附件 1

条码支付安全技术规范

（试行）

2017 年 12 月

目　次

1 范围

本规范规定了条码支付系统、终端、数据和交易的安全技术要求。

本规范适用于银行、非银行支付机构、清算机构开展条码支付业务时所需软硬件的设计、研发、集成和维护。

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

JR/T 0118—2015 金融电子认证规范

JR/T 0149—2016 中国金融移动支付 支付标记化技术规范

条码支付受理终端技术规范（试行）

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

由一组规则排列的条、空及其对应字符组成的标记，用以表示一定的信息，包括线性条码、二维条码等。

3.2

线性条码 linear bar code

一维条码 one-dimensional bar code

条形码 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。

3.3

二维条码 two-dimensional bar code

二维码 two-dimensional bar code

在线性条码的基础上扩展出另一维具有可读性的条码，使用具有明显色差的深浅色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。

3.4

静态条码 static bar code

具有较长时效，可多次重复使用的条码。

3.5

动态条码 dynamic bar code

通过显码设备展示，并且有较短时效的条码。

3.6

条码支付 bar code payment

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。

3.7

移动终端 mobile terminal

具有移动通讯、条码展示或识读能力的客户设备，如手机、平板电脑等。

3.8

受理终端 payment terminal

具有条码展示或识读等功能，参与条码支付的商户端专用机具，包括显码设备和扫码设备。

3.9

显码设备 bar code display device

具有条码展示功能的专用设备。

3.10

扫码设备 bar code reader

识读条码并且向后台系统发起支付指令的专用设备，包括但不限于带扫码装置的收银机、POS 终端、自助终端等。

4 系统安全

4.1 物理安全要求

物理安全应符合GB/T 22239—2008中7.1.1的相关要求。

4.2 网络安全要求

网络安全应符合GB/T 22239—2008中7.1.2的相关要求。

4.3 主机安全要求

主机安全应符合GB/T 22239—2008中7.1.3的相关要求。

4.4 应用安全要求

4.4.1 基本要求

应用安全应符合GB/T 22239—2008中7.1.4的相关要求。

其他基本要求如下：

——不应在日志中记录客户支付敏感信息；

——应采用数字签名等技术手段保证交易信息的完整性；

——基于浏览器的应用，应使用数字证书标识网站身份，使用即时加密等安全措施降低恶意软件窃取客户支付敏感信息的风险。

4.4.2 会话安全

会话安全要求如下：

——会话标识应唯一、随机、不可猜测；

——会话过程中应维持登录认证状态，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；

——应采取加密等措施防止会话令牌在传输、存储过程中被窃取；

——应用审计日志宜记录暴力破解会话令牌的事件。

4.4.3 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，包括但不限于以下手段：

——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）；

——应对条码中包含的网址等信息进行校验，对非法地址和恶意请求进行拦截；

——应具有防范暴力破解的保护措施；

——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；

——应使用安全的接口，防范接口被攻击和非授权调用；

——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；
——数据库宜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；
——宜通过自动化工具（如弱点扫描工具等）对应用程序进行检查。

4.5 数据安全及备份恢复

数据安全及备份恢复应符合GB/T 22239—2008中7.1.5的相关要求。

5 移动终端安全

5.1 人机交互安全

5.1.1 身份验证信息管理

身份验证信息管理应满足以下要求：
——原始身份验证信息不应明文保存在移动终端本地；
——客户输入交易密码时，应提供即时加密功能；
——验证操作结束后应及时清除缓存，防止信息泄漏；
——应严格限制使用初始交易密码，对交易密码复杂度进行校验，避免采用简单交易密码或与客户个人信息相似度过高的交易密码；
——应采取有效措施提醒客户避免设置与常用软件（如社交软件）、网站（如社交平台、论坛）相同或相似的用户名和密码组合；
——应采取有效措施引导客户设置独立的支付密码。

5.1.2 交易异常处理

当交易出现异常时，客户端应向客户提示出错等信息。

5.2 客户端软件安全

5.2.1 数据有效性校验

客户端软件应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，如输入的交易金额等信息应不含特殊字符、负数等非法参数。

