**AF-S300签名验签服务器**

**Java语言接口使用规范**

北京神州安付科技股份有限公司

2023-03-16

目录

**[1. 算法标识和数据结构 1](#_Toc19823)**

[1.1 获取设备信息 1](#_Toc9166)

[1.2 查询证书信任列表别名 1](#_Toc15084)

[1.3 解码数字信封 2](#_Toc25233)

[1.4 解码基于SM2算法的签名数据 3](#_Toc12695)

**[2. 签名服务器接口 3](#_Toc3032)**

[2.1 配置文件 3](#_Toc7052)

**[3. 设备接口描述 4](#_Toc29621)**

[3.1 获取随机数 4](#_Toc27995)

[3.2 获取设备信息 4](#_Toc29239)

[3.3 验证证书有效性 5](#_Toc26023)

[3.4 验证证书是否被吊销 5](#_Toc16126)

[3.5 导入CA证书 5](#_Toc10994)

[3.6 导出RSA公钥 5](#_Toc1630)

[3.7 RSA签名 6](#_Toc16563)

[3.8 对文件进行RSA签名运算 7](#_Toc27801)

[3.9 RSA验证签名 7](#_Toc22052)

[3.10 对文件进行RSA验证签名 9](#_Toc6144)

[3.11 RSA加密 10](#_Toc17510)

[3.12 RSA解密 11](#_Toc24821)

[3.13 SM2签名 12](#_Toc32500)

[3.14 基于证书的SM2签名 12](#_Toc32549)

[3.15 SM2文件签名 13](#_Toc4216)

[3.16 SM2内部密钥验证签名 14](#_Toc1399)

[3.17 SM2验证签名 14](#_Toc20353)

[3.18 使用内部密钥对文件进行 SM2验证签名运算 15](#_Toc19070)

[3.19 使用外部证书对文件进行SM2验证签名运算 16](#_Toc4522)

[3.20 SM2加密 17](#_Toc2416)

[3.21 SM2解密 17](#_Toc6446)

[3.22 导出SM2公钥 18](#_Toc10229)

[3.23 查询证书信任列表别名 19](#_Toc6151)

[3.24 获取证书个数 19](#_Toc12108)

[3.25 根据别名获取单个证书 19](#_Toc15617)

[3.26 获取应用策略 20](#_Toc15241)

[3.27 删除用户证书列表 20](#_Toc8810)

[3.28 获取服务器证书 20](#_Toc31244)

[3.29 根据策略名称，获取相应证书 21](#_Toc29513)

[3.30 获取证书中的OCSP URL地址 21](#_Toc22617)

[3.31 获取证书信息 21](#_Toc832)

[3.32 获取证书扩展信息 21](#_Toc20214)

[3.33 PKCS7格式的带签名的数字信封数据 22](#_Toc13956)

[3.34 PKCS7格式的签名数据 23](#_Toc20478)

[3.35 PKSC7格式的数字信封 23](#_Toc17039)

[3.36 PKSC7格式的签名数据 24](#_Toc24458)

[3.37 基于SM2算法的带签名的数字信封数据 25](#_Toc21887)

[3.38 基于SM2算法的签名数据 26](#_Toc19486)

[3.39 基于SM2算法的数字信封 26](#_Toc24888)

#### 算法标识和数据结构

**1.1获取设备信息**

|  |  |  |
| --- | --- | --- |
| 设备定义信息 | | |
| 字段名称 | 数据长度（字节） | 含义 |
| IssuerName | 40 | 设备生产厂商名称 |
| DeviceName | 16 | 设备型号 |
| DeviceSerial | 16 | 设备编号  包含：日期（8字符）、批次号（3字符）、流水号（5字符） |
| AsymAlgAbility | 2 |  |
| DeviceVersion |  | 密码设备内部软件的版本号 |
| StandardVersion |  | 密码设备支持的接口规范版本号 |
| SymAlgAbility |  | 所有支持的对称算法，表示方法为对称算法标识按位或运算结果 |
| HashAlgAbility |  | 所有支持的杂凑算法，表示方法为杂凑算法标识按位或运算结果 |
| BufferSize |  | 支持的最大文件储存空间 |

实际定义数据结构定义

public class DeviceInfo implements AFStruct {

private byte[] IssuerName = new byte[40];

private byte[] DeviceName= new byte [16];

private byte[] DeviceSerial = new byte[16];

private int DeviceVersion;

private int StandardVersion;

private int[] AsymAlgAbility = new int[2];

private int SymAlgAbility;

private int HashAlgAbility;

private int BufferSize;

}

###### 1.2 查询证书信任列表别名

|  |  |  |
| --- | --- | --- |
| 查询证书信任列表别名的数据结构定义 | | |
| 字段名称 | 数据长度（字节） | 含义 |
| certList |  |  |
| number |  |  |

实际定义数据结构定义

public class certAltNameTrustList {

private byte[] certList;

private int number;

}

###### 1.3 解码数字信封

1.3.1解码PKCS7格式的带签名的数字信封数据

|  |  |  |
| --- | --- | --- |
| 解码PKCS7格式的带签名的数字信封数据的数据结构定义 | | |
| 字段名称 | 数据长度（字节） | 含义 |
| data |  | 原始数据 |
| signerCertificate |  | 签名者证书 |
| digestAlgorithm |  | HASH算法 |
| signedData |  | Base64编码的签名值 |

实际定义数据结构定义

public class AFPkcs7DecodeData {

private byte[] data;

private byte[] signerCertificate;

private int digestAlgorithm;

private byte[] signedData;

}

1.3.2 解码基于SM2算法的带签名的数字信封数据

|  |  |  |
| --- | --- | --- |
| 解码基于SM2算法的带签名的数字信封数据的数据结构定义 | | |
| 字段名称 | 数据长度（字节） | 含义 |
| data |  | 原始数据 |
| signerCertificate |  | 签名者证书 |
| digestAlgorithm |  | HASH算法 |

