Solución alternativa para cargar el certificado del router serie RV32x

Summary

Un certificado digital certifica la propiedad de una clave pública por el sujeto designado del certificado. Esto permite que las partes que confían en ellas dependan de las firmas o afirmaciones hechas por la clave privada que corresponde a la clave pública certificada. Un router puede generar un certificado autofirmado, un certificado creado por un administrador de red. También puede enviar solicitudes a las autoridades de certificación (CA) para solicitar un certificado de identidad digital. Es importante disponer de certificados legítimos de aplicaciones de terceros.

Hay dos maneras en que CA firma los certificados:

1. CA firma el certificado con claves privadas.

2. CA firma los certificados mediante CSR generados por RV320/RV325.

RV320 y RV325 sólo admiten certificados en formato .pem. En ambos casos, debe obtener certificados en formato .pem de la Autoridad de Certificación. Si obtiene otro certificado de formato, debe convertir el formato por sí mismo o solicitar el certificado de formato .pem de nuevo desde la CA.

La mayoría de los proveedores de certificados comerciales utilizan certificados intermedios. Como el certificado intermedio es emitido por la CA raíz de confianza, cualquier certificado emitido por el certificado intermedio hereda la confianza de la raíz de confianza, como una cadena de certificación de confianza.

Esta guía describe cómo importar el certificado emitido por la Autoridad de Certificación Intermedia en RV320/RV325.

Fecha identificada

24 de febrero de 2017

Fecha de resolución

N/A

Productos afectados

RV320/RV325	1.1.1.06 y posteriores

Firma de certificado mediante claves privadas

En este ejemplo, asumimos que obtuvo un RV320.pem de la CA intermedia de terceros. El archivo tiene dicho contenido: clave privada, certificado, certificado CA raíz, certificado CA intermedio.

Nota: Obtener varios archivos de la CA intermedia en lugar de sólo un archivo es opcional. Pero puede encontrar las cuatro partes superiores de los varios archivos.

Verifique si el archivo de certificado de CA contiene tanto el certificado de CA raíz como el certificado intermedio. RV320/RV325 requiere el certificado intermedio y el certificado raíz en un orden determinado en el paquete CA, primero el certificado raíz y luego el certificado intermedio. En segundo lugar, debe combinar el certificado RV320/RV325 y la clave privada en un solo archivo.

