ICS 35.240.15
CCS L 70

中华人民共和国国家标准

GB/T 44901.1—2024

卡及身份识别安全设备　片上操作系统 第1部分:总体要求

Cards and security devices for personal identification—Chip operating system—Part 1: General requirements

2024-10-26 发布　　2025-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件是GB/T 44901《卡及身份识别安全设备　片上操作系统》的第1部分。GB/T 44901已经发布了以下部分：

——第1部分：总体要求。

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。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位：中国电子技术标准化研究院、北京智芯微电子科技有限公司、江苏赛西科技发展有限公司、深圳市创自技术有限公司、江苏意源科技有限公司、深圳赛西信息技术有限公司、东信和平科技股份有限公司、北京握奇数据股份有限公司、武汉天喻信息产业股份有限公司、飞天诚信科技股份有限公司、北京中电华大电子设计有限责任公司、金邦达有限公司、北京安御道合科技有限公司、中移动金融科技有限公司、北京华大智宝电子系统有限公司、北京华弘集成电路设计有限责任公司、新大陆数字技术股份有限公司、中铁十九局集团有限公司、中国银联股份有限公司、紫光同芯微电子有限公司、大唐微电子技术有限公司、上海复旦微电子集团股份有限公司、四川省商投信息技术有限责任公司、中关村芯海择优科技有限公司、楚天龙股份有限公司、上海密特印制有限公司、深圳市海思半导体有限公司、中国联合网络通信集团有限公司。

本文件主要起草人：曹国顺、许晶、雷云、蒋日友、徐木平、黄小鹏、赵轶、高健、蔡春水、苏昆、朱鹏飞、李延、刘宏梅、谢依夫、韩劢之、孙健、张磊、孙春桂、果艳红、管振祥、韩博、何军、张树良、徐文军、李洋、孙金刚、黄海明、束敏、白婧、马一茗、付青琴、曹海涛、宋奕婷、王海涛。

引　言

片上操作系统指运行在卡及身份识别安全设备的安全芯片上的操作系统，通常应用于智能卡、USBKEY、ESAM、SE 等产品。为了确立统一的卡及身份识别安全设备的片上操作系统架构、规范统一的应用格式及应用接口，提高外围设备与安全芯片之间的互操作性，为测试验证提供依据，制定了GB/T 44901《卡及身份识别安全设备　片上操作系统》。

GB/T 44901《卡及身份识别安全设备　片上操作系统》旨在保证片上操作系统的可用性及安全性，便于系统、设备间的互连、互通和兼容，利于规范不同类型的产品，按照功能、层次划分片上操作系统的组成部分，指导卡及身份识别安全设备片上操作系统的设计研发，拟由六个部分构成。

——第 1 部分：总体要求。目的在于确立片上操作系统架构及系统组成，为片上操作系统系列规范提供指南和索引，并规范片上操作系统总体功能、性能、安全性、兼容性、易用性等软件质量特性要求。

——第 2 部分：通用基础层技术要求。目的在于规范片上操作系统通用基础层的具体功能技术要求。

——第 3 部分：支持应用后下载的基础层技术要求。目的在于规范支持应用后下载的基础层的应用安装器及执行器具体功能技术要求。

——第 4 部分：应用支持层技术要求。目的在于规范应用支持层的应用管理、生命周期管理及应用全局服务的具体功能技术要求。

——第 5 部分：应用接口层技术要求。目的在于规范片上操作系统的数据通信、存储管理、文件系统等应用编程接口。

——第 6 部分：安全技术要求。目的在于规范片上操作系统的信息安全防护目标和信息安全功能技术要求。

本文件对卡及身份识别安全设备片上操作系统的总体技术要求进行标准化，提供了片上操作系统设计研发及测试检验的依据，便于用户对片上操作系统的使用，可提高行业间、设备间的互操作性，更好地促进卡及身份识别安全设备产业链之间的沟通交流及技术合作。

卡及身份识别安全设备　片上操作系统
第1部分:总体要求

1　范围

本文件规定了片上操作系统的系统架构、功能要求、性能要求及安全要求。

本文件适用于卡及身份识别安全设备的片上操作系统的研发、检测、验收及应用。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

安全芯片　security chip

含有密码算法、安全功能,可实现密钥管理机制的集成电路芯片。

[来源:GM/T 0008—2012,3.1.3]

3.2

片上操作系统　chip operating system

运行在卡及身份识别安全设备中的安全芯片上的操作系统。

注:通常应用于智能卡、USBKEY、ESAM、SE等产品形态。

3.3

应用　application

为满足特定功能所需的数据结构、数据元和程序模块。

[来源:GB/T 16649.4—2010,3.3]

3.4

可加载文件　loadable file

由应用编译器生成的,能够加载到片上操作系统中的特定文件。

3.5

可执行文件　executable file

由应用安装器生成,能够由片上操作系统执行的文件。

3.6

可执行模块　executable module

包含在可执行文件中的单个应用的可执行代码。

注:若可执行文件包含该模块,则安装,否则不安装。

3.7

原子操作　atomic operation

所涉及的非易失性存储区的数据操作全部操作成功或保持原态的单个操作单元。