Cómo lo hago exporte y convierta un certificado raíz de CA del pfx y ciérrelo de un Microsoft CA server

Pregunta:

Este artículo sobre Knowledge Base se refiere al software que no es mantenido ni es soportado por Cisco. La información se proporciona como cortesía para su conveniencia. Para la asistencia adicional, entre en contacto por favor al proveedor de software.

Los siguientes son instrucciones de exportar CA que firma el certificado raíz y la clave de un Microsoft CA server 2003. Hay varios pasos en este proceso. Es crucial que cada paso está seguido.

Exportación del certificado y de la clave privada del servidor MS CA
1. va al **"comienzo"** - > **"ejecutado"** - > el **MMC** 2. haga clic en el **"archivo"** - > **"agregue/quite Broche-en"** 3. Haga clic **"agrega…"** botón 4. **Los "Certificados** selectos entonces hacen clic **"agregan"** 5. **"cuenta** selecta de la **Computadora"** - > **"después"** - > **"computadora local"** - > **"final"** 6. tecleo **"cercano"** - > **"OK"** ***El MMC ahora se carga con los Certificados broche-en.*** 7. amplíe los **Certificados** - > y haga clic en **"personal"** - > los **"Certificados** 8. Haga clic con el botón derecho del ratón el CERT apropiado de CA y elija **"todas las tareas"** - > **"exportación"** ***El Asisitente de la exportación del certificado iniciará*** 9. haga clic **"después"** - > selecto **"sí, exporte la clave privada"** - > **"después"** 10. ***Desmarque todas las*** opciones aquí. El PKCS12 debe ser la única opción disponible. Tecleo **"después"** 11 Dé a clave privada una contraseña de su opción 12. Dé un nombre de fichero para salvar como y para hacer clic **"siguiente"**, después

“acabe” *Usted ahora tiene su CA que firma el certificado y la raíz exportados como archivo del PKCS12 (PFX).*
Extrayendo la clave pública (certificado)
Usted necesita el acceso a un OpenSSL corriente del ordenador. Copie su archivo PFX encima a este ordenador y funcione con el siguiente comando: *pkcs12 del openssl - en <filename.pfx> - clcerts - nokeys - hacia fuera certificate.cer* Esto crea el archivo de clave pública nombrado “certificate.cer”

Note: Estas instrucciones se han verificado usando el OpenSSL en Linux. Un cierto sintaxis puede variar en la versión de Win32.

Extrayendo y desencriptando la clave privada
El WSA requiere que la clave privada sea unencrypted. Utilice los comandos siguientes del OpenSSL: *pkcs12 del openssl - en <filename.pfx> - nocerts - hacia fuera privatekey-encrypted.key* Le indicarán para “**ingresa la contraseña de la importación**”. Ésta es la contraseña creada en el *paso 11* antedicho. También le indicarán para “**ingresa la palabra clave PEM**”. Es la contraseña del cifrado (usada abajo). Esto creará el archivo de clave privado cifrado nombrado “privatekey-encrypted.key” Para crear una versión desencriptada de esta clave, utilice el siguiente comando: **openssl rsa - en privatekey-encrypted.key - hacia fuera private.key**

El público y las claves privadas desencriptadas pueden ser instalados en el WSA de los **“Servicios de seguridad** - > **“proxy HTTPS”**