实际定义数据结构定义

public class AFSM2DecodeSignedAndEnvelopedData {

private byte[] data;

private byte[] signerCertificate;

private int digestAlgorithm;

}

###### 1.4 解码基于SM2算法的签名数据

|  |  |  |
| --- | --- | --- |
| 解码基于SM2算法的签名数据的数据结构定义 | | |
| 字段名称 | 数据长度（字节） | 含义 |
| signedData |  | Base64编码的签名值 |

实际定义数据结构定义

public class AFSM2DecodeSignedData extends AFSM2DecodeSignedAndEnvelopedData {

private byte[] signedData;

}

#### 签名服务器接口

2.1 获取设备

AFSVDevice device = new AFSVDevice.Builder("192.168.10.40", 8008, "abcd1234") // 服务器IP、端口、设备为必须参数  
  
 //以下为可选参数 根据实际情况设置  
 .connectTimeOut(10000) // 连接超时时间，默认5秒  
 .responseTimeOut(10000) // 响应超时时间，默认10秒  
 .retryCount(3) // 重试次数，默认3次  
 .retryInterval(1000) // 重试间隔，默认1秒  
 .bufferSize(1024 \* 1024) // 缓冲区大小，默认1M  
 .channelCount(10) // 通道数，默认10个  
 .build();

#### 设备接口描述

###### 3.1 获取随机数

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] getRandom(int length) throws AFCryptoException; | |
| 作用 | 获取随机数，用户获取指定长度的随机数数据 | |
| 调用 | byte[] random = device.getRandom(5); | device说明：  AFSVDevice device =new AFSVDevice.Builder(host, port, passwd)  .responseTimeOut(100000)  .build(); |
| 参数 | length | 待取得随机数的长度 |
| 返回值 | 返回取得的随机数数据,Base64编码格式,需要解码后为length长度 | |

###### 

###### 3.2 获取设备信息

|  |  |  |
| --- | --- | --- |
| 方法 | public DeviceInfo getDeviceInfo() throws AFCryptoException; | |
| 作用 | 获取设备信息，用户获取密码机的设备信息,查看设备信息时，可使用DeviceInfo中的toString()方法。 | |
| 例如：System.out.println(device.getDeviceInfo().toString()); | |
| 私有参数 | IssuerName | 设备生产厂商名称 |
| DeviceName | 设备型号 |
| DeviceSerial | 设备编号  包含：日期（8字符）、批次号（3字符）、流水号（5字符） |
| DeviceVersion |  |
| StandardVersion | 密码设备内部软件的版本号 |
| AsymAlgAbility | 密码设备支持的接口规范版本号 |
| SymAlgAbility | 所有支持的对称算法，表示方法为对称算法标识按位或运算结果 |
| HashAlgAbility | 所有支持的杂凑算法，表示方法为杂凑算法标识按位或运算结果 |
| BufferSize | 支持的最大文件储存空间 |
| 返回值 | 返回签名验签服务器设备信息 | |

###### 3.3 验证证书有效性

|  |  |  |
| --- | --- | --- |
| 方法 | public int validateCertificate(byte[] base64Certificate) throws AFCryptoException; | |
| 作用 | 验证证书有效性，通过OCSP模式获取当前证书的有效性。 注：选择此方式验证证书有效性，需连接互联网，或者可以访问到待测证书的OCSP服务器。 | |
| 参数 | base64Certificate | 待验证的证书--BASE64编码格式 |
| 返回值 | 返回证书验证结果，0为验证通过 | |

###### 

###### 3.4 验证证书是否被吊销

|  |  |  |
| --- | --- | --- |
| 方法 | boolean isCertificateRevoked(byte[] base64Certificate, byte[] crlData) throws AFCryptoException; | |
| 作用 | 验证证书是否被吊销，通过CRL模式获取当前证书的有效性。 | |
| 参数 | base64Certificate | 待验证的证书--BASE64编码格式 |
| crlData | 待验证证书的CRL文件数据 --BASE64编码格式 |
| 返回值 | 返回证书验证结果 | true ：当前证书已被吊销, |
| false ：当前证书未被吊销 |

###### 3.5 导入CA证书(已经废弃)

|  |  |  |
| --- | --- | --- |
| 方法 | int addCaCertificate(byte[] caAltName, byte[] base64CaCertificate) throws AFCryptoException; | |
| 作用 | 导入CA证书 | |
| 参数 | caAltName: | ca证书别名 |
| base64CaCertificate | 待导入的CA证书--BASE64编码格式 |
| 返回值 | 返回CA证书导入结果，0为导入成功 | |

###### 3.6 导出RSA公钥

3.61 导出RSA签名公钥

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] getRSASignPublicKey(int index) throws AFCryptoException; | |
| 作用 | 导出RSA公钥，导出密码机内部对应索引和用途的RSA公钥信息 | |
| 参数 | index | 密码设备内部存储的RSA索引号 |
| 返回值 | 返回Base64编码的公钥数据,符合ASN.1 DER编码格式 | |

3.62 导出RSA加密公钥

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] getRSAEncPublicKey(int index) throws AFCryptoException; | |
| 作用 | 导出RSA公钥，导出密码机内部对应索引和用途的RSA公钥信息 | |
| 参数 | index | 密码设备内部存储的RSA索引号 |
| 返回值 | 返回Base64编码的公钥数据 | |

###### 3.7 RSA签名

3.7.1 使用RSA内部密钥进行签名运算

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] rsaSignature(int keyIndex, byte[] inData) throws AFCryptoException ; | |
| 作用 | RSA签名，使用RSA内部密钥进行签名运算 | |
| 参数 | keyIndex | 密码设备内部存储的RSA索引号 |
| inData | 待签名的原始数据 |
| 返回值 | 返回Base64编码的签名数据 | |

