

ICS 305.40  
L 80



# 中华人民共和国国家标准

GB/T 31507—2015

---

## 信息安全技术 智能卡通用安全检测指南

Information security technology—  
General testing guide for security of smart card

2015-05-15 发布

2016-01-01 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

中 华 人 民 共 和 国  
国 家 标 准  
信 息 安 全 技 术  
智 能 卡 通 用 安 全 检 测 指 南  
GB/T 31507—2015

\*

中 国 标 准 出 版 社 出 版 发 行  
北 京 市 朝 阳 区 和 平 里 西 街 甲 2 号 (100029)  
北 京 市 西 城 区 三 里 河 北 街 16 号 (100045)

网 址 : [www.gb168.cn](http://www.gb168.cn)

服 务 热 线 : 400-168-0010

010-68522006

2015 年 5 月 第 一 版

\*

书 号 : 155066 · 1-51176

版 权 专 有 侵 权 必 究

## 目 次

前言 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语、定义和缩略语 .....	1
4 智能卡安全检测总则 .....	3
4.1 受测件的一般模型 .....	3
4.2 检测主体和客体 .....	4
4.3 检测目的 .....	4
4.4 检测依据 .....	5
4.5 检测内容 .....	5
4.6 检测要素 .....	5
4.7 检测过程 .....	6
5 安全功能查证 .....	6
5.1 概述 .....	6
5.2 实施说明 .....	8
5.3 实施内容 .....	8
6 渗透性检测 .....	11
6.1 概述 .....	11
6.2 渗透性检测准备 .....	12
6.3 渗透性检测实施方案 .....	13
6.4 渗透性检测实施 .....	14
6.5 渗透性检测报告 .....	15
7 检测报告 .....	15
7.1 概述 .....	15
7.2 报告主要内容 .....	15
7.3 关于攻击场景的描述尺度 .....	15
附录 A (资料性附录) 智能卡安全功能集 .....	16
附录 B (资料性附录) 智能卡攻击方法 .....	20
附录 C (资料性附录) 智能卡安全检测框架 .....	23
附录 D (资料性附录) 主题检测大纲文件结构举例 .....	26
附录 E (资料性附录) 定制化服务的检测方案模板 .....	30
附录 F (资料性附录) 实验室准备与启动 .....	32
附录 G (规范性附录) 智能卡安全检测分级方法 .....	38
参考文献 .....	42

图 1	封闭结构的智能卡产品 .....	3
图 2	开放结构的智能卡产品 .....	3
图 3	智能卡芯片的基本结构 .....	4
图 4	检测要素 .....	5
图 5	检测过程 .....	6
图 6	安全功能查证:输入、过程和输出 .....	7
图 7	安全功能查证主要内容 .....	8
图 8	文档审查:输入、输出 .....	9
图 9	源代码检查:输入、输出 .....	9
图 10	独立性安全功能检测:输入、过程和输出 .....	10
图 11	渗透性检测:输入、方法、工具、技术和输出 .....	12
图 12	渗透性检测过程 .....	14
图 C.1	渗透性芯片层检测框架示例图 .....	25
图 F.1	准备与启动阶段的三个子阶段 .....	32
图 F.2	实验室准备:输入、准备过程和输出 .....	33
图 F.3	项目准备:输入、输出 .....	34
图 F.4	检测内容与边界 .....	35
表 C.1	检测用例模板 .....	24
表 D.1	MCC01-1 半侵入-芯片准备-1 .....	28

## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家信息技术安全研究中心、中国电子技术标准化研究院、国民技术股份有限公司、中国信息安全测评中心、中国金融电子化公司标准化中心。

本标准主要起草人:方进社、宫亚峰、隋忻、贾嘉、熊克琦、张正义、王欢、杜楠、陈星、高建、牟宁波、张翀斌、杨永生、李国俊、韩建国、田小雨、赵晓荣。

# 信息安全技术

## 智能卡通用安全检测指南

### 1 范围

本标准规定了智能卡类产品进行安全性检测的一般性过程和方法。

本标准适用于智能卡安全性检测评估和认证。

### 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 20276—2006 信息安全技术 智能卡嵌入式软件 安全技术要求(EAL4 增强级)

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)

CCDB-2008-04-001 智能卡的潜在应用攻击 (Application of Attack Potential to Smartcards V.2.5)

### 3 术语、定义和缩略语

#### 3.1 术语和定义

下列术语和定义适用于本文件。

##### 3.1.1

**智能卡 smart card**

具有中央处理器(CPU)的集成电路(IC)卡,是将一个具有中央处理器的集成电路芯片镶嵌于塑料基片中,并封装成卡的形式。

注:从数据传输方式上可分为接触式智能卡和非接触式智能卡。

##### 3.1.2

**智能卡产品 smart card production**

具有 CPU 集成电路芯片和芯片操作系统的智能卡,且包括非标准形态但同样具有 CPU 集成电路芯片和芯片操作系统的产品。

注:智能卡产品的标准形态和技术规格被 GB/T 14916—2006 和 GB/T 16649 系列国家标准以及 ISO/IEC 7816、ISO/IEC 14443 国际标准所规定;智能卡产品整体可作为复合性受测件。

##### 3.1.3

**独立安全功能检测 independent security functional testing**

由评估者(或其委托的具有资质的专业实验室)所独立进行,但要根据并参考开发者的功能检测文档和(或)利用开发者的检测资源,对智能卡安全功能集合的子集(参见附录 A)和检测文档抽样进行的安全功能检测。