ICS 35.240.15
L 64

中华人民共和国国家标准

GB/T 16649.8—2002/ISO/IEC 7816-8:1999

识别卡　带触点的集成电路卡
第8部分:与安全相关的行业间命令

Identification cards—Intergrated circuit(s) cards with contacts—Part 8:Security related interindustry commands

(ISO/IEC 7816-8:1999,IDT)

2002-12-04 发布　　2003-05-01 实施

中华人民共和国
国家质量监督检验检疫总局　发布

目　　次

前　言

GB/T 16649《识别卡　带触点的集成电路卡》分为十个部分：

—— 第1部分：物理特性；
—— 第2部分：触点的尺寸和位置；
—— 第3部分：电信号和传输协议；
—— 第4部分：行业间交换用命令；
—— 第5部分：应用标识符的国家编号体系和注册规程；
—— 第6部分：行业间数据元；
—— 第7部分：用于结构化卡查询语言(SCQL)的行业间命令；
—— 第8部分：与安全相关的行业间命令；
—— 第9部分：附加的行业间命令和安全属性；
—— 第10部分：同步卡的电信号和复位应答。

本部分为GB/T 16649的第8部分。

本部分等同采用国际标准ISO/IEC 7816-8:1999《识别卡　带触点的集成电路卡　第8部分：与安全相关的行业间命令》。

为便于使用，对于ISO/IEC 7816-8:1999，本部分还做了下列编辑性修改：

a) “ISO/IEC 7816的本部分”改为“本部分”；

b) 删除ISO/IEC 7816-8:1999的前言和介绍。

本部分的附录A、附录B是资料性的附录。

本部分由中华人民共和国信息产业部提出。

本部分由中国电子技术标准化研究所归口。

本部分起草单位：中国电子技术标准化研究所。

本部分主要起草人：金倩、冯敬、蔡怀忠。

识别卡　带触点的集成电路卡
第8部分:与安全相关的行业间命令

1　范围

GB/T 16649的本部分规定了:

—— 卡中使用的安全协议;

—— 安全报文交换扩展;

—— 卡的安全功能/服务上的安全机制的映射,包括卡内安全机制的描述;

—— 安全支持的数据元;

—— 在卡上实现的算法的使用(算法本身并不详细描述);

—— 证书的使用;

—— 与安全相关的命令。

本部分没有涵盖卡内和/或外界的内部实现。

密码机制的选择和使用条件可能影响卡的输出。算法和协议的适宜性的评价在本部分的范围之外。

并不强制卡支持本部分描述的所有命令或支持命令的所有选项。

2　规范性引用文件

下列文件中的条款通过GB/T 16649的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB 15843.2　信息技术　安全技术　实体鉴别　第2部分:用对称加密算法的机制(GB 15843.2—1997,idt ISO/IEC 9798-2:1994)

GB/T 15843.3　信息技术　安全技术　实体鉴别　第3部分:用非对称签名技术的机制(GB/T 15843.3—1998,idt ISO/IEC 9798-3:1997)

GB 15851　信息技术　安全技术　带消息恢复的数字签名方案(GB 15851—1995,idt ISO/IEC 9796:1991)

GB/T 16649.3　识别卡　带触点的集成电路卡　第3部分:电信号和传输协议(GB/T 16649.3—1996,idt ISO/IEC 7816-3:1989)

GB/T 16649.6　识别卡　带触点的集成电路卡　第6部分:行业间数据元(GB/T 16649.6—2001,idt ISO/IEC 7816-6:1996)

ISO/IEC 7816-4　信息技术　识别卡　带触点的集成电路卡　第4部分:行业间交换用命令

ISO/IEC 7816-4/补篇1　信息技术　识别卡　带触点的集成电路卡　第4部分:行业间交换用命令　补篇1:APDU报文结构上的安全报文交换的影响

ISO/IEC 9979　数据密码技术　密码算法登记规程

3　术语和定义

下列定义适用于GB/T 16649的本部分。