ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 22186—2026
代替 GB/T 22186—2016

网络安全技术　具有中央处理器的IC卡芯片安全规范

Cybersecurity technology—Security specifications for IC card chip with CPU

2026-04-30 发布　　2026-11-01 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 ……Ⅲ
引言 ……Ⅳ
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　IC 卡芯片描述 ……3
6　安全问题 ……4
6.1　资产 ……4
6.2　威胁 ……4
6.3　安全策略和假设 ……5
7　安全目的 ……6
7.1　TOE 安全目的 ……6
7.2　环境安全目的 ……7
8　扩展组件 ……7
8.1　族 FPT_EMS ……7
8.2　族 FPT_TST ……8
9　安全要求 ……9
9.1　概述 ……9
9.2　安全功能要求 ……9
9.3　安全保障要求 ……14
10　安全功能要求的测试方法 ……16
10.1　概述 ……16
10.2　密钥生成 ……16
10.3　密码运算 ……17
10.4　随机数生成 ……18
10.5　子集访问控制 ……18
10.6　基于安全属性的访问控制 ……19
10.7　子集信息流控制 ……19
10.8　基本内部传送保护 ……20
10.9　存储数据完整性监视 ……21
10.10　存储数据完整性监视和行动 ……21
10.11　鉴别的时机 ……22
10.12　鉴别失败处理 ……23
10.13　受限能力 ……23
10.14　受限可用性 ……24
10.15　安全属性管理 ……24
10.16　静态属性初始化 ……25
10.17　TSF 数据的管理 ……25

10.18 管理功能 ……26
10.19 安全角色 ……26
10.20 失效即保持安全状态 ……27
10.21 内部 TSF 数据传送的基本保护 ……28
10.22 物理攻击抵抗 ……28
10.23 TSF 和用户数据信息泄漏 ……29
10.24 信息泄漏融合 ……30
10.25 子集 TSF 测试 ……31
10.26 受限容错 ……31
11 安全保障要求的评估方法 ……32
11.1 概述 ……32
11.2 脆弱性分析(AVA_VAN) ……32
附录 A(资料性) 攻击潜力计算指南 ……34
A.1 通则 ……34
A.2 识别和实施攻击 ……34
A.3 计算攻击潜力的因素 ……35
A.4 攻击潜力的评分规则 ……38
附录 B(资料性) 侧信道分析 ……41
B.1 概述 ……41
B.2 单源信息泄漏测试方法 ……42
B.3 信息泄漏融合测试方法 ……43
B.4 用于脆弱性分析的侧信道分析方法 ……44
附录 C(资料性) 侧信道分析能力校准 ……45
C.1 概述 ……45
C.2 符号说明和分析条件 ……46
C.3 使用方法 ……46
附录 D(资料性) 故障注入分析 ……48
附录 E(资料性) 侵入式分析 ……49
参考文献 ……50

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。

本文件替代GB/T 22186—2016《信息安全技术　具有中央处理器的IC卡芯片安全技术要求》，与GB/T 22186—2016相比，除结构调整和编辑性改动外，主要技术变化如下：

a）　增加了“信息泄漏”威胁的描述（见6.2.2）；

b）　增加了扩展组件FPT_EMS.2（见第8章）；

c）　更改了安全保障要求表述（见第9章，2016年版的第8章）；

d）　增加了随机数生成、TSF和用户数据信息泄漏、信息泄漏融合等安全功能组件（见9.2.4、9.2.23、9.2.24）；

e）　增加了安全功能要求的测试方法（见第10章）；

f）　增加了安全保障要求的评估方法（见第11章）。

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。

本文件由全国网络安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：中国信息安全测评中心、北京理工大学、紫光同芯微电子有限公司、大唐微电子技术有限公司、南京理工大学、华为技术有限公司、北京中电华大电子设计有限责任公司、国民技术股份有限公司、北京智芯微电子科技有限公司、上海航芯电子科技股份有限公司、国家信息技术安全研究中心、北京银联金卡科技有限公司、吉林信息安全测评中心、深圳市纽创信安科技开发有限公司、兴唐通信科技有限公司、上海市信息安全测评认证中心、中国电子科技集团公司第十五研究所、郑州信大捷安信息技术股份有限公司、长扬科技（北京）股份有限公司、中通服咨询设计研究院有限公司、广州明森科技股份有限公司、中国电信股份有限公司、中国信息通信研究院、国网经济技术研究院有限公司、北京多思科技工业园股份有限公司。

