

Apache 2.26

服务器证书安装使用指南



上海数字证书认证中心有限公司

2010/01/05



文档说明:

本文档是 Apache 2.26 证书安装使用指南，主要描述如何产生密钥对，web 证书在线申请和如何将 web 证书安装到 Apache 2.26 web 服务器上，实现 SSL。

版本信息:

当前版本 3.0 技术支持中心

版权信息:

SHECA 是上海数字证书认证中心有限公司的注册商标和缩写。

UCA 是上海数字证书认证中心有限公司研究开发的通用证书系统的商标和缩写。

本文的版权属于上海数字证书认证中心有限公司，未经许可，任何个人和团体不得转载、粘贴或发布本文，也不得部分的转载、粘贴或发布本文，更不得更改本文的部分词汇进行转贴。

未经许可不得拷贝，影印。

Copyright @2008 上海数字证书认证中心有限公司

文档发行说明

当您阅读完本文档，您应该能解决如下问题：

- 1、WEB 服务器证书的请求文件 CSR 的产生；
- 2、WEB 服务器证书的在线申请；
- 3、WEB 服务器证书的安装；
- 4、WEB 服务器 SSL 安全配置；
- 5、SSL 双向认证的配置；
- 6、使您的系统信任 SHECA 根证书；

文档书写环境说明：

为了测试基于 apache2.26 WEB 服务的 SSL 双向认证，本文档采用了最新的 Apache2.26 WEB 服务。以下是本文档的具体试验环境：

WEB 服务器：Windows 2003 Enterprise Server Edition +Apache2.26

客户端：Windows XP Professional English Version + Service Pack 3

安装环境：

Web 服务器，本文以 windows 操作系统为例。系统正确安装 openssl 和 Apache 2.26 版本软件。

通过 OPENSSSL 工具为服务器申请证书：

本文采用标准的 openssl 方式为 WEB 服务器提供 Private key、Identity Cert 和 Trusted Cert 存储。

1、产生密钥：

在 windows 操作系统上打开“命令提示符”窗口，在命令行模式下运行

例：

```
Openssl genrsa 1024 > pri.key
```

在执行命令的目录下产生密钥 pri.key；

2、产生证书请求（CSR）：

再运行，例：

```
Openssl req -new -key pri.key > server.csr
```

此时系统会提示您输入你的信息，请确保以下内容和您提交到上海 CA 的内容一致，以保证服务器证书的签发。

Common Name（服务器域名或者 IP）

Organization name（组织名或公司名）

Organization unit name（组织单位名或部门名）

City or location name（城市或区域名）

State or province name（省份或者州名）

Country name（国家名的两位编码，中国为“CN”）

输入完毕后，在执行命令的目录下产生证书请求文件“server.csr”；

3、申请服务器证书：

将“server.csr”文件提交 SHECA，CA 处理完毕申请，用户下载证书，证书可以使用 PEM 格式；

获取服务器证书：

第一步：登陆<http://www.sheca.com>，点击**证书申请**→ **立即申请安全站点证书**，请点击>>；

在方框里输入从 SHECA 证书受理点获取的密码信封序列号和信封密码

(注:由于申请的是 WEB 服务器证书,所以设定的私钥密码不起作用)

申请证书

证书申请信息
请正确输入以下各项

请输入密码信封序列号:

请输入密码信封密码:

请设定私钥保护密码:

请确认私钥保护密码:

确认

第二步：完成输入后，进入下一个页面,此时选择勾选“**高级选项**”，并选择“**用户自上送 P10 证书请求**”并在最底部的输入框内贴入证书请求中去除 BEGIN 以及 END 的部分内容，如下图所示

生成P10

生成P10
请生成P10的方式

*没有检测到USBKey, 使用证书管理器下载证书。
如果您有USBKey但没有插上的话, 请插上USBKey并点击重新检测。
如果您要下载到其他地方请勾选“高级选项”!

