ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0016—2023
代替 GM/T 0016—2012

智能密码钥匙密码应用接口规范

Smart token cryptography 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。

本文件代替GM/T 0016—2012《智能密码钥匙密码应用接口规范》，与GM/T 0016—2012相比，除结构调整和编辑性改动外，主要技术变化如下：

a）　删除了“填充方式”（见表11，2012年版的表11）；

b）　更改了“修改设备认证密钥”函数（见7.2.2，2012年版的7.2.2）；

c）　更改了“获得容器类型”（见7.5.7，2012年版的7.5.7）；

d）　更改了“导出公钥”（见7.6.18，2012年版的7.6.17）；

e）　更改了“导入会话密钥”（见7.6.19，2012年版的7.6.18）；

f）　更改了“安全要求”（见第8章，2012年版的第8章）；

g）　增加了HMAC相关接口（见7.6.36、7.6.37、7.6.38、7.6.39）；

h）　增加了验证调试类接口（见7.7）；

i）　增加了SM9应用接口（见附录B）；

j）　增加了VPN相关接口（见附录C）；

k）　增加了SM9编程范例（见附录D）。

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：北京海泰方圆科技股份有限公司、北京握奇智能科技有限公司、格尔软件股份有限公司、无锡江南信息安全工程技术中心、北京数字认证股份有限公司、兴唐通信科技有限公司、山东得安信息技术有限公司、北京三未信安科技发展有限公司、山东大学、北京大明五洲科技有限公司、恒宝股份有限公司、深圳市明华澳汉科技股份有限公司、武汉天喻信息产业股份有限公司、北京飞天诚信科技股份有限公司、华翔腾数码科技有限公司、北京鼎九信息工程研究院有限公司、北京百旺信安科技有限公司、中电科网络安全科技股份有限公司、北京国脉信安科技有限公司、北京小雷科技有限公司。

本文件主要起草人：刘平、蒋红宇、柳增寿、张立廷、罗俊、袁峰、封维端、靳京、张渊、陈国、李勃、郑强、李述胜、孔凡玉、王妮娜、马洪富、高志权、徐明翼、李增欣、于学东、郭宝安、石玉平、胡俊义、管延军、项莉、雷继业、胡鹏、赵再兴、段晓毅、刘玉峰、刘伟丰、陈吉、何永福、李高锋、黄东杰、王建承、汪雪林、赵李明、王烨。

本文件及其所代替文件的历次版本发布情况为：

——2012年首次发布版为GM/T 0016—2012；

——本次为第一次修订。

引　言

本文件的目标是为公钥密码基础设施应用体系框架下的智能密码钥匙设备制定统一的应用接口标准。通过该接口调用智能密码钥匙，向上层提供基础密码服务。为该类密码设备的开发、使用及检测提供标准依据和指导，有利于提高该类密码设备的产品化、标准化和系列化水平。

智能密码钥匙密码应用接口规范

1 范围

本文件规定了公钥密码体制下的智能密码钥匙应用接口标准、密码相关应用接口的函数、数据类型、参数的定义和设备的安全要求。

本文件适用于智能密码钥匙产品的研制、使用和检测。

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。

GM/T 0006—2023 密码应用标识规范

GM/T 0017—2023 智能密码钥匙密码应用接口数据格式规范

GM/T 0027—2014 智能密码钥匙技术规范

GM/T 0028—2014 密码模块安全要求

GM/Z 4001 密码术语

PKCS#1 RSA 密码规范版本 2.1(RSA Cryptography specification version 2.1)

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

容器 container

密码设备中用于保存密钥所划分的唯一性存储空间。

3.2

终端设备 terminal device

智能密码钥匙的统称。

3.3

设备认证 device authentication

智能密码钥匙对应用程序的认证。

3.4

设备认证密钥 device authentication key

用于设备认证的密钥。

3.5

设备标签 device label

终端设备的别名，可由用户进行设定并存储于设备内部。