ICS 35.240.40
A 11

中华人民共和国国家标准

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

Banking—Personal Identification Number management and security—Part 1：Basic principles and requirements for online PIN handling in ATM and POS systems

(ISO 9564-1：2002，MOD)

2007-09-05 发布　　2007-12-01 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 21078《银行业务　个人识别码的管理与安全》分为三个部分：

——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1部分。

本部分修改采用ISO 9564-1：2002《银行业务　个人识别码的管理和安全　第1部分：ATM和POS系统中联机PIN处理的基本原则和要求》(英文版)。

为便于使用，本部分删除了ISO前言。

针对我国金融业务密码算法的实际使用情况，删除了原国际标准第9章　加密算法的核准程序。

本部分的附录A到附录G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。

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、中国银联股份有限公司、中国光大银行、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。

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

1　范围

本部分规定了为有效的PIN管理提供所需要的最小安全措施的基本原则和技术。这些措施适用于那些负责实施PIN管理和保护技术的机构。

本部分也规定了联机环境中金融交易卡所应用的PIN保护技术和PIN数据交换的标准方法。这些技术适用于那些负责实施ATM和POS终端中PIN管理和保护技术的机构。

本部分的条款没有包括:

a)　脱机PIN环境中的PIN管理和安全,ISO 9564-3:2003中包含该项内容;

b)　电子商务环境中的PIN管理和安全,ISO 9564后续部分将会包含该项内容;

c)　防止顾客或者发卡行授权的员工丢失或者故意误用PIN;

d)　非PIN交易数据的保密性;

e)　交易报文的保护,防止修改或替换。如对PIN验证的授权响应;

f)　防止PIN或交易的重放;

g)　特定密钥管理技术。

2　规范性引用文件

下列文件中的条款通过GB/T 21078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标准。

GB/T 15694.1—1995　识别卡　发卡者标识　第1部分:编号体系(idt ISO/IEC 7812-1:1993)

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

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

ISO/IEC 7812-2　识别卡　发卡者标识　第2部分:申请和注册规程

ISO 9564-2:1991　银行业务　个人识别码管理和安全　第2部分:核准的PIN加密算法

ISO 9564-3:2003　银行业务　个人识别码管理和安全　第3部分:ATM和POS系统中脱机PIN处理要求

ISO 11568(所有部分)　银行业务　密钥管理(零售)

ISO 13491(所有部分)　银行业务　安全加密设备(零售)

3　术语和定义

下列术语和定义适用于GB/T 21078的本部分。

3.1

收单机构　acquirer

从受卡方接受与交易相关的数据并将数据导入交换系统的机构或其代理。