3.7.2 使用RSA外部密钥进行签名运算

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public byte[] rsaSignature(byte[] privateKey, byte[] inData) throws AFCryptoException; | | |
| 作用 | RSA签名，使用RSA外部密钥进行签名运算 | | |
| 参数 | privateKey | base64编码的RSA私钥数据，其结构应满足PKCS#1中的RSA结构定义 | 说明：  RSAPrivateKey ::= SEQUENCE {  version Version,  modulus INTEGER, --- n  publicExponent INTEGER, --- e  privateExponent INTEGER, --- d  prime1 INTEGER, --- p  prime2 INTEGER, --- q  exponent1 INTEGER, --- d mod (p-1)  exponent2 INTEGER, --- d mod (q-1)  coefficient INTEGER, --- (inverse of q) mod p  otherPrimeInfos OtherPrimeInfos OPTIONAL  } |
| inData | 待签名的原始数据 | |
| 返回值 | 返回Base64编码的签名数据 | | |

###### 3.8对文件进行RSA签名运算

3.8.1 使用RSA内部密钥对文件内容进行签名运算

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] rsaSignFile(int keyIndex, byte[] filePath) throws AFCryptoException; | |
| 作用 | 对文件进行RSA签名运算，使用RSA内部密钥对文件内容进行签名运算 | |
| 参数 | keyIndex | 密码设备内部存储的RSA索引号 |
| filePath | 待签名的文件路径 |
| 返回值 | 返回Base64编码的签名数据 | |

3.8.2 使用外部RSA密钥对文件内容进行签名运算

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public byte[] rsaSignFile(byte[] privateKey, byte[] filePath) throws AFCryptoException; | | |
| 作用 | 对文件进行RSA签名运算，使用外部RSA密钥对文件内容进行签名运算 | | |
| 参数 | privateKey | base64编码的RSA私钥数据，其结构应满足PKCS#1中的RSA结构定义 | 说明：  RSAPrivateKey ::= SEQUENCE {  version Version,  modulus INTEGER, --- n  publicExponent INTEGER, --- e  privateExponent INTEGER, --- d  prime1 INTEGER, --- p  prime2 INTEGER, --- q  exponent1 INTEGER, --- d mod (p-1)  exponent2 INTEGER, --- d mod (q-1)  coefficient INTEGER, --- (inverse of q) mod p  otherPrimeInfos OtherPrimeInfos OPTIONAL  } |
| filePath | 待签名的文件路径 | |
| 返回值 | 返回Base64编码的签名数据 | | |

###### 3.9 RSA验证签名

3.9.1 使用内部RSA密钥对数据进行验证签名运算

|  |  |  |
| --- | --- | --- |
| 方法 | public boolean rsaVerify(int keyIndex, byte[] inData, byte[] signatureData) throws AFCryptoException; | |
| 作用 | 对文件进行RSA签名运算，使用内部RSA密钥对数据进行验证签名运算 | |
| 参数 | keyIndex | 密码设备内部存储的RSA索引号 |
| inData | 原始数据 |
| signatureData | Base64编码的签名数据 |
| 返回值 | true | 验证成功 |
| false | 验证失败 |

3.9.2 使用外部RSA密钥对数据进行验证签名运算

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public boolean rsaVerify(byte[] publicKey, byte[] rawData, byte[] signatureData) throws AFCryptoException; | | |
| 作用 | 对文件进行RSA签名运算，使用外部RSA密钥对数据进行验证签名运算 | | |
| 参数 | publicKey | base64编码的RSA公钥数据，其结构应满足PKCS#1中的RSA结构定义 | 说明：  RSAPublicKey ::= SEQUENCE {  modulus INTEGER, --- n  publicExponent INTEGER, --- e  } |
| inData | 原始数据 | |
| signatureData | Base64编码的签名数据 | |
| 返回值 | true | 验证成功 | |
| false | 验证失败 | |

3.9.3 使用证书对数据进行验证签名运算

|  |  |  |
| --- | --- | --- |
| 方法 | public boolean rsaVerifyByCertificate(byte[] certificatePath, byte[] inData, byte[] signatureData) throws AFCryptoException; | |
| 作用 | RSA验证签名，使用证书对数据进行验证签名运算 | |
| 参数 | certificatePath | 证书路径 |
| inData | 原始数据 |
| signatureData | Base64编码的签名数据 |
| 返回值 | true | 验证成功 |
| false | 验证失败 |

3.9.4 使用证书对文件签名数据进行验证签名运算

|  |  |  |
| --- | --- | --- |
| 方法 | public boolean rsaVerifyFileByCertificate(byte[] certificatePath, byte[] filePath, byte[] signatureData) throws AFCryptoException ; | |
| 作用 | RSA验证签名，使用证书对文件签名数据进行验证签名运算 | |
| 参数 | certificatePath | base64编码的RSA数字证书路径 |
| fileName | 文件名称 |
| signatureData | Base64编码的签名数据 |
| 返回值 | true | 验证成功 |
| false | 验证失败 |

###### 3.10 对文件进行RSA验证签名

3.10.1 使用内部密钥对文件签名值进行验证

|  |  |  |
| --- | --- | --- |
| 方法 | public boolean rsaVerifyFile(int keyIndex, byte[] filePath, byte[] signatureData) throws AFCryptoException ; | |
| 作用 | 对文件进行RSA验证签名，使用内部密钥对文件签名值进行验证 | |
| 参数 | keyIndex | 密码设备内部存储的RSA索引号 |
| filePath | 文件路径 |
| signatureData | Base64编码的签名数据 |
| 返回值 | true | 验证成功 |
| false | 验证失败 |

3.10.2 使用外部密钥对文件签名值进行验证

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public boolean rsaVerifyFile(byte[] publicKey, byte[] filePath, byte[] signatureData) throws AFCryptoException; | | |
| 作用 | 对文件进行RSA验证签名，使用外部密钥对文件签名值进行验证 | | |
| 参数 | publicKey | base64编码的RSA公钥数据，其结构应满足PKCS#1中的RSA结构定义 | 说明：  RSAPublicKey ::= SEQUENCE {  modulus INTEGER, --- n  publicExponent INTEGER, --- e  } |
| filePath | 文件路径 | |
| signatureData | Base64编码的签名数据 | |
| 返回值 | true | 验证成功 | |
| false | 验证失败 | |

