https访问相关key文件和配置

app和rcs上需要生成key文件的jdk命令已编写到bat文件中，key文件生成需要绑定服务器的ip地址的，故生成前请先编辑bat文件。

**第一步：生成key相关文件**

genkey\_app\_server.bat 生成APP应用的key

genkey\_rcs\_server.bat 生成RCS应用的key

你只需要作以下修改：

1. 修改第5行、第6行的IP地址，修改为App或RCS的服务器IP地址或域名；
2. 修改第11行的文件生成路径；

其它参数不能修改，特别是文件名和密码，这两个参数目前是写死在代码中的。

bat文件修改完成后，生成相应应用下的3个文件：

genkey\_app\_server.bat 生成文件：hesapptomcatserver.keystore、hesappclient.truststore、hesapptomcatserver.cer

genkey\_rcs\_server.bat 生成文件：hesrcstomcatserver.keystore、hesrcsclient.truststore、hesrcstomcatserver.cer

**第二步：拷贝文件**

将hesappclient.truststore拷贝到app应用的以下目录：webroot\WEB-INF\classes\

将hesrcsclient.truststore拷贝到rcs应用的以下目录：webroot\WEB-INF\classes\

**第三步：部署服务**

下面是实现https访问的相关配置，请按照以下步骤进行。

1. 将hesapptomcatserver.keystore (此文件由java命令生成)文件拷贝到tomcat目录下的tomcatkey(新建)目录，此目录与文件名在第2步中需要填写(红色字体部分)；
2. 配置Tomcat，打开$CATALINA\_HOME/conf/server.xml，修改如下，

<Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="8443" />

修改参数=>

<Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="443" />

<!--

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

clientAuth="false" sslProtocol="TLS"/>

-->

去掉注释且修改参数=>

<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

clientAuth="false" sslProtocol="TLS"

**keystoreFile="D:\\tomcat\\tomcatkey\\** **hesapptomcatserver.keystore " keystorePass="Asmsc2016!"**

/>

<!--

<Connector port="8009" enableLookups="false" protocol="AJP/1.3" redirectPort="8443" />

-->

修改参数=>

<Connector port="8009" enableLookups="false" protocol="AJP/1.3" redirectPort="443" />

1. 强制https访问

在应用程序web.xml中的</welcome-file-list>后面加上这样一段：

<login-config>

<!-- Authorization setting for SSL -->

<auth-method>CLIENT-CERT</auth-method>

<realm-name>Client Cert Users-only Area</realm-name>

</login-config>

<security-constraint>

<!-- Authorization setting for SSL -->

<web-resource-collection >

<web-resource-name >SSL</web-resource-name>

<url-pattern>/\*</url-pattern>

</web-resource-collection>

<user-data-constraint>

<transport-guarantee>CONFIDENTIAL</transport-guarantee>

</user-data-constraint>

</security-constraint>

1. 上述配置完成后，重启TOMCAT后即可以使用SSL。IE地址栏中可以直接输入地址不必输入“http://” 或者 “https://” ；也可以输入 “http:// ” 会跳转成为 “https://” 来登录

**RCS https访问的相关配置同上。keystoreFile="D:\\tomcat\\tomcatkey\\ hesrcstomcatserver.keystore " keystorePass="Asmsc2016!"**

附：

将一个证书文件导入java信任证书库，命令如下：

keytool -import -trustcacerts -alias tomcat\_pso -file [keystore] -keypass changeit -keystore "%JAVA\_HOME%/jre/lib/security/cacerts"

注：%JAVA\_HOME%/jre/lib/security/cacerts为java自带的证书库，默认密码为changeit

例如：

1、导入App客户端证书到java信任证书库

keytool -import -trustcacerts -alias hesapptomcatserver -file D:\tomcat\tomcatkey\server\app\hesapptomcatserver.cer -keypass Asmsc2016! -keystore cacerts

2、导入RCS客户端证书到java信任证书库

keytool -import -trustcacerts -alias hesrcstomcatserver -file D:\tomcat\tomcatkey\server\rcs\hesrcstomcatserver.cer -keypass Asmsc2016! -keystore cacerts