Comment exporter et convertir un certificat et une clé racine d'autorité de certification pfx à partir d'un serveur d'autorité de certification Microsoft ?

Question :

Cet article de la base de connaissances se rapporte à un logiciel qui n'est pas mis à jour ou pris en charge par Cisco. Les informations sont fournies comme courtoisie pour votre commodité. Pour plus d'assistance, communiquez avec le fournisseur du logiciel.

Les instructions suivantes permettent d'exporter un certificat et une clé racine de signature d'autorité de certification à partir d'un serveur d'autorité de certification Microsoft 2003. Ce processus comporte plusieurs étapes. Il est essentiel que chaque étape soit suivie.

Exportation du certificat et de la clé privée à partir du serveur MS CA
1. Accédez à **'Démarrer'** -> **'Exécuter'** -> **MMC** 2. Cliquez sur **'Fichier'** -> **'Ajouter/Supprimer un composant logiciel enfichable'** 3. Cliquez sur le **'Ajouter...'.** bouton 4. Sélectionnez **'Certificats**, puis cliquez sur **'Ajouter'** 5. Sélectionnez **Compte d'ordinateur** -> **Suivant** -> **Ordinateur local** -> **'Terminer'** 6. cliquez sur **'Fermer** -> **OK'** *Le MMC est maintenant chargé avec le composant logiciel enfichable Certificats.* 7. Développez **Certificats** -> et cliquez sur **'-> 'Certificats'** 8. Cliquez avec le bouton droit de la souris sur le certificat d'autorité de certification approprié et choisissez **'Toutes les tâches** -> **'Exporter'** *L'Assistant Exportation de certificats va démarrer* 9. Cliquez sur **'Suivant** -> Sélectionnez **'Oui, Exporter la clé privée'** -> **'Suivant'** 10. ***Désélectionnez toutes*** les options ici. PKCS 12 doit être la seule option disponible. Cliquez sur **Suivant** 11. Donnez à la clé privée un mot de passe de votre choix

12. Donnez un nom de fichier à enregistrer et cliquez sur **'Suivant**, puis **'Terminer'**

Votre certificat de signature CA et votre racine sont maintenant exportés sous forme de fichier PKCS 12 (PFX).

Extraction de la clé publique (certificat)

Vous aurez besoin d'accéder à un ordinateur exécutant OpenSSL. Copiez votre fichier PFX sur cet ordinateur et exécutez la commande suivante :

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

Ceci crée le fichier de clé publique nommé « certificate.cer »

Note: Ces instructions ont été vérifiées à l'aide d'OpenSSL sous Linux. La syntaxe peut varier dans la version Win32.

Extraction et déchiffrement de la clé privée

Le WSA exige que la clé privée ne soit pas chiffrée. Utilisez les commandes OpenSSL suivantes :

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

Vous serez invité à entrer "**Enter Import Password**« . Il s'agit du mot de passe créé à l'*étape 11* ci-dessus.
Vous serez également invité à saisir la **phrase de passe PEM**. Le est le mot de passe de chiffrement (utilisé ci-dessous).

Cela créera le fichier de clé privée chiffré nommé « private-key-encryption.key »

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

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

Les clés privées publiques et décryptées peuvent être installées sur le WSA à partir du **proxy HTTPS -> Services de sécurité**