附 1

中 国 支 付 清 算 协 会 标 准

PCAC 0001: 2015

条码支付技术安全指引（报批稿）

2015-**-**发布　　2015-**-**实施

中国支付清算协会技术标准工作委员会 发布

带格式的：居中

目　次

带格式的：居中

前　言

本指引由中国支付清算协会提出。

本指引由中国支付清算协会技术标准工作委员会归口。

本指引主要起草单位为中国支付清算协会会员单位及行业相关单位，包括：中国支付清算协会~~技术与标准部~~秘书处、中国银行股份有限公司、中国工商银行股份有限公司、中国银联股份有限公司、中信银行股份有限公司、中国电信天翼电子商务有限公司、支付宝（中国）网络技术有限公司、财付通支付科技有限公司、易宝支付有限公司、新大陆科技集团、银行卡检测中心、深圳市快付通金融网络科技服务有限公司。

本指引主要起草人：蔡洪波、马国光、邢桂伟、于沛、陈志龙、吕涛、颜世杰、夏庆凡、丁豪、高晟凯、庄晓海、刘向辉、程志云、刘剑、方海峰、周俊、赵传飞、李丹丹、程伟、赵磊、许坚、刘峰、陈亮、王建新、魏博锴、伍向前、甄世泉、孟宏文、欧阳明、颜勇、张媛。

本指引为首次发布。

带格式的：居中

条码支付技术安全指引

1 范围

本指引用于规范会员单位开展面对面的条码支付业务时，所需应用系统的设计、研发、集成和维护。

条码支付实际上是指条码技术在支付领域中的应用，其本质是以条码为信息载体，通过移动终端或受理终端直接或间接获取支付要素，并利用已有支付渠道完成交易的一种支付方式。

本指引适用于付款人移动终端与商户受理终端（收款人特定专属设备）之间进行的以条码为信息载体的支付业务。各会员单位开展其它类型条码支付业务时可参照本指引相关条款，以提高风险防范能力。

本指引描述了条码支付交易涉及到的业务流程和应用安全，包括移动终端、商户系统与支付机构之间的交易模型和流程，及系统安全、终端安全、交易安全和密钥体系。

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，仅所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 22239-2008 信息安全技术 信息系统安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

条码 bar code

宽度不等的多个黑条和空白，按照一定的编码规则排列，用以表达一组信息的图形标识符。包括一维条码，二维条码等。

3.2

二维条码 2-dimensional bar code

二维码 2-dimensional code

在一维条码的基础上扩展出另一维具有可读性的条码，使用黑白矩形图案表示二进制数据，被设备识读和解码后可获取其中所包含的信息。二维条码一般在长度、宽度两个维度上均记载着数据。

