ICS 35.240.15
A 11

中华人民共和国国家标准

GB/T 16790.6—2006/ISO 10202-6:1994

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

Financial transaction cards—Security architecture of financial transaction systems using integrated circuit cards—Part 6:Cardholder verification

(ISO 10202-6:1994,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

中 华 人 民 共 和 国
国 家 标 准
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
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
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 0.75 字数 11千字
2007年3月第一版 2007年3月第一次印刷
*
书号:155066·1-29023 定价 14.00 元

GB/T 16790.6-2006

GB/T 16790.6—2006/ISO 10202-6:1994

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—2006第6部分。

本部分等同采用ISO 10202-6:1994《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》(英文版)。

为便于使用，本部分做了下列编辑性修改：

a) 删除ISO前言；

b) 第2章中，原标准漏掉了“ISO 10202-1　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1部分：卡生命周期”，现补上等同采用的GB/T 16790.1—1997。

本部分的附录A为规范性附录，附录B、附录C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。


STANDARDS PRESS OF CHINA

目　次

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

1　范围

本部分规定了当离散的持卡人身份识别值(CIV),如个人识别码(PIN),在集成电路卡(IC卡)(可以含有或不含有磁条)中使用时,对持卡人确认的安全要求。持卡人确认的目的是确定卡的出示者是卡的持有人。ISO 9564-1适用于本部分,除本部分中涉及使用IC卡特定方面的条款外。

本部分的规定不用来防止伪造的卡接收装置(CADs)的使用。

本部分适用于任何负责对CIV和IC卡连用而实施安全程序的组织。

本部分涉及关于持卡人持有的实物(如一张IC卡卡片)和持卡人了解的信息(即一个CIV,诸如PIN)相匹配的安全问题。同时也说明了IC卡和CAD相关的安全要求,其中IC卡和CAD可能只有一个集成电路(IC)或者同时包含磁条和IC功能。这里强调的是只有IC的系统。

注1:术语IC指嵌入IC卡中的IC。持卡人身份验证可在通用数据文件(CDF)或应用数据文件(ADF)级上执行。

注2:术语"发卡行"和"应用供应商"包括其各自的代理。

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 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 16790.5　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(GB/T 16790.5—2006,ISO 10202-5:1998,IDT)

ISO 9564-1:1991　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

3　术语和定义

GB/T 16790.1—1997中给出的定义和下列定义适用于本部分。

3.1

生物特征验证　biometric verification

一种对被观察的生物特征和参考值相比较的持卡人确认形式。

3.2

持卡人　cardholder

和主帐户关联并从受理卡片的机构请求交易的客户。

3.3

持卡人身份识别值　CIV,Cardholder Identification Value

用来确认持卡人身份的值。

注3:持卡人了解的离散的CIV(即PIN或口令)。生物特征验证的CIV是被观察到的持卡人生物特征的表现。

3.4

单一 IC 系统　IC-only system

仅依赖 IC 技术和相应的接口设备的卡系统。

3.5

混合 CAD　mixed CAD

接收 IC 卡和磁条卡的 CAD。

3.6

混合系统　mixed system

接收 IC 和磁条卡组合技术的系统。

3.7

口令　password

由唯一表示的字母和数字组成的离散的 CIV。

3.8

参考 CIV　reference CIV

用来验证交易 CIV 的 CIV。

3.9

交易 CIV　transaction CIV

交易中由卡出示人提供的 CIV。

4　离散值方法

本章规定了同时使用离散的 CIV 和 IC 卡的最低安全要求。这些离散值可以是如 ISO 9564-1:1991 中定义的 PIN,也可以是口令(参见附录 B)。

4.1　一般安全原则

本部分提供的安全程序应受以下一般原则制约:

a)　ISO 9564-1:1991 中规定的 PIN 管理的基本原则。

b)　对通用数据文件(CDF)级的持卡人确认的要求应由发卡行规定,而在应用数据文件(ADF)级上,应由应用供应商规定。

c)　离散参考 CIV 应以可控制的方式安全地装载到 IC 中。

d)　离散参考 CIV 应以能防止外部读操作的方式存储到 IC 中。

e)　如果有 CDF 级 CIV,应由发卡行控制离散参考 CIV 的装载、重载和更改过程。

f)　CDF 级 CIV 的验证过程宜适用于卡中的任何应用程序。

g)　如果有 ADF 级的 CIV,应由应用供应商控制离散参考 CIV 的装载、重载和更改过程。

h)　IC 卡系统的持卡人确认过程应以不危害该系统或任何其他 IC 卡或磁条卡系统的安全的方式执行。

i)　IC 卡系统的持卡人确认过程应以一个 IC 的泄露不会导致任何其他 IC 泄露的方式执行。

j)　离散 CIV 的校验过程应在 IC 中进行。

k)　如果离散交易 CIV 已被校验,那么 IC 应能防止对离散参考 CIV 的穷举搜索攻击。

4.2　个人识别码(PIN)