5.2.2 页面回退清除敏感信息机制

客户端软件应支持页面回退清除密钥、密码等敏感信息的机制。

5.2.3 反编译

客户端软件应采用防逆向工程保护措施，如客户端软件采取代码花指令、反调试、代码混淆等技术手段，防范攻击者对客户端软件的反编译分析。

5.2.4 客户端软件完整性

客户端软件完整性应满足以下要求：
——应对客户端软件进行签名，标识客户端软件的来源和发布者，保证客户所下载的客户端软件来源于所信任的机构；
——客户端软件启动和更新时，应进行真实性和完整性校验，防范客户端软件被篡改。

5.2.5 运行时安全

客户端软件运行时安全应满足以下要求：
——客户端软件应从木马病毒防范、信息加密保护、运行环境可信等方面提升安全防控能力；
——客户端软件应能监测并向后台系统反馈手机支付环境安全状况，作为风控策略的依据。

5.3 通信安全

5.3.1 网络通讯协议

网络通讯协议应满足以下要求：

——应在客户端与服务器之间建立安全的信息传输通道，通过公开网络进行数据传输时应进行双向认证，例如使用安全套接字层或传输层安全（SSL/TLS）、互联网协议安全（IPSec）等协议；

——如果使用 SSL/TLS 协议，应使用安全的版本，取消对存在安全隐患版本协议的支持。

5.3.2 抗抵赖

通过客户端发送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。

6 受理终端安全

受理终端安全应满足以下要求：

——参照《中国人民银行关于强化银行卡受理终端安全管理的通知》（银发〔2017〕21 号）等相关要求，应从终端产品选型、验收、现场检查等环节加强安全管理，确保终端的技术标准符合性；

——受理终端应使用经国家密码管理机构认可的商用密码产品；

——应符合《条码支付受理终端技术规范（试行）》相关要求。

7 交易安全

7.1 基本要求

交易安全应满足以下要求：

——应遵守国家安全、国家网络安全相关法律法规，严格落实《中国人民银行关于进一步加强银行卡风险管理的通知》（银发〔2016〕170 号）等相关规定，确保条码支付业务设施的安全、稳定和高效运行；

——应按照 JR/T 0149 的相关要求，对银行卡卡号、卡片验证码、支付账户等信息进行脱敏，支持基于支付标记化技术的交易处理，采取技术手段从源头控制信息泄露和欺诈交易风险；

——条码支付涉及的软硬件应使用经国家密码管理机构认可的商用密码产品；

——应定期开展支付敏感信息安全的内部审计；

——支付敏感信息的采集、存储、传输、使用等环节应符合《中国人民银行关于进一步加强银行卡风险管理的通知》（银发〔2016〕170 号）的要求。

7.2 码制

条码应使用符合国家标准的码制。

7.3 数据录入

数据录入应满足以下要求：

——客户输入交易密码等信息，客户端不应明文显示；

——客户输入支付敏感信息时，应采用信息输入安全防护、即时数据加密等安全措施防止数据被非法截获；

——客户输入支付敏感信息时，应采取防篡改机制防止数据被非法篡改；

——客户输入关键交易信息时，如收款人信息、交易金额等，应采取防篡改机制防止数据被非法篡改。

7.4 数据访问

数据访问应满足以下要求：

——应根据业务需要保证支付敏感信息仅供授权用户或授权应用组件访问；
——支付敏感信息应按业务需求进行保存和使用，显示时应进行屏蔽处理。

7.5 数据存储

数据存储应满足以下要求：
——在满足法律、管理规定的前提下，客户端应保留最少的客户信息，并限制数据存储量和保留时间；
——客户端在使用支付敏感信息后，应及时清除；
——不得留存非本机构的支付敏感信息，确有必要留存的，应取得客户本人及账户管理机构的授权并进行加密或不可逆变换。

7.6 数据传输

数据传输应满足以下要求：
——支付敏感信息通过公共网络传输时应采取加密措施，保证支付敏感信息传输的保密性；
——支付敏感信息在本地软件其他进程间传输时应采取加密措施，保证支付敏感信息传输的保密性；
——交易信息在传输时，客户端应采取安全措施如报文鉴别码（MAC）以确保交易信息的完整性。

7.7 条码生成

7.7.1 基本要求

条码支付分为收款扫码和付款扫码。收款扫码是指收款人通过识读付款人移动终端展示的条码完成支付的行为。付款扫码是指付款人通过移动终端识读收款人展示的条码完成支付的行为。

条码生成时，应满足以下基本要求：
——应使用支付标记化技术对支付账号、银行卡卡号等信息进行脱敏处理；
——应确保生成条码软硬件的安全性，防止生成的条码携带病毒、木马等恶意代码；
——应根据风控能力，严格设置条码使用有效期；
——应采用有效措施，确保条码信息的真实性、完整性、一致性和不可抵赖性。

