Como faço para exportar e converter um certificado raiz e uma chave de CA pfx de um servidor de CA da Microsoft

Pergunta:

Este artigo da base de conhecimento faz referência ao software para o qual a Cisco não oferece manutenção ou compatibilidade. As informações foram disponibilizadas como cortesia para sua conveniência. Para obter mais assistência, entre em contato com o fornecedor do software.

A seguir estão instruções para exportar um certificado raiz de assinatura CA e uma chave de um servidor de AC da Microsoft 2003. Há várias etapas neste processo. É crucial que cada passo seja seguido.

Exportando o certificado e a chave privada do servidor MS CA
1. Vá para **'Iniciar'** -> **'Executar'** -> MMC 2. Clique em **'Arquivo'** -> **'Adicionar/remover snap-in'** 3. Clique em **'Adicionar...'** botão 4. Selecione **'Certificados'** e clique em **'Adicionar'** 5. Selecione **'Conta do computador'** -> **'Próximo'** -> **'Computador local'** -> **'Concluir'** 6. clique em **'Fechar'** -> **'OK'** *O MMC agora está carregado com o snap-in Certificados.* 7. Expanda **Certificados** -> e clique em **'Pessoal'** -> **'Certificados'** 8. Clique com o botão direito do mouse no certificado CA apropriado e escolha **'Todas as tarefas'** -> **'Exportar'** *O Assistente para exportação de certificado será iniciado* 9. Clique em **'Avançar'** -> Selecione **'Sim, Exportar a chave privada'** -> **'Próximo'** 10. *Desmarque todas* as opções aqui. PKCS 12 deve ser a única opção disponível. Clique em **'Avançar'** 11. Forneça à chave privada uma senha de sua escolha 12. Dê um nome de arquivo para salvar como e clique em **'Avançar'**, depois **'Concluir'**

Agora, seu certificado de assinatura CA e a raiz são exportados como um arquivo PKCS 12 (PFX).

Extraindo a chave pública (certificado)

Você precisará de acesso a um computador que esteja executando o OpenSSL. Copie seu arquivo PFX para este computador e execute o seguinte comando:

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

Isso cria o arquivo de chave pública chamado "certificate.cer"

Note: Essas instruções foram verificadas usando o OpenSSL no Linux. Algumas sintaxe podem variar na versão Win32.

Extraindo e descriptografando a chave privada

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

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

Você será solicitado a inserir "**Enter Import Password**". Esta é a senha criada na *etapa 11* acima.
Você também será solicitado a inserir "**Inserir frase secreta PEM**". A é a senha de criptografia (usada abaixo).

Isso criará o arquivo de chave privada criptografada chamado "privatekey-encrypted.key"

Para criar uma versão descriptografada dessa chave, use o seguinte comando:

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

As chaves privadas públicas e descriptografadas podem ser instaladas no WSA de **'Serviços de segurança'** -> **'Proxy HTTPS'**