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。 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 ベンダーに連絡してください。

以下は Microsoft CA サーバ 2003 年から CA 署名ルート証明およびキーをエクスポートする指示です。 このプロセスにいくつかのステップがあります。 各ステップに従うことは重大です。

MS CA サーバから証明書およびプライベートキーをエクスポートすること
1. - > **「実行される」** - > MMC は**「開始」**に行きます 2. **「ファイル」を**クリックして下さい- > **「追加して下さい/取除いて下さいスナップイン」を** 3. **「追加します...」**クリックして下さい ボタン 4.選定された**「証明書は**それから**「追加します」**クリックします 5.選定された**「コンピューター アカウント」** - > **「次に」** - > **「ローカル コンピュータ」** - > **「完了** 6.クリックして下さい**「密接」** - > **「良い」** ***MMC にスナップ式証明書が今ロードされます。*** 7.**証明書**- > **「個人的」**クリックすれば- > **「証明書**拡張して下さい 8.適切な CA 証明書を右クリックし、**「すべてのタスク」を**- > **「エクスポート」**選択して下さい ***証明書 Export ウィザードは起動します*** 9. **「次に」**クリックして下さい- > 「選り抜き**はい、プライベートキー」をエクスポートして下さい**- > **「次に」** 10.オプション***すべての***ここに***チェックを外して下さい***。 PKCS 12 は利用可能な唯一のオプションであるはずです。 **「次に」**クリックして下さい 11.プライベートキーに選択のパスワードを与えて下さい

12. として保存し、**「次に」**クリックするためにファイル名をそして**「完了**与えて下さい

今 PKCS 12（PFX）ファイルとしてエクスポートされる CA 署名証明書およびルートがあります。

得ます公開キー（証明書）を

必要とします実行しているコンピューター OpenSSL へのアクセスを。 PFX ファイルをこのコンピュータにコピーし、次のコマンドを実行して下さい:

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

これは作成します「certificate.cer」と名付けられる公開キー ファイルを

注： これらの手順は Linux の OpenSSL を使用して確認されました。 構文は Win32 バージョンで変わるかもしれません。

プライベートキーを得、復号化します

WSA はプライベートキーが非暗号化であることを必要とします。 OpenSSL 次のコマンドを使用して下さい:

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

のために**「入力しますインポート パスワード」**をプロンプト表示されます。 これは上記の***ステップ 11***で作成されるパスワードです。
またのために**「入力します PEM パスフレーズ」**をプロンプト表示されます。 暗号化パスワードはです（下記に使用される）。

これは作成します「privatekey-encrypted.key」と名付けられた暗号化されたプライベートキーファイル

このキーの復号化されたバージョンを作成するために、次のコマンドを使用して下さい:

openssl RSA - privatekey-encrypted.key で- private.key

パブリックおよび復号化されたプライベートキーは**「セキュリティ サービス**から WSA でインストールすることができます- > **「HTTPS プロキシ」**