# 设备公钥导入文档

4

3

1

2

DeviceKeyImport

DBAdapter

FactorTool

FactorCryoter

HSMAdapter

## 接口1

URL：https:pkms.beanpodtech.com/key/import

Params:{MultipartFile file}

Response:{“code”:0,”message”:”密钥导入成功”}

### 加密文件结构

加密文件结构：

CTCount

Array<CipherText>

FactoryCrypterID

sign

encryptFileKey

Iv

CTCount:密文的条数，4字节

EncrypteFile:{CipherText,FactoryCrypterID,sign,encryptFileKey} 最终的加密文件由大括号四部分组成。

CipherText: AES256-CBC(deviceId ,publickey,timestamp:8,padding:8) 使用fileKey加密产生。

deviceId: {FactoryCrypterID:4,PhoneManufactureID:4,ChipManufactureID:4,SeManufactureID:4,ISEEVersion:4,DevSN:8,SeSN:8,RFU:12}

deviceId 由以上及部分组成。

publickey：32字节设备公钥

timestamp：8字节时间戳

Padding: 8字节填充

Mac：32字节mac

CipherText长度为：deviceId +publickey+timestamp+padding+Mac=48+32+8+8+32=128B

FactoryCrypterID：加密机ID, 4字节大小

Sign：RSA2048-PSS(CipherText,FactoryCrypterID) 使用加密机私钥签名

cipherText：上述密文

FactoryCrypterID：上述加密机ID

长度：256字节

encryptFileKey： RSA2048-OAEP(fileKey) 使用云端公钥加密。

fileKey：32字节 文件加密密钥，有终端加密软件随机产生，每个密钥对应一个文件。

Nonce:16字节随机数，每次调用AES256-CCM时随机产生。

### **加密和签名算法**

AES256-CCM:{byte[] plainData,byte[] key,int macSize,byte[] aad,byte[] Nonce} 需要以上几个参数。

PlainData:原数据

key:加密密钥

macSize: Mac字节数，定为16字节

aad:附加认证数据，固定 “1a2s3d4f5g”.getBytes

Nonce: 随机数，16字节

RSA2048-PSS-SHA256:{RSAKeyParameters prv,byte[] msg,byte[] slt}

prv:签名私钥

msg:准备签名的数据

Slt:盐值 ，复用aes-ccm的nonce。

RSA2048-OAEP:{RSAKeyParameters pubParameters, byte[] seed, byte[] plainData}

pubParameters:加密公钥

Seed：服用nonce

plainData：加密数据

## 接口2

说明：产线工具调用本地加密机（dongle）对数据做签名。

## 接口3

说明：云端调用加密机做filekey的解密。

注：依赖于HSMAdapter的重构项目。使用重构后的API。

云端密钥别名：“CloudDataEncryptKey”

## 接口4

说明：

1. 从DB获取FactorCrypter的公钥，做验签

新增Action：xxxx

1. 定义DeviceKey的数据表结构。

|  |  |  |
| --- | --- | --- |
| DevSN | deviceID | DevPubKey |
|  |  |  |

1. 存储DevicePubKey接口

新增Action：xxxx

# FactorCrypter

定义：产线HSM。

用途：用于产线和云端之间安全的传输数据，实现部分产线的关键逻辑。

本业务中，需要在HSM中实现整个上传文件的签名，以确保数据在上传过程中被篡改、伪造。

生产：

由豆荚根加密机派生，根加密机可以导出所有产线HSM的公钥给云端，云端保留一张映射表“FactorCryoterID -> FactorCryoterPubKey”

# 交付

|  |  |
| --- | --- |
| DeviceKeyImport | 微服务 |
| 设备密钥表 | 设计并实现 |
| 产线加密机密钥表 | 设计并实现 |
|  |  |
|  |  |