###### 3.11 RSA加密

3.11.1 使用内部密钥进行RSA加密

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] rsaEncrypt(int keyIndex, byte[] data) throws AFCryptoException; | |
| 作用 | RSA加密，使用内部密钥进行RSA加密 | |
| 参数 | keyIndex | 密码设备内部存储的RSA索引号 |
| data | 待加密的原始数据 |
| 返回值 | Base64编码的加密数据 | |

3.11.2 使用外部密钥进行RSA加密

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public byte[] rsaEncrypt(byte[] publicKey, byte[] data) throws AFCryptoException; | | |
| 作用 | RSA加密，使用外部密钥进行RSA加密 | | |
| 参数 | publicKey | base64编码的RSA公钥数据，其结构应满足PKCS#1中的RSA结构定义 | 说明：  RSAPublicKey ::= SEQUENCE {  modulus INTEGER, --- n  publicExponent INTEGER, --- e  } |
| data | 待加密的原始数据 | |
| 返回值 | Base64编码的加密数据 | | |

3.11.3 使用RSA数字证书对数据进行加密

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] rsaEncryptByCertificate(byte[] certificatePath, byte[] data) throws AFCryptoException; | |
| 作用 | RSA加密，使用RSA数字证书对数据进行加密 | |
| 参数 | certificatePath | 证书路径 |
| data | 待加密的原始数据 |
| 返回值 | Base64编码的加密数据 | |

###### 3.12 RSA解密

3.12.1 使用内部密钥进行RSA解密

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] rsaDecrypt(int keyIndex, byte[] encData) throws AFCryptoException; | |
| 作用 | RSA解密，使用内部密钥进行RSA解密 | |
| 参数 | keyIndex | 密码设备内部存储的RSA索引号 |
| encData | Base64编码的加密数据 |
| 返回值 | 原始数据 | |

3.12.2 使用外部密钥进行RSA加密

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public byte[] rsaDecrypt(byte[] privateKey, byte[] encData) throws AFCryptoException; | | |
| 作用 | RSA解密，使用外部密钥进行RSA解密 | | |
| 参数 | privateKey | base64编码的RSA私钥数据，其结构应满足PKCS#1中的RSA结构定义 | 说明：  RSAPrivateKey ::= SEQUENCE {  version Version,  modulus INTEGER, --- n  publicExponent INTEGER, --- e  privateExponent INTEGER, --- d  prime1 INTEGER, --- p  prime2 INTEGER, --- q  exponent1 INTEGER, --- d mod (p-1)  exponent2 INTEGER, --- d mod (q-1)  coefficient INTEGER, --- (inverse of q) mod p  otherPrimeInfos OtherPrimeInfos OPTIONAL  } |
| encData | Base64编码的加密数据 | |
| 返回值 | 原始数据 | | |

###### 3.13 SM2签名

3.13.1 使用签名服务器内部密钥进行 SM2签名运算

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] sm2Signature(int index, byte[] data) throws AFCryptoException; | |
| 作用 | SM2内部密钥签名，使用签名服务器内部密钥进行 SM2签名运算 | |
| 参数 | index | 待签名的签名服务器内部密钥索引 |
| data | 待签名的数据 |
| 返回值 | base64编码的签名数据 | |

3.13.2 SM2外部密钥签名

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public byte[] sm2Signature(byte[] privateKey, byte[] data) throws AFCryptoException; | | |
| 作用 | SM2外部密钥签名 | | |
| 参数 | data | 待签名的数据 | |
| privateKey | base64编码的SM2私钥数据, 其结构应满足 GM/T 0009-2012中关于SM2私钥结构的数据定义 | 说明：  SM2PrivateKey ::= INTEGER |
| 返回值 | base64编码的签名数据 | | |

###### 3.14 带Z值的SM2签名

3.14.1 无需证书的带Z值SM2签名

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | byte[] sm2SignatureByCertificate(byte[] data, byte[] privateKey, byte[] base64Certificate) throws AFCryptoException; | | |
| 作用 | 基于证书的SM2签名 | | |
| 参数 | data | 待签名的数据 | |
| privateKey | base64编码的SM2私钥数据, 其结构应满足 GM/T 0009-2012中关于SM2私钥结构的数据定义 | 说明：  SM2PrivateKey ::= INTEGER |
| 返回值 | base64编码的签名数据 | | |

3.14.2 需要证书的带Z值SM2签名

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public byte[] sm2SignatureByCertificate(byte[] privateKey, byte[] data, byte[] base64CertificatePath) throws AFCryptoException; | | |
| 作用 | 基于证书的SM2签名 | | |
| 参数 | data | 待签名的数据 | |
| base64CertificatePath | 证书路径 | |
| privateKey | base64编码的SM2私钥数据, 其结构应满足 GM/T 0009-2012中关于SM2私钥结构的数据定义 | 说明：  SM2PrivateKey ::= INTEGER |
| 返回值 | base64编码的签名数据 | | |

###### 3.15 SM2文件签名

3.15.1 使用签名服务器内部密钥对文件进行 SM2签名运算

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] sm2SignFile(int index, byte[] filePath) throws AFCryptoException; | |
| 作用 | SM2文件签名，使用签名服务器内部密钥对文件进行 SM2签名运算 | |
| 参数 | index | 待签名的签名服务器内部密钥索引 |
| fileNafilePathme | 待签名的文件路径 |
| 返回值 | base64编码的签名数据 | |

