



**数安时代科技股份有限公司**

**GDCA ® Tomcat5/6/7/8/9 SSL 服务器证书部  
署指南**

修订日期：2017/12/12

## 目录

|                                                          |   |
|----------------------------------------------------------|---|
| 一、 部署前特别说明 .....                                         | 3 |
| 二、 获取服务器证书 .....                                         | 3 |
| 1. 获取证书 .....                                            | 3 |
| 2. 私钥文件 .....                                            | 4 |
| 3. 合成证书 .....                                            | 4 |
| 三、 安装服务器证书 .....                                         | 5 |
| 1. 配置 TOMCAT .....                                       | 5 |
| 1) Tomcat 5 版本: (由于该版本漏洞较多, 建议立即升级到tomcat7+JDK1.7) ..... | 5 |
| 2) Tomcat 6/7/8 版本: .....                                | 5 |
| 3) Tomcat 9 版本: .....                                    | 6 |
| 2. 访问测试 .....                                            | 6 |
| 四、 服务器证书的备份及恢复.....                                      | 7 |
| 1. 服务器证书的备份 .....                                        | 7 |
| 2. 服务器证书的恢复.....                                         | 7 |



## 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”)主要描述如何通过 GDCA 在线系统产生密钥对证书部署到 Tomcat 服务器
2. 本部署指南适用于 linux、windows 系统下 Tomcat5/6/7/8/9 版本;
3. Tomcat 服务器部署恒信企业 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, 但地址栏不会变成绿色。
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。

## 二、获取服务器证书

### 1. 获取证书

在您完成申请数安时代 GDCA 服务器证书的流程后, 登录系统将会下载一个压缩文件, 使用压缩文件里面的 OtherServer.zip 文件

|                                                                                     |                         |                 |             |      |
|-------------------------------------------------------------------------------------|-------------------------|-----------------|-------------|------|
|  | ApacheServer.zip        | 2017/12/4 13:40 | 好压 ZIP 压缩文件 | 3 KB |
|  | IISServer.zip           | 2017/12/4 13:40 | 好压 ZIP 压缩文件 | 3 KB |
|  | NginxServer.zip         | 2017/12/4 13:40 | 好压 ZIP 压缩文件 | 3 KB |
|  | OtherServer.zip ← 解压此文件 | 2017/12/4 13:40 | 好压 ZIP 压缩文件 | 5 KB |
|  | README.txt              | 2017/12/4 13:40 | 文本文档        | 1 KB |

解压之后获得证书如下图:

| 名称                                                                                                                 | 修改日期            | 类型   |
|--------------------------------------------------------------------------------------------------------------------|-----------------|------|
|  issuer.crt ← 中级证书              | 2017/12/4 13:40 | 安全证书 |
|  root.crt                       | 2017/12/4 13:40 | 安全证书 |
|  testweb.95105813.cn.crt ← 证书公钥 | 2017/12/4 13:40 | 安全证书 |



## 2. 私钥文件

请找到之前提交 csr 时生成的.key 私钥文件，该文件为证书的私钥，请找到此文件，后面配置要用到此文件；

## 3. 合成证书

1)用浏览器打开以下链接: [https://www.trustauth.cn/SSLTool/tool/export\\_keystore.jsp](https://www.trustauth.cn/SSLTool/tool/export_keystore.jsp)

2) 用记事本或者文本编辑器打开上面的证书公钥、证书私钥、中级证书文件，根据下图填入合成证书信息，导出后会下载一个 `www.domainame.com.jks` 的文件，保存好这个文件。

 数安时代 | SSL免费工具

在线导出Keystore

CRT证书

NB67OKc8Mb168kOL6xbKrZveax74T7ZeSikfehTukfSUT6S9m3Z6vPFRepaogQ6D  
hz+Lr4ymzSesu...G4eH6mgMsW6Lhs5v5NuzB  
c/ozEmaV42kQtteqM/r2nUFtlq6voMxQX8MCLjp1vw1TMM=  
-----END CERTIFICATE-----

证书公钥  
test.95105813.cn.crt

私钥 Private Key

6AKCgYBXO...WKmjUed5OGRNMm0ch  
vSTdkjFhoVZ...74hVdvp7g9u6xov5mt6ZjcweUHEYt7Q55+qLUBvHKPKVGU+KZBk  
D+N/SH/nbk0VyjFoyNrsUpdhcA==  
-----END PRIVATE KEY-----

证书私钥key文件，在生成CSR文件生成  
test.95105813.cn.key

CA 根证书

tuJ/8Gq+SHSnQ1oIilvAnKmSw1hWLYfQf3/5QNqPIWYyXfqg8MMrbctUdl9R64lh  
pqVWVGKa4er...N3VOqGZq+IKi04ry5TdGSfj0U  
dlbDurgaToAZgdO7tpAXyVaYeiajjaBOQ4VUxafzHoYSMdGPc0LyBcZRqSn9WUJLJ  
huy30m27BYGiAk6XDZC711PQgi8fAoDXVEjX5o5u22Lkupzfz1AQJrw=  
-----END CERTIFICATE-----

中级证书 issuer.crt

Keystore密码

.....

