# Keystore接口文档

非对称密钥库类型为：JKS

Provider：SUN

对称密钥库类型为：jceks

Provider：SunJCE

## 密钥产生

### 对称密钥产生

@PostMapping(“/genSecretKey”)

String genSecretKey(String algorithm,int size,String alias)

algorithm: 算法(AES)

size: 密钥长度

alias: 密钥别名

响应：对称密钥的HexString

### 非对称密钥产生

@PostMapping(“/genKeyPair”)

String genKeyPair(String algorithm ,int size,String alias)

algorithm : 密钥算法

size: 密钥长度

alias : 密钥别名

响应：公钥HexString

### 云端公钥获取

@PostMapping(“/getPublickey”)

String getPublic(String alias)

Alias: 公钥别名

响应：公钥Base64编码

## 签名

签名算法：SHA256withRSA/PSS

@PostMapping(“/sign”)

byte[] sign([String](mk:@MSITStore:C:\\Users\\winter\\Desktop\\jdk\\jdk%20api%201.8_google.CHM::/java/security/../../java/lang/String.html" \o "class in java.lang) algorithm，String alias,byte[] originalData)

Algorithm:签名算法

alias : 别名主要用来指定密钥

originalData ：原数据

响应：签名数据

## 加密

加密算法：RSA/ECB/OAEPWithSHA-256AndMGF1Padding(1024,2048)

AES/CBC/NoPadding （128）

@PostMapping(“/cryptAndDecrypt/crypt”)

byte[] cipher([String](mk:@MSITStore:C:\\Users\\winter\\Desktop\\jdk\\jdk%20api%201.8_google.CHM::/java/security/../../java/lang/String.html" \o "class in java.lang) algorithm，String alias,byte[] plainData,String cipherType,byte[] iv)

Algorithm:签名算法

alias : 别名主要用来指定密钥

plainData：明文数据

cipherType:”0”:代表对称加密,”1”:代表非对称加密

Iv：加密向量，对称加密使用，非对称加密赋值为null

响应：加密后数据。

## 解密

算法：RSA/ECB/OAEPWithSHA-256AndMGF1Padding(1024,2048)

AES/CBC/NoPadding （128）

@PostMapping(“/cryptAndDecrypt/decrypt”)

byte[] cipher([String](mk:@MSITStore:C:\\Users\\winter\\Desktop\\jdk\\jdk%20api%201.8_google.CHM::/java/security/../../java/lang/String.html" \o "class in java.lang) algorithm，String alias,byte[] cipherData,String cipherType,byte[] iv)

Algorithm:签名算法

alias : 别名主要用来指定密钥

cipherData：密文数据

cipherType:”0”:代表对称加密,”1”:代表非对称加密

Iv：加密向量，对称加密使用，非对称加密赋值为null

响应：明文数据。

## 共享密钥的导入导出

密钥导入：

void importSecretKey(byte[] secretKey,String algorithm,String alias,String keyPass)

SecretKey: 使用云端公钥加密的密钥。

Algorithm：密钥算法

Alias:密钥别名  
keyPass：密钥密码

密钥导出：

byte[] exportSecretKey(String alias,String keyPass);

Alias：密钥别名

Keypass：密钥密码

响应：云端私钥加密的密钥