3.3

条码识读器 bar code reader

识读条码的设备。

3.4

移动终端 mobile device

具有移动通讯、条码展示和识读能力的终端设备，如手机、平板电脑等。

3.5

受理终端 point of sales

带格式的：居中

参与条码支付的商户端受理机具，具有条码展示或识读等功能，包括专用的条码支付受理设备，以及在原有 POS 等设备上进行扩展后能够处理条码展示或识读的设备。

3.6

条码支付系统 barcode payment system

提供移动终端接入、商户系统接入、受理终端接入、条码信息管理、交易信息、结算数据处理等功能的系统。

3.7

商户系统 merchant system

商户端提供交易订单并和支付机构进行交互的系统。

3.8

账户管理系统 account management system

为银行账户或非金融机构支付账户提供资金管理、结算等业务的系统。

4 应用系统架构

系统架构如下图所示：

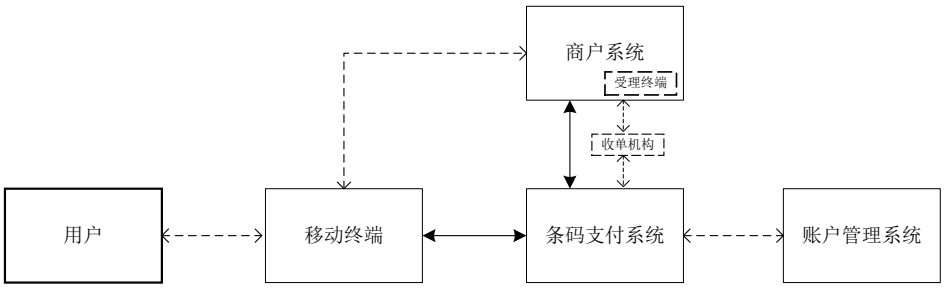


图 1：应用系统架构图

该系统架构定义条码支付各参与方之间的关系。参与方包括用户、移动终端、商户系统、条码支付系统、账户管理系统，具体说明如下：

——用户是支付过程中购买商品或服务的个人或企业；

——移动终端包含客户端程序、条码展示设备、条码识读器等；

——商户系统包含条码生成程序或者设备、条码展示设备、条码识读器、交易处理系统等；

——条码支付系统包括条码的生成、条码处理、移动终端和商户系统的交易接入和交易处理等；

——账户管理系统为银行账户或第三方支付账户提供条码信息管理、资金管理、结算等业务的系统。

本标准主要描述条码支付中移动终端、商户系统以及条码支付系统等实体之间的涉及到条码的业务环节，支付相关流程不在这里详细描述。根据业务的需求，支付可以从移动终端发起也可以从商户系统发起。