证书安装密码，请牢记！

导出Keystore格式

在线生成CSR

在线解码CSR

在线解码CRT证书

证书和私钥匹配检测

在线导出PFX、PKCS12

在线导出Keystore

ROCA漏洞检测

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



## 三、 安装服务器证书

### 1. 配置 Tomcat

操作前备份 server.xml，以备错误时恢复,复制上面合成的 www.youdomain.com.jks 文件到 Tomcat 安装目录下的 conf 目录，使用文本编辑器打开 conf 目录下的 server.xml 文件，找到并修改以下内容

```
<!--  
    <Connector port="8443"...../>  
-->
```

默认情况下<Connector port="8443"...../>是被注释的，配置时需把“<!-- -->”去掉，然后对其节点进行相应的修改，需区分 tomcat 版本来修改。

#### 1) Tomcat 5 版本: (由于该版本漏洞较多，建议立即升级到 tomcat7+JDK1.7)

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol" port="443" maxHttpHeaderSize="8192"  
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75" SSLEnabled="true"  
    enableLookups="false" disableUploadTimeout="true"  
    acceptCount="100" scheme="https" secure="true"  
    keystoreFile="conf/gdca.jks" keystorePass="密钥库密码"  
    clientAuth="false" sslProtocol="TLS" />
```

#### 2) Tomcat 6/7/8 版本:

```
<Connector port="443" protocol="HTTP/1.1"  
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"  
    keystoreFile="keystore/www.youdomain.com.jks" keystorePass="证书密码"  
    clientAuth="false" sslProtocol="TLS"/>
```



### 3) Tomcat 9 版本:

```
<Connector port="443" protocol="HTTP/1.1"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    keystoreFile="keystore/www.youdomain.com.jks" keystorePass="证书密码"
    clientAuth="false" sslProtocols = "TLS" keyAlias="私钥别名"/>
```

#### 参数说明:

port: 端口号(默认 https 端口为 443);

KeystoreFile: 证书路径(例如: conf/name.jks);

KeystorePass: 证书密码(上面合成时设置的密码);

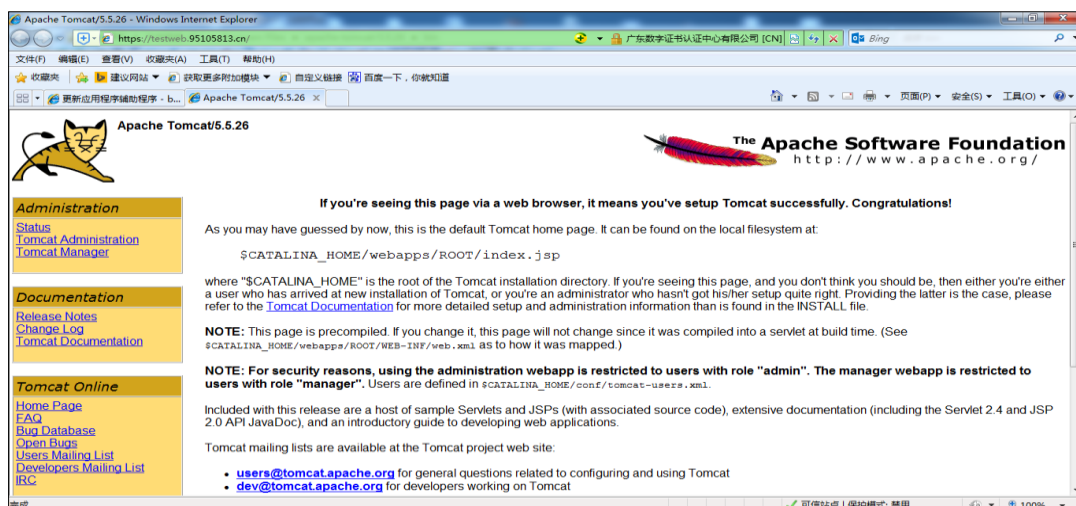
KeyAlias: 证书别名(Tomcat9 和以上版本需要配置这个参数, 别名为你的域名名称)

最后保存该配置文件, 然后重启 Tomcat 后再次访问即可。

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

## 2. 访问测试

服务器若部署了睿信 SSL 证书, 浏览器访问时将出现安全锁标志; 若部署了恒信企业 EV SSL 证书, 浏览器除了显示安全锁标志, 地址栏会变成绿色, 如下图:



## 四、 服务器证书的备份及恢复

在您成功的安装和配置了服务器证书之后，请务必依据下面的操作流程，备份好您的服务器证书，以防证书丢失给您带来不便。

### 1. 服务器证书的备份

备份服务器证书密钥库文件 `www.youdomain.com.jks` 文件即可完成服务器证书的备份操作。

### 2. 服务器证书的恢复

请参照服务器证书安装部分，将服务器证书密钥库 `www.youdomain.com.jks` 文件恢复到您的服务器上，并修改配置文件，恢复服务器证书的应用。若服务器证书丢失，请联系 GDCA 重新签发。

