时间戳服务器
接口手册

中安云科科技发展(山东)有限公司

2019 年 12 月

目 录

1 引言 1

1.1 概述 1
1.2 使用方法 1
1.3 接口日志 1

2 接口使用说明 2

2.1 连接初始化接口 2
2.2 连接释放 2
2.3 生成时间戳请求数据 2
2.4 生成应答数据 2
2.5 验证应答数据有效性 3
2.6 获取应答数据信息 3
2.7 获取应答数据详细信息 3
2.8 验证明文数据有效性 3

3 附录 5

3.1 错误码定义 5
3.2 分组密码算法标识 7
3.3 非对称密码算法标识 7
3.4 密码杂凑算法标识 7
3.5 签名算法标识 8
3.6 应答解析项标识 8

1 引言

1.1 概述

中安云科时间戳服务器（以下简称“时间戳服务器”）是由中安云科科技发展(山东)有限公司自主研发的高性能密码设备，能够为各类业务系统提供高性能的、多任务并行处理的密码运算，支持 SM1、SM2、SM3、SM4 等多种国产密码算法，具有证书管理、密钥安全存储、设备管理、访问控制、高速密码运算、真随机数生成、日志审计和设备自检等功能。可以满足应用系统数据的签名/验证、加密/解密的要求，保证传输信息的机密性、完整性和有效性，同时提供安全、完善的密钥管理机制，自身具备较强的安全防护能力。

1.2 使用方法

中安云科时间戳服务器 JAVA 版客户端接口支持 JDK1.8 以及以上版本，使用接口要有以下配置：

1.将开发包中的 ZAYKTSAAPI-1.0.6.jar 文件添加到应用程序中；

2.接口的调用要引用 com.zayk.tsa.api.ZaTSAApi,所有接口的实现在 ZaTSAApi 类中。

3.系统错误码定义在com.zayk.tsa.util.ConstErr 中，调用 ConstErr.getErrString(int ErrCode)可以返回错误码代表的详细解释；

4.系统常量定义在 com.zayk.tsa.util.ConstUtil 类中，包含附录中 3.2-3.6 所示的各种标识内容。

5.客户端接口库配置信息格式如下（默认文件名：zayktsa.ini）：

```
HsmIp =192.168.6.20,192.168.6.12     //时间戳服务器IP地址,可以配置多台
HsmPort=13559       //时间戳服务器服务端口，不需要修改
LogLevel=4         //日志级别 0：不打印日志 1：ERR 2：WARN 3.INFO 4.DEBUG
writeFile=false       //是否打印请求和返回的数据 false：不打印 true：打印
SocketTimeOut = 300 //超时时间，根据需要进行修改，单位秒
ConnectCount = 5     //socket连接数
selectTime = 50       //select选择时间，根据需要进行修改，单位秒
HeartBeatSleepTime=5   //心跳间隔时间 单位分钟    0 代表关闭心跳
```

1.3 接口日志

WIN环境：在用户主目录下，例如C:\Users\test，建“zayk_log”文件。

Linux环境：在/tmp下建“zayk_log”文件。

建议压力测试或系统上线正常运行后删除或修改该文件夹名称，防止影响性能和占用磁盘空间。

2 接口使用说明

2.1 连接初始化接口

功能描述	连接初始化	
函数原型	public static int STF_InitEnvironment(TSHandle handle)	
参数	TSHandle handle	句柄对象
返回值	0 -- 执行成功 !=0 -- 执行错误，详见附录	

2.2 连接释放

功能描述	连接释放	
函数原型	public static int STF_ClearEnvironment(TSHandle handle)	
参数	TSHandle handle	句柄对象
返回值	0 -- 执行成功 !=0 -- 执行错误，详见附录	

2.3 生成时间戳请求数据

功能描述	获得随机数	
函数原型	public static byte[] STF_CreateTSRequest(TSHandle handle, byte[] pucInData, int reqType, byte[] pucTSExt, int hashAlg)	
参数	TSHandle handle	句柄对象
	byte[] pucInData	明文数据
	int reqType	请求时间戳的服务类型。 0：时间戳响应包含时间戳服务器的证书； 1：时间戳响应不包含时间戳服务器的证书
	byte[] pucTSExt	时间戳请求包的其他扩展，DER 编码格式
	int hashAlg	摘要算法，见附录 3.4
返回值	!null -- 执行成功,返回内容就是获得的请求数据 null -- 执行错误	

2.4 生成应答数据

功能描述	对明文数据进行摘要运算	
函数原型	public static byte[] STF_CreateTSResponse(TSHandle handle, byte[] pucTSRequest, int signAlgID)	
参数	TSHandle handle	句柄对象

	byte[] pucTSRequest	请求数据
	int signAlgID	签名算法，见附录 3.5
返回值	!null - 执行成功 数据为应答数据 null -执行错误	

