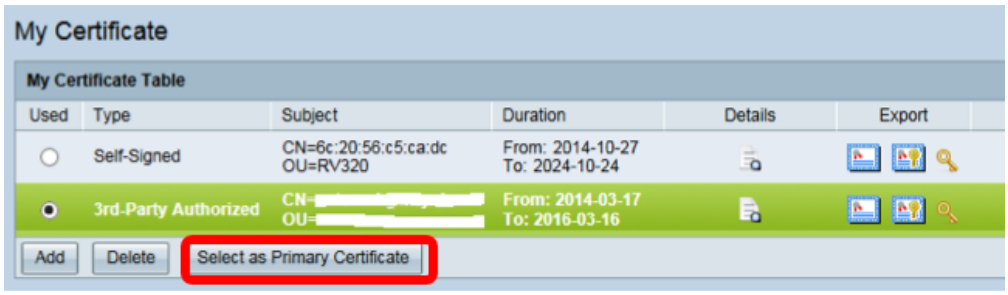
Note: Se você estiver executando um firmware posterior à versão 1.1.0.6, clique no botão escolher e localize o arquivo necessário.

Passo 7. Click **Save**.

Os certificados foram importados com êxito. Agora, ele pode ser usado para acesso HTTPS,

VPN SSL ou VPN IPSec.

Etapa 8. (Opcional) Para usar o certificado para HTTPS ou SSL VPN, clique no botão de opção do certificado e clique no botão **Selecionar como certificado primário**.

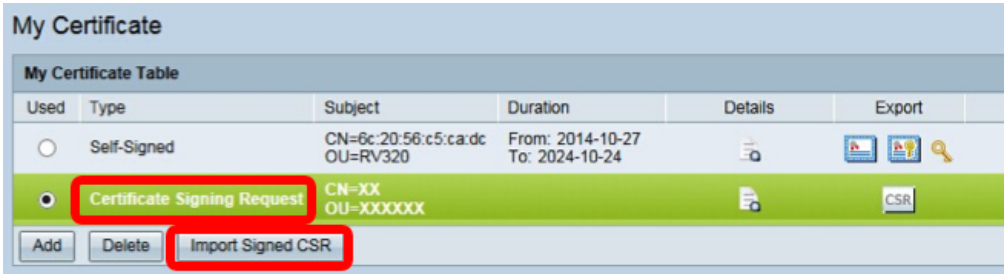


Agora você deve ter importado com êxito um certificado.

Assinatura de certificado usando CSR

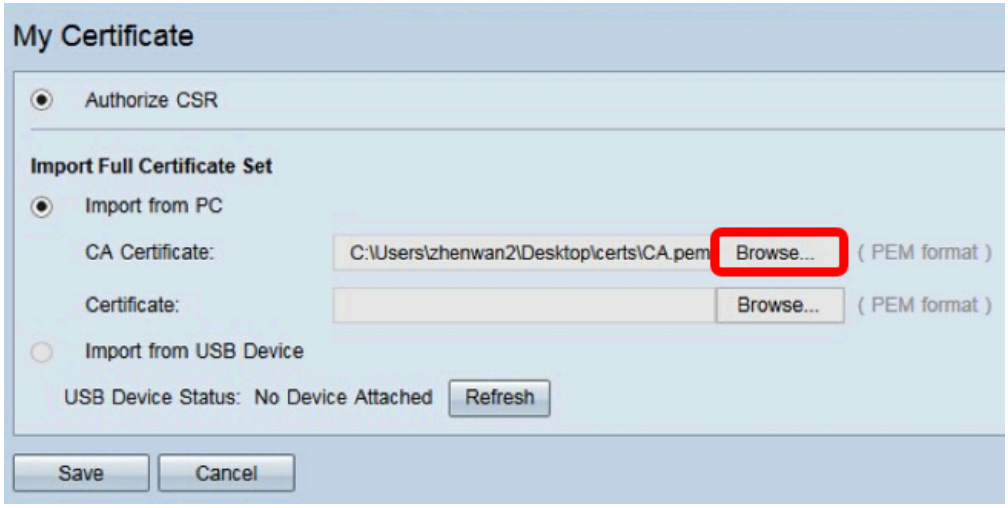
Etapa 1. Gere uma solicitação de assinatura de certificado (CSR) no RV320/RV325. Para saber como gerar um CSR, clique aqui.

