Q/CUP

中国银联股份有限公司企业标准

Q/CUP 067—2016

中国银联二维码支付安全规范

Security Specifications for UnionPay Payment using Two-Dimensional Code

2016-12-09 发布　　2016-12-09 实施

中国银联股份有限公司 发布

目　　次

前　言

本规范对二维码支付所涉及的系统、受理终端、移动设备、加密强度等提出安全要求，以保证各机构在推广二维码支付时，能执行统一的安全要求，保障持卡人账户信息安全和敏感数据的安全。

本规范由中国银联股份有限公司提出。

本规范的主要起草单位：中国银联股份有限公司、北京银联金卡科技有限公司。

本规范的主要起草人：宋汉石、鲁志军、李伟、谭颖、汪之婴、周思捷、孙茂增、蒋利兵、魏博锴。

中国银联二维码支付安全规范

1 范围

本要求对二维码支付所涉及设备、相关应用及系统提出安全要求，包括二维码识读设备、二维码显示设备、相关应用软件、二维码支付处理系统、支付服务业务系统等受理各环节。

本要求适用于二维码信息中包含订单和账号等信息的支付场景下所涉及的设备、应用及系统。二维码其他应用，包括但不限于票务类、优惠券类、交易凭证类、机构标识类、商品标识类、防伪标识类的安全要求可依据实际应用安全需求参考本要求相应章节执行，具体不在本要求中规定。

本要求适用于二维码支付的终端生产企业、应用软件开发商及收单机构。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

ISO/IEC 15423 信息技术自动识别和数据采集技术条形码扫描仪和解码器性能测试

AIMC 0001 条码阅读设备通用技术规范

GB/T 18284-2000 中华人民共和国国家标准——快速响应矩阵码

Q/CUP 007 银联卡受理终端安全规范

Q/CUP 056 银联卡支付应用软件安全规范

Q/CUP 058 银联卡密码算法使用与密钥管理规范

Q/CUP 059 银联卡身份识别与认证规范

银联卡收单机构账户信息安全管理标准（银联风管委【2013】9号）

银联卡账户信息与交易数据安全管理规则（银联风管委【2006】6号）

PCAC/T 0001-2016 个人信息保护技术指引

PCAC 0002-2016 条码支付安全技术指引

JR/T 0149-2016 中国金融移动支付 支付标记化技术规范

中国银联支付标记化技术指引

中国人民银行.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）.2016年6月15日

3 术语和定义

下列术语和定义适用于本标准。

3.1 二维码 two-dimensional Code

二维码是在平面上使用若干个与二进制相对应图形的来表示记录数据信息的几何形体。

3.2 应用软件 application software

安装在二维码识读设备和/或显示设备（例如手机或其他设备）上，可完成二维码识读/显示、二维码编/解码和安全传输持卡人授权或结算数据等功能的软件。

3.3 销售点终端 point of sale（POS）

指银联卡受理终端，可安全获取并保护账户信息、验证信息和交易报文，功能应包括：证书及密钥的安全存储，与后台系统之间的认证及建立安全通道，安全读取和加密银行卡信息（包括磁条卡和IC卡），接受用户输入并加密个人标识码（PIN），安全显示交易类型、金额、结果等交易提示信息，以及加密账户信息、计算报文鉴别码（MAC）等。

3.4 二维码识读设备 scanning device of two-dimensional Code

一种完成二维码图像采集和解码的设备，包括但不限于智能移动终端和销售点终端（POS）。可分为被集成于其他设备内和外接于其他设备外等两种。应具备防信息泄漏、防篡改等安全功能。

3.5 个人标识码 personal identification number: PIN

个人标识码是在联机交易中识别持卡人身份合法性的数据信息,在计算机和网络系统中的任何环节都不应以明文方式出现。

3.6 账户信息 account information

账户信息包括银行卡上记录的所有信息和银行卡交易相关的用户身份验证信息。记录在银行卡上的信息包括：银行卡主账号（PAN）、持卡人姓名、磁道信息、有效期、卡片验证码（CVN及CVN2）。与银行卡交易相关的用户身份验证信息包括：个人标识代码（PIN），网上业务、电话银行、手机银行等业务中的用户注册名、真实姓名、身份证件号码、联系方式等。

