386--中国人民银行办公厅关于加强条码支付安全管理的通知  
（银办发〔2017〕242号）

中国人民银行上海总部，各分行、营业管理部，各省会（首府）城市中心支行，各副省级城市中心支行；各国有商业银行、股份制商业银行，中国邮政储蓄银行；中国银联股份有限公司，中国支付清算协会，中国互联网金融协会，网联清算有限公司；各非银行支付机构：

为加强条码支付安全管理，切实保障人民群众财产安全和合法权益，现将《条码支付安全技术规范（试行）》（见附件1）和《条码支付受理终端技术规范（试行）》（见附件2）印发给你们，并提出如下工作要求，请一并遵照执行：

一、强化条码支付技术风险防范

各商业银行、非银行支付机构、清算机构要严格落实《条码支付安全技术规范（试行）》，强化条码支付技术风险防范。一是采取安全单元（SE）、支付标记化（Tokenization）、有效期控制、条码防伪识别等手段，保障条码的可靠性和有效性。二是运用交易验证强度与交易额度相匹配的技术措施提高条码支付交易的安全性。三是合理应用大数据分析、用户行为建模等手段建立条码支付风险监控机制，强化条码支付交易风险监测与预警。四是从木马病毒防范、信息加密保护、运行环境可信等方面提升条码支付客户端软件的安全防护能力。

二、推进条码支付受理终端注册管理

各商业银行、非银行支付机构、清算机构要严格落实《条码支付受理终端技术规范（试行）》，加强条码支付受理终端（含扫码设备、显码设备等）技术管理。清算机构应于2018年1月31日前完成条码支付受理终端注册管理、大数据分析校验等平台建设，并启动受理终端注册相关工作。各商业银行、非银行支付机构应积极配合清算机构做好受理终端注册等工作。

三、规范条码支付交易报文管理

各商业银行、非银行支付机构、清算机构要严格落实《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）要求，加强条码支付交易报文管理。一是采用数字签名、加密传输等措施，加强对支付指令真实性管理，防范交易信息被篡改或隐匿。二是在交易报文中准确记录发起方、接收方、网络路由等信息，采用唯一交易流水号、受理终端编码等，保障资金的可追溯性和支付指令的一致性。三是完善付款方、商户、渠道、订单等方面交易信息，精准刻画交易全貌，确保支付指令的完整性。

四、加强条码支付产品质量管理

各商业银行、非银行支付机构、清算机构、行业协会要严格落实《中国人民银行国家认证认可监督管理委员会关于加强支付技术产品标准实施与安全管理的通知》（银发[2017]208号）要求，加强标准落地实施，强化条码支付产品质量和安全管理，健全条码支付风险防控机制，有效提升条码支付产品的技术标准符合性和安全性。

五、加大督导管理力度

人民银行分支机构要统筹做好指导协调、政策宣传、情况通报等工作，对辖区内条码支付技术标准的落地实施情况进行监督，加大条码支付技术管理力度。行业协会要加强条码支付技术风险自律管理，定期向人民银行报送相关情况。

请人民银行上海总部，各分行、营业管理部，各省会（首府）城市中心支行，各副省级城市中心支行及时将本通知转发至辖区内各城市商业银行、农村商业银行、农村合作银行、民营银行、村镇银行、城市信用社、农村信用社和外资银行，加强组织落实

执行中如遇问题，请及时向人民银行报告。

联系人：张宏基　汤沁莹

联系电话：010-66194677　010-66194650

附件：1．条码支付安全技术规范（试行）

2．条码支付受理终端技术规范（试行）

中国人民银行办公厅

2017年12月22日

附件1

**条码支付安全技术规范**

（试行）

2017年12月

目次

1　范围

2　规范性引用文件

3　术语和定义

4　系统安全

5　移动终端安全

6　受理终端安全

7　交易安全

附录A（资料性附录）防伪技术要求

参考文献

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／T22239--2008　信息安全技术　信息系统安全等级保护基本要求

