产品名称 Product name	密级 Confidentiality level
mToken GM3000	
产品版本 Product version	
V1.2	

mToken GM3000 开发者指南

Prepared by 拟制		Date 日期	
Reviewed by 评审人		Date 日期	
Approved by 批准		Date 日期	

北京世纪龙脉科技有限公司
Beijing Century Longmai Technology Co., Ltd.

Revision Record 修改记录

Date 日期	Revision Version 修订版本	Sec No. 修改章节	Change Description 修改描述	Author 作者
2013/10/22	V1.0		初始版本	

目录

第一章 GM3000 开发说明

龙脉 mToken GM3000 提供符合国际规范的 CSP 和 PKCS11 应用接口以及国家密码局标准规范的应用接口供应用软件和开发人员使用，并可根据用户需求提供自定义接口。

GM3000 CSP 应用接口遵循微软 MS CryptoAPI 接口标准，开发人员可直接通过微软提供的标准接口即可实现对 GM3000 的操作及应用，相关 API 请参考微软 MSDN 文档说明。

GM3000 PKCS11 应用接口符合 PKCS11 V2.2 标准， 并支持 Windows, Linux , Mac OS 等多个开发平台，开发人员可通过 PKCS11 接口标准对 GM3000 在各个平台下使用。

GM3000 国密应用接口符合《GM/T 0016-2012 智能密码钥匙密码应用接口规范》接口标准，并支持多个开发平台，可用于国密算法应用。

第二章 GM3000 CSP 接口应用规范

本章讲述 GM3000 所支持 CryptoAPI 接口开发的相关情况，涉及的内容包括 GM3000 的 CSP 接口名称及支持的函数和算法实现情况。

GM3000 CSP 模块

GM3000 通过提供标准的 CSP 模块来实现与 Crypto API 应用程序的无缝集成。GM3000 的 CSP 模块遵从微软的 Crypto Service Provider 编程规范编写，可以兼容现有的和将来的 Crypto API 应用

GM3000 CSP 支持的算法描述

算法	默认长度(bit)	最小长度(bit)	最大长度(bit)	用途类别
CALG_RC2	128	128	128	加解密
CALG_RC4	128	128	128	
CALG_DES	56	56	56	
CALG_3DES	168	168	168	
CALG_3DES_112	112	112	112	
CALG_AES_128	128	128	128	
CALG_AES_192	128	128	128	
CALG_AES_256	128	128	128	
CALG_SHA1	160	160	160	散列
CALG_SHA_256	256	256	256	
CALG_SHA_512	512	512	512	
CALG_MD5	128	128	128	
CALG_SSL3_SHAMD5	288	288	288	
CALG_RSA_SIGN	1024	1024	2048	签名验证
CALG_RSA_KEYX	1024	1024	2048	加解密、签名验证

GM3000 CSP 支持的函数实现描述

下表中列出了CSP接口各函数的支持和实现情况，"未实现"表示在CSP模块中有该接口，但是并没有实现，"未支持"表示在 CSP 模块中没有该函数入口。
由于 GM3000 的 CSP 类型为 PROV_RSA_FULL，不支持下表中所列出的标有"未支持"的函数是很正常的。标示为"未实现"的函数都返回 FALSE 并置 ErrorCode 为 E_NOTIMPL。这些函数是 CSP 接口，CryptoAPI 应用程序不需要直接调用这些接口。

名称	描述	支持情况
连接函数		
CPAcquireContext	为应用程序创建一个上下文	已实现
CPGetProvParam	返回CSP相关的信息	已实现
CPReleaseContext	释放CPAcquireContext.创建的上下文	已实现
CPSetProvParam	设置CSP的参数操作	已实现
密钥生成和交换函数		
CPDeriveKey	从一个数据散列中生成一个会话密钥，它保证生成的密钥互不相同	已实现
CPDestroyKey	释放一个密钥句柄，释放后，句柄将无效，密钥将无法再被访问	已实现
CPDuplicateKey	创建密钥的一个拷贝	未支持
CPExportKey	从CSP容器中导出密钥	已实现
CPGenKey	用来生成密钥或密钥对	已实现
CPGenRandom	使用随机数填充一个缓冲	已实现
CPGetKeyParam	用来得到加密操作密钥的属性	已实现
CPGetUserKey	用来获取CSP容器中的持久密钥对	已实现
CPImportKey	从一个blob中导入密钥到CSP容器中	已实现
CPSetKeyParam	设置密钥的属性	已实现
数据加密函数		
CPDecrypt	用来解密先前被加密的数据	已实现
CPEncrypt	用来加密明文	已实现
散列和数字签名函数		
CPCreateHash	初始化并散列输入数据	已实现
CPDestroyHash	删除一个散列对象句柄	已实现
CPDuplicateHash	创建一个散列对象的拷贝	未支持
CPGetHashParam	获取散列对象的计算结果	已实现
CPHashData	散列输入的数据	已实现
CPHashSessionKey	散列一个会话密钥而不向应用程序暴露密钥的值	已实现
CPSetHashParam	定制一个散列对象的属性	已实现
CPSignHash	签名一个散列对象	已实现
CPVerifySignature	校验一个数字签名	已实现

