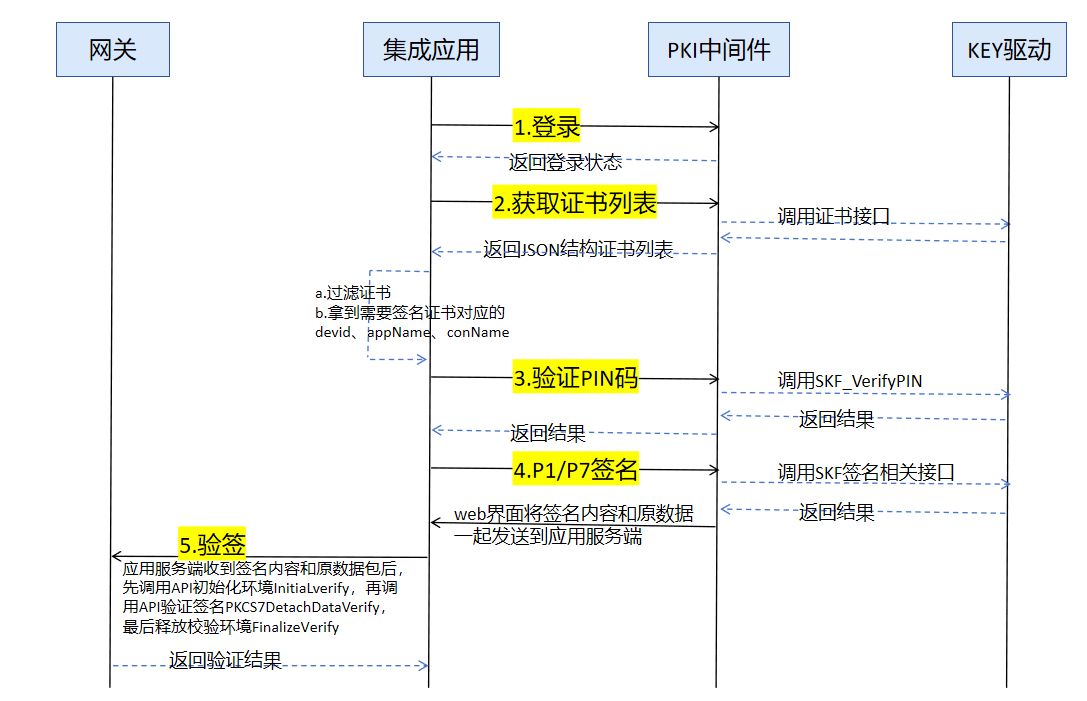
**绵阳H9Y应用对接格尔网关实现签名验签**

**的快速对接手册**

# 对接所需要的材料

# 二、时序图

主要关注带编号、背景为黄色的调用流程即可



# 三、集成注意事项

* 测试
* 请先安装中间件
* 集成过程
* 调用接口时，json数据解析/封装
* 有效数据过滤
* **过滤出签名key**
* 调用getAllCert后获得响应的json数据后，匹配manufacturer字段，将KOAL、 Microsoft \*\*数据过滤后，即为实际签名使用的key
* **过滤出签名证书**
* 调用getAllCert后获得响应的json数据后，keyUsage字段，0是加密证书、1是签名证书、2是签名加密证书。过滤keyUsage为1的数据即可
* 签名相关
* 具体查看签名快速集成指导以及PKI安全中间件接口规范
* 验签相关
* 具体查看对接说明

# 对接时需要调用的接口

**WEB应用集成**

* 具体接口调用看demo源码

**本地应用集成**

**1.登录**

* 初始化AGENT createAgent
* 登录Agent loginAgent

appName：ZF-App

appID：7ea7b92a-3091-3d79-639f-3ef4c3e2d6d7

token：7ea7b92a-3091-3d79-639f-3ef4c3e2d6d7

**2.获取证书列表**

* 获取证书列表接口 getAllCertList
* 解析证书列表接口参数 parseGetcertlist

列出签名证书 (通过这三个参数筛选正确的证书，signflag=1，keyUsage等于1或者2，issuerName.cn 颁发者是固定值，CAEPUserCA是商密，ZWYCA是pm)

弹窗显示 用户名列表，pin 输入框，用户选择某个证书，及输入pin

**3.验证PIN码**

* pin 校验，校验失败 提示错误，中止登录

**4.签名**

* 证书算法类型 SM2/RSA

1) 生成随机字符串

2）gSignx.syncSignData 签名数据

3）SyncDevice syncExportCertificate 导出证书数据

4) 将以上3个数据 传输到后台验签（发送至应用服务器，应用服务器调用网关接口验签）

* 证书算法类型 PM-BD

1) 生成随机字符串

2）gSignx.syncSignData 签名数据

3）SyncSignX syncDupCertWithTemplate 生成证书数据

4) 将以上3个数据 传输到后台验签（发送至应用服务器，应用服务器调用网关接口验签）

**5.验签**

* 应用服务端收到签名内容和原数据包后，先调用API初始化环境InitiaLverify，再调用API验证签名PKCS7DetachDataVerify，最后释放校验环境FinalizeVerify
* 返回验签结果至应用