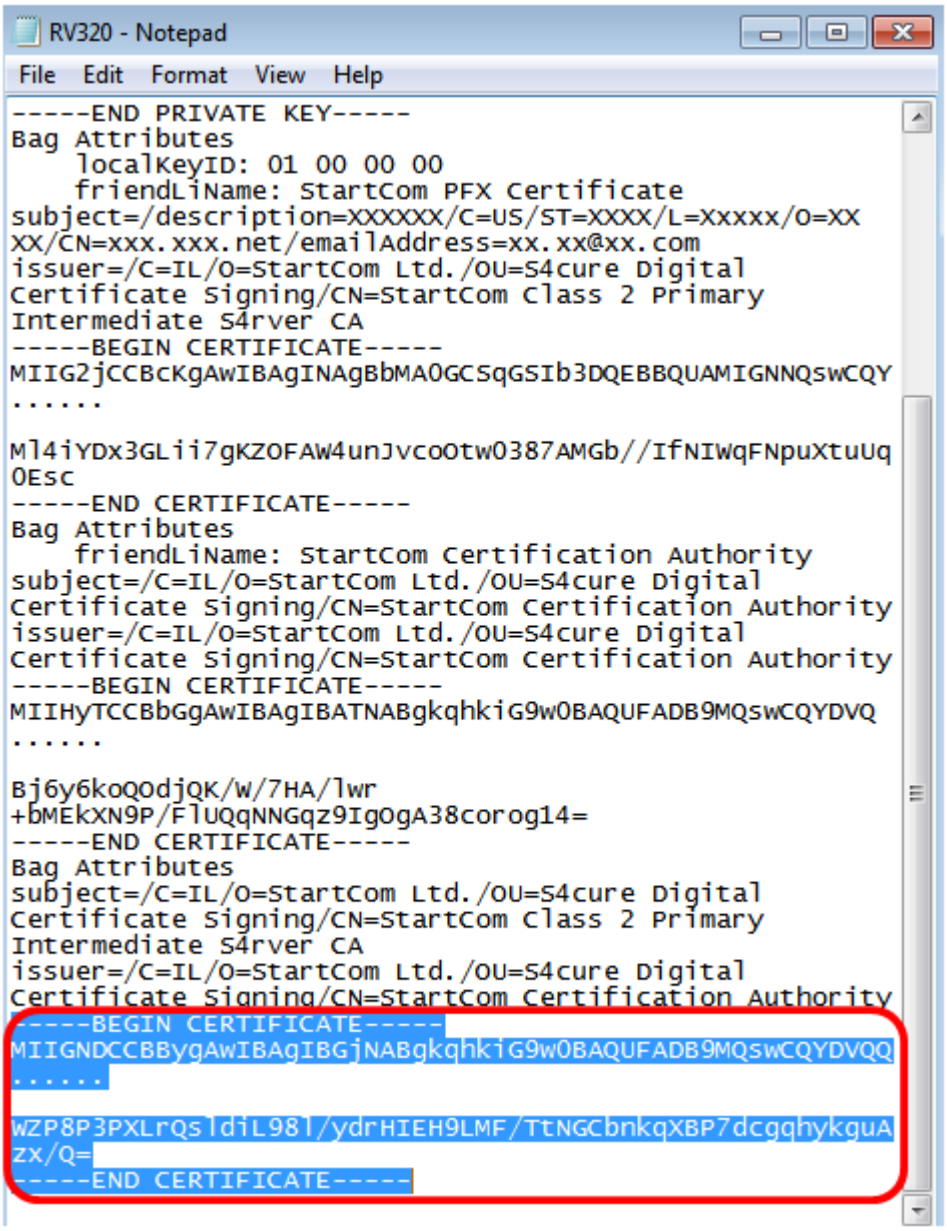
Nota: Cualquier editor de texto se puede utilizar para abrir y editar los archivos. Es importante asegurarse de que cualquier línea, espacio o retorno de carro extra en blanco no hará que el plan funcione como se esperaba.

Combinación de certificados

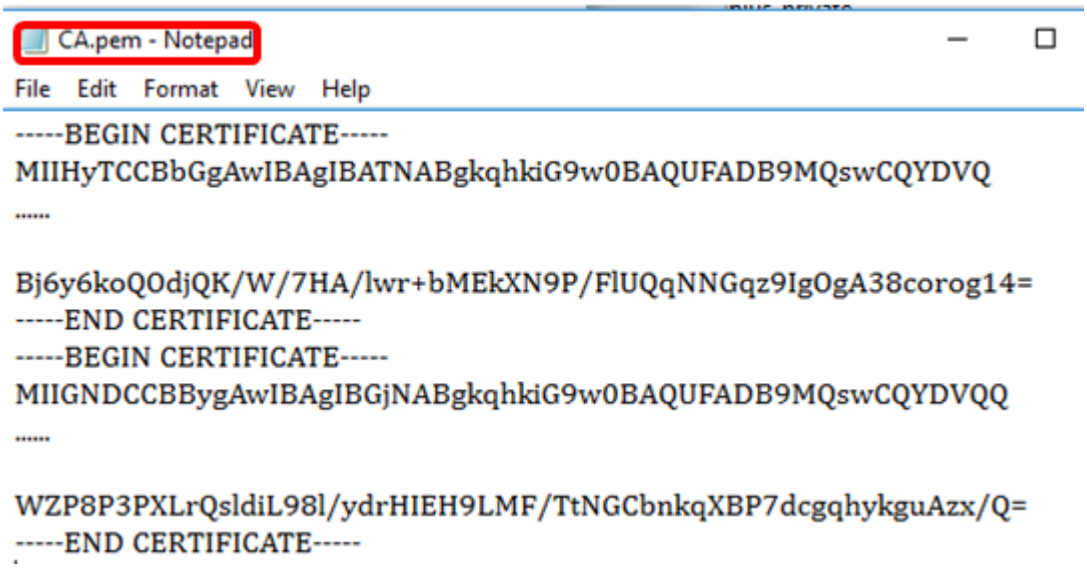
Paso 1. Abra el RV320.pem, copie el segundo certificado (certificado raíz) y el tercer certificado (certificado intermedio), incluido el mensaje de inicio/fin.

