ICS 35.240.15
L 64

中华人民共和国国家标准

GB/T 16649.15—2010/ISO/IEC 7816-15:2004

识别卡　集成电路卡
第15部分:密码信息应用

Identification cards—Integrated circuit cards—
Part 15:Cryptographic information application

(ISO/IEC 7816-15:2004,IDT)

2010-12-01 发布　　2011-04-01 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

GB/T 16649 在总标题《识别卡　集成电路卡》下目前由下述部分构成：

——第 1 部分：带触点的卡　物理特性；

——第 2 部分：带触点的卡　触点的尺寸和位置；

——第 3 部分：带触点的卡　电信号和传输协议；

——第 4 部分：用于交换的结构、安全和命令；

——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：用于卡管理的命令；

——第 10 部分：带触点的卡　同步卡的电信号和复位应答；

——第 11 部分：通过生物识别方法的个人验证(制定中)；

——第 12 部分：带触点的卡　USB 电气接口和操作规程；

——第 13 部分：在多应用环境中用于应用管理的命令(制定中)；

——第 15 部分：密码信息应用。

本部分为 GB/T 16649 的第 15 部分。

本部分等同采用国际标准 ISO/IEC 7816-15:2004《识别卡　集成电路卡　第 15 部分：密码信息应用》(英文版)。

为便于使用，本部分作了下列编辑性修改：

a)　删除国际标准前言；

b)　将“本文件”改为“本部分”。

本部分的附录 A 是规范性附录，附录 B、附录 C 和附录 D 是资料性附录。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分起草单位：中国电子技术标准化研究所、北京华大智宝电子系统有限公司。

本部分主要起草人：金倩、冯敬、李金良、耿力、袁理、王文峰、乔申杰。

引　言

GB/T 16649 是规定集成电路卡参数和交换中集成电路卡使用的国家标准。

具有密码功能的集成电路卡可以用于信息系统使用者的安全识别，以及其他核心安全服务，例如通过数字签名达成不可否认性、发行用于保密的编码密钥。GB/T 16649 的本部分的目的是基于可用的标准对这些服务提供一种构架。一个主要目的是提供解决方案，其可用于为具有若干可兼容卡的发行者的大型系统提供交换。该系统足够灵活以用于多种不同环境，同时还保持了对交互性的要求。

已经提供了多种数据结构来管理私有密钥和关键数据，以支持公共密钥证书基础设施、灵活管理用户和实体鉴别。

GB/T 16649 的本部分是基于 PKCS ＃15 v1.1(见参考文献)。这些文件之间的关系如下：

——两个文件的共同核心部分相同；

——删除了 PKCS ＃15 中不涉及 IC 卡的内容；

——GB/T 16649 的本部分包括了满足特定 IC 卡要求的增加部分。

识别卡　集成电路卡
第15部分:密码信息应用

1　范围

GB/T 16649的本部分规定了卡的一种应用。该应用包含密码功能的信息。本部分定义了用于密码信息的通用语法和格式,以及在适当时共享该信息的机制。

本部分旨在:

——便于运行于不同平台的各部分间的交互性(平台无关);

——使外部应用能利用多个制造商的产品和部分(厂商无关);

——使无需重写应用层的软件也能使用更先进的技术(应用无关);

——在维持现有的、相关的标准一致性的同时,进行必要的和可行的扩展。

本部分支持下列功能:

——在卡中存储密码信息的多个实例;

——使用密码信息;

——检索密码信息,这一功能的关键因素在于"目录文件"的概念,它提供了卡上对象和这些对象的实际格式之间的一个间接层;

——适当时,用GB/T 16649的其他部分中定义的数据对象来交叉引用密码信息;

——不同的鉴别机制;

——多个密码算法(它们的适用性不属于GB/T 16649的本部分的范围)。

本部分不包括卡内和/或外部的内部实现。不强制要求执行本部分的所有选项。

在本部分主要部分和附录A的模块中对ASN.1的定义有差异的情况下,以附录A为准。

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/T 13000　信息技术　通用多八位编码字符集(UCS)(ISO/IEC 10646:2003,IDT)

GB/T 16262(所有部分)　信息技术　抽象语法记法1(ASN.1)(idt ISO/IEC 8824)

GB/T 16263.1　信息技术　ASN.1编码规则　第1部分:基本编码规则(BER)、规范编码规则(CER)和非典型编码规则(DER)的规范(GB/T 16263.1—2006,ISO/IEC 8825-1:2002,IDT)

GB/T 16264.8　信息技术　开放系统互连　目录　第8部分:公钥和属性证书框架(GB/T 16264.8—2005,ISO/IEC 9594-8:2001,IDT)

GB/T 16649(所有部分)　识别卡　集成电路卡(ISO/IEC 7816,IDT)

GB/T 21078.1　银行业务　个人识别码的管理与安全　第1部分:ATM和POS系统中联机PIN处理的基本原则和要求(GB/T 21078.1—2007,ISO/IEC 9564-1:2002,MOD)

ISO/IEC 7816-11　识别卡　集成电路卡　第11部分:通过生物识别方法的身份验证

3　术语和定义

下列术语和定义适用于本部分。