Como faço eu exporte e converta um certificado de raiz de CA do pfx e feche-o de um Microsoft CA server

Pergunta:

Este artigo da base de conhecimento provê o software que não é mantido nem é apoiado por Cisco. A informação é fornecida como uma cortesia para sua conveniência. Para a assistência adicional, contacte por favor o fornecedor de software.

Os seguintes são instruções para exportar CA que assina o certificado de raiz e a chave de um Microsoft CA server 2003. Há diversas etapas neste processo. É crucial que cada etapa está seguida.

Exportando o certificado e a chave privada do server MS CA
1. vai ao **"começo"** - > **"sido executado"** - > o MMC 2. clique sobre o **"arquivo"** - > **"adicionar/remova Pressão-em"** 3. Clique **"adiciona…"** botão 4. Os **"Certificados** seletos clicam então **"adicionam"** 5. do **"conta** seleta **computador"** - > **"em seguida"** - > **"computador local"** - > **"revestimento"** 6. clique **"próximo"** - > **" OK "** *O MMC é carregado agora com os Certificados pressão-em.* 7. expanda **Certificados** - > e clique sobre **"pessoal"** - > **"Certificados** 8. Clicar com o botão direito o CERT apropriado de CA e escolha **"todas as tarefas"** - > **"exportação"** *O assistente da exportação do certificado lançar-se-á* 9. clique **"em seguida"** - > seleto **"sim, exporte a chave privada"** - > **"em seguida"** 10. *Desmarcar todas as* opções aqui. O PKCS12 deve ser a única opção disponível. Clique **"em seguida"** 11. Dê à chave privada uma senha de sua escolha

12. Dê um nome de arquivo para salvar como e clicar **"seguinte"**, a seguir **"termine"**

Você tem agora seu CA que assina o certificado e a raiz exportados como um arquivo do PKCS12 (PFX).

Extraindo a chave pública (certificado)

Você precisa o acesso a um OpenSSL running do computador. Copie seu arquivo PFX sobre a este computador e execute o comando seguinte:

pkcs12 do OpenSSL - em <filename.pfx> - clcerts - nokeys - para fora certificate.cer

Isto cria o arquivo de chave pública nomeado "certificate.cer"

Note: Estas instruções foram verificadas usando o OpenSSL em Linux. Alguma sintaxe pode variar na versão de Win32.

Extraindo e decifrando a chave privada

O WSA exige que a chave privada seja unencrypted. Use os seguintes comandos do OpenSSL:

pkcs12 do OpenSSL - em <filename.pfx> - nocerts - para fora privatekey-encrypted.key

Você será alertado para "**incorpora a senha da importação**". Esta é a senha criada em *etapa 11* acima.
Você será alertado igualmente para "**incorpora a frase de acesso PEM**". É a senha da criptografia (usada abaixo).

Isto criará o arquivo-chave privado cifrado nomeado "privatekey-encrypted.key"

Para criar uma versão decifrada desta chave, use o comando seguinte:

rsa do OpenSSL - em privatekey-encrypted.key - para fora private.key

O público e as chaves privadas decifradas podem ser instalados no WSA dos **"Serviços de segurança** - > **"proxy HTTPS"**