**KDStorageCrypt加密库接口说明文档**

**v0.1**

|  |  |  |  |
| --- | --- | --- | --- |
| **公司名称** | 金证股份 | **文档编号** |  |
| **文档名称** | 接口文档 | **文档版本** | 0.1 |
| **起草** |  | **起草日期** | 2018-06-05 |
| **审批** |  | **审批日期** |  |

修订历史

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本号 | 日期 | 状态 | 修订人 | 摘要 |
| 0.1 | 20180605 | C | 李学 |  |
|  | 20180605 | M | 李学 | 1. 增加CipherToGMCipher接口，专门做存储密文转国密存储密文 2. 将CipherTextToGMCipherText\_W、CipherTextToGMCipherText\_U和CipherTextToGMCipherText\_KBSS三个接口不再对外暴露 3. 给每个接口增加参数类型的说明 4. 针对部分接口的参数后面的备注进行相应补充 5. 给每个接口入参加上const |
|  | 20180606 | M | 李学 | 1. 将接口名称由GMCipherTextCheck改为GM\_CipherCheck 2. QueryType接口增加nPlatformType参数 |
|  | 20180607 | M | 李学 | 1. 取消QueryType接口的nPlatformType参数 2. 修改QueryType接口的返回值说明 3. 修改GM\_CipherCheck接口的返回值说明 4. 修改GM\_CommEncrypt接口和GM\_Encrypt接口第二个出参的备注说明 |
|  | 20180611 | M | 李学 | 1. 修改CipherToGMCipher接口的返回值说明，增加-7的返回值说明 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

状态标识：C –Created A- Added M - Modified D – Deleted

目录

[1 引言 4](#_Toc516048355)

[1.1 目的和范围 4](#_Toc516048356)

[1.2 参考资料 4](#_Toc516048357)

[2 概述 4](#_Toc516048358)

[3 接口说明 5](#_Toc516048359)

[3.1 GM\_CommEncrypt 5](#_Toc516048360)

[3.2 GM\_CommDecrypt 5](#_Toc516048361)

[3.3 GM\_Encrypt 6](#_Toc516048362)

[3.4 GMCipherTextCheck 6](#_Toc516048363)

[3.5 CipherToGMCipher 7](#_Toc516048364)

[3.6 QueryType 8](#_Toc516048365)

[4 接口调用场景说明 9](#_Toc516048366)

[4.1 场景一 9](#_Toc516048367)

[4.2 场景二 10](#_Toc516048368)

# 引言

## 目的和范围

KDStorageCrypt加密库是因国密改造而产生的，同时兼具以后发展的考虑，统一公司内部的所有加密库，将加密集中起来，结束各产品部门采用自己加密库导致产品之间对接困难的状态，以后各产品部门的通讯加密和存储加密都可以采用KDStorageCrypt库。

## 参考资料

# 概述

本文档主要分两块内容：

1. KDStorageCrypt加密库接口说明
2. KDStorageCrypt加密库接口调用场景说明

# 接口说明

KDStorageCrypt加密库的接口的参数的顺序是做了规定的，出参在前面，入参在后面

## GM\_CommEncrypt

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称：GM\_CommEncrypt | | | | |
| 接口说明：国密通讯加密 | | | | |
| 参数 | 参数类型 | 参数名称 | 数据类型 | 备注 |
| 出参 | pCipherText | unsigned char \* | 密文 |
| 出参 | nCipherTextBufLen | int | 密文缓冲区大小 |
| 入参 | pPlainText | const unsigned char\* | 明文 |
| 入参 | nPlainTextLen | int | 明文大小 |
| 入参 | pKey | const unsigned char\* | 密钥 |
| 入参 | nKeyLen | int | 密钥大小 |
| 返回值 | 返回值 | | 备注 | |
| 大于0的正整数 | | 加密成功，并返回密文长度 | |
| -1 | | 加密失败 | |
| -2 | | 明文为空 | |
| -3 | | 密钥为空 | |
| -4 | | 密文缓冲区不足 | |

## GM\_CommDecrypt

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称：GM\_CommDecrypt | | | | |
| 接口说明：国密通讯解密 | | | | |
| 参数 | 参数类型 | 参数名称 | 数据类型 | 备注 |
| 出参 | pPlainText | unsigned char \* | 明文 |
| 出参 | nPlainTextBufLen | int | 明文缓冲区大小，解密成功后其值表示明文的长度 |
| 入参 | pCipherText | const unsigned char\* | 密文 |
| 入参 | nCipherTextLen | int | 密文大小 |
| 入参 | pKey | const unsigned char\* | 密钥 |
| 入参 | nKeyLen | int | 密钥大小 |
| 返回值 | 返回值 | | 备注 | |
| 大于0的正整数 | | 解密成功，并返回明文长度 | |
| -1 | | 加密失败 | |
| -2 | | 密文为空 | |
| -3 | | 密钥为空 | |
| -4 | | 明文缓冲区不足 | |