5 交易处理流程

5.1 交易分类说明

根据业务处理特点的不同，基于条码的支付业务包括付款扫码支付和收款扫码支付。

带格式的：居中

5.2 付款扫码支付

5.2.1 概述

此模式下，由付款人通过移动终端识读代表收款人的条码（订单或账户信息），并由付款人发出支付指令，实现付款交易。

5.2.2 交易模型

典型流程如下图所示：

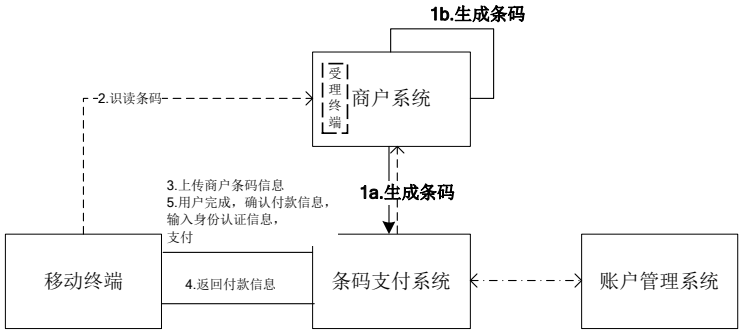


图 2：付款扫码支付典型流程

5.2.3 交易流程

步骤 1: 生成商户条码（有 a 或 b 两种技术实现方式）

步骤 1a: 商户系统请求条码支付系统生成条码，条码支付系统返回条码，商户系统展示条码；

步骤 1b：商户系统生成条码；

步骤 2: 付款人通过移动终端识读条码；

步骤 3: 付款人通过移动终端向条码支付系统上传条码信息；

步骤 4: 条码支付系统返回付款信息给移动终端进行展示；

步骤 5: 付款人在移动终端上确认付款信息，输入身份认证信息，支付。

5.3 收款扫码支付

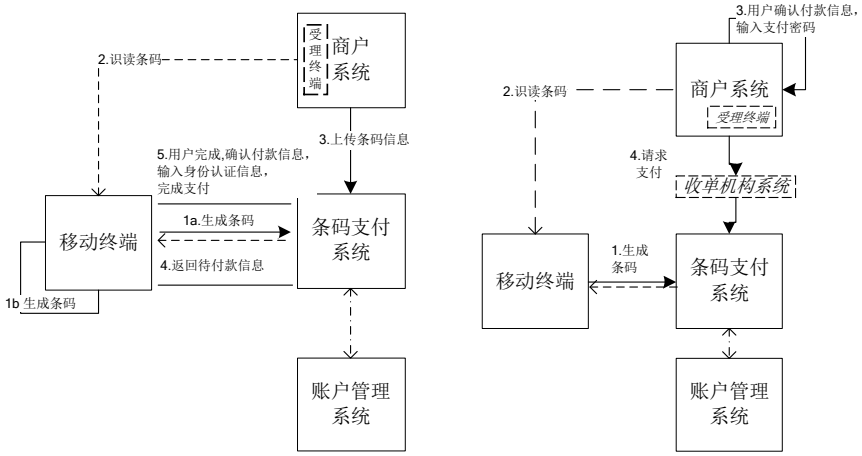
5.3.1 概述

此模式下，由商户扫描代表付款人的条码，并由商户发出交易指令，以完成收款业务。

5.3.2 交易模型

付款人可通过移动终端或者商户系统进行交易确认，典型流程如下图所示：

带格式的：居中



A: 付款人在移动终端进行交易确认　　B: 付款人在商户系统进行交易确认

图 3：收款扫码支付典型流程

5.3.3　交易流程 A

步骤 1: 生成付款条码（有 a 或 b 两种技术实现方式）

方案 1a:　移动终端向条码支付系统请求生成付款条码；

方案 1b:　移动终端本地生成付款条码；

步骤 2: 商户系统通过条码识读器识读条码；

步骤 3: 商户系统上传条码信息到条码支付系统，发起支付；

步骤 4: 条码支付系统返回付款信息给移动终端进行展示；

步骤 5: 付款人在移动终端上完成付款信息，确认付款信息，输入身份认证信息，请求支付。

5.3.4　交易流程 B

步骤 1: 生成付款条码（有 a 或 b 两种技术实现方式）

步骤 1a:　移动终端向条码支付系统请求生成付款条码；

步骤 1b:　移动终端本地生成付款条码；

步骤 2: 商户系统通过条码识读器识读用户条码，发起交易；

步骤 3: 付款人在商户受理终端上确认付款信息，输入身份认证信息；

步骤 4: 商户系统发出支付指令。

5.4 异常流程处理

异常流程处理如下：

——商户系统与条码支付系统建立连接失败或无法发送请求报文，则提示商户系统失败或提示商户系统重试；

——移动终端与条码支付系统建立连接失败或无法发送请求报文，则通知移动终端提示用户失败或提示用户重试；

——商户系统请求条码支付系统生成条码失败，则提示商户系统失败或提示商户系统重试；

——移动终端请求条码支付系统生成条码失败，则提示用户重试或者放弃；

——移动终端若不能识读条码，则提示错误或者提示重试或者流程结束；

——商户系统通过条码识读器若不能识读条码，则提示错误或者提示重试或者流程结束；

带格式的：居中

——商户系统上传条码信息到条码支付系统失败，则提示商户系统失败或提示商户系统重试；
——移动终端上传条码到条码支付系统失败，则提示错误或者提示重试；
——条码支付系统收到移动终端不合法的请求报文，则丢弃该报文并通知移动终端；条码支付系统处理移动终端交易请求出错，则通知移动终端提示用户交易失败，通知商户系统提示交易失败；
——条码支付系统收到商户系统不合法的请求报文，则丢弃该报文并通知商户系统；条码支付系统处理商户系统交易请求出错，则通知商户系统提示交易失败，通知移动终端提示用户交易失败；
——条码支付系统请求账户系统支付失败，则交易中止，或由条码支付系统发起冲正，通知移动终端提示用户交易失败，通知商户系统提示交易失败。

6 系统安全

6.1 物理安全要求

按GB/T 22239-2008中第三级基本要求中的7.1.1执行。

6.2 网络安全要求

按GB/T 22239-2008中第三级基本要求中的7.1.2执行。

6.3 主机安全要求

按GB/T 22239-2008中第三级基本要求中的7.1.3执行。

6.4 应用安全要求

6.4.1 通用安全

按GB/T 22239-2008中第三级基本要求中的7.1.4执行。
其他基本要求：
——不应在日志中记录敏感信息；
——采用有效的密码技术保证通讯过程中交易数据的完整性。

6.4.2 会话安全

会话应满足但不限于如下安全要求：
——会话标识应唯一、随机、不可猜测；
——会话过程中应维持认证状态，防止信息未经授权访问；
——会话应设置超时时间，当空闲时间超过设定时间应自动终止会话；
——会话结束后，应及时清除会话信息；
——应采取措施防止会话令牌在传输、存储过程中被窃取。
增强要求：
——应用审计日志应记录暴力破解会话令牌的事件。