JR／T0118--2015　金融电子认证规范

JR／T0149--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　barcode

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　Iinearbarcode

一维条码　one-dimensionalbarcode

条形码　barcode

宽度不等的多个熙条和空白，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-dimensionalbarcode

二维码two-dimensionalbarcode

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staticbarcode

具有较长时效，可多次重复使用的条码。

3．5　动态条码　dynamicbarcode

通过显码设备展示，并且有较短时效的条码。

3．6　条码支付　barcodepayment

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mobileterminal

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paymenttorminal

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batcodedisplaydevice

具有条码展示功能的专用设备。

3．10　扫码设备barcodereader

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／T22239--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／T22239--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／T22239--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／T22239--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／T22239--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；

--应按照了JR／T0149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／T0118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│

A级

│

│行验证的（具体要求见7．9条）。

　│

　│

├───────────────────────────┼─────────────┤

│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│

B级

│

│进行验证的（具体要求见7．9条）。

│

　│

├───────────────────────────┼─────────────┤

│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／㎡～120g／㎡。

防伪封签克重（面纸加底纸）宜为120g／㎡～160g／㎡。

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／T12406--2008　表示货币和资金的代码

[2]GB／T22080--2016　信息技术　安全技术　信息安全管理体系　要求

[3]GB／T22081--2016　信息技术　安全技术　信息安全控制实践指南

附件2

条码支付受理终端技术规范

（试行）

2017年12月

目次

1　范围

2　规范性引用文件

3　术语和定义

4　显码设备技术要求

5　扫码设备技术要求

6　安全性技术要求

7　适应性技术要求

8　可靠性技术要求

参考文献

1　范围

本规范规定了条码支付涉及到的受理终端在展示、识读、安全保护、适应性和可靠性方面的技术要求。

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受理终端的设计、研发、维护和采购。

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　18030--2005　信息技术　中文编码字符集

GB／T23704--2009　信息技术　自动识别与数据采集技术　二维条码符号印制质量的检验

JR／T0120．1　银行卡受理终端安全规范　第1部分，销售点（POS）终端

JR／T0120．2　银行卡受理终端安全规范　第2部分，受理商户信息系统

JR／T0120．5　银行卡受理终端安全规范　第5部分：PIN输入设备

3　术语和定义

下列术语和定义适用于本文件。

3．1　条码　barcode

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linearbarcode

一维条码one-dimensionalbarcode

条形码barcode

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-dimensicnalbarcode

二维码two-dimensionalcode

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　条码支付　barcodepayment

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。

3．5　受理终端paymentterminal

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。

3．6　显码设备barcodedisplaydevice

具有条码展示功能的专用设备。

3．7　扫码设备barcodereader

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。

3．8　移动终端　mobileterminal

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。

3．9　打印对比度printcontrastsignal

码图（条码符号）中浅色模块反射率（用Rmax表示）、深色模块反射率（用Rmin表示）之差与浅色模块反射率的百分比，用PCS表示。

计算公式：PCS＝[（Rmax-Rmin）／Rmax]×100％

3．10　测试版testchart

由各种码图样本及其它信息构成的测试卡片，包含标准测试版、打印对比度测试版、低品质测试版等。

3．11　标准测试版standardtestchart

由GB／T23704--2009中规定符号等级为“A”的码图样本组成，用于考察产品对标准条码的识读效果。

4　显码设备技术要求

4．1　数据要求

4．1．1　正确性

显码设备的数据正确性应满足以下要求：

--输入数据信息转成一个或多个条码，被识读解码后应完全重现输入数据信息，不得出现任何差异；

--条码的表达应符合相应的国家标准。输入数据信息转成一个或多个条码，被条码识读设备识读后的数据信息应具有唯一性。

4．1．2　规范性

显码设备的数据规范性应满足以下要求：

--输入数据信息，如果包含采用GB18030--2005编码的汉字，且条码码制支持汉字编码类型，应优先采用汉字编码类型表述输入数据信息中的汉字；

--输入数据信息，如果能被条码码制用多种内部数据编码类型表述的，应优先采用最紧凑的数据编码类型表述。输入数据信息可以分段采用不同的内部数据编码类型，实现整体的紧凑表述；