## GM\_Encrypt

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称：GM\_Encrypt | | | | |
| 接口说明：国密存储加密 | | | | |
| 参数 | 参数类型 | 参数名称 | 数据类型 | 备注 |
| 出参 | pCipherText | unsigned char \* | 密文 |
| 出参 | nCipherTextBufLen | int | 密文缓冲区大小 |
| 入参 | pPlainText | const unsigned char\* | 明文 |
| 入参 | nPlainTextLen | int | 明文大小 |
| 入参 | pKey | const unsigned char\* | 密钥 |
| 入参 | nKeyLen | int | 密钥大小 |
| 返回值 | 返回值 | | 备注 | |
| 大于0的正整数 | | 加密成功，并返回密文长度 | |
| -1 | | 加密失败 | |
| -2 | | 明文为空 | |
| -3 | | 密钥为空 | |
| -4 | | 密文缓冲区不足 | |

## GM\_CipherCheck

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称：GM\_CipherCheck | | | | |
| 接口说明：国密存储密文校验 | | | | |
| 参数 | 参数类型 | 参数名称 | 数据类型 | 备注 |
| 入参 | pGMCipherText1 | const unsigned char\* | 国密存储密文1 |
| 入参 | nGMCipherTextLen1 | int | 国密存储密文1大小 |
| 入参 | pGMCipherText2 | const unsigned char\* | 国密存储密文2 |
| 入参 | nGMCipherTextLen2 | int | 国密存储密文2大小 |
| 入参 | pKey | const unsigned char\* | 密钥 |
| 入参 | nKeyLen | int | 密钥大小 |
| 返回值 | 返回值 | | 备注 | |
| 0 | | 校验成功 | |
| -1 | | 加密失败 | |
| -2 | | 密文为空 | |
| -3 | | 密钥为空 | |
| -4 | | 密文解密失败 | |
| -5 | | 非国密密文 | |
| -6 | | 非国密存储密文 | |

## CipherToGMCipher

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称：CipherToGMCipher | | | | |
| 接口说明：存储密文转国密存储密文 | | | | |
| 参数 | 参数类型 | 参数名称 | 数据类型 | 备注 |
| 出参 | pGMCipherText | unsigned char \* | 国密存储密文 |
| 出参 | nGMCipherTextBufLen | int | 密文缓冲区大小，转换成功后其值表示密文的长度 |
| 入参 | pGMKey | const unsigned char\* | 密钥(加密用) |
| 入参 | nGMKeyLen | int | 密钥大小 |
| 入参 | pCipherText | const unsigned char\* | 存储密文 |
| 入参 | nCipherTextLen | int | 密文大小 |
| 入参 | pKey | const unsigned char\* | 密钥(解密用) |
| 入参 | nKeyLen | int | 密钥大小 |
| 入参 | nCipherTextEncryptType | int | 存储密文加密方式，其送值可参看接口头文件里EM\_PlatformType的定义 |
| 返回值 | 返回值 | | 备注 | |
| 大于0的正整数 | | 转换成功，并返回密文长度 | |
| -1 | | 转换失败 | |
| -2 | | 密文为空 | |
| -3 | | 密钥为空 | |
| -4 | | 密文解密失败 | |
| -5 | | 加密失败 | |
| -6 | | 密文缓冲区不足 | |
| -7 | | 待转换密文已是国密密文 | |

## QueryType

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称：QueryType | | | | |
| 接口说明：密文类型查询 | | | | |
| 参数 | 参数类型 | 参数名称 | 数据类型 | 备注 |
| 出参 | pOutType | unsigned char\* | 密文类型，其值可参看接口头文件里EM\_EncryptType的定义 |
| 入参 | pCipherText | const unsigned char\* | 密文 |
| 入参 | nCipherTextLen | int | 密文大小 |
| 返回值 | 返回值 | | 备注 | |
| 0 | | 查询成功 | |
| -1 | | 密文为空 | |
| -2 | | 非国密密文 | |

# 接口调用场景说明

调用场景将说明以上接口会在什么情况下使用

## 场景一



## 场景二

