如何从Microsoft CA服务器导出和转换pfx CA根证书和密钥

问题：

此知识库文章引用不是由思科维护或支持的软件。提供该信息只是为了方便您使用。如需进一步协助，请联系软件供应商。

以下是从Microsoft CA服务器2003导出CA签名根证书和密钥的说明。此过程中有几个步骤。每一步都要遵循，这一点至关重要。

从MS CA服务器导出证书和私钥
1.转到'开始' ->'运行' -> MMC 2.单击“文件”->“添加/删除管理单元” 3.单击“添加……” 按钮 4.选择“证书”，然后单击“添加” 5.选择“计算机帐户”->“下一步” — >“本地计算机”->“完成” 6.单击“关闭”->“确定” *MMC现在已加载证书管理单元。* 7.展开证书 — >，然后单击“个人”->“证书” 8.右键单击相应的CA证书，然后选择“所有任务”->“导出” *证书导出向导将启动* 9.单击“下一步”->选择“是，导出私钥”->“下一步” 10.取*消选中*此处的所有选项。PKCS 12应是唯一可用的选项。单击“Next” 11.为私钥提供您选择的密码 12.提供要另存为的文件名，然后单击“下一步”，然后单击“完成” *现在，您的CA签名证书和根证书已导出为PKCS 12(PFX)文件。*
提取公钥（证书）
您需要访问运行OpenSSL的计算机。将PFX文件复制到此计算机并运行以下命令： *openssl pkcs12 -in <filename.pfx> -clcerts -nokeys -out certificate.cer*

这将创建名为“certificate.cer”的公钥文件

注意：这些说明已在Linux上使用OpenSSL进行验证。Win32版本的某些语法可能有所不同。

提取和解密私钥

WSA要求未加密私钥。使用以下OpenSSL命令：

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

系统将提示您输入“**输入导入密**码”。 这是在上述步骤11中***创建的***密码。
系统还会提示您输入“**Enter PEM pass phrase”(输入PEM口令**)。 是加密密码（用于下面）。

这将创建名为“privatekey-encrypted.key”的加密私钥文件

要创建此密钥的解密版本，请使用以下命令：

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

可以从“安全服务”(Security Services)->“HTTPS代**理”(HTTPS Proxy)将公**用密钥和解**密的私钥安装到WSA上**