Nota: En este ejemplo, la cadena de resaltado del texto es el certificado raíz.

Nota: En este ejemplo, la cadena de texto resaltada es el certificado intermedio.

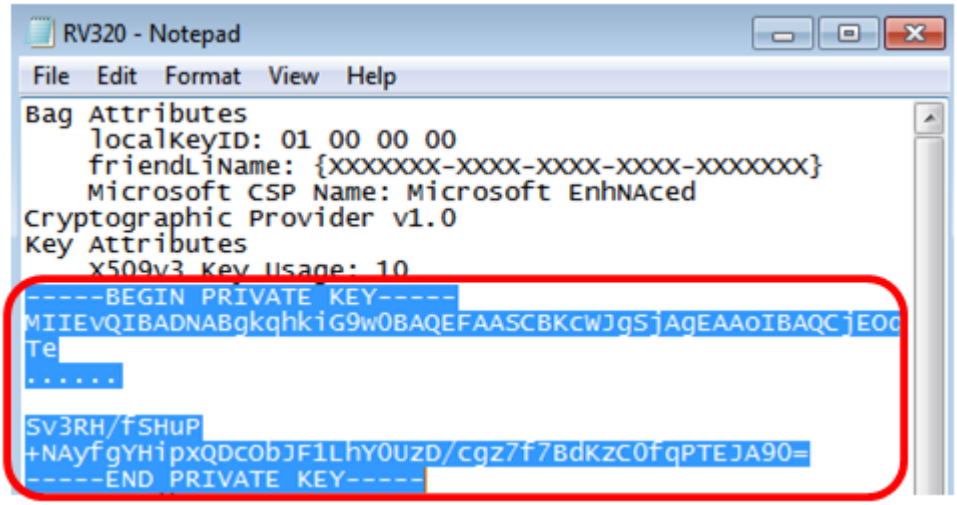


Paso 2. Pegue el contenido en un nuevo archivo y guárdelo como CA.pem.

