Microsoft CA サーバから pfx CA ルート証明書とキーをエクスポートして変換するにはどうしますか。

質問：

このナレッジ ベース記事では、シスコによる保守およびサポートの対象でないソフトウェアを参照しています。この情報は、利便性のために無償で提供されています。さらにサポートが必要な場合は、ソフトウェアのベンダーに連絡してください。

Microsoft CAサーバ2003からCA署名ルート証明書とキーをエクスポートする手順は、次のとおりです。このプロセスには、いくつかのステップがあります。各ステップに従うことが重要です。

MS CAサーバからの証明書と秘密キーのエクスポート
1. 'Start' -> 'Run' -> MMCに移動します 2.「ファイル」 ->「スナップインの追加と削除」をクリック 3. [追加]をクリックしてください。 ボタン 4. [証明書]を選択し、[追加]をクリックします 5. 'コンピュータアカウント' -> '次' -> 'ローカルコンピュータ' -> "完了"を選択してください 6.[閉じる] -> [OK]をクリックします。 *これで、MMCに[証明書]スナップインがロードされました。* 7. [Certificates]を展開し、[Personal] -> [Certificates]をクリックします。 8.適切なCA証明書を右クリックし、[All Tasks] -> [Export]を選択します *証明書エクスポートウィザードが起動します* 9.[次へ]をクリックし、[はい、秘密キーを書き出す] -> [次へ]を選択 10.ここですべてのオプションをオフにします。PKCS 12は、使用可能な唯一のオプションである必要があります。[次へ]をクリックします 11.秘密キーに任意のパスワードを指定します 12.名前を付けて保存するファイル名を指定し、「次へ」をクリックし、「終了」をクリックします

これで、CA署名証明書とルートがPKCS 12(PFX)ファイルとしてエクスポートされました。

公開キー（証明書）の抽出

OpenSSLを実行しているコンピュータにアクセスする必要があります。PFXファイルをこのコンピュー

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

これにより、「certificate.cer」という名前の公開キーファイルが作成されます

注：これらの手順は、Linux上のOpenSSLを使用して検証されています。構文によっては、Win32バージョンによって異なる場合があります。

秘密キーの抽出と復号化

WSAでは、秘密キーの暗号化を解除する必要があります。次のOpenSSLコマンドを使用します。

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

「Enter Import Password」というプロンプトが表示されます。 これは、上記のステップ11で作成したパスワードです。
「Enter PEM pass phrase」というプロンプトも表示されます。 は暗号化パスワードです（以下で使用）。

これにより、「privatekey-encrypted.key」という名前の暗号化された秘密キーファイルが作成されます

このキーの復号化されたバージョンを作成するには、次のコマンドを使用します。

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

公開キーと復号化された秘密キーは、[セキュリティサービス] -> [HTTPSプロキシ]からWSAにインストールできます