Etapa 2. Para importar o certificado, escolha **Certificate Signing Request** e clique em **Import Signed CSR**.

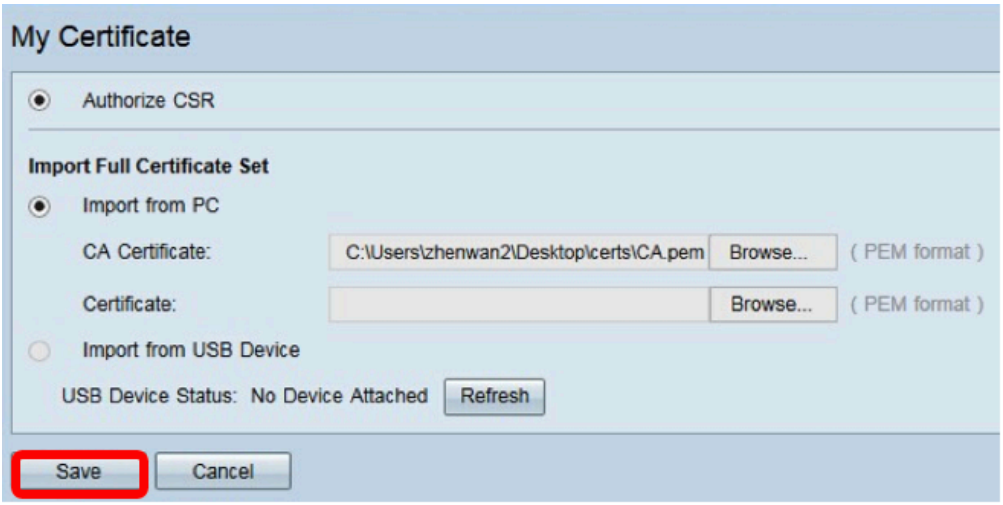


Etapa 3. Clique em **Procurar...** e escolha o arquivo de certificado CA. Contém o certificado CA raiz + CA intermediário.

Note: Neste exemplo, a chave privada não é necessária, pois o certificado é gerado usando CSR.



Etapa 4. Click **Save**.



Agora você deve ter carregado com êxito um certificado usando o CSR.

Appendix:

Conteúdo do RV320.pem

Atributos de tag

localKeyID: 01 00 00 00

Nome daLiamiga: {{XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXX}}

Nome do Microsoft CSP: Microsoft EnhNAced Cryptographic Provider v1.0

Principais atributos

Uso da chave X509v3: 10

—INICIAR CHAVE PRIVADA—

MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBKcWJgSjAgEAAoIBAQCjEOqTe

.....

Sv3RH/fSHuP+NAyfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=

—CHAVE PRIVADA FINAL—

Atributos de tag

localKeyID: 01 00 00 00

Nome daLiamiga: Certificado StartCom PFX

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

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

—INICIAR CERTIFICADO—

MIIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNNQswCQY

.....

Ml4iYDx3GLii7gKZOFAW4unJvcoOtw0387AMGb//IfNIWqFNpuXtuUq0Esc

—CERTIFICADO FINAL—

Atributos de tag

Nome daLiamiga: Autoridade de Certificação StartCom

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

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

—INICIAR CERTIFICADO—

MIIHyTCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

.....

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

—CERTIFICADO FINAL—

Atributos de tag

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

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

—INICIAR CERTIFICADO—

MIIGNDCCBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dcgqhykguAzx/Q=

—CERTIFICADO FINAL—