关于 CryptoAPI,请参考微软 MSDN 帮助文档。

开发示例

开发人员可以在 SDK 包中的 Samples\CryptAPI 目录下找到使用 GM3000 的 CryptAPI 接口的示例程序并可以编译调试，有些示例程序您可能需要安装微软的 Platform SDK。

第三章 GM3000 PKCS11 接口应用规范

本章讲述 GM3000 所支持的 PKCS#11 接口开发的相关情况，涉及的内容包括 GM3000 的 PKCS#11 接口名称及支持的函数和算法实现情况。

GM3000 PKCS#11 模块描述

GM3000为不同的平台提供了PKCS11标准接口模块，包括Windows, Linux和Mac OS X, 并可根据用户的需求提供其它平台的相关PKCS11模块。

GM3000 PKCS11 模块实现了 RSA PKCS#11 标准中定义的所有接口函数，如果开发人员需要使用这个接口，并且所访问的都是 PKCS#11 规范规定的标准接口和定义，则必须在工程项目中包含 cryptoki.h 头文件，并参考相关例程进行开发。

GM3000 PKCS#11 函数的算法实现描述

下表列出了所有GM3000的PKCS#11模块支持的密码学算法：

算法	加解密	签名校验	散列	密钥对生成	封装
CKM_RSA_PKCS_KEY_PAIR_GEN				√	
CKM_RSA_PKCS	√	√			√
CKM_RSA_X_509	√	√			
CKM_SHA1_RSA_PKCS		√			
CKM_SHA256_RSA_PKCS		√			
CKM_SHA384_RSA_PKCS		√			
CKM_SHA512_RSA_PKCS		√			
CKM_MD5_RSA_PKCS		√			
CKM_RC2_KEY_GEN				√	
CKM_RC2_ECB	√				
CKM_RC2_CBC	√				
CKM_RC4_KEY_GEN				√	
CKM_RC4	√				
CKM_DES_KEY_GEN				√	
CKM_DES_ECB	√				√
CKM_DES_CBC	√				√
CKM_DES_CBC_PAD	√				√
CKM_DES3_KEY_GEN				√	
CKM_DES3_ECB	√				√
CKM_DES3_CBC	√				√

CKM_DES3_CBC_PAD	√				√
CKM_AES_KEY_GEN	√				
CKM_AES_ECB	√				
CKM_AES_CBC	√				
CKM_MD5			√		
CKM_SHA_1			√		
CKM_SHA256			√		
CKM_SHA384			√		
CKM_SHA512			√		

第四章 GM3000 国密接口

请参考《龙脉 mToken GM3000 国密 KEY 用户手册》

第五章 GM3000 用户自定义接口

由于 MS CryptoAPI 和 PKCS11 接口相对比较复杂，对开发人员有一定的要求，因此龙脉科技可根据用户的需求提供用户自定义接口来简化用户的开发，降低用户开发难度，可联系龙脉科技获得更多细节。

联系我们

公司总部

地址：北京市海淀区王庄路甲1号工控办公楼三层

电话：010-62323636

传真：010-62313636

热线：400-666-0811 (7x24免费热线)

邮箱：longmai@longmai.com.cn

网站：http://www.longmai.com.cn

商城：http://smart2000.taobao.com/

邮编：100083

杭州办事处

地址：浙江省杭州市西湖区文三西路499号西溪风尚5幢420

电话：0571-86908895

邮箱：hangzhou@longmai.com.cn

邮编：310012

广州办事处

地址：广东省广州市天河区黄埔大道中路262号恒安大厦恒福轩14D

电话：020-85272610

邮箱：guangzhou@longmai.com.cn

邮编：510630

申请试用

如果您对产品感兴趣，可先申请试用，测试通过后再进行购买。申请试用，请到龙脉官方网站填写试用单或直接打电话与我们联系：

试用：http://www.longmai.com.cn/apply/index.htm

邮箱：sales@longmai.com.cn

购买产品

如果您希望咨询产品价格或正式购买产品，可以通过如下方式与销售人员联系：

电话：010-62323636

邮箱：sales@longmai.com.cn

技术支持

我们提供了多种方式的技术支持服务，您可通过如下方式向技术人员咨询：

电话：010-62323636-661

邮箱：support@longmai.com.cn