ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 21078.3—2011/ISO/TR 9564-4:2004

银行业务　个人识别码的管理与安全 第3部分:开放网络中PIN处理指南

Banking—Personal identification number (PIN) management and security—Part 3:Guidelines for PIN handling in open networks

(ISO/TR 9564-4:2004,IDT)

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

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3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分等同采用ISO/TR 9564-4:2004《银行业务　个人识别码的管理与安全　第4部分：开放网络中PIN处理指南》(英文版)。

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

开放网络环境是一个高风险的环境。对基于 PIN 的交易尤其是这样，因为发卡方或收单方对 PIN 输入设备都是无法控制的。在许多情况下，是持卡人来决定使用什么样网络访问设备。

本部分提供了一个指南，以帮助支付系统的参与者在开放网络系统中减少 PIN 泄露带来的风险，以及防止在 GB/T 21078.1 和 GB/T 21078.2 涵盖的支付系统中随 PIN 泄露可能出现的欺诈。其目的是在开放网络环境中定义一个最小 PIN 安全准则。如果 PIN 在这种环境中的安全性不足，卡的数据也被泄露，则两者(卡数据和 PIN)就有很高的可能性在 ATM、POS 或开放网络环境中被欺诈性地使用。

鉴别机制的完整性取决于 PIN 和持卡人数据的机密性。在开放网络环境下，由于缺乏控制使得 PIN 的保护变得困难，因此，保护持卡人数据是必要的，这可以把在开放网络环境下卡数据盗用和 PIN 泄露造成的欺诈风险降到最小。

银行业务　个人识别码的管理与安全
第3部分:开放网络中PIN处理指南

1　范围

本部分规定了在开放网络系统中PIN的处理指南;在发卡方及收单方没有直接对PIN管理进行控制的环境中,或在发生交易前PIN输入设备与收单方没有关系的情况下,为管理PIN和处理金融卡发起的交易提供金融业务安全措施的最佳实践。

本部分适用于需要验证PIN的金融卡发起的交易,并适用于负责在开放网络系统中使用的终端和PIN输入装置中实施PIN管理技术的组织。

本部分不适用于:

——联机PIN环境下的PIN管理和安全,GB/T 21078.1和GB/T 21078.2包含该项内容;

——核准的PIN加密算法;

——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;

——非PIN交易数据的私密性;

——保护交易报文,防止修改或替换,例如联机授权响应;

——防止PIN或交易重放;

——特定的密钥管理技术;

——由基于服务器的应用(例如:电子钱包)来访问并储存卡数据;

——金融机构布放的、持卡人激活的、安全的PIN输入设备。

2　术语和定义

下列术语和定义适用于本文件。

2.1

收单方　acquirer

从受卡方获得与交易相关的数据并将数据提交给交换系统的机构或其代理。

2.2

泄露　compromise

〈密码学〉对保密性和(或)安全性的破坏。

2.3

加密　encipherment

采用某种编码机制将文本翻译为未授权者不可理解的形式。

2.4

集成电路卡(IC卡)　integrated circuit card(ICC)

ID—1型卡,根据GB/T 14916、GB/T 15120、GB/T 15694和GB/T 17552的定义,其中嵌入了一个或多个集成电路。

注:参见GB/T 16649.1。

2.5

发卡方　issuer

拥有主账号所标识账户的机构。

2.6

网络访问设备(NAD)　network access device(NAD)

个人计算机、机顶盒、移动电话、掌上电脑(PDA)、固网电话支付终端或其他可以访问开放网络的设备。

2.7

开放网络　open network

传输数据的完整性和机密性不能保证的公共网络。

示例：因特网、电话网。

2.8

个人识别码(PIN)　personal identification number(PIN)

客户持有的用于身份验证的代码或口令。

2.9

PIN 输入设备(PED)　PIN entry device(PED)

PIN 键盘　PIN pad

PIN 输入键盘　PIN entry keypad

持卡人输入 PIN 的设备。

2.10

主账号(PAN)　primary account number(PAN)

标识发卡方和持卡人信息的代码，由发卡方标识、持卡人标识和校验位组成，参见 GB/T 15694 中的定义。

3　开放网络模型

3.1　网络模型

GB/T 21078.1 和 GB/T 21078.2 描述了在 ATM(自动柜员机)或 POS(销售点)环境下基于 PIN 交易(联机或脱机)的 PIN 的安全性。

技术发展为在开放网络中使用基于 PIN 的金融交易提供了可行性。

在开放网络环境中，网络访问设备与世界上任何一个拥有开放网络连接的商户发生交易，且该商户可以使用任意的开放网络设备收单。因此，当在开放网络交易中使用 PIN 来验证持卡人时，交易的收单方不能控制 PIN 输入设备。这与 ATM 和 POS 环境下，收单方独自负责 PIN 输入设备的运行和安全不同。

