



**数安时代科技股份有限公司**

**GDCA 信鉴易® SSL 服务器证书部署指南**

**For 深信服 VPN**

修订日期：2017/06/08

## 目录

一、 部署前特别说明.....	3
一、 合成 PFX 证书.....	4
1. 获取证书.....	4
2. 私钥证书.....	4
3. 合成证书.....	5
二、 安装 SSL 证书 .....	5
1. 测试 SSL 证书 .....	6
三、 服务器证书的备份.....	6
四、 服务器证书的恢复.....	6



## 一、部署前特别说明




1. GDCA 信鉴易® SSL 服务器证书部署指南(以下简称“本部署指南”)主要描述如何生成证书请求和如何将 SSL 服务器证书部署到 JBoss 服务器
2. 本部署指南的适用范围：深信服 VPN 设备
3. 深信服 VPN 部署恒信企业 EV SSL 和睿信 SSL 证书的操作步骤一致, 区别在于: 前者在 IE7 以上浏览器访问时, 浏览器会显示安全锁标志, 地址栏会变成绿色; 而后者在浏览器访问时, 浏览器显示安全锁标志, 但地址栏不会变绿色。
4. 本部署指南使用 testweb.95105813.cn 作为样例进行安装配置, 实际部署过程请用户根据正式的域名进行配置。



## 一、合成 PFX 证书

### 1. 获取证书

在您完成申请 GDCA 服务器证书的流程后，GDCA 将会在返回给您的邮件中附上根证书 GDCA\_TrustAUTH\_R5\_ROOT.cer 和相应的 CA 证书。如果您申请的是 OV SSL 证书（Organization Validation SSL Certificate），CA 证书就是文件就是 GDCA\_TrustAUTH\_R4\_OV\_SSL\_CA.cer；如果您申请的是 EV SSL 证书（Extended Validation SSL Certificate），CA 证书就是文件就是 GDCA\_TrustAUTH\_R4\_EV\_SSL\_CA.cer,请确认所收到的证书文件是您需要的 CA 证书。（注意：所发至邮箱的文件是压缩文件，里面有 3 张证书，请确认所收到的证书文件是您需要的 CA 证书文件）

名称	修改日期	类型
 GDCA TrustAUTH R4 EV SSL_CA.cer ← 中级证书	2017/5/3 9:50	安全证书
 GDCA TrustAUTH R5 ROOT.cer ← 顶级证书	2017/5/3 9:50	安全证书
 testweb.95105813.cn.crt ← 公钥证书	2017/5/3 10:52	安全证书

Globalsign 产品获得证书如下图：

名称	修改日期	类型	大小
 证书文件.crt	2017/5/24 14:37	安全证书	3 KB
 中级根.crt	2017/5/24 14:37	安全证书	2 KB

### 2. 私钥证书

请找到之前提交 csr 时会生成一个.key 文件，该文件为证书的私钥，后面配置要用到。

名称	修改日期	类型	大小
 testweb.95105813.cn.csr	2017/5/24 14:37	CSR 文件	3 KB
 testweb.95105813.cn.key ← 证书私钥	2017/5/24 14:37	KEY 文件	2 KB



### 3. 合成证书

- 1)用浏览器打开以下链接: <https://www.trustauth.cn/SSLTool/>
- 2)选择右侧的“在线导出 PFX、PKCS12”
- 3)用记事本或者文本编辑器打开上面的证书文件和私钥文件,根据下图填入合成证书信息,导出后会下载一个 [www.domainname.com.pfx](#) 的文件,保存好这个文件。

数安时代 | SSL免费工具

#### 在线导出PFX、PKCS12

证书

```
FHQ08NfRdbSIHriesZuVn+kH9mvRZ7nJ0yfaF2UYuHJoGX4nddSdGCwAjvK5vhA  
WGrfdQ8QG1+2sMN9Q5hVaaAK0dChFzr6xvDy 1pjh8hH/zxW8Arh98iCez5yKYMutb  
95vc0vc3tRz3Qjgtv3W4P7880eMIe3hdmFDNwxkdKNet6o2I/wSQisbmm7feGaz/  
WQ1scdd0G1h5sq54lmwcdmJ+raL9fy+!wxTzQVP10KHMPAa55qY+!2yc4KQDc8  
XizT.GvUivotakeP97s!thoSeKge16cqlb1NSQ4xpueYYZUrc2wIDAQABo4IEPDCC
```

证书公钥

私钥 Private Key

```
34iUIMqnFYBBsaf8qPCDNI09C9BDaddLHlnupV0Y/XwNwukmf+F15Rbe4XsiWBj4Xdp6YkutUBKq  
8jahAoGAJU6IXpVGEHEuk9MOnKP7N2HTzYtqQOFCIJDhc6WqDJkwy/Daw6P5B3Z7ZTelrnGzv5FM  
Z0Mv2PeAkkKarsrswpPNIA5oHDQCv0QvVnsRoCmUHB5Zt826EtpHy/zD50GwsSghI060h6ki0ef  
Ve+dHx7ypNqNVmq+7BJW/q+M+/E=  
-----END PRIVATE KEY-----
```

证书私钥, key文件, 在生成csr的时候已经生成!