--二维条码纠错等级应选用可恢复码字比例不小于15％的等级；

--在满足上述条件基础上，二维条码应选用最小的符号版本。

4．1．3　码制

条码应使用符合国家标准的码制。

4．2　条码表现要求

4．2．1　外形

显码设备显示的条码外形应满足以下要求：

--应表现在平面介质上，不得扭曲、变形、破坏；

--应完整表现，且条码外围空白区应符合码制要求。

4．2．2　介质

条码可表现在以下介质上：

--主动发光表面介质，包括但不限于液晶显示器（LCD）、发光二极管（LED）屏幕等；

--半主动发光表面介质，包括但不限于光学投影幕墙等；

--被动反射表面介质，包括但不限于电子墨水屏幕等。

4．2．3　颜色

显码设备显示的条码颜色应满足以下要求：

--条码主体应采用黑白或深浅反差尽量大的两种色块表示；

--对于被动反射表面介质，要求PCS值不小于30％。

4．2．4　精度

不同条码表现介质上的精度应满足以下要求：

--对于被动反射表面介质，最高表示精度不应超过0．254mm（10mil）；

--对于主动、半主动发光表面介质，最高表示精度不应超过0．381mm（15mil）。

5　扫码设备技术要求

5．1　数据要求

5．1．1　准确性

扫码设备识读条码应满足以下要求：

--条码支付交易过程一次识读后输出的数据信息，应具有唯一性和可重复性；

--条码的识读解码机制应符合相应的国家标准，输出数据信息的表达应没有歧义。

5．1．2　规范性

扫码设备识读条码后的输出数据信息如果包含汉字，汉字编码字符集应符合GB18030--2005等。

5．2　性能要求

5．2．1　精度

扫码设备识读条码的精度应满足以下要求：

--对于被动反射表面介质，最高识读精度应达到0．254mm（10mil）；

--对于主动、半主动发光表面介质，最高识读精度应达到0．381mm（15mil）。

5．2．2　识读速度

扫码设备识读一个条码的时间应不超过1秒。

5．2．3　出错率

对于识读解码能力范围内的标准测试版，出错率应小于0．01％。

6　安全性技术要求

条码支付受理终端应符合以下安全性技术要求：

--应保证条码识读结果的机密性，避免条码信息泄露。

--应保证条码解析的准确性。

--应保证条码识读解析结果表达的规范性。

--受理终端如果用于个人识别码（PIN）输入相关场景，应具备物理、逻辑安全机制，包括但不限于：

·应具备入侵检测机制；

·应防止PIN输入过程被监听；

·应保证支付敏感信息的安全存储；

·应具备完整的密钥体系；

·在PIN输入设备和非接触式读卡器间传输PIN相关信息时，应采取有效措施保护所传输的数据；

·PIN输入设备应符合JR／T0120．5的要求。

--在条码支付交易过程中，受理终端应符合JR／T0120．1、JR／T0120．2等相关要求；涉及支付敏感信息处理的还应符合《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。

--在条码支付交易过程中，受理终端需要输入身份验证信息的，应对身份验证信息的输入方式、过程及内容具备安全防护机制。

--受理终端应具有唯一标识，唯一标识应以安全方式保护，以保障无法被篡改，如使用安全单元（SE）、可信执行环境（TEE）等；交易报文中应包含受理终端标识，并采取加密绰措施保证在交易过程中不可被篡改。

--应采取技术手段实现条码支付受理终端、通讯网络与商户自身业务系统的隔离。

--应在受理终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。

7　适应性技术要求

7．1　电源适应能力

在额定电压偏差±5％范围内的条件下，受理终端应能正常工作。

7．2　接口

受理终端需要与外部进行数据传输交换的，应支持以下全部或部分类型的接口：

--串行通讯接口（RS232、RS485等）；

--USB接口；

--红外通讯接口；

--以太网通讯接口；

--蓝牙通讯接口；

--无线通讯接口；

--其他。

7．3　环境适应性

7．3．1　气候环境适应性

气候环境适应性应满足表1的要求。

表1　气候环境适应性（略）