3.7 支付二维码处理系统 management system for two-dimensional Code

二维码支付的集中管理平台，提供安全的二维码编解码(含二维码有效期管理)、业务分发处理、终端/客户端的管理、权限认证、密钥管理、身份认证等功能。

4 支付二维码体系架构

4.1 支付二维码分类

二维码支付根据持卡人使用二维码的方式，可分为持卡人主动和持卡人被动两种模式。其中：持卡人主动模式指持卡人使用手机等智能终端作为二维码识读设备读取目标设备上的二维码信息并完成支付的模式，本要求中主要指被扫二维码信息中包含订单信息等内容；持卡人被动模式指柜员等商户人员使用专用二维码识读设备读取持卡人手机等智能终端上的二维码并完成支付的模式,本要求中主要指二维码信息中包含银行卡等账户信息等内容。

4.2 体系架构

本要求所述二维码支付体系架构如图1。

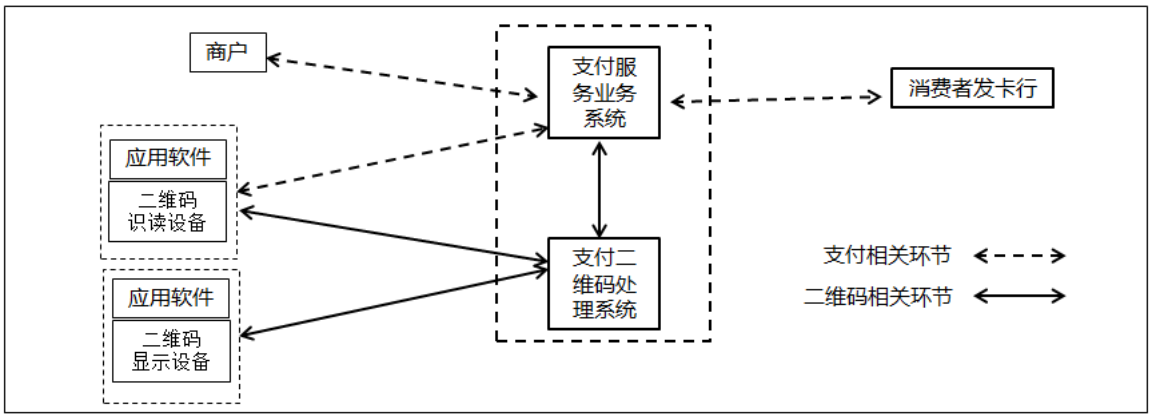

图1 二维码支付系统架构

——应用软件：见3.2。

——二维码识读设备：见3.4。

——二维码显示设备：能正确安全显示二维码支付的设备。

——支付二维码处理系统：见3.7。

——支付服务业务系统：指实际完成二维码支付的业务平台，实现对应的业务处理逻辑。

5 安全目标

通过业务的安全开通、二维码中信息不被泄露和篡改、安全的信息传输、安全的支付过程等多方面的安全目标来保证个人、商户/机构信息及支付交易的安全。

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，确保二维码支付业务设施的安全、稳定和高效运行。

5.1 业务开通安全

二维码支付业务开通环节应确保用户账户及个人资料不被泄露。

5.2 二维码信息安全

——含有账户信息的二维码应防重放；

——应确保账户信息不被泄露；

——数据解析过程应对二维码中数据信息的完整性、真实性、不可抵赖性及时效性进行鉴别，对于未通过鉴别等非法二维码应予以阻止。

5.3 账户信息安全

——账户信息不应在任何设备和系统中存储；

——账户信息只可用于完成当前合法交易，不应用于任何其他用途，且应采用支付标记化技术对银行卡卡号、卡片验证码、支付机构支付账户等信息进行脱敏处理，采取技术手段从源头控制信息泄露和欺诈交易风险；

——账户信息应按照PCAC/T 0001：2016的要求进行保护，根据自身业务范围、安全管理要求和客户服务要求确定条码支付交易中的敏感信息范围，高敏感级别信息宜包括静态密码、动态密码等，中敏感级别信息宜包括银行卡号、身份证号、护照号、手机号等，低敏感级别宜包括姓名、地址、邮箱、交易信息等；其采集、展示、存储、传输、使用等环节应符合PCAC/T 0001：2016的要求。

5.4 传输信息安全

公网环境下，二维码信息不应以明文形式传输，在传输过程中不被泄露、窃取和篡改。

5.5 支付过程安全

二维码支付过程相关设备及系统应保证支付过程的安全，包括但不限于真实性、不可抵赖性等。

6 安全功能和实施要求

6.1 二维码数据生成/解析安全要求

——二维码应用于支付环节时应包含可供验证二维码来源合法性的信息，可采用包括但不限于数字签名、合法来源白名单等机制。解码时，应根据对应机制验证二维码来源合法性，确保二维码中不含有木马、病毒和非法链接等有害信息，并应对非法二维码予以明确提示后拒绝交易；