2.5 验证应答数据有效性

功能描述	验证应答数据有效性	
函数原型	public static int STF_VerifyTSValidity(TSHandle handle, byte[] pucTSResponse, int uiHashAlgID, int uiSignatureAlgID, byte[] pucTSCert)	
参数	TSHandle handle	句柄对象
	byte[] pucTSResponse	应答数据
	int uiHashAlgID	摘要算法，见附录 3.4
	int uiSignatureAlgID	签名算法，见附录 3.5
	byte[] pucTSCert	证书数据，null 为不验证
返回值	0 -- 执行成功，验证通过 !=0 -- 验证失败，详见附录	

2.6 获取应答数据信息

功能描述	获取应答数据信息	
函数原型	public static Map<String, Object> STF_GetTSInfo(TSHandle handle, byte[] pucTSResponse)	
参数	TSHandle handle	句柄对象
	byte[] pucTSResponse	应答数据
返回值	!null--执行成功，返回 Map 对象获取证书信息 null --执行错误	

2.7 获取应答数据详细信息

功能描述	获取应答数据详细信息	
函数原型	public static byte[] STF_GetTSDetail(TSHandle handle, byte[] pucTSResponse, int uiItemNumber)	
参数	TSHandle handle	句柄对象
	byte[] pucTSResponse	应答数据
	int uiItemNumber	要获取的信息类型：见 3.6
返回值	!null --执行成功 返回信息数据 null --执行错误	

2.8 验证应答和明文数据有效性

功能描述	验证应答和明文数据有效性

函数原型	public static int STF_VerifyTSValidity_Data(TSHandle handle, byte[] pucInData, byte[] pucTSResponse, int uiHashAlgID, int uiSignatureAlgID, byte[] pucTSCert)	
参数	TSHandle handle	句柄对象
	byte[] pucInData	明文数据
	byte[] pucTSResponse	应答数据
	int uiHashAlgID	摘要算法，见附录 3.4
	int uiSignatureAlgID	签名算法，见附录 3.5
	byte[] pucTSCert	证书数据，null 为不验证
返回值	0 -- 执行成功，验证通过 !=0 -- 验证失败，详见附录	

3 附录

3.1 错误码定义

宏定义	错误码	描述
GM_SUCCESS	0	正常返回
GM_ERROR_BASE	0x04000000	错误码起始值
GM_ERROR_CERT_ID	0x04000001	错误的证书标示
GM_ERROR_CERT_INFO_TYPE	0x04000002	错误的证书信息类型
GM_ERROR_SERVER_CONNECT	0x04000003	CRL 或OCSP 服务器无法连接
GM_ERROR_SIGN_METHOD	0x04000004	签名算法类型错误
GM_ERROR_KEY_INDEX	0x04000005	签名者私钥索引值错误
GM_ERROR_KEY_VALUE	0x04000006	签名者私钥权限标识码错误
GM_ERROR_CERT	0x04000007	证书非法或服务器内不存在
GM_ERROR_CERT_DECODE	0x04000008	证书接吗错误
GM_ERROR_CERT_INVALID_AF	0x04000009	证书过期
GM_ERROR_CERT_INVALID_BF	0x0400000A	证书尚未生效
GM_ERROR_CERT_REMOVED	0x0400000B	证书已被吊销
GM_INVALID_SIGNATURE	0x0400000C	签名无效
GM_INVALID_DATA_FORMAT	0x0400000D	数据格式错误
GM_SYSTEM_FAILURE	0x0400000E	系统内部错误
GM_ERR_MALLOC_FAILURE	0x0400A001	分配内存错误
GM_ERR_CERT_NO_EXTENSION	0x0400A002	缺少指定扩展
GM_ERR_CERT_NO_NAME_ENTRY	0x0400A003	缺少名称字段
GM_ERR_NO_ISSUER_CERT	0x0400A004	没找到颁发者证书
GM_ERR_NO_SIGNER_ID	0x0400A005	没有对应的证书 ID
GM_ERR_NO_SIGNER_PUBLIC_KEY	0x0400A006	没有颁发者公钥
GM_ERR_NO_SIGNER_SIGN_CERT	0x0400A007	没有颁发者证书
GM_ERR_SIGN_METHOD	0x0400A008	签名算法错误
GM_ERR_DIGEST_METHOD	0x0400A009	摘要算法错误