3.15.2 使用外部密钥对文件进行 SM2签名运算

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public byte[] sm2SignFile(byte[] privateKey, byte[] filePath) throws AFCryptoException; | | |
| 作用 | SM2文件签名，使用外部密钥对文件进行 SM2签名运算 | | |
| 参数 | filePath | 待签名的文件路径 | |
| privateKey | base64编码的SM2私钥数据, 其结构应满足 GM/T 0009-2012中关于SM2私钥结构的数据定义 | 说明：  SM2PrivateKey ::= INTEGER |
| 返回值 | base64编码的签名数据 | | |

3.15.3 基于证书的SM2文件签名

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public byte[] sm2SignFileByCertificate(byte[] privateKey, byte[] filePath, byte[] base64CertificatePath) throws AFCryptoException; | | |
| 作用 | 基于证书的SM2文件签名 | | |
| 参数 | filePath | 待签名的文件路径 | |
| privateKey | base64编码的SM2私钥数据, 其结构应满足 GM/T 0009-2012中关于SM2私钥结构的数据定义 | 说明：  SM2PrivateKey ::= INTEGER |
| base64CertificatePath | 签名的外部证书路径 | |
| 返回值 | base64编码的签名数据 | | |

###### 3.16 SM2内部密钥验证签名

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public boolean sm2Verify(int keyIndex, byte[] data, byte[] signature) throws AFCryptoException; | | |
| 作用 | SM2内部密钥验证签名，使用签名服务器内部密钥进行 SM2验证签名运算 | | |
| 参数 | keyIndex | 待验证签名的签名服务器内部密钥索引 | |
| data | 待验证签名的原始数据 | |
| signature | 待验证签名的签名数据---BASE64编码格式, 其结构应满足 GM/T 0009-2012中关于SM2签名数据结构的定义 | 说明：  SM2Signature ::= {  R INTEGER, --签名值的第一部分  S INTEGER --签名值的第二部分  } |
| 返回值 | true | 验证签名成功 | |
| false | 验证签名失败 | |

###### 3.17 SM2证书验证签名

3.17.1 根据签名服务器内部CA证书，验证证书有效性

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public boolean sm2VerifyByCertificate(byte[] certPath, byte[] data, byte[] signature) throws AFCryptoException; | | |
| 作用 | 基于证书的SM2验证签名，使用外部证书进行 SM2验证签名运算，根据签名服务器内部CA证书，验证证书有效性 | | |
| 参数 | certPath | 待验证签名的外部证书路径-证书Base64编码 | |
| data | 待验证签名的原始数据 | |
| signature | 待验证签名的签名数据---BASE64编码格式, 其结构应满足 GM/T 0009-2012中关于SM2签名数据结构的定义 | 说明：  SM2Signature ::= {  R INTEGER, --签名值的第一部分  S INTEGER --签名值的第二部分  } |
| 返回值 | true | 验证签名成功 | |
| false | 验证签名失败 | |

3.17.2 通过CRL文件验证证书有效性(**暂时不开放**)

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | boolean sm2VerifyByCertificate(byte[] base64Certificate, byte[] crlData, byte[] data, byte[] signature) throws AFCryptoException; | | |
| 作用 | 基于证书的SM2验证签名，使用外部证书进行 SM2验证签名运算, 通过CRL文件验证证书有效性 | | |
| 参数 | base64Certificate | 待验证签名的外部证书---BASE64编码 | |
| crlData | 待验证证书的CRL文件数据 --BASE64编码格式 | |
| data | 待验证签名的原始数据 | |
| signature | 待验证签名的签名数据---BASE64编码格式, 其结构应满足 GM/T 0009-2012中关于SM2签名数据结构的定义 | 说明：  SM2Signature ::= {  R INTEGER, --签名值的第一部分  S INTEGER --签名值的第二部分  } |
| 返回值 | true | 验证签名成功 | |
| false | 验证签名失败 | |

###### 3.18 使用内部密钥对文件进行 SM2验证签名运算

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public boolean sm2VerifyFile(int keyIndex, byte[] filePath, byte[] signature) throws AFCryptoException; | | |
| 作用 | SM2内部密钥验证w文件签名，使用签名服务器内部密钥对文件进行 SM2验证签名运算 | | |
| 参数 | keyIndex | 待验证签名的签名服务器内部密钥索引 | |
| filePath | 文件路径 | |
| signature | 待验证签名的签名数据---BASE64编码格式, 其结构应满足 GM/T 0009-2012中关于SM2签名数据结构的定义 | 说明：  SM2Signature ::= {  R INTEGER, --签名值的第一部分  S INTEGER --签名值的第二部分  } |
| 返回值 | true | 验证签名成功 | |
| false | 验证签名失败 | |

###### 3.19 使用外部证书对文件进行SM2验证签名运算

3.19.1 根据签名服务器内部CA证书，验证证书有效性

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public boolean sm2VerifyFileByCertificate(byte[] base64CertificatePath, byte[] filePath, byte[] signature) throws AFCryptoException; | | |
| 作用 | 基于证书的SM2验证文件签名，使用外部证书对文件进行SM2验证签名运算，根据签名服务器内部CA证书，验证证书有效性 | | |
| 参数 | base64CertificatePath | 待验证签名的外部证书路径---证书BASE64编码 | |
| filePath | 文件路径 | |
| signature | 待验证签名的签名数据---BASE64编码格式, 其结构应满足 GM/T 0009-2012中关于SM2签名数据结构的定义 | 说明：  SM2Signature ::= {  R INTEGER, --签名值的第一部分  S INTEGER --签名值的第二部分  } |
| 返回值 | true | 验证签名成功 | |
| false | 验证签名失败 | |

3.19.2 通过CRL文件验证证书有效性(**暂时未开放**)

