Wie exportiere und konvertiere ich ein pX CA-Root-Zertifikat und einen pX-Schlüssel von einem Microsoft CA-Server?

Frage:

Dieser Knowledge Base-Artikel bezieht sich auf Software, die nicht von Cisco verwaltet oder unterstützt wird. Die Informationen werden Ihnen zu Ihrer Zufriedenheit zur Verfügung gestellt. Wenden Sie sich für weitere Unterstützung an den Softwareanbieter.

Im Folgenden finden Sie Anweisungen zum Exportieren eines Root-Zertifikats und -Schlüssels der Zertifizierungsstellen eines Microsoft CA-Servers 2003. Dieser Prozess umfasst mehrere Schritte. Jeder Schritt muss unbedingt befolgt werden.

Exportieren des Zertifikats und des privaten Schlüssels vom MS CA-Server
1. Gehen Sie zu **'Start'** -> **'Run'** -> **MMC.** **2.** Klicken Sie auf **'Datei'** -> **'Snap-In hinzufügen/entfernen'.** **3.** Klicken Sie auf **'Hinzufügen..'.** Schaltfläche **4.** Wählen Sie **'Zertifikate'** und klicken Sie dann auf **'Hinzufügen'.** **5.** Wählen Sie **'Computerkonto'** ->**'Weiter'** -> **'Lokaler Computer'** -> **'Fertig stellen' aus.** **6.** Klicken Sie auf **'Schließen'** -> **'OK'.** ***Der MMC wird nun mit dem Snap-In "Zertifikate" geladen.*** **7.** Erweitern Sie **Zertifikate** ->, und klicken Sie auf **'Personal'** -> **'Certificates'.** **8.** Klicken Sie mit der rechten Maustaste auf das entsprechende Zertifizierungsstellenzertifikat, und wählen Sie **"Alle Aufgaben"** -> **"Exportieren" aus.** ***Der Assistent für den Zertifikatsexport wird gestartet.*** **9.** Klicken Sie auf **'Weiter'** -> Wählen Sie **'Ja, den privaten Schlüssel exportieren'** -> **'Weiter'.** **10.** ***Deaktivieren Sie alle*** Optionen hier. PKCS 12 sollte die einzige verfügbare Option sein. Klicken Sie auf **"Weiter".** **11.** Geben Sie dem privaten Schlüssel ein Kennwort Ihrer Wahl.

12. Geben Sie einen Dateinamen ein, der gespeichert werden soll, und klicken Sie auf **"Weiter"** und dann auf **"Fertig stellen".** ***Sie haben nun Ihr Zertifizierungsstellenzertifikat und Ihren Root als PKCS 12 (PFX)-Datei exportiert.***

Extrahieren des öffentlichen Schlüssels (Zertifikat)
Sie benötigen Zugriff auf einen Computer, auf dem OpenSSL ausgeführt wird. Kopieren Sie die PFX-Datei auf diesen Computer und führen Sie den folgenden Befehl aus: ***openssl pkcs12 -in <Dateiname.pfx> -clcerts -nokeys -out certificate.cer*** Dadurch wird die öffentliche Schlüsseldatei mit dem Namen "certificate.cer" erstellt.

Hinweis: Diese Anweisungen wurden mit OpenSSL unter Linux verifiziert. Einige Syntax kann von der Win32-Version abweichen.

Extrahieren und Entschlüsseln des privaten Schlüssels
Für die WSA muss der private Schlüssel unverschlüsselt sein. Verwenden Sie die folgenden OpenSSL-Befehle: ***openssl pkcs12 -in <Dateiname.pfx> -nocerts -out privatekey-encrypted.key*** Sie werden zur Eingabe des **Importpassworts** aufgefordert. Dabei handelt es sich um das in ***Schritt 11*** erstellte Kennwort. Sie werden auch zur Eingabe der **PEM-Kennzeichenfolge** aufgefordert. Das ist das Verschlüsselungskennwort (wird unten verwendet). Dadurch wird die verschlüsselte private Schlüsseldatei namens "privatekey-encrypted.key" erstellt. Um eine entschlüsselte Version dieses Schlüssels zu erstellen, verwenden Sie den folgenden Befehl: **openssl rsa -in privatekey-encrypted.key -out private.key**

Die öffentlichen und entschlüsselten privaten Schlüssel können in der WSA über **'Security Services'** -> **'HTTPS Proxy'** installiert werden.