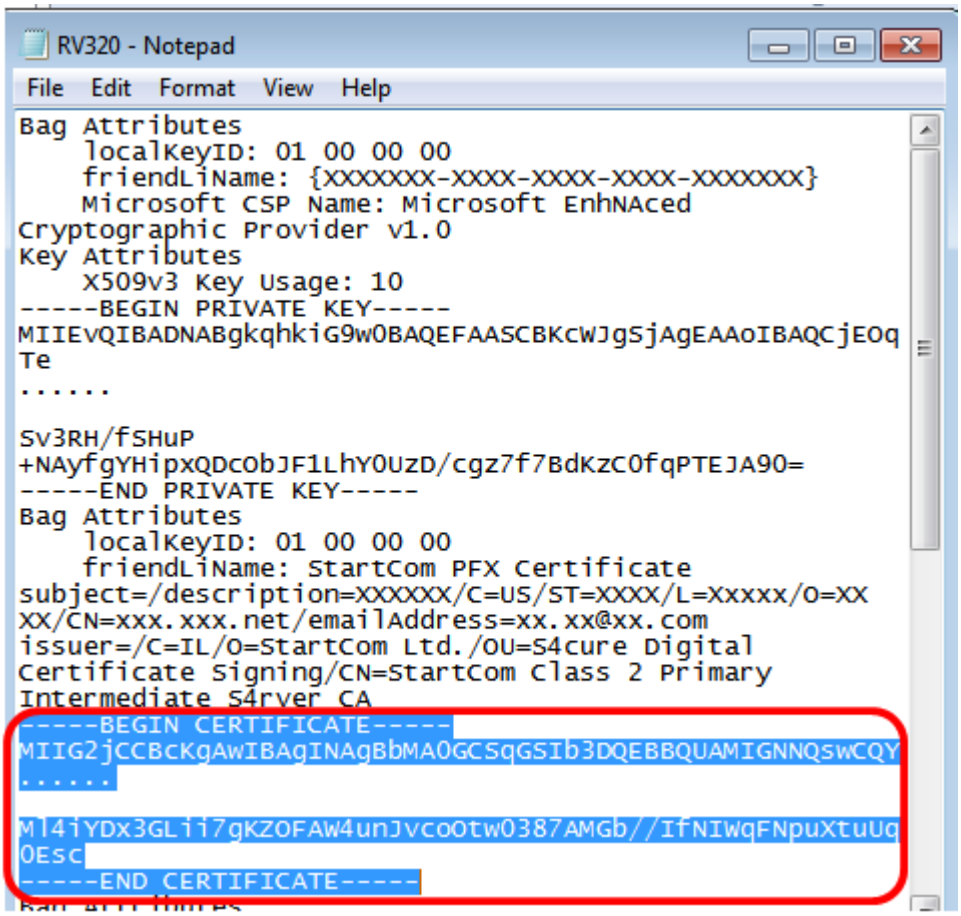


Paso 3. Abra el RV320.pem y copie la sección de clave privada y el primer certificado, incluido el mensaje de inicio/fin.

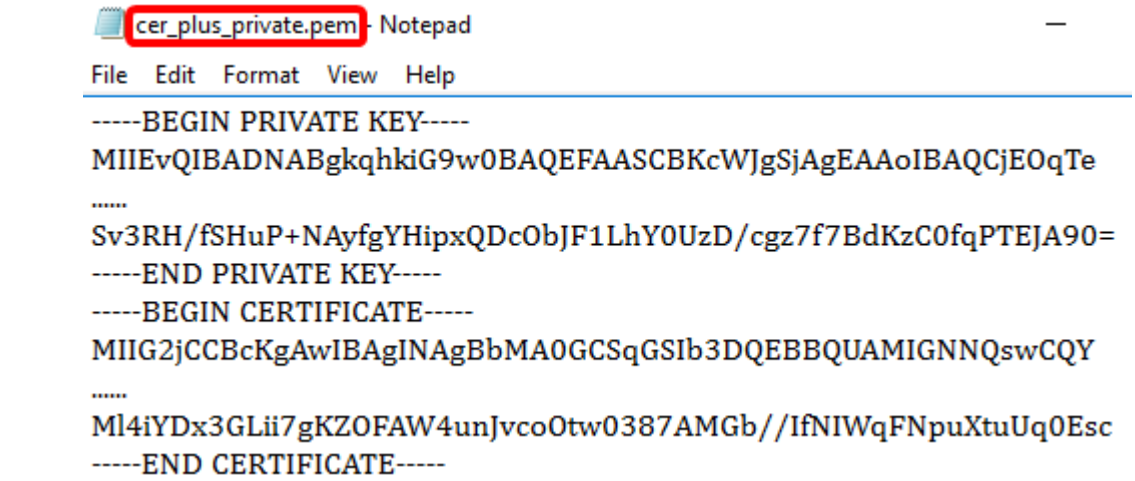
Nota: En el ejemplo siguiente, la cadena de texto resaltada es la sección de clave privada.



Nota: En el ejemplo siguiente, la cadena de texto resaltada es el primer certificado.