——二维码中的账户信息应采用Token技术或加密方式进行数据处理，其中：加解密算法及密钥应满足《银联卡密码算法使用与密钥管理规范》；

——二维码中的账户信息应防重放，可采用包括但不限于时效性、动态生成等机制；

——二维码数据解析时应验证二维码所包含信息的有效性、合法性及真实性，并确保账户信息和用户私密信息（例如证件信息等）不被泄露及明文存储。

6.2 传输安全要求

在易被攻击的网络上传输账户信息时应进行数据加密处理，包括但不限于以下要求：

——应使用强壮的加密算法和安全协议，例如传输层安全（TLS 1.0或以上版本）和IP安全协议（IPSEC）来保护账户信息在开放/公共的网络（例如：Internet、全球移动通讯系统GSM、第三代无线通信网络3G等）上的传输。

6.3 用户安全鉴别要求

——二维码支付业务的使用者应具备唯一的身份标识，保证对二维码支付的操作能够被追溯到用户；

——用户身份识别和认证应符合《银联卡身份识别与认证规范》；

——PIN输入设备安全应符合《银联卡受理终端安全规范 第6部分 PIN输入设备安全规范》；

——应严格限制使用初始密码，对密码复杂度进行校验，避免采用简单密码或与客户个人信息相似度过高的密码。

6.4 应用软件安全要求

——二维码生成/解析安全要求见6.1节；

——应用软件与后台处理系统间数据传输安全要求参见6.2节；

——应具有扫恶意代码（启动木马、转恶意网址等）不跳转或不启动恶意软件等功能；

——应用软件程序应从木马病毒防范、信息加密保护、运行环境可信等方面提升安全防控能力；

——应用软件中实现支付功能的部分应符合《银联卡支付应用软件安全规范》（Q/CUP 056）；

——二维码支付相关证书存储及管理应满足《银联卡身份识别与认证规范 第1部分：数字证书应用安全规范》；

——二维码支付指令验证应满足《银联卡身份识别与认证规范第2部分：静态与动态口令应用安全要求》；

——交易过程中，应提供安全提示机制，确保交易过程中关键环节（如：交易金额及交易类型确认，密码输入等）及交易结果能安全、有效向用户提示，用户确认后才可进行下一步操作；

——应用软件程序应具有抗逆向分析、抗反汇编等安全性防护措施，防范攻击者对客户端程序的调试、分析和篡改；

——应用软件程序的临时文件中不应出现账户信息，临时文件包括但不限于Cookies；

——应用软件程序应禁止在身份认证结束后明文存储账户信息，防止账户信息泄露；

——应用软件程序应在可信运行环境中执行；

——应用软件程序应能检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；

——应用软件程序应经过外部合规评估。

6.5 二维码识读/显示设备安全要求

——二维码生成/解析安全要求见6.1节；

——二维码识读/显示设备与后台处理系统间数据传输安全要求参见6.2节；

——二维码识读和显示设备中固件和应用程序安全要求参见6.4节；

——专用二维码识读设备安全要求应满足《银联卡受理终端安全规范 第1部分 销售点（POS）终端安全技术规范》；

——二维码识读设备和系统应能抵御重放攻击，防止加密数据和交易报文被重用；

——二维码识读设备固件和应用程序应由收单机构或其授权的生产、维护企业进行签名，设备应对下载的程序文件签名进行合法性验证；

——受理终端应具备唯一的标识编码，能够通过标识编码追溯到参与交易的受理终端设备。交易报文中应包含受理终端标识编码，并采用技术加密措施和管理措施保证终端标识编码在交易过程中不可被篡改；

——机构应具备相应的终端验证平台，能够根据终端安全编号校验终端的合规性。

6.6 支付二维码处理系统安全要求

——二维码生成/解析安全要求参见6.1节；

——系统传输安全要求参见6.2节；

——系统应符合《银联卡收单机构账户信息安全管理标准》（银联风管委【2013】9号）和《银联卡账户信息与交易数据安全管理规则》（银联风管委【2006】6号）；

——系统的信息系统安全保护等级应为三级或以上；

——应符合人民银行非金融支付机构支付服务业务系统检测要求；

——系统不应留存支付敏感信息；

——系统应通过加密技术，保障敏感信息传输及使用安全；

——应以安全形态（加密）存储用户登录凭证，防止其被破解或被重放攻击。

6.7 其他安全要求

——客户端程序发行单位应能识别本单位发行的客户端程序；

——特约商户签约单位应能识别本单位特约商户受理终端，且交易上送的相关信息中应包括受理终端（网络支付接口）类型和代码；

——应定期开展敏感信息安全的内部审计。