



# 中华人民共和国国家标准

GB/T 21078.2—2011

---

## 银行业务 个人识别码的管理与安全 第 2 部分:ATM 和 POS 系统中脱机 PIN 处理的要求

Banking—Personal identification number management and security—  
Part 2: Requirements for offline PIN handling in ATM and POS systems

(ISO 9564-3:2003,MOD)

2011-12-30 发布

2012-02-01 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 .....	III
引言 .....	IV
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 在 PIN 输入设备(PED)和 IC 卡读卡器之间传输时的 PIN 保护 .....	2
5 物理安全 .....	2
6 PIN BLOCK 格式 .....	3
6.1 概述 .....	3
6.2 格式 2 的 PIN BLOCK .....	3
参考文献 .....	4

## 前 言

GB/T 21078《银行业务 个人识别码的管理和安全》分为以下 3 个部分：

——第 1 部分：ATM 和 POS 系统中联机 PIN 处理的基本原则和要求；

——第 2 部分：ATM 和 POS 系统中脱机 PIN 处理的要求；

——第 3 部分：开放网络中 PIN 处理指南。

本部分为 GB/T 21078 的第 2 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分修改采用 ISO 9564-3:2003《银行业务 个人识别码的管理与安全 第 3 部分：ATM 和 POS 系统中脱机 PIN 处理的要求》(英文版)。

本部分与 ISO 9564-3:2003 的技术性差异为：根据国内的实际应用情况，将 6.1 中“应为每笔交易使用惟一密钥”的要求扩展为“应为每笔交易使用惟一密钥或者定期更换加密密钥”。有关技术性差异已编入正文并在其涉及的条款的页边空白处用垂直单线标识。

本部分删除了 ISO 前言。

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(SAC/TC 180)归口。

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：中国工商银行、中国银行、交通银行、中国人民银行兴化市中心支行、中国银联股份有限公司。

本部分主要起草人：王平娃、陆书春、李曙光、贾树辉、赵志兰、仲志晖、王治纲、冉平、周燕媚、张凡、贾静、刘运、景芸、张艳。

## 引 言

内置集成电路的金融交易卡在技术上已可使用 IC 卡进行脱机的 PIN 验证。目前发卡方可以选择脱机或者联机方式进行 PIN 验证。GB/T 21078 的本部分为脱机处理 PIN 提出了明确的要求。

脱机 PIN 验证不要求把持卡人的 PIN 发送到发卡方主机验证,因此通过网络进行 PIN 保护的相关安全要求不适用。但是,尽管 PIN 可以脱机验证,许多通用的 PIN 保护原则和技术仍然适用。GB/T 21078 的本部分给出了对脱机类 PIN 处理的具体要求,除非明确说明,GB/T 21078.1—2007 给出的 PIN 管理的基本原则适用于本部分。

ISO 10202 的第 6 部分定义了使用 IC 卡进行持卡人验证的安全要求。应当指出,ISO 10202 定义了对 IC 卡自身的要求,而非对收单方 IC 卡接受设备的要求,因此可以看成是对 GB/T 21078 的补充。

# 银行业务 个人识别码的管理与安全

## 第 2 部分:ATM 和 POS 系统中脱机 PIN 处理的要求

### 1 范围

本部分规定了脱机 PIN 处理的最低安全要求和在脱机环境下交换 PIN 数据的标准方法。

本部分适用于要求脱机 PIN 验证的卡发起的金融交易,也适用于那些负责在 ATM 和收单方布放的 POS 终端中实施 PIN 管理和保护技术的机构。

本部分不适用于下列情况:

- a) 联机 PIN 环境下的 PIN 管理和安全,GB/T 21078.1 包含该项内容;
- b) 核准的 PIN 加密算法;
- c) 在开放网络环境下使用 PIN,GB/T 21078.3 包含该项内容;
- d) 防止用户或者发卡方及其代理商的授权雇员丢失或故意误用而采取的 PIN 保护;
- e) 非 PIN 交易数据的私密性;
- f) 保护交易报文,防止修改或替换,例如联机授权响应;
- g) 防止 PIN 或交易重放;
- h) 特定的密钥管理技术;
- i) IC 卡是否接受加密 PIN 的决策;
- j) 非接触式 IC 卡。

GB/T 21078.1—2007 的第 4 章描述的 PIN 管理的基本原则也适用于本部分。

与多应用 IC 卡相关的要求由发卡方负责,不包括在本部分内。

本部分适用于 IC 卡技术,但不局限于 IC 卡技术。

### 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 16649(所有部分) 识别卡 带触点的集成电路卡(ISO/IEC 7816-1:1998,MOD)

GB/T 21078.1—2007 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(ISO 9564-1:2002,MOD)

EMV2000 支付系统的集成电路卡规范 第 2 册:安全和密钥管理(4.0 版) 2000.12(EMV2000, Integrated Circuit Card Specification for Payment Systems,Book 2—Security and Key Management,Version 4.0,December,2000)

### 3 术语和定义

GB/T 21078.1—2007 界定的以及下列术语和定义适用于本文件。

#### 3.1

**集成电路(IC) integrated circuit (IC)**

按照 GB/T 16649 中的规定,(典型的)嵌入在 IC 卡中的微处理器。