Cómo se exporta y convierte un certificado raíz y una clave de CA de pfx desde un servidor de CA de Microsoft

Pregunta:

Este artículo sobre Base de conocimiento hace referencia a software que no es mantenido ni soportado por Cisco. La información se proporciona como cortesía para su conveniencia. Para obtener asistencia adicional, comuníquese con el proveedor de software.

A continuación se indican las instrucciones para exportar un certificado raíz de firma de CA y una clave desde un servidor de Microsoft CA 2003. Hay varios pasos en este proceso. Es crucial que se siga cada paso.

Exportación del certificado y la clave privada desde el servidor MS CA
1. Vaya a **'Inicio'** -> **'Ejecutar'** -> **MMC** 2. Haga clic en **'Archivo'** -> **'Agregar/Eliminar complemento'** 3. Haga clic en **'Agregar...'** botón 4. Seleccione **'Certificados'** y luego haga clic **'Agregar'** 5. Seleccione **'Cuenta de Computadora'** -> **'Siguiente'** ->'Equipo Local' > **'Finalizar'** 6. haga clic en **'Cerrar'** -> **'Aceptar'** *El MMC se carga ahora con el complemento Certificados.* 7. Expanda **Certificados** -> y haga clic en **'Personal'** -> **'Certificados'** 8. Haga clic con el botón derecho del ratón en el certificado de CA correspondiente y elija **'Todas las tareas'** -> **'Exportar'** *Se iniciará el Asistente para exportación de certificados* 9. Haga clic en **'Siguiente'** -> Seleccione **'Sí, Exportar la clave privada'** ->'Siguiente' 10. *Desmarque todas* las opciones aquí. PKCS 12 debe ser la única opción disponible. Haga clic en **'Siguiente'** 11. Proporcione la clave privada una contraseña de su elección 12. Asigne un nombre de archivo para guardarlo y haga clic en **'Siguiente'**, luego

'Finalizar'

El certificado de firma de CA y la raíz se exportan como un archivo PKCS 12 (PFX).

Extracción de la clave pública (certificado)

Necesitará acceso a un ordenador que ejecute OpenSSL. Copie el archivo PFX en este equipo y ejecute el siguiente comando:

openssl pkcs12 -in <filename.pfx> -clcerts -nokeys -out certificate.cer

Esto crea el archivo de clave pública denominado "certificate.cer"

Nota: Estas instrucciones se han verificado mediante OpenSSL en Linux. Algunas sintaxis pueden variar en la versión Win32.

Extracción y descifrado de la clave privada

WSA requiere que la clave privada esté descifrada. Utilice los siguientes comandos OpenSSL:

openssl pkcs12 -in <filename.pfx> -nocerts -out privatekey-encryption.key

Se le solicitará que introduzca "**Enter Import Password**" (Introducir contraseña de importación). Ésta es la contraseña creada en el *paso 11* anterior.
También se le solicitará "**Introducir la frase de paso PEM**". La es la contraseña de cifrado (utilizada a continuación).

Esto creará el archivo de clave privada cifrada denominado "privatekey-encryp.key"

Para crear una versión descifrada de esta clave, utilice el siguiente comando:

openssl rsa -in privatekey-encryption.key -out private.key

Las claves privadas públicas y descifradas se pueden instalar en el WSA desde **'Servicios de Seguridad'** -> **'Proxy HTTPS'**