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | boolean sm2VerifyFileByCertificate(byte[] base64Certificate, byte[] crlData, byte[] fileName, byte[] signature) throws AFCryptoException; | | |
| 作用 | 基于证书的SM2验证签名，使用外部证书对文件进行SM2验证签名运算, 通过CRL文件验证证书有效性 | | |
| 参数 | base64Certificate | 待验证签名的外部证书---BASE64编码 | |
| crlData | 待验证证书的CRL文件数据 --BASE64编码格式 | |
| fileName | 文件名称 | |
| signature | 待验证签名的签名数据---BASE64编码格式, 其结构应满足 GM/T 0009-2012中关于SM2签名数据结构的定义 | 说明：  SM2Signature ::= {  R INTEGER, --签名值的第一部分  S INTEGER --签名值的第二部分  } |
| 返回值 | true | 验证签名成功 | |
| false | 验证签名失败 | |

###### 3.20 SM2加密

3.20.1 使用内部密钥进行SM2加密

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] sm2Encrypt(int keyIndex, byte[] inData) throws AFCryptoException; | |
| 作用 | sm2加密，使用内部密钥进行SM2加密 | |
| 参数 | keyIndex | 密码设备内部密钥索引 |
| inData | 待加密的数据原文 |
| 返回值 | Base64编码的密文数据 | |

3.20.2 使用外部密钥进行SM2加密

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public byte[] sm2Encrypt(byte[] publicKey, byte[] inData) throws AFCryptoException; | | |
| 作用 | sm2加密，使用外部钥进行SM2加密 | | |
| 参数 | publicKey | base64编码的SM2公钥数据, 其结构应满足 GM/T 0009-2012中关于SM2公钥结构的数据定义 | 说明：  SM2PublicKey ::= BIT STRING  其结构为 04||X||Y |
| inData | 待加密的数据原文 | |
| 返回值 | Base64编码的密文数据 | | |

3.20.3 使用SM2证书对数据进行加密

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] sm2EncryptByCertificate(byte[] certificatePath, byte[] inData) throws AFCryptoException; | |
| 作用 | sm2加密，使用SM2证书对数据进行加密 | |
| 参数 | certificcertificatePathate | 证书路径 |
| inData | 待加密的数据原文 |
| 返回值 | Base64编码的密文数据 | |

###### 3.21 SM2解密

3.21.1 使用内部密钥进行SM2解密

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public byte[] sm2Decrypt(int keyIndex, byte[] encData) throws AFCryptoException; | | |
| 作用 | sm2解密，使用内部密钥进行SM2解密 | | |
| 参数 | keyIndex | 密码设备内部密钥索引 | |
| encData | Base64编码的加密数据, 其结构应满足 GM/T 0009-2012中关于SM2公钥结构的数据定义 | 说明：  SM2Cipher ::= SEQUENCE {  XCoordinate INTEGER, --x分量  YCoordinate INTEGER, --y分量  HASH OCTET STRING SIZE(32), --杂凑值  CipherText OCTET STRING, --密文  } |
| 返回值 | 原文数据 | | |

3.21.2 使用外部密钥进行SM2解密

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public byte[] sm2Decrypt(byte[] privateKey, byte[] encData) throws AFCryptoException; | | |
| 作用 | sm2解密，使用外部钥进行SM2解密 | | |
| 参数 | privateKey | base64编码的SM2私钥数据, 其结构应满足 GM/T 0009-2012中关于SM2私钥结构的数据定义 | 说明：  SM2PrivateKey ::= INTEGER |
| encData | Base64编码的加密数据, 其结构应满足 GM/T 0009-2012中关于SM2公钥结构的数据定义 | 说明：  SM2Cipher ::= SEQUENCE {  XCoordinate INTEGER, --x分量  YCoordinate INTEGER, --y分量  HASH OCTET STRING SIZE(32), --杂凑值  CipherText OCTET STRING, --密文  } |
| 返回值 | 原文数据 | | |

###### 3.22 导出SM2公钥

3.22.1 导出SM2签名公钥

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] getSM2SignPublicKey(int index) throws AFCryptoException; | |
| 作用 | 导出SM2公钥，导出密码机内部对应索引和用途的SM2公钥信息 | |
| 参数 | index | 密码设备内部存储的SM2索引号 |
| 返回值 | 返回Base64编码的公钥数据 | |

3.22.2 导出SM2 加密公钥

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] getSM2EncryptPublicKey(int index) throws AFCryptoException; | |
| 作用 | 导出SM2公钥，导出密码机内部对应索引和用途的SM2公钥信息 | |
| 参数 | index | 密码设备内部存储的SM2索引号 |
| 返回值 | 返回Base64编码的公钥数据 | |

###### 3.23 查询证书信任列表别名

|  |  |
| --- | --- |
| 方法 | public CertAltNameTrustList getCertTrustListAltName() throws AFCryptoException; |
| 作用 | 查询证书信任列表别名 |
| 返回值 | 信任列表别名组合 |
| 如： CA001|CA002|CA003 |

###### 3.24 获取证书个数

|  |  |  |
| --- | --- | --- |
| 方法 | public int getCertCountByAltName(byte[] altName) throws AFCryptoException; | |
| 作用 | 获取证书的个数，根据证书别名获取信任证书的个数 | |
| 参数 | altName | 证书别名 |
| 返回值 | 证书的个数 | |

###### 3.25 根据别名获取单个证书

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] getCertByAltName(byte[] altName, int certIndex) throws AFCryptoException; | |
| 作用 | 根据别名获取单个证书 | |
| 参数 | altName | 证书别名 |
| certIndex | 证书索引号(与函数getCertCountByAltName中获取到的值相匹配) |
| 返回值 | Base64编码的证书文件 | |

###### 3.26 获取应用策略

|  |  |  |
| --- | --- | --- |
| 方法 | public AFSvCryptoInstance getInstance(String policyName) throws AFCryptoException ; | |
| 作用 | 获取应用策略，根据策略名称获取应用策略，此应用策略为用户在管理程序中创建。用户获取应用策略后，签名服务器会根据用户设定的策略内容进行相关的服务操作 | |
| 参数 | policyName | 策略名称 |
| 返回值 | AFSvCryptoInstance | public class AFSvCryptoInstance {  public String policyName; //应用实体名称  public int keyIndex; //密钥索引  public int keyType; //密钥类型 3:SM2 4:RSA  public int policy; //策略 该参数无用，兼容以前版本  } |

