ICS 35.040
L 80
备案号:62991—2018

GM

中华人民共和国密码行业标准

GM/T 0056—2018

多应用载体密码应用接口规范

Specification of cryptography application interface with multi-applications equipment

2018-05-02 发布　　2018-05-02 实施

国家密码管理局　　发 布

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　多应用载体系统框架 …… 2
6　多应用载体密码应用接口调用流程 …… 3
6.1　密码应用接口调用流程 …… 3
6.2　密码算法能力标识 …… 4
6.3　密码应用接口规格 …… 4
7　Java 技术方案密码应用接口 …… 4
7.1　简介 …… 4
7.2　密码算法能力标识 …… 4
7.3　密码应用包定义 …… 5
7.4　密码应用接口定义 …… 5
7.5　密码应用类信息 …… 6
附录 A（资料性附录）　多应用安全管理的密码应用要求 …… 28
附录 B（资料性附录）　多应用安全管理的证书格式 …… 33
参考文献 …… 35

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：北京中电华大电子设计有限责任公司、上海华虹集成电路有限责任公司、北京同方微电子有限公司、恒宝股份有限公司、北京握奇数据系统有限公司、东信和平科技股份有限公司、北京华大智宝电子系统有限公司、上海复旦微电子集团股份有限公司、国民技术股份有限公司、北京南瑞智芯微电子科技有限公司、成都信息工程大学、武汉天喻信息产业股份有限公司、华大半导体有限公司。

本标准主要起草人：兰天、吴秉男、苑中魁、袁巧、陈操、刘平、王庆林、王怀英、耿佳、白长虹、汪雪琳、张楠、王永吉、李志远、陈悦、李静进、何迪、赵永刚、王宝鹍、陈安新、吴震、饶金涛、黄惠瑜、许晶、刘欣。

引　言

本标准中多应用载体是指具备独立、开放的片上操作系统、提供多应用运行环境、支持载体上多个应用的下载、安装、重用、共存和安全隔离的载体，通常由硬件、驱动、COS 和应用构成。

多应用载体中的用户应用在使用 SM2/3/4 系列算法时，需要载体的多应用环境提供 SM2/3/4 系列算法的密码应用调用接口。由于目前多应用载体相关标准未定义 SM2/3/4 系列算法的应用接口，造成用户应用无法使用的问题。为此，编制本标准以规范 SM2/3/4 系列算法在多应用载体中的密码算法能力标识、接口规格，保障用户应用使用密码功能的统一性和完整性。

多应用载体可以使用不同的技术方案实现，如 Java 技术方案、C 技术方案等。本版本主要描述了 Java 技术方案中的密码应用接口，其他技术方案的密码应用接口根据应用发展情况在后续版本中给出。

多应用载体密码应用接口规范

1 范围

本标准规定了多应用载体中 SM2/3/4 系列算法的密码应用接口，包括：

——定义 SM2/SM3/SM4 的算法在多应用载体中的标识。

——定义 SM2/SM3/SM4 的算法的密码应用接口规格。

本标准适用于各种多应用载体的研制，也可用于指导多应用载体的密码应用检测。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4 分组密码算法

GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

ISO 9797 信息技术 安全技术 消息认证代码(MACs)

RFC 2898 Specification of PKCS #5

3 术语和定义

下列术语和定义适用于本文件。

3.1

命令 command

终端向载体发出的一条信息，该信息启动一个操作或请求一个应答。

3.2

响应 response

载体处理完成收到的命令报文后，回送给终端的报文。

3.3

报文 message

由终端向载体或载体向终端发出的，不含传输控制字符的字节串。

3.4

多应用载体 multi-applications equipment

具备独立、开放的片上操作系统、提供多应用运行环境、支持载体上多个应用的下载、安装、重用、共存和安全隔离的载体，通常由硬件、驱动、COS 和应用构成。

3.5

SM2 算法 SM2 algorithm

由 GB/T 32918 定义的一种算法。

3.6

SM3 算法 SM3 algorithm

由 GB/T 32905—2016 定义的一种算法。