ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 22186—2016
代替 GB/T 22186—2008

# 信息安全技术 具有中央处理器的IC卡芯片安全技术要求

**Information security techniques—
Security technical requirements for IC card chip with CPU**

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

# 目　　次

# 前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 22186—2008《信息安全技术　具有中央处理器的集成电路(IC)卡芯片安全技术要求(评估保证级 4 增强级)》。本标准与 GB/T 22186—2008 相比,主要变化如下:

——标准名称变更为《信息安全技术　具有中央处理器的 IC 卡芯片安全技术要求》;

——第 3 章对术语进行了更新描述;

——第 4 章重新描述了 IC 卡芯片的结构,并进行了更清晰的 TOE 范围定义;

——第 5 章对安全问题定义进行了整合和精简,共定义了 6 个威胁,2 项组织安全策略和 2 个假设;

——第 6 章根据新的安全问题定义更新了对 TOE 安全目的的描述;

——第 7 章描述了两个扩展族 FMT_LIM 和 FPT_TST,分别用于处理对 TOE 的受限可用性以及自检相关的安全功能要求,以便更合理的描述 IC 卡芯片的安全性;

——第 8 章对安全功能要求进行了调整,以细化新的安全目的描述,明确指出了 EAL4+、EAL5+和 EAL6+分别应满足的安全功能要求;并对安全保证要求进行了调整,增加了 EAL5+和 EAL6+要求的保障组件;

——第 9 章对新的安全问题定义与安全目的、安全目的与安全要求之间的对应关系基本原理进行了更新描述,并分析了组件之间的依赖关系。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国信息安全测评中心、北京多思科技工业园股份有限公司、清华大学、吉林信息安全测评中心。

本标准主要起草人:杨永生、张翀斌、石竑松、高金萍、王宇航、李贺鑫、贾炜、曹春春、沈敏锋、乌力吉、张向民、唐喜庆、闻明、昌彦伟、方欣。

本标准所代替标准的历次版本发布情况为:

——GB/T 22186—2008。

# 引　言

IC卡芯片应用范围的扩大和应用环境复杂性的增加，要求IC卡芯片具有更强的保护数据能力。

本标准的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。

# 信息安全技术
# 具有中央处理器的IC卡芯片安全
# 技术要求

## 1 范围

本标准规定了对具有中央处理器的集IC卡芯片达到EAL4＋、EAL5＋、EAL6＋所要求的安全功能要求及安全保障要求，涵盖了安全问题定义、安全目的、扩展组件定义、安全要求、基本原理等内容。

本标准适用于IC卡芯片产品的测试、评估和采购，也可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 18336（所有部分） 信息技术 安全技术 信息技术安全评估准则

GB/T 25069—2010 信息安全技术 术语

## 3 术语和定义、缩略语

### 3.1 术语和定义

GB/T 25069—2010和GB/T 18336.1界定的以及下列术语和定义适用于本文件。

3.1.1

**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。这些专用软件通常在生产过程中用于测试，也可以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。

3.1.2

**初始化数据 initialization data**

由IC卡芯片制造者定义，用于标识芯片以便追踪生产过程和生命周期阶段的数据，如IC卡芯片的唯一标识号。

3.1.3

**预个人化数据 pre-personalization data**

在IC卡芯片制造阶段由制造者写入非易失性存储器中的数据，以便后续生命周期阶段追溯IC卡芯片的制造过程。

3.1.4

**IC卡嵌入式软件 IC card embedded software**

存放在具有中央处理器的IC卡的非易失性存储器(例如ROM、EEPROM或Flash等)中，并在IC卡芯片内运行的软件。该软件用于管理芯片硬件资源和数据，通过芯片的通信接口与IC卡终端设备交换信息，以响应用户发起的数据加密、数据签名及鉴权认证等应用请求，实现对应用功能的支持。