

## 问题：

此知识库文章参考没有维护也思科不支持的软件。信息被提供作为礼貌为您的便利。对于进一步协助，请联系软件供应商。

下列是说明导出签署根证明和密钥从Microsoft CA服务器的CA 2003年。有在此进程的几个步骤。是关键每个步骤跟随。

<b>导出证书和专用密钥从MS CA服务器</b>
<ol style="list-style-type: none"><li>1.去‘开始’ -&gt; ‘运行’ -&gt; MMC</li><li>2.请点击‘文件’ -&gt; ‘请添加/删除管理单元’</li><li>3.点击‘添加...’按钮</li><li>4.挑选‘证书的然后单击‘添加’</li><li>5.挑选‘计算机帐户’ -&gt; ‘其次’ -&gt; ‘本地计算机’ -&gt; ‘芬通社’</li><li>6.请点击‘Close’ -&gt; ‘好’</li></ol> <p><b>MMC当前装载与卡扣式的证书。</b></p> <ol style="list-style-type: none"><li>7.请展开证书-&gt;和请点击‘个人’ -&gt; ‘证书的</li><li>8.用鼠标右键单击适当的CA cert并且选择‘所有任务的-&gt; ‘出口’</li></ol> <p><b>Export向导的证书将启动</b></p> <ol style="list-style-type: none"><li>9.请单击‘其次’ -&gt;挑选‘是，导出专用密钥’ -&gt; ‘其次’</li><li>10.不选定所有选项此处。PKCS12应该唯一选择取得到。单击‘其次’</li><li>11.给专用密钥您的选择密码</li><li>12.给文件名保存作为和单击‘其次’，然后‘请完成’</li></ol> <p><b>您当前有您的签署证书和根的CA导出作为PKCS12 (PFX)文件。</b></p>
<b>解压缩公共密钥(证书)</b>
<p>您需要对计算机运行Openssl的访问。复制您的PFX文件到此计算机并且运行以下命令：</p> <pre>openssl pkcs12 -在&lt;filename.pfx&gt; - clcerts - nokeys - certificate.cer</pre> <p>这创建名为“certificate.cer的”公共密钥关键文件</p>

**注意：**使用在Linux的Openssl这些说明验证。若干语法在Win32版本可能变化。

<b>解压缩和解密专用密钥</b>
-------------------

WSA要求专用密钥未加密。请使用以下Openssl命令：

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

将提示对于“回车导入密码”。这是在**步骤**创建的密码**11**以上。  
也将提示对于“回车PEM通行证惯用语”。是加密密码(下面使用)。

这将创建名为“privatekey-encrypted.key的”已加密专用密钥文件

要创建此密钥一个解密的版本，请使用以下命令：

```
openssl rsa -在privatekey-encrypted.key -private.key
```

公共和解密的专用密钥在从‘安全服务的WSA可以安装- > ‘HTTPS代理’