迪曼森
Dimensen.com

签名验签服务器
客户端接口手册(Java 版)

版本：V1.9

迪曼森科技

版权声明

目　录

1 引言.....4
1.1 概述.....4
1.2 使用方法.....4
2 接口说明.....4
2.1 客户端连接初始化接口.....4
2.2 获取当前使用签名验签服务器连接信息接口.....4
2.3 生成随机数接口.....4
2.4 获取服务端可信标识信息接口.....5
2.5 验证可信标识有效性接口.....5
2.6 解析可信标识接口.....6
2.7 数字签名接口.....7
2.8 验证数字签名接口.....7
2.9 多包数字签名初始化接口.....8
2.10 多包数字签名更新接口.....9
2.11 多包数字签名完成接口.....9
2.12 多包验证数字签名初始化接口.....10
2.13 多包验证数字签名更新接口.....10
2.14 多包验证数字签名完成接口.....11
2.15 PKCS7 签名（消息签名）接口.....12
2.16 验证 PKCS7 签名（消息签名）接口.....13
2.17 封装数字信封接口.....14
2.18 解封数字信封接口.....14
3 错误信息定义.....15

1 引言

1.1 概述

IKI 签名验签服务器客户端接口实现签名验签服务器所有功能的调用。所有的功能性调用，都需要在调用客户端连接初始化接口，初始化客户端连接之后进行。

1.2 使用方法

IKI 签名验签服务器客户端接口库以 Java-jar(JDK1.8)包形式提供给应用程序调用，用户只需要将 sv-client.jar 引入应用程序工程中即可。

2 接口说明

2.1 客户端连接初始化接口

功能描述	根据传入的签名验签服务器 IP 地址，构建客户端连接初始化信息	
函数原型	boolean SVS_InitServerConnect(String serverIP, int port)	
接口参数	String serverIP	签名验签服务器 IP 地址
	int port	签名验签服务器服务端口
返回值	boolean	true：初始化连接成功;
异常信息	SVS_ServerConnectException	签名验签服务连接失败
	SVS_CipherInitException	PCIe 卡密码运算初始化失败

2.2 获取当前使用签名验签服务器连接信息接口

功能描述	获取当前使用签名验签服务器连接信息	
函数原型	String SVS_GetServerInfo()	
返回值	String	当前使用签名验签服务器 IP 及端口信息

2.3 生成随机数接口

功能描述	生成随机数	
函数原型	byte[] SVS_GenerateRandom(int length)	
接口参数	int length	生成随机数的长度(字节数)
返回值	byte[]	生成随机数 byte 数组

异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_GenerateRandomException	产生随机数失败

2.4 获取服务端可信标识信息接口

功能描述	获取服务端可信标识信息	
函数原型	Certificate SVS_GetCertInfo(String certSubject)	
接口参数	String certSubject	可信标识 subject 信息
返回值	org.bouncycastle.asn1.x509.Certificate	服务端可信标识
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_ExportCertException	获取可信标识失败
	SVS_NotFoundCertException	找不到对应可信标识

2.5 验证可信标识有效性接口

功能描述	验证可信标识有效性	
函数原型	boolean SVS_VerifyCert(Certificate cert)	
接口参数	org.bouncycastle.asn1.x509.Certificate cert	可信标识
返回值	boolean	true：可信标识有效;
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_CertNotTrustException	无效可信标识
	SVS_CertExpiredException	可信标识超过有效期
	SVS_CertCancelException	可信标识已作废
	SVS_CheckIRLException	可信标识验证撤销列表失败
	SVS_CertIneffectiveException	可信标识未生效
	SVS_CertException	验证可信标识未知错误
	SVS_VerifyCertException	可信标识验证失败
	SVS_NotFoundPKMException	找不到可信标识颁发机构公钥矩阵