高级选项

下一步 重新检测

*请选择生成密钥对和P10证书请求的方式

通过密码设备生成

通过证书管理器生成

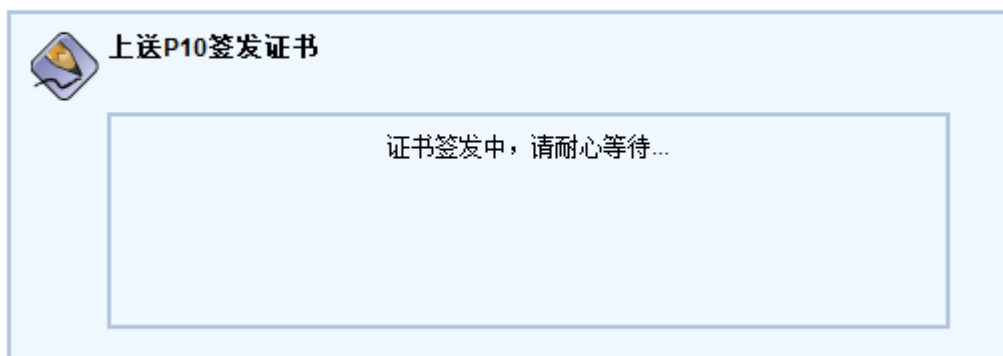
用户自上送P10证书请求

*如果P10证书请求中存在“-BEGIN...”与“-END...”部分, 请自行去除后上送。
在此贴入证书请求当中去除“-BEGIN...”“-BEGIN...”的部分

下一步

第三步：请耐心等待证书签发

上送P10签发证书

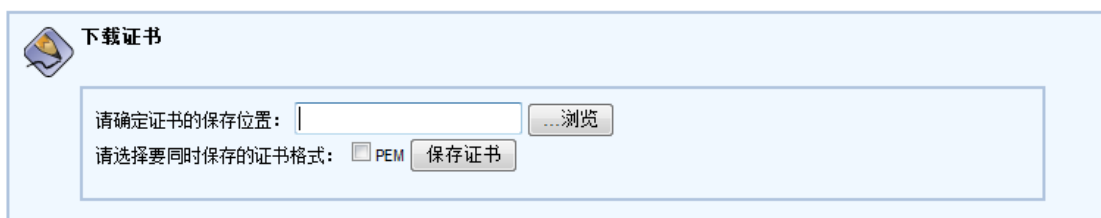


上送P10签发证书

证书签发中，请耐心等待...

第四步：请选择证书保存的路径，如需保存为 PEM 格式，则勾选“PEM”，并点击保存证书。

下载证书



下载证书

请确定证书的保存位置： ...浏览

请选择要同时保存的证书格式： PEM 保存证书

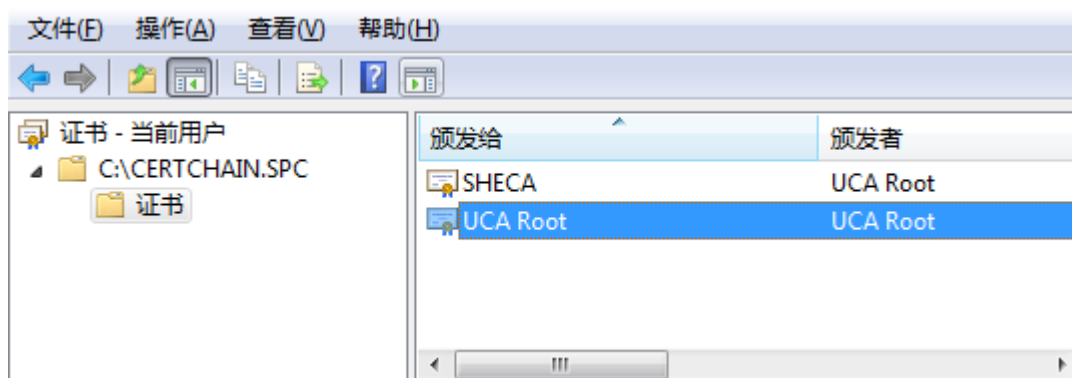
第五步：申请完证书之后，将证书文件保存。有必要说明的是，以上各种文件可以是 PEM 或 DER 格式。

注：Apache 服务器需要证书的格式为 PEM 格式，建议用户直接将证书勾选保存 PEM 格式，并得到 **UserCert.Cer** 文件，此文件可以在接下来的配置中直接使用。