7.7.2 收款扫码

收款扫码的条码生成方式包括服务器端生成条码和移动终端生成条码两大类。其中，服务器端生成条码方式包括移动终端实时获取、移动终端批量获取；移动终端生成条码方式包括安全单元（SE）加密动态生成、客户端软件通过生成因子加密动态生成。

采用收款扫码方式时，应满足以下基本要求：
——展示条码的客户端应先进行身份验证；
——条码应限制一次使用且展示周期原则上应小于 1 分钟；
——应采取有效措施防止展示条码被截屏等方式窃取；
——应采用加密方式生成条码。

对于服务器端生成、由移动终端批量获取的条码生成方式，还应满足以下要求：
——移动终端客户端软件从后台服务器批量获取预生成的条码，应以安全的方式在移动终端上保存；
——保存的条码应与移动终端的唯一标识信息绑定，防止被非法复制到其他移动终端使用；
——预生成的条码应定期更换,更新周期宜小于 24 小时；
——应采取密码技术对预生成的条码进行保护，防止受到未授权的访问；
——从后台服务器获取条码时，后台服务器应对客户端软件进行身份验证，防止恶意获取条码。

对于移动终端客户端软件通过生成因子加密动态生成条码的方式，还应满足以下要求：
——移动终端客户端软件应从后台服务器获取条码生成因子，以安全的方式保存，并通过生成因子加密动态生成条码；
——条码生成因子应与移动终端的唯一标识信息绑定，防止被非法复制到其他移动终端使用；

——条码生成因子应定期更换，更新周期宜小于 7 天；
——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。

7.7.3 付款扫码

采用付款扫码方式时，条码生成应满足以下要求：
——采用显码设备展示条码时：
- 条码应加密、动态生成，原则上应实时生成或从后台服务器获取，并限一次性使用。

——采用静态条码时：
- 条码应由后台服务器加密生成；
- 宜采用防伪纸张展示条码，可参考附录 A；
- 展示条码的介质应放置在商户收银员视线范围内，并采用防护罩等物理防护手段避免条码被覆盖或替换，商户应定期对介质进行检查；宜使用防伪封签对防护罩等物理防护手段进行标记，及时发现物理防护手段被人为破坏，可参考附录 A；
- 应在介质显著位置明显展示收款人信息，便于客户核对信息。

7.8 条码识读与解析

条码识读设备应保证识读结果的保密性，避免条码信息泄露。
条码解析时应满足以下要求：
——应对条码的完整性进行校验；
——应对条码的真实性进行校验；
——应保证条码解析程序自身的健壮性；
——应识别病毒、木马等恶意代码，保障交易的安全性。

7.9 交易验证与确认

交易验证可以组合选用下列三类要素：
——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密码等；
——客户本人生物特征要素，如指纹等。
交易验证要素的使用，应满足以下要求：
——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；
——采用数字证书、电子签名作为验证要素的，数字证书及生成电子签名的过程应符合《中华人民共和国电子签名法》、JR/T 0118 等有关规定，确保数字证书的唯一性、完整性及交易的抗抵赖性；
——采用一次性密码作为验证要素的，应切实防范一次性密码获取端与支付指令发起端为相同物理设备而带来的风险，并将一次性密码有效期严格限制在最短的必要时间内；
——采用客户本人生物特征作为验证要素的，应符合国家、金融行业标准和相关信息安全管理要求，防止被非法存储、复制或重放。
采用付款扫码支付方式时，应满足以下要求：
——应在移动终端展现交易信息，并在界面的显著位置展示收款人信息，便于客户核对；
——应经过客户确认并进行交易验证，交易验证宜同时采用上述三类要素中的两类要素，不足两类的应采取相应的风险补偿措施；
——由付款人发起支付指令，交易信息包含但不限于收款人名称、金额等。
采用收款扫码支付方式时，应满足以下要求：
——应经过客户确认并进行交易验证，交易验证宜同时采用上述三类要素中的两类要素，不足两类的应采取相应的风险补偿措施；
——在移动终端进行交易验证时，应在移动终端上展现交易信息。