	SVS_GetIRLException	获取撤销列表失败

2.6 解析可信标识接口

功能描述	解析可信标识	
函数原型	Object SVS_ParseCertInfo(Certificate cert, int infoType, ASN1ObjectIdentifier extTypeOID)	
接口参数	org.bouncycastle.asn1.x509.Certificate cert	可信标识
	int infoType	可信标识解析数据类型，1：可信标识主题 DN； 2：可信标识颁发者 DN； 3：可信标识序列号； 4：可信标识版本号； 5：可信标识生效日期； 6：可信标识失效日期； 7：可信标识扩展项
	org.bouncycastle.asn1. ASN1ObjectIdentifier extTypeOID	可信标识解析扩展类型 oid，当 infoType 为 7 时有效。 org.bouncycastle.asn1.x509.Extension.keyUsage：密钥用途； org.bouncycastle.asn1.x509.Extension.extendedKeyUsage：扩展密钥用途；
返回值	Object(String)	infoType 为 1-6 时，返回对应可信标识信息的字符串
	Object (org.bouncycastle.asn1.x509.Extension)	infoType 为 7 时，返回对应可信标识信息的扩展项值
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_CertParseNoSupportExtTypeExcepti	可信标识解析不支持扩展类

	on	型错误
	SVS_CertParseNoSupportTypeException	可信标识解析不支持类型错误
	SVS_ParseCertException	解析可信标识失败

2.7 数字签名接口

功能描述	数字签名	
函数原型	byte[] SVS_SignData(int keyIndex, String keyValue, byte[] inData)	
接口参数	int keyIndex	签名私钥索引值（从管理系统应用标识管理处获取，对应到相应的签名应用）
	String keyValue	签名私钥权限标识码（从管理系统应用标识管理处获取，对应到相应的签名应用）
	byte[] inData	待签名原文
返回值	byte[]	签名结果，数据结构遵循 GM/T 0009(SM2Signature)
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_PrivatekeyAccessRightException	获取私钥使用权限失败
	SVS_SignDataException	签名失败

2.8 验证数字签名接口

功能描述	验证数字签名	
函数原型	boolean SVS_VerifyData(Certificate cert, byte[] inData, byte[] signature,int verifyLevel)	
接口参数	org.bouncycastle.asn1.x509.Certificate	签名可信标识

	cert	
	byte[] inData	待签名原文
	byte[] signature	数字签名值
	int verifyLevel	可信标识验证级别， 0：验证时间； 1：验证时间和颁发机构矩阵签名； 2：验证时间，颁发机构矩阵签名和 IRL
返回值	boolean	true：验证成功
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_SignatureEncodeException	请求签名值编码错误
	SVS_CertTypeException	请求可信标识类型错误
	SVS_SignatureException	签名值无效
	SVS_CertNotTrustException	无效可信标识
	SVS_CertExpiredException	可信标识超过有效期
	SVS_CertCancelException	可信标识已作废
	SVS_CheckIRLException	可信标识验证撤销列表失败
	SVS_CertIneffectiveException	可信标识未生效
	SVS_CertException	验证可信标识未知错误
	SVS_VerifyDataException	数字签名验证失败
	SVS_NotFoundPKMException	找不到可信标识颁发机构公钥矩阵
	SVS_GetIRLException	获取撤销列表失败

2.9 多包数字签名初始化接口

功能描述	多包数字签名初始化
函数原型	byte[] SVS_SignDataInit(Certificate cert, byte[] inData)

接口参数	org.bouncycastle.asn1.x509.Certi-ficate cert	最终签名可信标识
	byte[] inData	待签名原文（第一段原文）
返回值	byte[]	初始化第一段原文结果
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_CertEncodeException	可信标识编码格式错误
	SVS_CertTypeException	可信标识类型错误
	SVS_SignDataInitException	多包数字签名初始化失败

2.10 多包数字签名更新接口

功能描述	多包数字签名更新	
函数原型	byte[] SVS_SignDataUpdate(byte[] hashValue, byte[] inData)	
接口参数	byte[] hashValue	多包数字签名初始化或更新完毕的数据结果
	byte[] inData	多包数字签名需要更新的原文数据
返回值	byte[]	多包数字签名更新完毕的结果
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_SignDataUpdateException	更新失败

2.11 多包数字签名完成接口

功能描述	多包数字签名完成	
函数原型	byte[] SVS_SignDataFinal(int keyIndex, String keyValue, byte[] hashValue)	
接口参数	int keyIndex	签名私钥索引值（从管理系统应用标识管理处获取，对应到相应的签名应用）
	String keyValue	签名私钥权限标识码（从管理系统

		应用标识管理处获取，对应到相应的签名应用）
	byte[] hashValue	多包最后更新完毕的数据
返回值	byte[]	签名结果，数据结构遵循 GM/T 0009(SM2Signature)
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_PrivatekeyAccessRightException	获取私钥使用权限失败
	SVS_SignDataFinalException	多包数字签名完成失败