###### 3.27 删除用户证书列表(已废弃)

|  |  |  |
| --- | --- | --- |
| 方法 | void deleteCertList(byte[] altName) throws AFCryptoException; | |
| 作用 | 删除用户证书列表，根据证书别名删除证书列表 | |
| 参数 | altName | 证书列表别名 |

###### 3.28 获取服务器证书

3.28.1 获取签名证书或者加密证书

|  |  |
| --- | --- |
| 方法 | public byte[] getServerCert() throws AFCryptoException; |
| 作用 | 获取服务器证书，读取当前应用的服务器的签名证书，如果有签名证书则得到签名证书，否则得到加密证书 |
| 返回值 | Base64编码的服务器证书 |

3.28.2 获取指定的设备证书

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | public byte[] getServerCertByUsage(int usage) throws AFCryptoException; | | |
| 作用 | 获取服务器证书，根据证书用途，获取当前的服务器证书 | | |
| 参数 | usage | 证书用途 | 1：服务器加密证书 |
| 2：服务器签名证书 |
| 返回值 | Base64编码的证书 | | |

###### 3.29 根据策略名称，获取相应证书

3.29.1 获取加密证书

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] getEncCertByPolicyName(byte[] policyName) throws AFCryptoException ; | |
| 作用 | 根据策略名称，获取相应的证书 | |
| 参数 | policyName | 策略名称 |
| 返回值 | Base64编码的加密证书 | |

**3.29.2 获取签名证书**

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] getSignCertByPolicyName(String policyName) throws AFCryptoException; | |
| 作用 | 根据策略名称，获取相应的证书 | |
| 参数 | policyName | 策略名称 |
| 返回值 | Base64编码的签名证书 | |

###### 3.30 获取证书中的OCSP URL地址

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] getOcspUrl(byte[] base64Certificate) throws AFCryptoException; | |
| 作用 | 获取证书中的OCSP URL地址 | |
| 参数 | base64Certificate | Base64编码的证书 |
| 返回值 | OCSP URL地址 | |

###### 3.31 获取证书信息

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] getCertInfo(byte[] base64Certificate, int certInfoType) throws AFCryptoException ; | |
| 作用 | 获取证书信息，获取用户指定的证书信息内容 | |
| 参数 | base64Certificate | Base64编码的证书文件 |
| certInfoType | 用户待获取的证书内容类型 : 类型定义在类 certParseInfoType 中 |
| 返回值 | 用户获取到的证书信息内容 | |

###### 3.32 获取证书扩展信息

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] getCertInfoByOid(byte[] base64Certificate, byte[] certInfoOid) throws AFCryptoException; | |
| 作用 | 获取证书扩展信息，获取用户指定的证书扩展信息内容 | |
| 参数 | base64Certificate | Base64编码的证书文件 |
| certInfoOid | 用户待获取的证书内容类型OID值 : OID值定义在类 certParseInfoType 中 |
| 返回值 | 用户获取到的证书信息内容 | |

###### 3.33 PKCS7格式的带签名的数字信封数据

3.33.1 编码PKCS7格式的带签名的数字信封数据

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] encodeEnvelopedDataForSM2(byte[] priKey, byte[] symKey, byte[] signCert, byte[] encCert, byte[] data) throws AFCryptoException; | |
| 作用 | 编码数字信封，编码PKCS7格式的带签名的数字信封数据 | |
| 参数 | priKey | 签名私钥 |
| symKey | 对称密钥 |
| signCert | Base64编码的签名证书 |
| encCert | Base64编码的加密证书 |
| data | 代签名 |
| 返回值 | Base64编码的数字信封数据 | |

3.33.2 解码PKCS7格式的带签名的数字信封数据

|  |  |  |
| --- | --- | --- |
| 方法 | public AFPkcs7DecodeData decodeEnvelopedDataForSM2(byte[] priKey, byte[] encodeData) throws AFCryptoException; | |
| 作用 | 解码数字信封，解码PKCS7格式的带签名的数字信封数据 | |
| 参数 | priKey | 私钥 |
| encodeData | Base64编码的pkcs7格式的数字信封数据 |
| 返回值 | 解码后的数据，包括原始数据、签名证书、签名值等 | |

###### 3.34 PKCS7格式的签名数据

3.34.1 编码签名数据

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] encodeSignedDataForSM2(byte[] priKey, byte[] base64Certificate, byte[] data) throws AFCryptoException; | |
| 作用 | 编码签名数据，编码PKCS7格式的签名数据 | |
| 参数 | priKey | 私钥 |
| base64Certificate | Base64编码的签名者证书 |
| data | 待签名的数据 |
| 返回值 | Base64编码的签名数据 | |

3.34.2 解码签名数据

|  |  |  |
| --- | --- | --- |
| 方法 | public AFSM2DecodeSignedData decodeSignedDataForSM2(byte[] signedData) throws AFCryptoException; | |
| 作用 | 解码签名数据，解码PKCS7格式的签名数据 | |
| 参数 | signedData | Base64编码的pkcs7格式的签名数据 |
| 返回值 | 解码后的数据，包括原始数据、签名证书、签名值等 | |

###### 3.35 PKSC7格式的数字信封(暂未开放)

3.35.1 编码数字信封

|  |  |  |
| --- | --- | --- |
| 方法 | byte[] encodeEnvelopedDataForPkcs7(byte[] data, byte[] encodeCertificate, int symmAlgorithm) throws AFCryptoException; | |
| 作用 | 编码数字信封，编码PKCS7格式的数字信封 | |
| 参数 | data | 需要做数字信封的数据 |
| encodeCertificate | Base64编码的接收者证书 |
| signerCertificate | 对称算法参数 |
| 返回值 | Base64编码的数字信封数据 | |

