ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0127—2023

移动终端密码模块应用接口规范

Mobile terminal cryptographic module application interface specification

2023-12-04 发布　　2024-06-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：中国科学院数据与通信保护研究教育中心、中国科学技术大学、中国科学院信息工程研究所、北京数字认证股份有限公司、北京理工大学、长春吉大正元信息技术股份有限公司、北京交通大学、中国信息通信研究院、北京信安世纪科技股份有限公司、中国人寿保险股份有限公司研发中心、国家计算机网络应急技术处理协调中心、中国电子技术标准化研究院、中国工业互联网研究院、中电科网络安全科技股份有限公司、格尔软件股份有限公司、北京中电华大电子设计有限责任公司、北京创原天地科技有限公司、北京小雷科技有限公司、北京国脉信安科技有限公司、财付通支付科技有限公司、北京炼石网络技术有限公司、深信服科技股份有限公司、北京路云天网络安全技术研究院有限公司。

本文件主要起草人：林璟锵、贾世杰、郑昉昱、徐博文、马原、夏鲁宁、夏冰冰、王安、高旭、黎琳、徐秀、汪宗斌、徐丽娟、张晓娜、黄晶晶、李琳、王平建、刘丽敏、王伟、牛莹姣、赵欣怡、吕娜、雷灵光、钱文飞、唐明环、于成丽、张立廷、尹一桦、赵丽丽、黄福飞、李涛、王睿、肖云松、柳增寿、袁峰、何畅、吴怡、白小勇、鲍旭华、孔勇。

引　言

在移动终端上调用各类密码模块实现密码服务的方式已逐渐普及，本文件目标是为各类移动终端密码模块的实现提供统一的应用接口规范，进一步推动密码算法在移动终端上的部署和应用。为移动终端密码模块的开发、使用及检测提供标准依据和指导，有利于提高移动终端密码模块的产品化、标准化和系列化水平。

移动终端密码模块应用接口规范

1 范围

本文件规定了移动终端密码模块的结构模型、数据类型定义、应用接口及安全要求。

本文件适用于移动终端密码模块产品的研制和使用，以及基于该类密码产品的应用开发与检测。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 15852.1 信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 37092 信息安全技术 密码模块安全要求

GM/T 0017—2023 智能密码钥匙密码应用接口数据格式规范

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

密码模块 cryptographic module

实现了安全功能的硬件、软件和/或固件的集合，并且被包含在密码边界内。

3.2

模块鉴别 module authentication

移动终端密码模块对应用程序的鉴别。

3.3

模块鉴别密钥 module authentication key

用于模块鉴别的密钥。

3.4

容器 container

密码模块中用于保存密钥所划分的唯一性存储空间。

3.5

应用 application

包括PIN、文件和容器的一种结构，具备独立的权限管理。