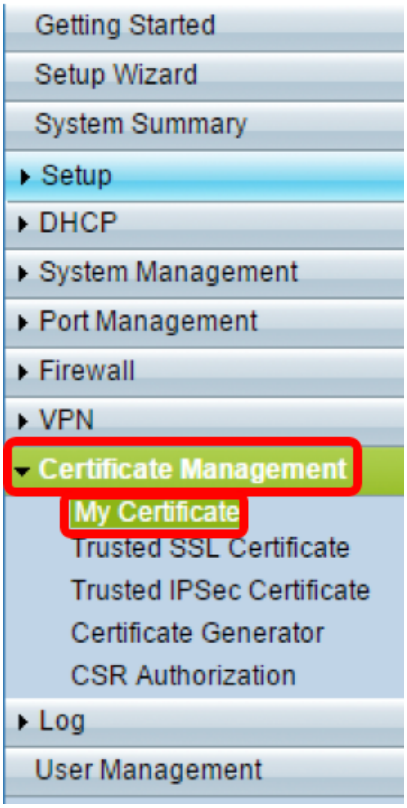
Paso 4. Pegue el contenido en un nuevo archivo y guárdelo como cer_plus_private.pem



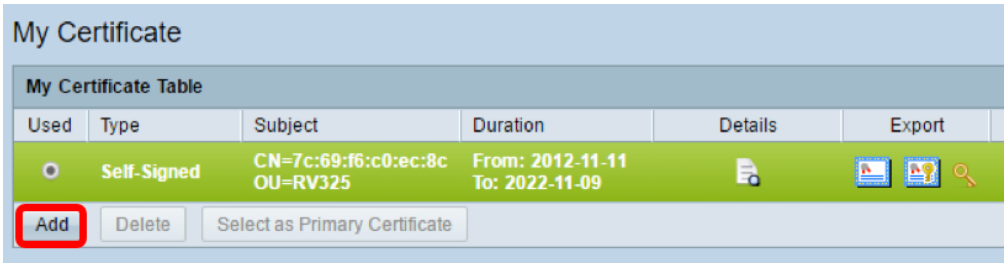
Nota: Si la versión del firmware de RV320/RV325 es inferior a 1.1.1.06, asegúrese de que hay dos fuentes de línea al final del archivo (cer_plus_private.pem). En el firmware posterior a 1.1.1.06, no es necesario agregar dos fuentes de línea más. En este ejemplo, sólo se muestra una versión abreviada del certificado con fines de demostración.

Importar CA.pem y cer_plus_private.pem en RV320/RV325

Paso 1. Inicie sesión en la utilidad basada en web del RV320 o RV325 y elija **Administración de certificados > Mi certificado**.



Paso 2. Haga clic en **Agregar** para importar el certificado.



Paso 3. Haga clic en el botón de opción *Autorizado de terceros* para importar el certificado.

Paso 4. En el área *Importar conjunto completo de certificados*, haga clic en un botón de opción para elegir el origen de los certificados guardados. Las opciones son:

- *Importar desde PC*: elija esta opción si los archivos se encuentran en el equipo.
- *Importar desde USB*: seleccione esta opción para importar los archivos desde una unidad flash.

Nota: En este ejemplo, se elige **Importar desde PC**.

Paso 5. En el área *CA Certificate*, haga clic en **Browse...** y busque CA.pem. archivo.

Nota: Si está ejecutando firmware después de 1.1.0.6, haga clic en el botón Choose (Seleccionar) y busque el archivo necesario.

Paso 6. En el área *Certificado + Clave privada*, haga clic en **Examinar...**y busque el archivo thecer_plus_private.pem.