6.4.3 常见攻击防范

应对常见的攻击（如跨站脚本攻击、注入攻击、拒绝服务攻击等）进行有效防范，包括但不限于如下手段：
——应在服务器端对提交的数据进行有效性检查（如对提交的表单、参数等进行合法性判断和非法字符过滤等），或对输出的数据进行安全处理；
——应具有防范暴力破解静态密码的保护措施，例如使用图形验证码等；

带格式的：居中

——应进行代码审查，防范应用程序中不可信数据被解析为命令或查询语句等；
——应开发安全的接口，如通过避免语句的完全解释或采用参数化接口等方式实现；
——应采取有效措施防范针对服务器端的拒绝服务攻击；
——应对文件的上传和下载进行访问控制，避免执行恶意文件或未授权访问。
增强要求：
——数据库应使用存储过程或参数化查询，并严格定义数据库用户的角色和权限；
——应通过自动化工具（如弱点扫描工具、静态代码检测工具等）对应用程序进行检查；
——基于浏览器的应用，应使用安全控件等措施以降低恶意软件窃取用户敏感信息的风险。

6.4.4 数据安全及备份恢复

按GB/T 22239-2008中第三级基本要求中的7.1.5执行。

6.4.5 敏感信息保护

敏感信息保护应满足以下要求：
——禁止明文显示密码，应使用相同位数的同一特殊字符（例如*和#）代替；
——密码应有复杂度的要求；
——应具有防范暴力破解静态密码的保护措施，例如在登录和交易时使用图形认证码；
——使用软键盘方式输入密码时，应防范密码被窃取；
——应保证密码的加密密钥的安全。

7 移动终端安全

7.1 人机交互安全

7.1.1 密码管理

支付密码应满足以下安全管理要求：
——支付密码不能保存在移动终端本地；
——用户输入支付密码时，应提供即时加密功能；
——认证操作结束后立即清除缓存，防止信息泄漏。
登录密码等其它密码应满足以下安全管理要求：
——登录密码等其它密码不能明文保存在移动终端本地；
——用户输入登录密码等其它密码时，应提供即时加密功能；
——认证操作结束后立即清除缓存，防止信息泄漏。

