ICS 35.240.15
A 11

中华人民共和国国家标准

GB/T 16790.7—2006/ISO 10202-7:1998

金融交易卡　使用集成电路卡的金融交易系统的安全体系　第7部分:密钥管理

Financial transaction cards—Security architecture of financial transaction systems using integrated circuit cards—Part 7:Key management

(ISO 10202-7:1998,IDT)

2006-09-18 发布　　2007-03-01 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

GB/T 16790《金融交易卡　使用集成电路卡的金融交易系统的安全体系》包括以下8个部分：

——第1部分：卡生命周期

——第2部分：交易过程

——第3部分：密钥关系

——第4部分：安全应用模块

——第5部分：算法应用

——第6部分：持卡人身份验证

——第7部分：密钥管理

——第8部分：通用原则及概要

本部分为GB/T 16790第7部分。

本部分等同采用ISO 10202-7:1998《金融交易卡　使用集成电路卡的金融交易系统的安全体系　第7部分：密钥管理》(英文版)。

为便于使用，本部分删除了ISO前言。

本部分的附录A到附录E均为资料性附录。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会归口管理。

本部分负责起草单位：中国金融电子化公司。

本部分参加起草单位：中国人民银行、中国银行、中国建设银行、中国光大银行、中国银联股份有限公司、北京启明星辰公司。

本部分主要起草人：谭国安、杨竑、陆书春、李曙光、刘运、杜宁、刘志军、张艳、张德栋、戴宏、张晓东、马云、李红建、王威、王沁、孙卫东、李春欢。

本部分为首次制定。

金融交易卡　使用集成电路卡的金融交易系统的安全体系　第7部分:密钥管理

1　范围

本部分规定了使用集成电路卡的金融交易系统的密钥管理要求。它对集成电路卡环境中在卡生命周期内和交易处理过程中所用密钥的安全管理的程序和过程作出了定义。本部分描述了对称与非对称密钥管理方案,并规定了最低密钥管理要求。

密钥管理是这样一种过程,在这过程中,密钥被用在授权的通信各方之间,这些密钥在被销毁之前一直受安全程序保护。被加密的数据的安全取决于对密钥的泄露以及未经授权的密钥的更改、替换、插入或删除的防范。因此,密钥管理与密钥生成、存储、分发、使用及销毁程序有关。同样,通过对这些程序的规范,可以制定审计跟踪的条例。

本部分适用于联机和脱机交易处理环境中的IC卡和SAM之间,以及联机(端对端)环境下的IC卡和SAM或主机安全模块之间。

2　规范性引用文件

下列文件中的条款通过GB/T 16790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 15694.1—1995　识别卡　发卡者标识　第1部分:编号系统(idt ISO/IEC 7812-1:1993)

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

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

GB/T 16790.1—1997　金融交易卡　使用集成电路卡的金融交易系统的安全结构　第1部分:卡的生命周期(idt ISO 10202-1:1991)

GB/T 16791.1—1997　金融交易卡　集成电路卡与卡接受设备之间的报文　第1部分:概念与结构(idt ISO 9992-1:1990)

GB/T 16790.5—2006　金融交易卡　使用集成电路卡的金融交易系统的安全体系　第5部分:算法应用(ISO 10202-5:1998,IDT)

GB/T 16790.6—2006　金融交易卡　使用集成电路卡的金融交易系统的安全体系　第6部分:持卡人身份确认(ISO 10202-6:1994,IDT)

ISO/IEC 7812-2　识别卡　发卡者标识　第2部分:申请和注册流程

ISO 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 7816-5　识别卡　带触点的集成电路卡　第5部分　应用标识符的编号系统和注册程序

ISO 8732　银行业务　密钥管理(批发)

ISO 8908　银行业和相关金融服务业　词汇和数据元

ISO 9992-2　金融交易卡　集成电路卡及其接收装置间的报文　第2部分:功能、报文(指令和响应)、数据元和结构

ISO 10202-2　金融交易卡　使用集成电路卡的金融交易系统的安全体系　第2部分:交易过程