如果 PIN 被用在采用 IC 卡技术的系统中,则 ISO 9564-1:1991 的要求应适用并受本部分条款的约束。

4.2.1　PIN 的装载与重载

初始参考 PIN 装载或参考 PIN 重载到 IC(例如,更换遗忘的 PIN)应在物理安全环境中实施,或使用 GB/T 16790 中规定的适当密钥进行密码保护。

4.2.2 PIN 更改

对 CDF 的参考 PIN 或 ADF 的参考 PIN 的更改可由持卡人来实施，但是应采用分别由发卡行或应用供应商提供的并包括当前 PIN 确认的程序。

4.2.3 PIN 存储

存储在 IC 中的参考 PIN 应能防止来自外部的读操作。如果 IC 卡满足了以下条件，IC 中的参考 PIN 可以作为明文存储：

a) 对存储在 IC 中的参考 PIN 的非授权确认应导致 IC 的破坏，以至该 IC 不能重新提供服务。而且，IC 中已使用或将使用的参考 PIN 的确认要求使用专业设备和技术，而这些设备和技术通常情况下不可利用。

b) 对 IC 卡的侵入不应泄露足够的信息以推断出任何其他 IC 卡的参考 PIN。

在单一 IC 系统中，PIN 确认应在 IC 中进行。而且参考 PIN 不应由发卡行或应用供应商来保留或重新生成并应只能存储在 IC 中。

4.2.4 PIN 传输

IC 卡交易 PIN 应被传输到 IC 且 IC 卡参考 PIN 不应离开 IC。

在混合的 CAD 中，交易 PIN 在离开 PIN 键盘时，应对其进行密码保护。但如果 IC 读卡机和 PIN 键盘之间的连接是物理安全的，则 PIN 可以用明文形式传输到 IC 中(见 GB/T 16790.5 有关密码保护的细节。)

注 4：更可取的方案是 PIN 键盘和 IC 卡读卡机实现物理集成。

在单一 IC 系统中以及在 IC 卡中不包含使用相同 PIN 的磁条的情况下，PIN 键盘和 IC 之间 PIN 的密码安全传输不是强制性的。

4.2.5 PIN 确认

交易 PIN 应在 IC 中与参考 PIN 进行校验。来自 IC 的关于 PIN 确认的输出的响应不必密码保护(见 ISO 10202-2)。

IC 卡应通过限制对 PIN 的连续尝试次数来防止对参考 PIN 的穷举搜索攻击。发卡行或应用供应商有权决定 IC 在 CDF 级或 ADF 级所允许的 PIN 验证连续失败的次数和随后所采取的处理。

直到 IC 已经记录或可以保证它能记录确认结果时，IC 才应给出持卡确认结果的指示。

附 录 A
（规范性附录）
CIV 表 示

当CIV是一组以明文表示的4到12位的数字集时，在IC卡中它应以ISO 9564-1:1991中8.3.1.1（明文域）中定义的PIN分组格式表示，并且控制域C应为2（即0010）。

附 录 B
（资料性附录）
口令和生物特征验证法

B.1 口令

IC卡使用典型的6到12个字符的口令是可行的。如果在国际交换中IC卡口令的使用成为可行的建议，那么可以考虑将其并入到本部分。

B.2 生物特征验证法

IC卡允许使用生物特征验证法。

附 录 C
（资料性附录）
参 考 文 献

[1] 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）

[2] 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）

[3] GB/T 17552—1998 识别卡 金融交易卡（idt ISO/IEC 7813:1995）

[4] GB/T 16790.7—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7部分：密钥管理（ISO 10202-7:1998，IDT）

[5] ISO 10202-4 Financial transaction cards—Security architecture of financial transaction systems using integrated cards—Part 4:Secure application modules