GM_ERR_PARAMETER	0x0400A010	输入参数错误
GM_ERR_KEY_TYPE	0x0400A011	密钥类型错误
GM_ERR_ALG_TYPE	0x0400A012	算法类型错误
GM_ERR_CERT_USAGE	0x0400A013	证书用法错误
GM_ERR_RANDOM_FAILURE	0x0400A014	生成随机数错误
GM_ERR_SYSTEM_STATUS	0x0400A015	系统内部状态错误
GM_ERR_ACCESS_DENIED	0x0400A021	访问文件错误
GM_ERR_WRITE_FAULT	0x0400A022	写入文件错误
GM_ERR_DIGEST_FAILED	0x0400A031	计算摘要错误
GM_ERR_DIGEST_INIT_FAILED	0x0400A032	摘要运算初始化错误
GM_ERR_DIGEST_UPDATE_FAILED	0x0400A033	摘要运算更新错误
GM_ERR_DIGEST_FINAL_FAILED	0x0400A034	摘要运算结束错误
GM_ERR_SIGN_FAILED	0x0400A041	签名错误
GM_ERR_VERIFY_FAILED	0x0400A042	验签错误
GM_ERR_ENCRYPT_FAILED	0x0400A043	加密错误
GM_ERR_DECRYPT_FAILED	0x0400A044	解密错误
GM_ERR_KEY_PARSE_ERROR	0x0400A051	解析密钥错误
GM_ERR_CERT_PARSE_ERROR	0x0400A052	解析证书错误
GM_ERR_CRL_PARSE_ERROR	0x0400A053	解析 CRL 错误
GM_ERR_PKCS7_PARSE_ERROR	0x0400A054	解析 PKCS7 错误
GM_ERR_PKCS12_PARSE_ERROR	0x0400A055	解析 PKCS12 错误
GM_ERR_URL_PARSE_ERROR	0x0400A056	解析 URL 错误
GM_ERR_XML_PARSE_ERROR	0x0400A057	解析 XML 错误
GM_ERR_JSON_PARSE_ERROR	0x0400A058	解析 JSON 错误
GM_ERR_CIPHER_INIT_FAILED	0x0400A061	对称运算初始化错误
GM_ERR_CIPHER_UPDATE_FAILED	0x0400A062	对称运算更新错误
GM_ERR_CIPHER_FINAL_FAILED	0x0400A063	对称运算结束错误
GM_ERR_INVALID_KEY_LENGTH	0x0400A064	密钥长度错误

GM_ERR_INVALID_IV_LENGTH	0x0400A065	IV 长度错误
GM_ERR_INVALID_IN_DATA_LENGTH	0x0400A066	输入数据长度错误

3.2 分组密码算法标识

标签	标识符	描述
SGD_SM1_ECB	0x00000101	SM1 算法 ECB 加密算法
SGD_SM1_CBC	0x00000102	SM1 算法 CBC 加密算法
SGD_SM1_CFB	0x00000103	SM1 算法 CFB 加密算法
SGD_SM1_OFB	0x00000108	SM1 算法 OFB 加密算法
SGD_SM4_ECB	0x00000401	SM4 算法 ECB 加密算法
SGD_SM4_CBC	0x00000402	SM4 算法 CBC 加密算法
SGD_SM4_CFB	0x00000404	SM4 算法 CFB 加密算法
SGD_SM4_OFB	0x00000408	SM4 算法 OFB 加密算法

3.3 非对称密码算法标识

标签	标识符	描述
SGD_RSA	0x00010000	RSA 算法
SGD_RSA_SIGN	0x00010100	RSA 签名算法
SGD_RSA_ENC	0x00010200	RSA 加密算法
SGD_SM2	0x00020100	SM2 椭圆曲线密码算法
SGD_SM2_1	0x00020200	SM2 椭圆曲线签名算法
SGD_SM2_2	0x00020400	SM2 椭圆曲线密钥交换协议
SGD_SM2_3	0x00020800	SM2 椭圆曲线加密算法

3.4 密码杂凑算法标识

标签	标识符	描述
SGD_SM3	0x00000001	SM3 杂凑算法
SGD_SHA1	0x00000002	SHA1 杂凑算法
SGD_SHA256	0x00000004	SHA256 杂凑算法

3.5 签名算法标识

标签	标识符	描述
SGD_SHA1_RSA	0x00010002	基于 SHA1 算法和 RSA 算法签名
SGD_SHA256_RSA	0x00010004	基于 SHA256 算法和 RSA 算法签名
SGD_SM3_SM2	0x00020201	基于 SM3 算法和 SM2 算法的签名

3.6 应答解析项标识

标签	标识符	描述
STF_TIME_OF_STAMP	0x00000001	签发时间
STF_CN_OF_TSSIGNER	0x00000002	签发者的通用名
STF_ORINGINAL_DATA	0x00000003	时间戳请求的原始信息
STF_CERT_OF_TSSERVER	0x00000004	时间戳服务器的证书
STF_CERTCHAIN_OF_TSSERVER	0x00000005	时间戳服务器的证书链
STF_SOURCE_OF_TIME	0x00000006	时间戳的来源
STF_TIME_PRECISION	0x00000007	时间精度
STF_PESPOUSE_TYPE	0x00000008	响应方式
SSTF_SUBJECT_COUNTRY_OF_TSSIGNER	0x00000009	签发者国家
STF_SUBJECT_ORGNIZATION_OF_TSSIGNER	0x0000000A	签发者组织
STF_SUBJECT_CITY_OF_TSSIGNER	0x0000000B	签发者城市
STF_SUBJECT_EMAIL_OF_TSSIGNER	0x0000000C	签发者联系用电子信箱