3.2　开放网络访问设备

本部分详细说明了当使用 PIN 结合开放网络访问设备进行验证时，获得可接受的最低安全级别的方法。

采用下面的支付流程：

a)　持卡人使用经由开放网络进行通信的网络访问设备与商户接触；

b)　商户与其收单方经由开放网络或常规的“商户-收单方”通信方式进行通信；

c)　收单方与发卡方使用常规的授权和结算网络进行通信。

本部分描述在开放网络设备中的 PIN 输入方法的最低安全建议。因为涵盖到的所有设备都被假定为是不可信的，因此本部分提供了保护卡数据并且在开放网络设备中控制欺诈风险的方法。

尽管非 PIN 的持卡人验证方法超出了本部分的范围，但并不意味着其他方法没有 PIN 方法合适。

4 开放网络设备中 PIN 的安全原则

4.1 概述

PIN 的安全原则是基于 PIN 的机密性，而不提供对磁条卡中数据的保护。在开放网络环境下，难以确保 PIN 的机密性。因此，为了最小化 PIN 泄露的潜在风险，本部分关注于通过禁止使用磁条访问设备来保护磁条数据。

任何情况下，卡数据不应被保存在收单和发卡金融机构的系统以外的任何设备上。

要保证系统的安全，核心是确保 IC 卡释放的信息不足以制造出伪造的磁条卡，例如，通过确保磁条中的卡数据验证值和 IC 卡环境中的不同。

4.2 卡数据源

4.2.1 IC 卡

在不存在读磁条能力的脱机 PIN 开放网络环境中，欺诈的风险被极大地降低，因为 IC 卡为卡数据提供了足够的保护。因此，与 GB/T 21078.1 和 GB/T 21078.2 的要求相比，对提供健壮 PIN 安全的要求被降低了。

4.2.2 磁条卡

不支持在开放网络环境下使用磁条卡，因为这样 PIN 会遭受 GB/T 21078.1 和 GB/T 21078.2 所描述环境中的安全风险。支持和不支持 PIN 的环境见表 1。

4.2.3 手工 PAN 输入

当手工输入卡数据时，网络访问设备(NAD)不应提示 PIN 输入。

表 1 支持和不支持 PIN 的环境

	网络访问设备(NAD)	
	联机 PIN	脱机 PIN
IC 卡	不支持	支持
磁条	不支持	不支持
手工 PAN 输入	不支持	不支持

5 最小可接受 PED

根据第 4 章的原则产生了表 1 中的支持环境。为了提供支持环境的功能，需要使用符合本章要求的最小可接受 PED。

最小可接受 PED 是一个网络访问设备(NAD)，包括一个 IC 卡读卡器和一个能让持卡人输入 PIN 的设备。IC 卡读卡器插槽应：

a) 当卡在 IC 卡读卡器里时，应没有空间容纳一个泄露 PIN 的恶意装置；

b) 应不能被扩大而为一个泄露 PIN 的恶意装置提供空间；

c) 其放置方式应让用户能及时发现有恶意装置和其相连。

应提供必要的电子保护线路，以防止在IC卡读卡器内安装窃听装置。

6 连接到开放网络的脱机PIN处理设备的PIN安全

6.1 概述

本部分支持的环境仅包括通过PED使用IC卡。本章说明了在IC卡环境里的脱机PIN处理。

6.2 在开放网络访问设备中的脱机PIN验证

当IC卡进行脱机PIN验证时，PIN通常以明文的方式从PED传输给IC卡。有些支付应用要求使用IC卡的公钥加密PIN后提交给IC卡。在此情况下，只有当网络访问设备能执行该加密时，交易才能完成。

为了协助IC卡预防欺骗性访问，建议要求持卡人在交易之间移开IC卡，或者支付应用应要求在交易之间进行卡的物理复位。

6.3 对开放网络金融交易的一般建议

在一个开放网络中使用IC卡时，强烈建议应指导持卡人全程控制对其IC卡的访问。例如，当持卡人的卡在网络访问设备(NAD)中时，他们离开卡的时间不应超过完成交易所需的时间。

强烈建议建立起在网络访问设备(NAD)中使用的PED，以防止明文PIN离开PED(明文PIN被直接发送给IC卡除外)。

参 考 文 献

[1] GB/T 14916—2006 识别卡 物理特性(ISO 7810:2003,IDT)

[2] GB/T 15120—1994 识别卡 记录技术(GB/T 15120—1994,ISO 7811:1985,IDT)

[3] GB/T 15694.2—2002 识别卡 发卡者标识 第2部分:申请和注册规程(ISO 7812-2:2000,IDT)

[4] GB/T 16649.1—2006 识别卡 带触点的集成电路卡 第1部分:物理特性(ISO 7816-1:1998,IDT)

[5] ISO/IEC 7812-1:2000 识别卡 发卡者标识 第1部分:编号体系

[6] ISO/IEC 7813:2001 识别卡 金融交易卡

[7] ISO 13491-1:1998 银行业务 安全的加密设备(零售) 第1部分:概念、要求及评估方法