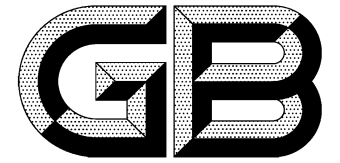


参 考 文 献

- [1] GB/T 14916—2006 识别卡物理特征
- [2] GB/T 16649 识别卡带触点的集成电路卡
- [3] YD/T 1625—2007 电信智能卡安全技术要求
- [4] ISO/IEC 7816 Identification cards—Intergrated circuit(s) cards
- [5] ISO/IEC 10536-2;1995 Identification cards—Contactless integrated circuit (s) cards—Part 2; Dimensions and location of coupling areas.
- [6] ISO/IEC 14443 Identification cards—Contactless integrated circuit cards—Proximity cards.
- [7] ISO/IEC 17025-2005-5-15 General requirements for the competence of testing and calibration laboratories.
- [8] ISO/IEC 17825;2012 Information technolgy—Security technique—Testing methods for the mtigation of non-invasive attack classes against cryptographic modules.
- [9] ISO/IEC 19790;2012 Information technology—security requirements for cryptographic modules.
- [10] CCDB-2007-09-001 Composite product evaluation for Smartcards and similar devices V1.0
- [11] CCDB-2007-09-002 ETR template for composite evaluation of Smart Cards and similar devices V1.0
- [12] CCMB-2007-09-004 Common Methodology for Information Technology Security EvaluationV3.1.
- [13] CCDB-2008-04-001 Application of Attack Potential to Smartcards V.2.5
- [14] CCDB-2009-03-003 Requirements to perform Integrated Circuit Evaluations
- [15] CCDB-2010-03-001 CC support Document Guidance—Smartcard Evaluation—February 2010 Version 2.0
- [16] CCDB-2012-04-004 Security Architecture requirements(ADV_ARC) for smart cards and similardevices—Appendix 1
- [17] BSI-CC-PP-0035-2007 Security IC Platform Protection Profile V1.0
- [18] Visa Chip Security Program—Security Testing Process V1.0
- [19] Joint Interpretation Library—Application of Attack Potential to Smatcard-V.2.7. February 2009
- [20] Visa Chip Security Program—Security Testing Process V2.0 2010-10

GB/T 31507—2015



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



GB/T 31507—2015

版权专有 侵权必究

*

书号:155066·1-51176

定价: 42.00 元

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

的 COS 检测认证；

智能卡的应用系统运营商或集成商挑选具有适应自己应用系统安全需求的芯片层某级别安全证书和 COS 层某安全级别证书的智能卡产品入围，并可进行相应的应用层安全级检测认证。

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.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 3 字数 83 千字
2015 年 5 月第一版 2015 年 5 月第一次印刷

*

书号: 155066·1-51176 定价 42.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107

——检测项目:参见附录 A 中关于芯片防止敏感信息泄漏的安全功能检测、参见附录 B 中 B.3 介绍的非侵入攻击。

——对等级别:GB/T 22186 对智能卡芯片的安全技术要求。

f) A2(芯片半侵入安全级):

——抵抗力指标:该级别受测件能抵御攻击者的各种半侵入攻击。

——检测项目:参见附录 A 中相关的安全功能检测、参见附录 B 中 B.2 介绍的各类半侵入攻击。

——对应级别:暂无。

g) A3(芯片侵入安全级):

——抵抗力指标:该级别受测件能抵御攻击者的各种侵入攻击。

——检测项目:参见附录 A 中相关的安全功能检测、参见附录 B 中 B.1 介绍的各类侵入攻击。

——对应级别:A1+A2+A3 的渗透性检测项目等同于国际 CC 组织和 EMVCO 组织认可的,满足脆弱性要求(组件 AVA_VLA.5)的智能卡芯片安全评估保障级 EAL4+或 EAL5+水平。

G.3 智能卡安全分级检测框架应用原则

G.3.1 公共服务

智能卡安全分级检测框架为整个智能卡产业链和应用提供服务。

G.3.2 适度检测

避免过度检测,节约智能卡产业链、应用链在安全性检测环节花费的成本和时间。

G.3.3 受测方选择

受测方根据自身在产业链的位置和需求,灵活选择某层面中某级别、多级别或多层面多级别的检测。

G.3.4 检测方定位

检测机构根据自身能力定位,发展并在获得相应能力认证后向社会提供三个层面、七个级别中某些或所有级别的检测服务。

G.4 检测评估认证体系

智能卡安全分级检测框架应用的理想环境是作为一个子体系在国家范围的智能卡安全检测评估认证体系下运行。这个体系由一个认证机构、几个专业委员会和若干个可提供不同级别检测评估服务的检测机构所构成。

检测机构需通过认证机构和专业委员会的测评、审核得到某级别或某几个级别的检测评估资质;

认证机构还负责审核、认证检测机构的检测报告,为合格的受测件颁发安全级别证书;

专业委员会则对检测认证实体的运行进行监督、指导,必要时也参与某些事物的审核。

理想的安全检测评估认证体系应导致产业链产生如下局面:

芯片商在产品投放市场之际根据自己的目标市场选择分级检测框架芯片层的某(几)个级别进行检测认证;

卡商、COS 商亦根据自己的目标市场选择符合该级别证书的芯片装载自己的 COS,并进行某级别

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