7.1.2 交易异常处理

当交易出现异常时，客户端应向用户提示出错信息。

7.2 软件安全

7.2.1 数据有效性校验

客户端宜提供数据有效性校验功能，保证通过人机接口或通信接口输入的数据格式或长度等信息符合系统设定要求，如输入的资金金额、账户等信息应不含特殊字符。

7.2.2 页面回退清除敏感信息机制

客户端宜支持页面回退清除敏感信息的机制。

带格式的：居中

7.2.3 反编译

客户端宜采用防逆向工程保护措施，如客户端可采取代码混淆等技术手段，防范攻击者对客户端的反编译分析。

7.2.4 防篡改

客户端启动和更新时，宜进行真实性和完整性校验，防范客户端被篡改。

7.2.5 客户端完整性

应对客户端程序进行签名，标识客户端程序的来源和发布者，保证客户所下载的客户端程序来源于所信任的机构。

7.3 数据安全

7.3.1 数据录入

数据录入应符合下列要求：

——对于密码等敏感数据，客户端不应明文显示；

——用户输入敏感数据时，应采取安全措施防止敏感数据被非法截获；

——用户输入敏感数据时，应采取防篡改机制保证数据不被非法篡改。

7.3.2 数据访问

宜根据业务需要保证敏感数据仅供授权用户或授权应用组件访问。

7.3.3 数据存储

数据存储应符合下列要求：

——在满足法律、管理规定和业务需求的前提下，客户端宜保留最少的用户敏感数据（如登录密码、账户信息等），并限制数据存储量和保留时间；

——客户端不应保存用户支付信息（如支付密码等）及其密文；

——客户端显示敏感信息时，宜屏蔽部分内容，如银行账号、身份证号等；

——客户端在使用过身份认证、交易等敏感信息后，应及时清除敏感数据。

7.3.4 数据传输

数据传输应符合下列要求：

——身份认证信息等敏感数据通过公共网络传输时应采取加密措施，保证敏感数据传输的保密性；

——身份认证信息等敏感数据在本地软件其他进程间传输时应采取加密措施，保证敏感数据传输的保密性；

——交易数据在传输时，客户端应采取安全措施（如MAC等）以确保交易数据的完整性。

7.4 通信安全

7.4.1 网络通讯协议

网络通讯协议应符合下列要求：

——应在客户端与服务器之间建立安全的信息传输通道，宜进行双向认证，例如使用SSL/TLS或IPSEC等协议；

——如使用SSL协议，应使用相对高版本的协议，取消对低版本协议的支持；

——客户端到条码支付系统的对称算法、非对称算法、摘要算法应采用安全可靠的密码算法。

带格式的：居中

7.4.2 安全认证

客户端的网络协议层应对条码支付系统进行身份认证。

7.4.3 抗抵赖

通过客户端发送的报文的关键要素宜进行数字签名，以确保支付内容的真实性和抗抵赖性。

8 受理终端安全

受理终端安全应符合以下要求：

——应保证对条码识读结果的私密性，避免条码信息泄露；

——应保证对条码解析的准确性；

——应保证对条码识读解析结果表达的规范性；

——应采用符合国家及金融行业相关标准、通过权威机构检测认证的硬件密码键盘对输入的密码进行保护；

——对于在原有POS或ATM等设备上进行扩展后能够处理条码展示或识读的设备还应遵守国家及金融行业相关标准。

9 交易安全

9.1 条码生成

应确保生成条码的软件、设备的安全性，防止生成的条码携带病毒、木马等数据或者链接，防止生成的条码被篡改、替换。

采用收款扫码方式时：

——条码应由后台服务器加密动态生成或由移动终端安全单元（SE）加密动态生成；

——采用服务器加密动态生成条码时，原则上应实时从后台服务器获取。若无法实时从后台服务器获取的，应满足以下条件：

- 移动终端软件应定期从后台服务器获取条码生成因子，通过生成因子加密动态生成条码；
- 条码生成因子的有效时间应小于24小时；
- 应采取密码技术对生成因子进行保护，防止生成因子受到未授权的访问，以确保其唯一性；
- 应与移动终端的唯一标识信息绑定，防止生成因子被非法复制到其他移动终端使用。

——应使用可靠的加密技术实时、动态生成条码，条码应限制一次使用且有效时间应小于30分钟，防止信息重复使用；

——条码不应存储敏感信息，应采用加密技术进行保护。

采用付款扫码方式时：

——条码应加密、动态生成；

——应采用有效措施，确保条码信息的真实性、完整性、一致性和抗抵赖性。

9.2 条码识读与解析

条码识读设备应保证识读结果的私密性，避免条码信息泄露。

条码解析时应满足以下要求：

——应对条码完整性进行校验；

——应对条码的真实性进行校验；；

——应识别病毒、木马等恶意数据，保障交易的安全性。

带格式的：居中

9.3 身份认证与交易确认

采用付款扫码支付方式时，应在付款方终端展现交易信息，经过用户确认并通过客户身份认证后，由付款方终端发起支付指令。交易信息包含但不限于收款方名称、金额等。客户身份认证原则上应同时采用下列至少两类要素：

——仅客户本人知悉的要素，如静态密码等；

——仅客户本人持有并特有的，不可复制或者不可重复利用的要素，如经过安全认证的数字证书、电子签名，以及通过安全渠道生成和传输的一次性安全验证码等。其中，采用数字证书、电子签名作为认证要素的，数字证书及生成电子签名的过程应通过安全硬件进行保护，确保数字证书的唯一性、完整性及交易的抗抵赖性；

——客户本人生物特性要素，如指纹等。采用的生物特性要素宜通过安全硬件进行保护，防止被非法存储、复制和重放。

同时，应确保采用的要素相互独立，即部分要素的损坏或者泄露不应导致其他要素损坏或者泄露；采用一次性安全验证码作为认证要素的，应切实防范一次性安全验证码获取端与交易指令发起端为相同物理设备而带来的风险。