3.35.2 解码数字信封

|  |  |  |
| --- | --- | --- |
| 方法 | byte[] decodeEnvelopedDataForPkcs7(int keyIndex, int decodeKeyUsage, byte[] envelopedData) throws AFCryptoException; | |
| 作用 | 解码数字信封，解码PKCS7格式的数字信封 | |
| 参数 | keyIndex | 密钥索引 |
| decodeKeyUsage | 密钥用途 |
| envelopedData | Base64编码的数字信封数据 |
| 返回值 | 数据原文 | |

###### 3.36 PKSC7格式的签名数据(暂未开放)

3.36.1 编码摘要数据

|  |  |  |
| --- | --- | --- |
| 方法 | byte[] encodeDigestDataForPkcs7(int digestAlgorithm, byte[] data) throws AFCryptoException; | |
| 作用 | 编码签名数据，编码PKCS7格式的签名数据 | |
| 参数 | digestAlgorithm | 杂凑算法标识 |
| data | 原文数据 |
| 返回值 | Base64编码的摘要数据 | |

3.36.2 解码摘要数据

|  |  |  |
| --- | --- | --- |
| 方法 | AFPkcs7DecodeDigestData decodeDigestDataForPkcs7(int digestAlgorithm, byte[] digestData) throws AFCryptoException; | |
| 作用 | 解码摘要数据，解码PKCS7格式的摘要数据 | |
| 参数 | digestAlgorithm | 杂凑算法标识 |
| digestData | Base64编码的摘要数据 |
| 返回值 | 解码后的数据，包括原文和摘要值 | |

###### 3.37 基于SM2算法的带签名的数字信封数据(暂未开放)

3.37.1 编码数字信封

|  |  |  |
| --- | --- | --- |
| 方法 | byte[] encodeSignedAndEnvelopedDataForSM2(int keyIndex, int signKeyUsage, byte[] signerCertificate, int digestAlgorithms, byte[] encodeCertificate, int symmAlgorithm, byte[] data) throws AFCryptoException; | |
| 作用 | 编码数字信封，编码基于SM2算法的带签名的数字信封数据 | |
| 参数 | keyIndex | 密钥索引 |
| signKeyUsage | 密钥用途 |
| signerCertificate | Base64编码的签名者证书 |
| digestAlgorithms | HASH算法 |
| encodeCertificate | Base64编码的接收者证书 |
| symmAlgorithm | 对称算法参数 |
| data | 原文数据 |
| 返回值 | Base64编码的数字信封数据 | |

3.37.2 解码数字信封

|  |  |  |
| --- | --- | --- |
| 方法 | AFSM2DecodeSignedAndEnvelopedData decodeSignedAndEnvelopedDataForSM2(int keyIndex, int decodeKeyUsage, byte[] signedAndEnvelopedData) throws AFCryptoException; | |
| 作用 | 解码数字信封，解码基于SM2算法的带签名的数字信封数据 | |
| 参数 | keyIndex | 密钥索引 |
| decodeKeyUsage | 密钥用途 |
| signedAndEnvelopedData | Base64编码的数字信封数据，其格式应符合GM/T 0010《SM2密码算法加密签名消息语法规范》中SignedAndEnvelopedData的数据类型定义 |
| 返回值 | 解码后的数据，包括原文、签名者证书以及HASH算法标识 | |

###### 3.38 基于SM2算法的签名数据(暂未开放)

3.38.1 编码签名数据

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | byte[] encodeSignedDataForSM2(int keyType, int keyIndex, int signKeyUsage, byte[] signerCertificate, int digestAlgorithm, byte[] data) throws AFCryptoException; | | |
| 作用 | 编码签名数据，编码基于SM2算法的签名数据 | | |
| 参数 | keyType | 消息签名格式 | 1：带原文 |
| 2：不带原文 |
| keyIndex | 密钥索引 | |
| signKeyUsage | 密钥用途 | |
| signerCertificate | Base64编码的签名者证书 | |
| digestAlgorithm | HASH算法标识 | |
| data | 需要签名的数据 | |
| 返回值 | Base64编码的签名数据 | | |

3.38.2 解码签名数据

|  |  |  |
| --- | --- | --- |
| 方法 | AFSM2DecodeSignedData decodeSignedDataForSM2(byte[] signedData) throws AFCryptoException; | |
| 作用 | 解码签名数据，解码基于SM2算法的签名数据 | |
| 参数 | signedData | Base64编码的签名数据，其格式应符合GM/T 0010《SM2密码算法加密签名消息语法规范》中SignedData的数据类型定义 |
| 返回值 | 解码后的数据，包括签名者证书，HASH算法标识，被签名的数据以及签名值 | |

###### 3.39 基于SM2算法的数字信封(暂未开放)

3.39.1 编码数字信封

|  |  |  |
| --- | --- | --- |
| 方法 | byte[] encodeEnvelopedDataForSM2(byte[] data, byte[] encodeCertificate, int symmAlgorithm) throws AFCryptoException; | |
| 作用 | 编码数字信封，编码基于SM2算法的数字信封 | |
| 参数 | data | 需要做数字信封的数据 |
| encodeCertificate | Base64编码的接受者证书 |
| symmAlgorithm | 对称算法标识 |
| 返回值 | Base64编码的数字信封数据 | |

3.39.2 解码数字信封

|  |  |  |
| --- | --- | --- |
| 方法 | byte[] decodeEnvelopedDataForSM2(int keyIndex, int decodeKeyUsage, byte[] envelopedData) throws AFCryptoException; | |
| 作用 | 解码数字信封，解码基于SM2算法的数字信封 | |
| 参数 | keyIndex | 密钥索引 |
| decodeKeyUsage | 密钥用途 |
| envelopedData | Base64编码的数字信封数据，其格式应符合GM/T 0010《SM2密码算法加密签名消息语法规范》中EnvelopedData的数据类型定义 |
| 返回值 | 数据原文 | |