ICS 35.240.40
A 11

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

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。

4 在 PIN 输入设备(PED)和 IC 卡读卡器之间传输时的 PIN 保护

IC 卡读卡器和 PIN 输入设备(PED)既可以分成两个独立的设备,也可以集成在一个设备中,见表 1。

当 IC 卡读卡器和 PED 被集成为符合 GB/T 21078.1—2007 的 6.3 要求的设备,而且以明文形式提交 PIN 给 IC 卡时,PED 不需要加密 PIN。

当 PIN 以明文形式通过未受保护的环境传输至 IC 卡读卡器并提交至 IC 卡时,应按照 GB/T 21078.1—2007 的要求对 PIN 加密。IC 卡读卡器应解密 PIN,并以明文形式提交给 IC 卡。

当 PIN 以加密形式提交给 IC 卡时,无论是集成还是非集成的设备,PIN 均应在一个符合 GB/T 21078.1—2007 的 6.3 要求的设备内使用 IC 卡加密密钥加密。

如果 PIN 被传输到一个符合 GB/T 21078.1—2007 的 6.3 要求设备的外面,则它应该按照 GB/T 21078.1—2007 的要求加密或使用 IC 卡加密密钥加密。

5 物理安全

本章给出了对 PED 和 IC 卡读卡器的物理安全的要求和建议。除以下情况外,对用于脱机 PIN 验证的 PED 的要求与在 GB/T 21078.1—2007 给出的要求相同。

PED 应是 GB/T 21078.1—2007 的 6.3 定义的“物理安全设备”。否则,它至少应满足 GB/T 21078.1—2007 的 6.3 对 PED 的要求。

为了使收单方能够检测出 PED 上的攻击,PED 自己应能向收单方验证它自己,即如果被攻击,它将不再能向收单方验证自己。

此外,如果 PED 用于处理联机的 PIN 交易(且符合 GB/T 21078.1—2007 的要求),收单方应定期验证它的完整性。

配备 IC 卡读卡器的设备应满足 GB/T 21078.1—2007 的 6.3 对 PED 的要求。

IC 卡读卡器的插卡槽:

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

b) 应不能被扩大而为泄漏 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电路,以防止在 IC 卡读卡器内安装窃听装置。

表 1 根据本章和第 4 章的要求,总结了对不同的终端配置及 PIN 提交方式的 PIN 保护的要求。

表 1 PIN 保护要求

PIN 提交方式	IC 卡读卡器和 PED 按照 GB/T 21078.1—2007 的 6.3 要求集成为一个设备	IC 卡读卡器和 PED 没有按照 GB/T 21078.1—2007 的 6.3 要求集成为一个设备
加密的 PIN BLOCK 提交给 IC 卡	PIN BLOCK 应该使用一个 IC 卡加密密钥[注]加密,然后提交给 IC 卡	PIN BLOCK 在 PED 和 IC 卡读卡器之间应按照 GB/T 21078.1—2007 的要求加密或者使用一个 IC 卡加密密钥加密。 PIN BLOCK 应该使用一个 IC 卡加密密钥加密,然后提交给 IC 卡
明文 PIN BLOCK 提交给 IC 卡	不要求加密	PIN BLOCK 在 PED 和 IC 卡读卡器之间应按照 GB/T 21078.1—2007 的要求加密
注:参见 EMV2000。		

6 PIN BLOCK 格式

6.1 概述

IC 卡读卡器提交给 IC 卡的 PIN 包含在一个 PIN BLOCK 中，该块符合 6.2 的要求。这适用于 PIN 以明文的方式提交或使用一个 IC 卡的加密密钥加密后提交。

在 PED 和 IC 卡读卡器之间传输的加密 PIN 应使用 GB/T 21078.1—2007 中规定的 PIN BLOCK 格式。当使用“格式 2 的 PIN BLOCK”时，应为每笔交易使用惟一密钥或者定期更换加密密钥。

6.2 格式 2 的 PIN BLOCK

PIN BLOCK 由 2 个部分连接构成：明文 PIN 部分和填充部分。

格式 2 PIN BLOCK 应使用下面格式：

位：

1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	64
C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

其中：

C＝控制域	4 位域，值为 0010(2)；
N＝PIN 长度	4 位二进制数，允许值为 0100(4)到 1100(12)；
P＝PIN 数字位	4 位域，允许值为 0000(0)到 1001(9)；
P/F＝PIN 数字位或填充位	这些域由 PIN 长度域决定；
F＝填充位	4 位域，值为 1111(15)。

参 考 文 献

[1] GB/T 16790(所有部分) 金融交易卡 使用集成电路卡的金融交易系统的安全体系