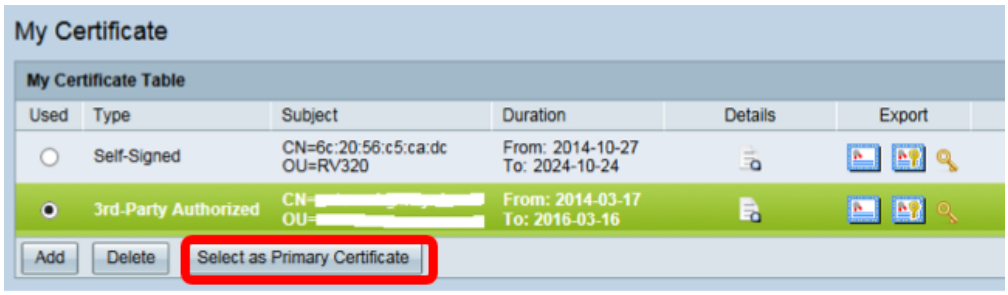
Nota: Si está ejecutando firmware después de 1.1.0.6, haga clic en el botón Choose (Seleccionar) y busque el archivo necesario.

Paso 7. Click **Save**.

Los certificados se importan correctamente. Ahora se puede utilizar para acceso HTTPS,

VPN SSL o VPN IPSec.

Paso 8. (Opcional) Para utilizar el certificado para HTTPS o SSL VPN, haga clic en el botón de opción del certificado y haga clic en el botón **Seleccionar como certificado primario**.

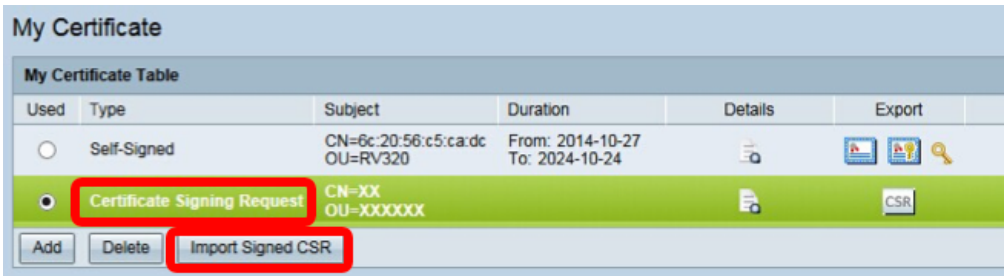


Ahora debería haber importado correctamente un certificado.

Firma de certificado mediante CSR

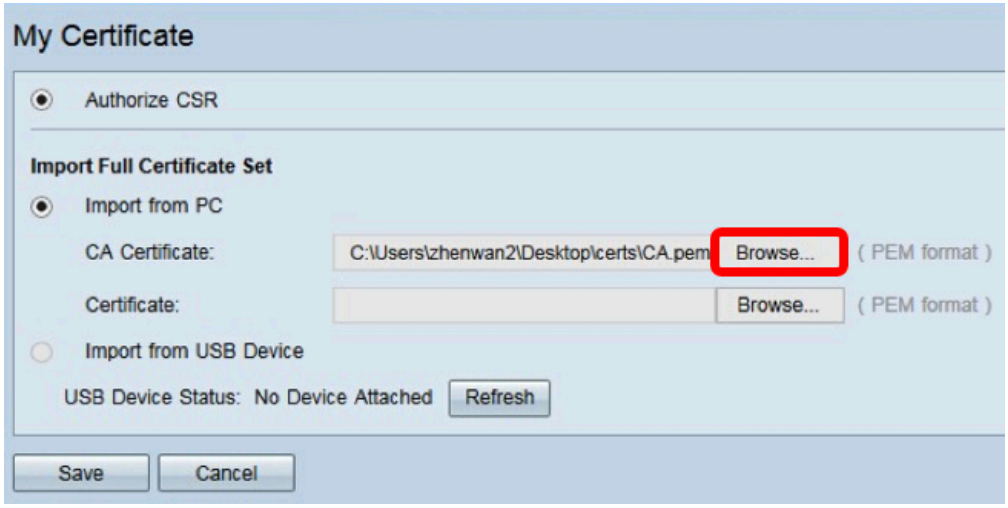
Paso 1. Genere una solicitud de firma de certificado (CSR) en RV320/RV325. Para aprender cómo generar una RSE, haga clic aquí.