2.12 多包验证数字签名初始化接口

功能描述	多包验证数字签名初始化	
函数原型	byte[] SVS_VerifyDataInit(Certificate cert, byte[] inData)	
接口参数	org.bouncycastle.asn1.x509.Certi-ficate cert	签名可信标识
	byte[] inData	被签名原文（第一段原文）
返回值	byte[]	初始化第一段被签名原文结果
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_CertEncodeException	可信标识编码格式错误
	SVS_CertTypeException	可信标识类型错误
	SVS_VerifyDataInitException	多包验证数字签名初始化失败

2.13 多包验证数字签名更新接口

功能描述	多包验证数字签名更新	
函数原型	byte[] SVS_VerifyDataUpdate(byte[] hashValue, byte[] inData)	
接口参数	byte[] hashValue	多包验证数字签名初始化或更新完毕的数据结果
	byte[] inData	多包验证数字签名需要更新的

		原文数据
返回值	byte[]	多包验证数字签名更新完毕的结果
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_VerifyDataUpdateException	更新失败

2.14 多包验证数字签名完成接口

功能描述	多包验证数字签名完成	
函数原型	boolean SVS_VerifyDataFinal(Certificate cert, byte[] hashValue, byte[] signature,int verifyLevel)	
接口参数	org.bouncycastle.asn1.x509.Certi -ficate cert	签名可信标识
	byte[] hashValue	多包验证数字签名最后更新完毕的数据
	byte[] signature	签名结果，数据结构遵循 GM/T 0009(SM2Signature)
	int verifyLevel	可信标识验证级别， 0：验证时间； 1：验证时间和颁发机构矩阵签名；2：验证时间，颁发机构矩阵签名和 IRL
返回值	boolean	true：验证成功
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_SignatureEncodeException	签名值编码错误
	SVS_SignatureException	签名值无效
	SVS_CertTypeException	可信标识类型错误
	SVS_CertNotTrustException	无效可信标识
	SVS_CertExpiredException	可信标识超过有效期

	SVS_CertCancelException	可信标识已作废
	SVS_CheckIRLException	可信标识验证撤销列表失败
	SVS_CertIneffectiveException	可信标识未生效
	SVS_CertException	验证可信标识未知错误
	SVS_VerifyDataFinalException	多包验证数字签名失败
	SVS_NotFoundPKMException	找不到可信标识颁发机构公钥矩阵
	SVS_GetIRLException	获取撤销列表失败

2.15 PKCS7 签名（消息签名）接口

功能描述	PKCS7 签名	
函数原型	byte[] SVS_PKCS7SignData(int keyIndex, String keyValue, byte[] inData, boolean originalText, boolean irls)	
接口参数	int keyIndex	签名私钥索引值（从管理系统应用标识管理处获取，对应到相应的签名应用）
	String keyValue	签名私钥权限标识码（从管理系统应用标识管理处获取，对应到相应的签名应用）
	byte[] inData	待签名原文
	boolean originalText	签名值是否附加原文属性
	boolean irls	签名值是否附加撤销列表
返回值	byte[]	PKCS 签名结果(org.bouncycastle.asn1.pkcs.SignedData)
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_PrivatekeyAccessRightException	私钥使用权限获取失败

	SVS_PKCS7SignDataException	PKCS7 签名失败
	SVS_GetIRLException	获取撤销列表失败

2.16 验证 PKCS7 签名（消息签名）接口

功能描述	验证 PKCS7 签名	
函数原型	boolean SVS_PKCS7VerifyData(boolean originalText, boolean irls, byte[] inData, byte[] signedMessage)	
接口参数	boolean originalText	签名值是否附加原文属性
	boolean irls	签名值是否附加撤销列表
	byte[] signedMessage	PKCS7 签名值(org.bouncycastle.asn1.pkcs.SignedData)
	byte[] inData	被签名原文(优先取这里的原文数据，若这里的原文数据为空，则根据 originalText 参数从 PKCS7 签名值中取原文数据）
返回值	boolean	true：验证成功
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_SignedDataEncodeException	签名值编码错误
	SVS_SignatureException	签名值无效
	SVS_CertNotTrustException	无效可信标识
	SVS_CertExpiredException	可信标识超过有效期
	SVS_CertCancelException	可信标识已作废
	SVS_CheckIRLException	可信标识验证撤销列表失败
	SVS_CertIneffectiveException	可信标识未生效
	SVS_CertException	验证可信标识未知错误
	SVS_NotFoundOriginalTextException	找不到被签名原文

