如何從Microsoft CA伺服器匯出和轉換pfx CA根證書和金鑰

問題：

本知識庫文章所參考的軟體不是思科維護或支援的。此資訊出於方便而提供。如需更多幫助，請與軟體供應商聯絡。

以下為從Microsoft CA server 2003匯出CA簽名根證書和金鑰的說明。此過程有幾個步驟。至關重要的是要遵循每一個步驟。

從MS CA伺服器匯出證書和私鑰
1.轉到「**開始**」->「**運行**」-> MMC **2.**按一下「**檔案**」->「**新增/刪除管理單元**」 **3.**按一下「**新增……**」 按鈕 **4.選**擇「**證書**」，然後單**擊「新增」** **5.選**擇「**電腦帳戶**」->「下**一個**」->「**本地電腦**」->「**完成**」 **6.**單**擊「關閉**」 — > 「**確定**」 ***MMC現在載入了證書管理單元。*** **7.**展開Certificates ->，然後點選「Personal」 -> 「Certificates」 **8.右**鍵點選適當的CA證書，然後選擇**「所有任務」**->「**匯出**」 ***證書匯出嚮導將啟動*** **9.單**擊「**下一步**」->選擇**「是，匯出私鑰」**->「**下一步**」 **10.*取消選中***此處的所有選項。PKCS 12應是唯一可用的選項。按一下**「下一步」** **11.**為私鑰提供您選擇的密碼 **12.給**出要另存為的檔名，然後**按一下**「下一步」，**「完成」** ***現在，您的CA簽名證書和根證書已匯出為PKCS 12(PFX)檔案。***
提取公鑰（證書）
您需要訪問運行OpenSSL的電腦。將PFX檔案複製到此電腦，然後運行以下命令： *openssl pkcs12 -in <filename.pfx> -clcerts -nokeys -out certificate.cer*

這將建立名為「certificate.cer」的公鑰檔案

附註：已在Linux上使用OpenSSL驗證這些指令。部分語法可能因Win32版本而異。

提取和解密私鑰

WSA要求不加密私鑰。使用以下OpenSSL命令：

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

系統將提示您輸入「**輸入匯入密碼**」。 這是在上述步驟11中***建立的***密碼。
系統也會提示您輸入「**Enter PEM pass phrase**」。 是加密密碼（在下面使用）。

這將建立名為「privatekey-encrypted.key」的加密私鑰檔案

要建立此金鑰的解密版本，請使用以下命令：

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

可以在WSA上通過「安全服務」 — >「**HTTPS代理**」**安**裝公鑰**和解密私鑰**