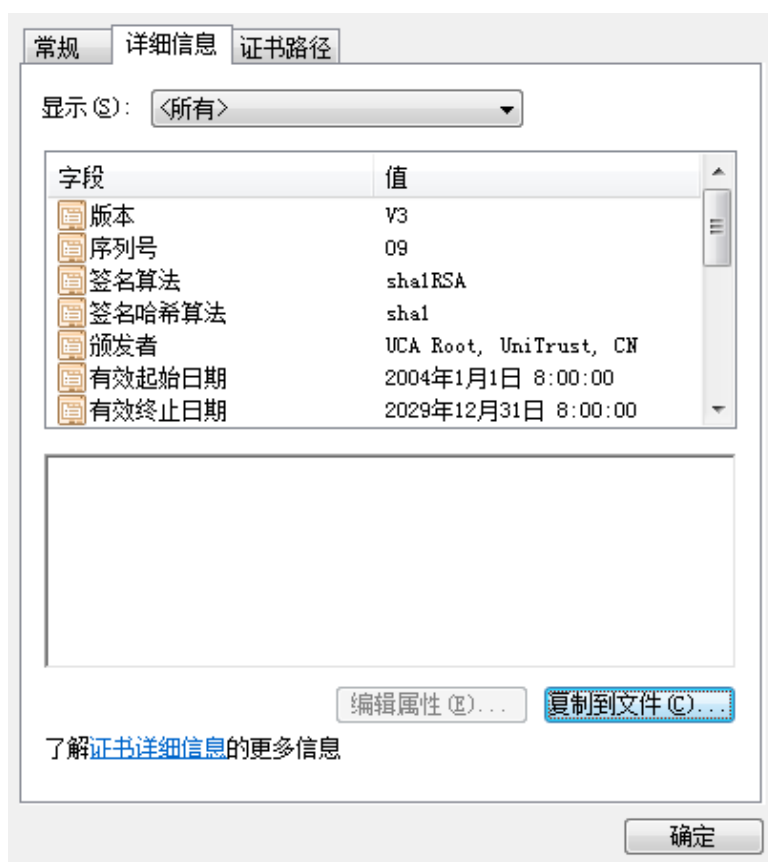
根证书以及中级证书的获取：

1、获取根证书 UCA Root:

将 CertChain.SPC 文件打开，选中 UCA Root 这张证书右键选择“打开”



在详细信息的标签栏中选择“复制到文件”



选择 Base64 编码导出证书

导出文件格式

可以用不同的文件格式导出证书。

选择要使用的格式：

- DER 编码二进制 X.509 (.CER) (D)
- Base64 编码 X.509 (.CER) (S)
- 加密消息语法标准 - PKCS #7 证书 (.P7B) (C)
 - 如果可能，则数据包括证书路径中的所有证书 (I)
- 个人信息交换 - PKCS #12 (.PFX) (F)
 - 如果可能，则数据包括证书路径中的所有证书 (U)
 - 如果导出成功，删除密钥 (K)
 - 导出所有扩展属性 (A)
- Microsoft 序列化证书存储 (.SST) (T)

[了解证书文件格式的详细信息](#)

< 上一步 (B) 下一步 (N) > 取消

保存为文件 root.cer

2、获取中级证书 SHECA

按照步骤一，同样的将 CertChain.SPC 文件当中的 SHECA 证书导出为 sheca.cer

配置 APACHE2.26

- 1、打开 Apache 服务器中的 httpd.conf 文件，打开 SSL 模块

```
LoadModule ssl_module modules/mod_ssl.so
```

```
Include conf/extra/httpd-ssl.conf
```

- 2、打开 Apache 服务器中的 ssl.conf 文件，并在相关配置的地方修改

SSLCertificateFile conf/ssl.crt/UserCert.Cer 部署服务器证书（PEM 格式）

SSLCertificateKeyFile conf/ssl.crt/pri.key 部署密钥，既步骤一所生成

SSLCertificateChainFile conf/ssl.crt/sheca.cer 部署中级证书，即 sheca.cer

SSLCACertificateFile conf/ssl.crt/root.cer 部署根证书，即 root.cer

SSLVerifyClient require 是否客户端验证，如需验证则为 require，无需为 none

SSLVerifyDepth 2 可查找 CA 证明

- 3、配置结束后重启 Apache 服务器，并连接<https://localhost:443>测试