	SVS_VerifyPKCS7SignDataException	验证 PKCS7 签名失败
	SVS_NotFoundPKMException	找不到可信标识颁发机构公钥矩阵
	SVS_GetIRLException	获取撤销列表失败

2.17 封装数字信封接口

功能描述	封装数字信封	
函数原型	byte[] SVS_EncryptEnvelope(Certificate cert, byte[] inData)	
接口参数	org.bouncycastle.asn1.x509.Certi-ficate cert	数字信封数据接受者可信标识
	byte[] inData	被封装数据
返回值	byte[]	数字信封 byte 数组
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_CertTypeException	可信标识类型错误
	SVS_EncryptEnvelopeException	封装数字信封失败

2.18 解封数字信封接口

功能描述	解封数字信封	
函数原型	byte[] SVS_DecryptEnvelope(byte[] envelopeData, int keyIndex, String keyValue)	
接口参数	byte[] envelopeData	数字信封 byte 数组
	int keyIndex	封装数字信封私钥索引值（从管理系统应用标识管理处获取，对应到相应的应用）
	String keyValue	封装数字信封私钥权限标识码（从管理系统应用标识

		管理处获取，对应到相应的应用）
返回值	byte[]	数字信封中封装的明文数据
异常信息	SVS_InvalidParameterException	无效的请求参数
	SVS_EnvelopeEncodeException	数字信封编码格式错误
	SVS_PrivatekeyAccessRightException	获取私钥使用权限失败
	SVS_DecryptEnvelopeException	解封数字信封失败

3 错误信息定义

IKI 签名验签服务器客户端接口错误信息以 Java 异常形式提供：

异常描述	说明
SVS_CertCancelException	可信标识已作废
SVS_CertEncodeException	可信标识数据编码格式错误
SVS_CertException	可信标识验证未知错误
SVS_CertExpiredException	可信标识已过期
SVS_CheckIRLException	可信标识验证撤销列表失败
SVS_GetIRLException	获取撤销列表失败
SVS_CertIneffectiveException	可信标识未生效
SVS_CertNotTrustException	可信标识不被信任
SVS_NotFoundPKMException	找不到可信标识颁发机构公钥矩阵
SVS_CertParseNoSupportExtTypeException	可信标识解析不支持扩展类型错误
SVS_CertParseNoSupportTypeException	可信标识解析不支持类型错误
SVS_CertTypeException	可信标识类型错误（错误的签名或加密可信标识）

SVS_CipherInitException	密码卡运算初始化失败
SVS_DecryptEnvelopeException	解封数字信封失败
SVS_EncryptEnvelopeException	封装数字信封失败
SVS_EnvelopeEncodeException	数字信封数据编码格式错误
SVS_ExportCertException	获取服务端可信标识失败
SVS_GenerateRandomException	产生随机数失败
SVS_InvalidParameterException	接口请求参数无效
SVS_NotFoundCertException	服务端找不到对应可信标识
SVS_NotFoundOriginalTextException	找不到原文数据
SVS_ParseCertException	可信标识解析失败
SVS_PKCS7SignDataException	PKCS7 签名失败
SVS_PrivatekeyAccessRightException	获取私钥使用权限失败
SVS_ServerConnectException	签名验签服务连接失败
SVS_SignatureEncodeException	数字签名数据编码格式错误
SVS_SignatureException	签名值无效
SVS_SignDataException	数字签名失败
SVS_SignDataFinalException	多包数字签名完成失败
SVS_SignDataInitException	多包数字签名初始化失败
SVS_SignDataUpdateException	多包数字签名更新失败
SVS_SignedDataEncodeException	PKCS7 签名值数据编码格式错误
SVS_VerifyCertException	可信标识验证失败
SVS_VerifyDataException	数字签名验证失败
SVS_VerifyDataFinalException	多包验证数字签名完成失败
SVS_VerifyDataInitException	多包验证数字签名初始化失败
SVS_VerifyDataUpdateException	多包验证数字签名更新失败
SVS_VerifyPKCS7SignDataException	验证 PKCS7 签名失败