

## Question :

*Cet article de la base de connaissances met en référence le logiciel qui n'est pas mis à jour ou est pris en charge par Cisco. Les informations sont données comme courtoisie pour votre commodité. Pour davantage d'assistance, contactez s'il vous plaît le fournisseur de logiciels.*

Ce qui suit sont des instructions d'exporter un certificat racine de signature et la clé CA d'un serveur 2003 de Microsoft CA. Il y a plusieurs étapes dans ce processus. Il est crucial que chaque étape soit suivie.

### **Exporter le certificat et la clé privée du serveur du MS CA**

1. allez au « début » - > « exécuté » - > MMC
2. cliquez sur en fonction le « fichier » - > « ajout/suppression SNAP-dans »
3. Cliquez sur « ajoutent... » bouton
4. Les « Certificats choisis cliquent sur alors « ajoutent »
5. « compte d'ordinateur » choisi - > « ensuite » - > « ordinateur local » - > « finition »
6. clic « étroit » - > « CORRECT »

*Le MMC est maintenant chargé avec les Certificats SNAP-dans.*

7. développez les **Certificats** - > et cliquez sur en fonction « personnel » - > les « Certificats
8. Cliquez avec le bouton droit le CERT approprié CA et choisissez « toutes les tâches » - > « exportation »

*L'assistant d'exportation de certificat lancera*

9. cliquez sur « ensuite » - > choisi « oui, exportez la clé privée » - > « ensuite »
10. **Décochez toutes les** options ici. PKCS 12 devrait être la seule option disponible. Clic « ensuite »
11. Donnez à la clé privée un mot de passe de votre choix
12. Donnez un nom du fichier pour sauvegarder en tant qu'et pour cliquer sur « prochain », puis « terminez »

*Vous avez maintenant votre certificat de signature et racine CA exportés comme fichier PKCS 12 (PFX).*

### **Extrayant la clé publique (certificat)**

Vous avez besoin de l'accès à un ordinateur exécutant OpenSSL. Copiez votre fichier PFX plus de sur cet ordinateur et exécutez la commande suivante :

```
openssl pkcs12 - dans <filename.pfx> - clcerts - nokeys - certificate.cer
```

Ceci crée le fichier principal public nommé « certificate.cer »

*Remarque: Ces instructions ont été vérifiées utilisant OpenSSL sur le Linux. Une certaine syntaxe peut varier sur la version de Win32.*

#### **Extrayant et déchiffrant la clé privée**

Le WSA exige que la clé privée soit décryptée. Utilisez les commandes suivantes d'OpenSSL :

```
openssl pkcs12 - dans <filename.pfx> - nocerts - privatekey-encrypted.key
```

Vous serez incité pour « **entrez le mot de passe d'importation** ». C'est le mot de passe créé dans l'*étape 11* ci-dessus.

Vous serez également incité pour « **écrivez le mot de passe PEM** ». Est le mot de passe de cryptage (utilisé ci-dessous).

Ceci créera le fichier principal privé chiffré nommé « privatekey-encrypted.key »

Pour créer une version déchiffrée de cette clé, utilisez la commande suivante :

```
openssl RSA - dans privatekey-encrypted.key - private.key
```

Le public et les clés privées déchiffrées peuvent être installés sur le WSA des « **Services de sécurité** - > « **proxy HTTPS** »