7.10 交易风险控制

应采用大数据分析、客户行为建模等手段，建立交易风险监控模型和系统，对异常交易进行及时预警，并采取调查核实、风险提示、延迟结算等处理措施。

针对批量或高频登录等异常行为，应利用IP地址、终端设备标识等信息进行综合识别，及时采取附加验证、拒绝请求等手段。

对于资金类交易等高风险业务，应在确保客户联系方式有效的前提下，及时告知客户其资金变化情况。

应按照7.9条进行交易验证，根据不同风险防范能力设置相应的日累计交易限额。

使用动态条码进行支付的，风险防范能力分级见表1。

表 1　风险防范能力分级表

交易验证方式	风险防范能力
采用包括数字证书或电子签名在内的两类（含）以上有效要素进行验证的（具体要求见 7.9 条）。	A 级
采用不包括数字证书、电子签名在内的两类（含）以上有效要素进行验证的（具体要求见 7.9 条）。	B 级
采用不足两类有效要素进行验证的（具体要求见 7.9 条）。	C 级

使用静态条码进行支付的，风险防范能力为D级。

7.11　交易过程安全

7.11.1　交易报文安全

按照《中国人民银行办公厅关于印发<网络支付报文结构及要素技术规范（V1.0）>的通知》（银办发〔2016〕222号）等相关规定，交易报文安全应满足以下要求：

——应防止对交易的重放攻击；

——应保证交易的抗抵赖性，包括但不限于数字证书、电子签名等技术手段；

——在交易报文传输过程中应使用安全协议保证传输安全；

——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，拒绝不完整的交易请求；

——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；

——应提供用户客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客户身份标识、身份鉴别信息不易被冒用。

7.11.2　风险识别与干预

风险识别与干预应满足以下要求：

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

——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。

7.11.3　交易监控

交易监控应满足以下要求：

——应建立交易监控系统，能够甄别并预警潜在风险的交易，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、查结机制；

——应对监控到的风险交易进行及时分析与处置；

——应建立条码支付的黑白名单验证和管理机制，在黑名单中的应直接拒绝。

7.11.4 客户和商户教育

客户和商户教育应满足以下要求：

——应通过公开渠道向客户提供安全的包含条码支付功能的客户端程序；

——应向客户宣传条码支付的安全知识，提高客户安全防范意识；

——应在支付过程中向客户明确提示相关的安全风险和注意事项；

——应加强对交易密码等信息的保护管理和客户安全教育，提示客户及时修改密码；

——应向商户提示静态条码的风险及防范措施。

附　录　A
（资料性附录）
防伪技术要求

A.1　概述

防伪纸张适用于通用打印机打印，主要用于打印静态条码，粘贴在商户经营场所内进行静态条码展示。

防伪封签单面可粘贴，粘贴后不易脱落，主要用于静态条码展示介质物理防护手段的标记。防伪封签贴在静态条码展示介质物理防护手段开口处，避免后期人为替换静态条码。

防伪纸张和防伪封签采用特种印刷工艺生产，具有易识别、防复制、难伪造、可追溯的特点，便于长期使用和识别。

A.2　防伪技术

防伪纸张的材质为特种防伪纸，防伪封签的材质为特种防伪不干胶纸，应采用防伪技术，具备多种防伪特征，如炫彩动感光变开窗安全线、光彩光变图案、雕刻凹印图案、环形光角变色纤维、有色荧光图案、有色荧光号码等。

A.3　技术要求

A.3.1　规格

防伪纸张宜为矩形，方便打印，中间预留方形静态条码打印区域。

防伪纸张克重宜为100g/m^2～120g/m^2。

防伪封签克重（面纸加底纸）宜为120g/m^2～160g/m^2。

A.3.2　外观质量

表面平整光洁，不得有破损、残缺、卷边、多边、卷角、荷叶边等。

文字图案线条清晰，墨色适当，无模糊、浅花、断线、蹭脏等问题。

开窗安全线开窗规整，不得出现无线、乱线、多根线、翻面线、子母线等。

A.3.3　荧光特征

防伪纸张和防伪封签的荧光特征明显、图案完整、颜色鲜明。

A.3.4　物化耐性

防伪纸张和防伪封签应具有较强的耐酸、耐碱、耐热水、耐光等特性。

参 考 文 献

[1]GB/T 12406—2008　表示货币和资金的代码
[2]GB/T 22080—2016　信息技术　安全技术　信息安全管理体系　要求
[3]GB/T 22081—2016　信息技术　安全技术　信息安全控制实践指南