对接必读_V1.0

简介

- 该文档是第三方应用通过 PKI 中间件获取签名后与格尔安全认证网关对接进行验签操作时的参考 demo。
- 该 demo 支持 SM 算法和 PM 算法的验签。

术语简介

术语名	解释
验签 demo	指本 demo：供第三方应用参考对接格尔签名验签网关的验签接口。
PKI 中间件	格尔的 PKI 中间件服务：提供了签名、与 key 交互等接口。
SM 算法	商密算法
PM 算法	普密算法

提供的材料

1. 本 demo 的 war 包：`svsdemo.war`，可在 tomcat 中间件下直接运行。
2. 本 demo 的源码：`svsdemo-pkimiddleware.zip`，可用第三方应用参考验签的对接流程与实现。

对接流程

1 前提

第三方应用需要提前与格尔 PKI 中间件对接完成，成功获取到签名值与证书内容。

1. SM 算法
    1. 调用 PKI 中间件的 **P1 签名**接口获取签名内容
    2. 调用 PKI 中间件的**导出证书**接口获取证书内容
2. PM 算法
    1. 调用 PKI 中间件的**普通签名**接口获取 PM 算法签名内容
    2. 调用 PKI 中间件的**生成证书**接口获取 PM 算法证书内容

2 对接验签接口

1 首先导入外部依赖的 Jar。

参考 svsdemo-pkimiddleware\web\WEB-INF\lib

2 构造验签时需要的参数。

参考 demo 的 \svsdemo-pkimiddleware\src\com\koal\h9y\svs\demo\servlet\SvsDemoServlet.java 类中的 doGet() 方法。

```java
// 对接关键流程 START
SvsClientHelper svsClientHelper = SvsClientHelper.getInstance();
THostInfoSt tHostInfoSt = new THostInfoSt();

//设置网关ip+端口
svsClientHelper.initialize(gwIP, gwPort, MAX_WAIT_TIME, B_CIPHER, SOCKET_TIME_OUT);
tHostInfoSt.setSvrIP(gwIP);
tHostInfoSt.setPort(gwPort);

int result = 0;

// 注：签名原文需要传原文数据，而不是base64编码的数据
byte[] arrayOriginData = Base64.decode(originDataB64);

try {
    result = svsClientHelper.verifySign( nSignType: -1,  nSignStyle: -1, arrayOriginData,
            arrayOriginData.length, certContentB64, signDataB64, tHostInfoSt);
}catch (SvsClientException e) {
    System.err.println("验签失败！" + e);
    error = "签名验签失败，" + e.getMessage();
    sendResp(resp, error);
    return;
}
// 对接关键流程 END
```

3 demo 演示操作步骤

1. 将 war 包目录下的 svsdemo.war 拷贝至 tomcat 服务器的 webapps 目录下。如我本地的 tomcat 服务器目录为 D:\Program Files\apache-tomcat-8.5.11-windows-x64\

2. 启动 tomcat 程序。在 tomcat 安装目录的 bin 目录下，启动即可。
3. 访问该程序。如我本地的 tomcat 端口为 8080，则访问 http://localhost:8080/svsdemo/，填写对应的信息，点击“验签测试”，查看 tomcat 控制台对应的日志信息排查问题即可。

localhost:8080/svsdemo/

验签demo

注意：该demo为第三方应用提供验签功能的参考，目前支持SM和PM算法。demo流程执行流程已经调试通过，但是内部实现仅供参考！

网关IP：192.168.190.7

网关端口：10009

签名值(base64编码)：

签名原文(base64编码)：

注意：如果是SM算法，则调用PKI中间件的"导出证书"接口，将证书的base64内容粘贴至以下框中。

如果是PM算法，则只需要调用PKI中间件的"生成证书"接口，将证书的base64内容粘贴至以下框中。

证书内容(base64编码)：

验签测试