# Microsoft CA 서버에서 pfx CA 루트 인증서 및 키를 내보내고 변환하는 방법

## 질문:

*이 기술 자료 문서는 Cisco에서 유지 관리하거나 지원하지 않는 소프트웨어를 참조합니다.이 정보는 귀하의 편의를 위해 제공됩니다.자세한 내용은 소프트웨어 공급업체에 문의하십시오.*

다음은 Microsoft CA 서버 2003에서 CA 서명 루트 인증서 및 키를 내보내는 지침입니다.이 프로세스에는 여러 단계가 있습니다.각 단계를 따르는 것이 중요합니다.

| MS CA 서버에서 인증서 및 개인 키 내보내기 |
| --- |
| 1. **'시작'** -> **'실행'** -> MMC<br><br>2. **'파일'** -> '스냅인 추가**/제거'를 클릭합니다.**<br><br>3. '추가**..'를 클릭합니다.** 단추<br><br>4. **'인증서'를 선택한** 다음 '추가'를 클릭합니다.<br><br>5. **'컴퓨터 계정'** -> **'다음'** -> **'로컬 컴퓨터'** -> **'마침'을 선택합니다.**<br><br>6.**'닫기'** -> **'확인'을 클릭합니다.**<br><br>*이제 MMC에 인증서 스냅인이 로드되었습니다.*<br><br>7. Certificates(**인증서**) ->를 확장하고 **'Personal' ->'Certificates(인증서)를** 클릭합니다.<br><br>8. 적절한 CA 인증서를 마우스 오른쪽 버튼으로 클릭하고 **'All Tasks'** -> **'Export'를 선택합니다.**<br><br>*인증서 내보내기 마법사가 시작됩니다.*<br><br>9. **'다음'** -> **'예, 개인 키 내보내기' -> '다음'을 클릭합니다.**<br><br>10.여기에서 ***모든*** 옵션을 선택 취소합니다.PKCS 12만 사용할 수 있습니다.**'다음'을 클릭합니다.**<br><br>11. 개인 키에 원하는 암호를 지정합니다.<br><br>12. 다른 이름으로 저장할 파일 이름을 지정하고 **'Next'**, 'Finish'를 차례로 클릭합니다.<br><br>*이제 CA 서명 인증서 및 루트를 PKCS 12(PFX) 파일로 내보냈습니다.* |
| **공개 키 추출(인증서)** |
| OpenSSL을 실행하는 컴퓨터에 액세스해야 합니다.PFX 파일을 이 컴퓨터에 복사하고 다 |

음 명령을 실행합니다.

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

이렇게 하면 "certificate.cer"라는 공개 키 파일이 생성됩니다.

***참고:이러한 지침은 Linux에서 OpenSSL을 사용하여 확인되었습니다.일부 구문은 Win32 버전에 따라 다를 수 있습니다.***

**개인 키 추출 및 해독**

WSA에서는 개인 키가 암호화되지 않아야 합니다.다음 OpenSSL 명령을 사용합니다.

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

"Enter Import **Password**(가져오기 **비밀번호 입력**)"라는 메시지가 표시됩니다. 위 ***11단계***에서 생성된 비밀번호입니다.
"Enter PEM pass phrase(PEM **암호 입력)"**도 **표시됩니다**. 는 암호화 비밀번호입니다(아래 사용).

이렇게 하면 "privatekey-encrypted.key"라는 암호화된 개인 키 파일이 생성됩니다.

이 키의 암호 해독된 버전을 만들려면 다음 명령을 사용합니다.

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

공개 및 암호 해독된 개인 키는 **'Security Services'** -> 'HTTPS **Proxy'**에서 WSA에 설치할 수 있습니다.