ICS 35.240.15
A 11

中华人民共和国国家标准

GB/T 16790.5—2006/ISO 10202-5:1998

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5部分:算法应用

Financial transaction cards—Security architecture of financial transaction systems using integrated circuit cards—Part 5:Use of algorithms

(ISO 10202-5:1998,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》分成以下 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 的第 5 部分。

本部分等同采用 ISO 10202-5:1998《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 5 部分：算法应用》(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 H 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。

引　言

《金融交易卡　使用集成电路卡的金融交易系统的安全体系》分成以下 8 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

本部分描述了可供使用的密码过程，可用来实现第 2、4 和 6 部分定义的需要密码算法的安全功能。

GB/T 16790 可采用对称或非对称算法执行所有安全功能。GB/T 16790 未涉及零点知识技术，该技术可能在以后阶段并入。

参与给定密码过程的每一节点应能执行所要求的密码功能。

执行安全功能所必需的密码过程通过选项进行说明。在每个密码过程中，为每个算法类型规定了一单独选项。还为需要额外通信步骤的密码过程的每个变量规定了一单独选项。

第 5 章将安全功能映射到可用来实现这些安全功能的密码过程。

第 6 章规定了密码过程细节，本部分不是实施规格说明书，但它确实指出了为确保按照要求的安全程序完成密码过程双方节点所需的那些数据元素。

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

1　范围

本部分适用于密码交换,其中至少一个节点是IC卡(集成电路卡)或SAM,其他系统节点之间的交换不属于本部分的范围。

任何安全功能的规定均是可选的,其使用取决于系统要求。需要采用的功能应以本部分说明的方法实行。

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 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 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 16790.6　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:持卡人身份验证(GB/T 16790.6—2006,ISO 10202-6:1994,IDT)

GB/T 16790.7　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(GB/T 16790.7—2006,ISO 10202-7,1998,IDT)

ISO 4909　银行卡　第3磁道数据内容

ISO 9564-1　银行业务　个人识别码管理和安全　第1部分:PIN保护原理和技术

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

ISO 10202-3　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3部分:密钥关系

ISO 10202-4　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4部分:安全应用模块

ISO 10202-8　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8部分:通用原则及概要

3　术语和定义

下列术语和定义适用于本部分。

3.1

非对称算法　asymmetric algorithm

一种加密密钥和解密密钥不同的算法,并且对于该算法不能由一个密钥计算推导出另一个密钥。

3.2

证书　certificate

见3.24“公钥证书”。