采用收款扫码支付方式时，应满足以下要求：

——在商户端输入密码时应在收款方终端展现交易信息；在移动终端输入密码时应移动终端上展现交易信息；

——应经过用户确认并输入支付密码。

9.4 交易风险控制

对于资金类等高风险业务，应在确保客户联系方式有效的前提下，通过短信等方式实时告知客户其资金变化情况。

采用收款扫码支付方式时，为防范条码被窃取、复制、偷窥等风险，应由客户输入支付密码予以确认，并根据不同的风险防范能力设置相应的单笔、日累计交易限额。

在受理终端上输入身份认证信息时，风险防范能力分级如表1：

表1

条码生成方式	风险防范能力
移动终端 SE 加密动态生成条码；	A 级
服务器端加密动态生成条码，移动终端软件实时获取；	B 级
移动终端软件从服务器端获取条码生成因子，通过生成因子加密动态生成条码；	C 级

在移动终端上输入身份认证信息时，风险防范能力分级如表2：

表2

身份认证方式	条码生成方式	风险防范能力
使用数字证书、电子签名作为认证要素（具体要求见 9.3 节）	移动终端 SE 加密动态生成条码； 或服务器端加密动态生成条码	A 级
未使用数字证书、电子签名作为认证要素	移动终端 SE 加密动态生成条码	B 级
	服务器端加密动态生成，移动终端软件实时获取； 或移动终端软件从服务器端获取条码生成因子，通过生成因子加密动态生成条码	C 级

带格式的：居中

采用付款扫码支付方式时，应按照9.3条进行客户身份认证，并根据不同风险防范能力设置相应的单笔、日累计交易限额，风险防范能力分级如表3：

表3

身份认证方式	风险防范能力
采用双要素认证，且使用数字证书、电子签名作为认证要素（具体要求见 9.3 节）	A 级
采用双要素认证，但未使用数字证书、电子签名作为认证要素（具体要求见 9.3 节）	B 级
未采用双要素认证，但应采用支付密码等需要联机认证的要素（具体要求见 9.3 节）	C 级

9.5 敏感信息保护

敏感信息保护应符合下列要求：

——条码承载的信息不应包含明文的账户、个人身份标识、密钥等敏感数据；

——敏感信息应按业务要求进行保存和使用，显示时应进行屏蔽处理；

——应保证交易隐私信息的保密性，如姓名、有效身份证件号码、联系方式、交易内容等。

9.6 交易过程安全

9.6.1 交易报文安全

交易报文安全应符合下列要求：

——应可防止对交易的重放攻击；

——宜保证交易的抗抵赖性，包含但不局限于证书签名等技术手段；

——在交易报文传输过程中应使用安全传输协议保证传输安全，包含但不限于 SSL/TLS 协议；

——应用系统应保证在一段时期内同一商户交易、订单的唯一性；

——应用系统应检查交易请求报文中记载的交易要素是否完整并符合业务规则，并拒绝不完整或者不符合业务规则的交易请求；

——应用系统应防止对支付成功的订单重复支付；

——应对条码识别后的内容进行严格的安全校验，保证只有合法有效的条码才能进入后续支付流程；

——应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用，保证对条码支付的操作能够被追溯到用户。

9.6.2 风险识别与干预

风险识别与干预应符合下列要求：

——应采取必要措施，在交易过程中给予必要的支付风险提示。支付风险的提示可每次提示，也可在业务开通时给予提示；

——支付机构从用户的账户管理机构获取的支付结果中应包含支付及风险防范相关的数据要素；

——应对交易过程进行风险识别与干预，防范潜在的非法交易、欺诈交易。

9.6.3 交易监控

交易监控应符合下列要求：

——应建立交易监控系统，能够甄别并预警潜在风险交易，例如套现、洗钱、欺诈等可疑交易，并生成风险监控报告；

——应根据交易的风险特征建立风险交易模型，有效监测可疑交易，对可疑交易建立报告、复核、

带格式的：居中

查结机制；

——应对监控到的风险交易进行及时分析与处置；

——应建立条码支付网址的黑白名单验证和管理机制，在黑名单中直接拒绝，其它网址应进行风险提示。

9.7 用户教育

用户教育应符合下列要求：

——应通过公开渠道向用户提供安全的包含条码支付功能的客户端程序；

——应向用户宣传条码支付的安全知识，提高用户安全防范意识；

——应在支付使用过程中向客户明确提示相关的安全风险和注意事项。

10 密码算法

条码支付使用的密码算法应符合国家密码管理部门相关要求，并使用国家密码管理部门公布的商用密码产品目录的密码产品。

带格式的：居中