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 Tomcat5/6/7/8/9 版本

修订日期：2017/05/25

目录

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

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 Tomcat 服务器
2. 本部署指南的适用范围：Tomcat 5/6/7/8/9 版本,Tomcat4 以下版本(含 Tomcat 4)没有经过严格测试
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。

一、 合成 JKS 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*）

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

Globalsign 产品获得证书如下图：

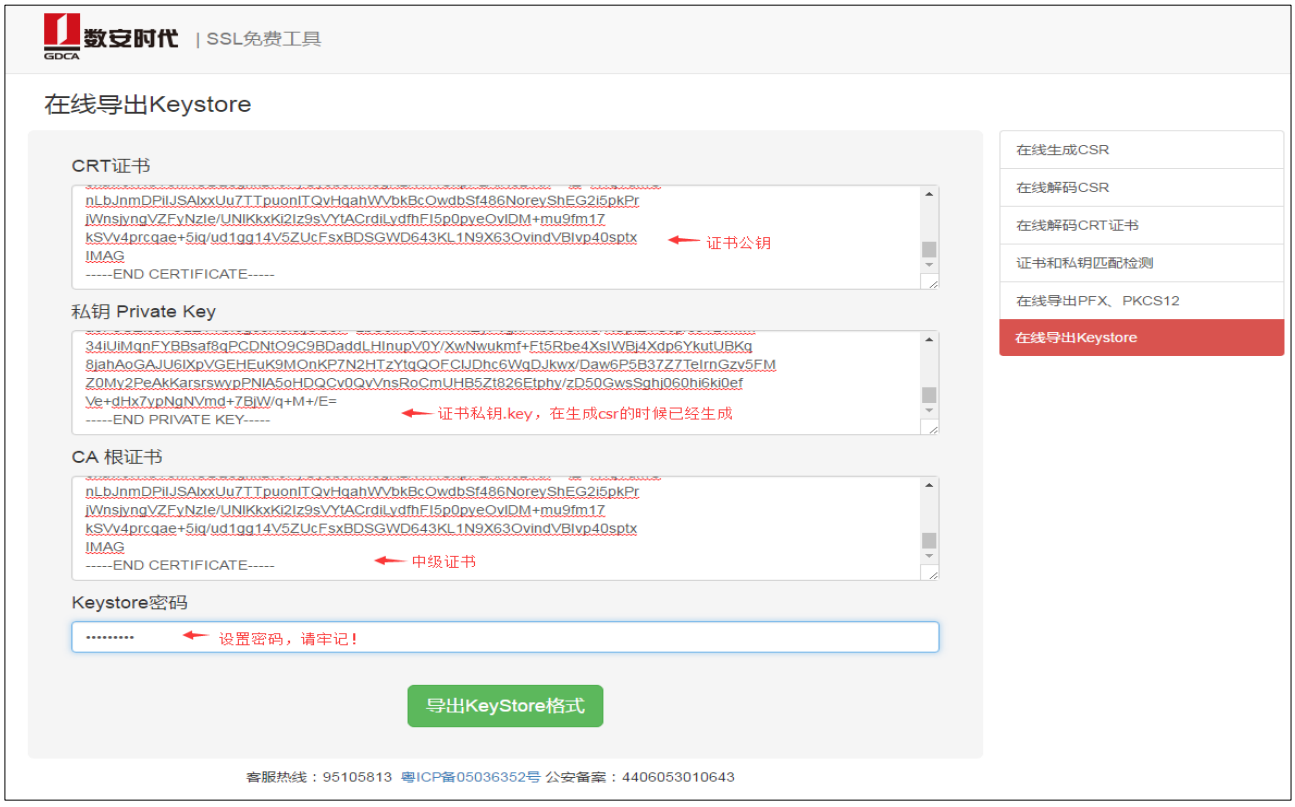
2. 私钥证书

请找到提交 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。

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

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。



地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

二、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="org.apache.coyote.http11.Http11Protocol"
                maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
                keystoreFile="keystore/www.youdomain.com.jks"    keystorePass="证书密码"
                clientAuth="false" sslProtocol = "TLS"/>
```


地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

3) Tomcat 9 版本：

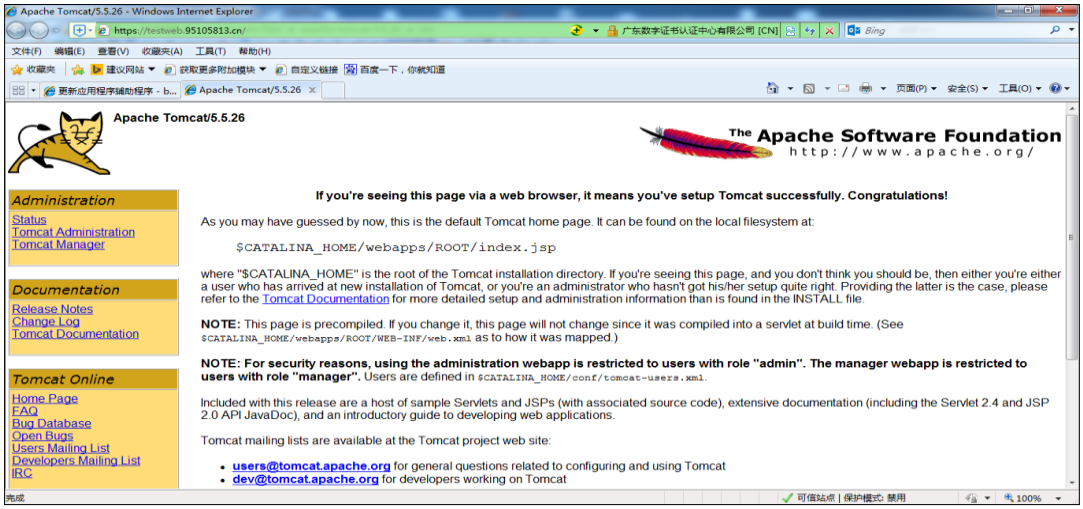
```
< Connector port="443" protocol="org.apache.coyote.http11.Http11Protocol"
                maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
                keystoreFile="keystore/www.youdomain.com.jks"    keystorePass="证书密码"
                clientAuth="false" sslProtocols = "TLS" keyAlias="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，则您需要使 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：



三、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

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

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。

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813