Hoe ik een PDF CA root certificaat en een sleutel van een Microsoft CA-server exporteren en converteren

Vraag:

Deze Kennis Base artikel verwijst naar software die niet onderhouden of ondersteund wordt door Cisco. Deze informatie wordt ter beschikking gesteld als hoffelijkheid voor uw gemak. Voor verdere assistentie kunt u contact opnemen met de verkoper van de software.

De volgende instructies zijn om een CA te exporteren die wortelcertificaat ondertekenen en sleutel van een Microsoft CA server 2003. Er zijn verschillende stappen in dit proces. Het is van cruciaal belang dat elke stap wordt gevolgd.

Het certificaat en de privé sleutel van MS CA server uitvoeren
1. Ga naar **'Start'** -> **'Run'** -> **MMC** 2. Klik op **'File'** -> **'Add / Remove Magnetisch-in'** 3. Klik op **'Add...'** knoop 4. Selecteer **'Certificaten'** en klik vervolgens op **'Toevoegen'** 5. Selecteer **'Computer-account'** -> **'Volgende'** -> **'Local Computer'** -> **'Finish'** 6. klik op **'Close'** -> **'OK'** ***De MMC is nu geladen met de Certificaten onverwacht.*** 7. **Certificaten** uitbreiden -> en op **'Persoonlijk'** klikken -> **'Certificaten '** 8. Klik met de rechtermuisknop op de juiste CA-indeling en kies **'Alle taken'** -> **'Exporteren'** ***De wizard Certificaat exporteren start*** 9. Klik op **'Next'** -> Selecteer **'Yes, Export the private key'** -> **'Next'** 10. ***Schakel*** hier alle opties uit. PKCS 12 moet de enige beschikbare optie zijn. Klik op **'Volgende'** 11. Geef de privétoets een wachtwoord naar keuze 12. Geef een bestandsnaam op om op te slaan als en klik op **'Volgende'**, dan **'Voltooien'**

U hebt nu uw CA-ondertekeningscertificaat en -wortel geëxporteerd als een PKCS 12 (PFX)-bestand.

De openbare toets uittrekken (certificaat)

U hebt toegang nodig tot een computer waarop OpenSSL wordt uitgevoerd. Kopieert uw PFX-bestand naar deze computer en voer de volgende opdracht uit:

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

Dit maakt het openbare sleutelbestand "certificaat.cer".

Opmerking: Deze instructies zijn geverifieerd met OpenSSL op Linux. Sommige syntaxis kan van de Win32-versie verschillen.

De privétoets uittrekken en decrypteren

De WSA vereist dat de privé sleutel wordt niet gecodeerd. Gebruik de volgende opdrachten van OpenSSL:

openssl pkcs12 -in <filename.pfx> -necerts -out, privé-versleuteld.key

U wordt gevraagd "**Wachtwoord voor importeren in te voeren**". Dit is het wachtwoord dat in ***stap 11*** hierboven is gemaakt.
U wordt ook gevraagd naar "**Voer de PEM-passterminologie in**". Het is het coderingswachtwoord (hieronder gebruikt).

Dit maakt het gecodeerde privé-sleutelbestand met de naam "privé-gecodeerde.key".

Om een gedecrypteerde versie van deze sleutel te maken, gebruik de volgende opdracht:

openssl rsa - in private - gecodeerd.key - out private.key

De openbare en gedecrypteerde privé sleutels kunnen op WSA van **'Security Services'** -> **'HTTPS Proxy' worden** geïnstalleerd