Paso 2. Para importar el certificado, elija **Solicitud de firma de certificado** y haga clic en **Importar CSR firmado**.

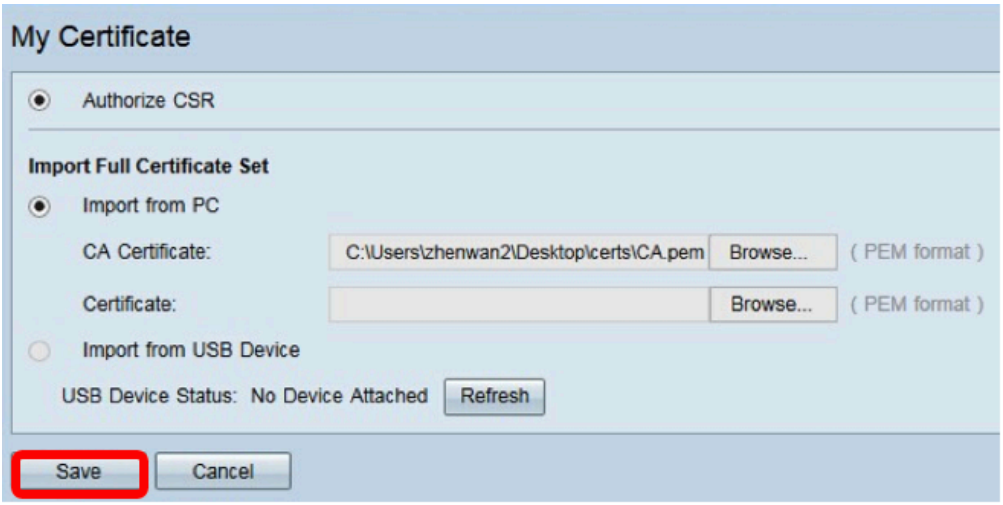


Paso 3. Haga clic en **Examinar...** y elija el archivo de certificado de CA. Esto contiene el certificado CA raíz + CA intermedia.

Nota: En este ejemplo, no se requiere clave privada porque el certificado se genera utilizando CSR.



Paso 4. Click **Save**.



Ahora debería haber cargado correctamente un certificado mediante el CSR.

Appendix:

Contenido de RV320.pem

Atributos de la bolsa

localKeyID: 01 00 00 00

friendLiName: {{XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXX}}

Nombre de CSP de Microsoft: Proveedor criptográfico de Microsoft EnhNA v1.0

Atributos clave

Uso de claves X509v3: 10

—COMENZAR CLAVE PRIVADA—

MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBKcWJgSjAgEAAoIBAQCjEOte

.....

Sv3RH/fSHuP+NAyfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=

—FINALIZAR CLAVE PRIVADA—

Atributos de la bolsa

localKeyID: 01 00 00 00

friendLiName: Certificado PFX de StartCom

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

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

—CERTIFICADO DE INICIO—

MIIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNQswCQY

.....

Ml4iYDx3GLii7gKZOFAW4unJvcoOtw0387AMGb//IfNIWqFNpuXtuUq0Esc

—CERTIFICADO FINAL—

Atributos de la bolsa

friendLiName: Autoridad de certificación StartCom

subject=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signing/CN=Autoridad de certificación StartCom

emisor=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signing/CN=Autoridad de certificación StartCom

—CERTIFICADO DE INICIO—

MIIHyTCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

.....

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

—CERTIFICADO FINAL—

Atributos de la bolsa

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

emisor=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signing/CN=Autoridad de certificación StartCom

—CERTIFICADO DE INICIO—

MIIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQQ

.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dcgqhykguAzx/Q=

—CERTIFICADO FINAL—