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。