CA 证书

```
I87qDBKOlndJzqdUfy4oy9RU0LMeYmcl+Sfny+NmuCQbiWqJRGXy2UzSWBvMTsCV  
odTzY84I0qu/5ZR8LrYPZJwR2UcnnNvtGAMXOLRc3bqr07i5TelRS+Kiz6HzDm  
MTh89N1SvNTBCVXVmaU6Avu5gMUTu79bZRknl7OedSvps9AsUSoPocZXun4IRZZ  
Uw==  
-----END CERTIFICATE-----
```

中级证书

PFX密码

..... | pfx文件的密码, 请牢记!

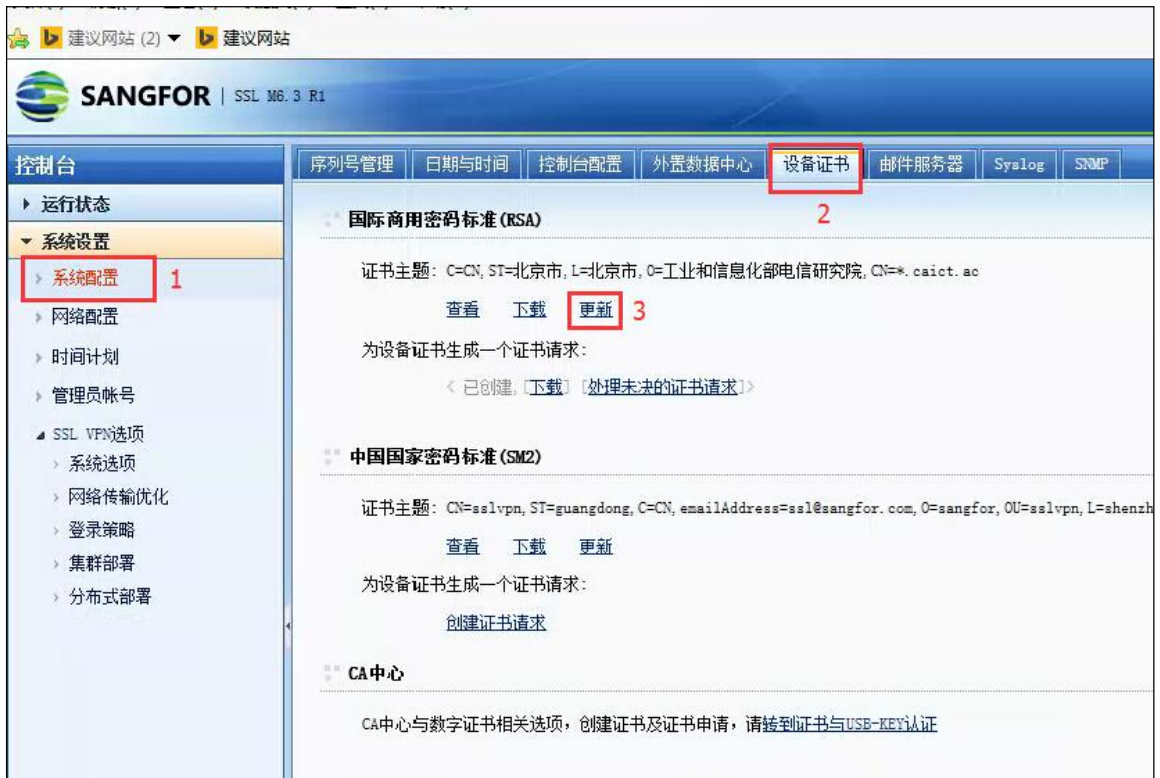
导出成PFX

客服热线: 95105813 粤ICP备05036352号 公安备案: 4406053010643

## 二、 安装 SSL 证书

- 1、需要按照如图下导入,登录深信服 SSL VPN 管理后台,点击系统配置--设置证书--更新,按照提示导入 pfx 证书,密码同压缩文件的密码。





## 2、保存重启生效 VPN

### 1. 测试 SSL 证书

默认的 SSL 访问端口号为 443，如果使用其他端口号，则您需要使用 `https://yourdomain:port` 的方式来访问您的站点，防火墙要开放相应的 port。

## 三、 服务器证书的备份

保存好生产的 PFX 文件即可完成服务器证书的备份操作。

## 四、 服务器证书的恢复

参照步骤“三、安装服务器证书”即可完成恢复操作