本文件主要起草人：陈佳哲、王宇航、石竑松、王安、孙磊、王昊、黄小莉、杨静、魏伟、雷翻翻、张同、周永彬、王晓楠、陈波涛、刘戬、韩绪仓、邢益传、刘辉志、刘红明、李英的、李彦昭、刘占丰、闻明、王宗岳、陶文卿、蔡子凡、董晶晶、潘莹、张宝峰、杨永生、李贺鑫、饶华一、高宜文、李寒雨、王天宇、贾津、刘昱函、张靖奇、刘安女、谢蒂、赵华、刘为华、李岑、王小鹏、吴伟文、李红平、袁琦、郑学欣、刘铮、李亚威、彭乾、杨丹、陈玲、李海滨、陈守双、张茜歌、邹静、王州府。

本文件及其所代替文件的历次版本发布情况为：

——2008年首次发布为GB/T 22186—2008，2016年第一次修订；

——本次为第二次修订。

引　言

具有中央处理器的IC卡芯片是一类重要的基础性安全部件，可为应用安全提供信息存储和密码运算方面的安全保障。随着该类芯片应用范围的扩大和应用环境复杂性的增加，要求其具有更强的安全功能。

本文件以GB/T 18336.1规定的安全模型为基础，主要用于规范具有中央处理器的IC卡芯片的安全功能要求和安全保障要求，其中规范的EAL4+是在EAL4的基础上将AVA_VAN.3增强为AVA_VAN.4；EAL5+是在EAL5的基础上将ALC_DVS.1增强为ALC_DVS.2，AVA_VAN.4增强为AVA_VAN.5；EAL6+是在EAL6的基础上增加ALC_FLR.1。

网络安全技术　具有中央处理器的IC卡芯片安全规范

1　范围

本文件给出了具有中央处理器的IC卡芯片描述，规定了安全问题、安全目的、扩展组件、安全要求，描述了对应的安全功能要求的测试方法和安全保障要求的评估方法。

本文件适用于具有中央处理器的IC卡芯片产品的测试和评估活动，也用于指导该类产品的研制和开发。

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 18336.1　网络安全技术　信息技术安全评估准则　第1部分：简介和一般模型

GB/T 18336.2　网络安全技术　信息技术安全评估准则　第2部分：安全功能组件

GB/T 18336.3　网络安全技术　信息技术安全评估准则　第3部分：安全保障组件

GB/T 25069　信息安全技术　术语

GB/T 30270　网络安全技术　信息技术安全评估方法

GB/T 32915　信息安全技术　二元序列随机性检测方法

ISO/IEC 17825：2024　信息技术　安全技术　密码模块非侵入式攻击缓解技术测试方法（Information technology—Security techniques—Testing methods for the mitigation of non-invasive attack classes against cryptographic modules）

ISO/IEC 18033（所有部分）　信息安全　加密算法（Information security—Encryption algorithms）

3　术语和定义

GB/T 25069、GB/T 18336.1界定的以及下列术语和定义适用于本文件。

3.1

评估对象　target of evaluation；TOE

评估的主体，是软件、固件和/或硬件的集合。

注：本文件的TOE是指具有中央处理器的IC卡芯片，简称“IC卡芯片”。

[来源：GB/T 18336.1，3.53，有修改]

3.2

IC专用软件　IC dedicated software

由IC卡芯片设计者开发，并存在于IC卡集成电路中的专用软件。

注：通常在生产过程中用于测试，也用来提供额外的服务以便于硬件使用，其中专用测试软件的部分功能只限定在特定阶段使用。