附件 1

银联卡支付信息安全管理标准

（2018 年中国银联风险管理委员会会议审议通过）

第一章　总则

1.1　目的

为加强银联卡支付信息安全管理，进一步明确和细化各业务参与方支付信息安全管理要求，防范支付信息泄漏风险，根据《银联卡账户信息与交易数据安全管理规则》，特制定本标准。

1.2　适用范围

本标准适用于基于银联卡开展支付业务的主体及为支付业务主体提供相关服务的机构，包括但不限于:

1.2.1　直接参与方

是指直接参与支付业务的主体，包括但不限于银联卡发卡机构、基于银联卡的支付账户发行方[1]、涉及银联卡交易的银行卡清算机构、从事银联卡收单业务的收单机构、银联卡收单特约商户、基于银联卡的二维码应用服务方等。

1.2.2　间接参与方

是指向支付业务直接参与方提供专业化服务的机构，包括但不限于银联卡卡片生产厂商、聚合技术服务商、托管服务提供商[2]、受理终端厂商、软件供应商及其他专业化服务机

1 是指根据客户的真实意愿为其开立支付账户、通过绑定或关联银联卡等方式实现支付功能的获得互联网支付业务许可的支付机构。

2 本标准所指的托管服务提供商是向支付业务直接参与方提供数据中心托管（含云服务）、安全托管、呼叫中心托管等服务，可能影响银联卡支付信息安全的机构。

构。

对于上述机构，只要业务涉及银联卡卡号的采集、传输、处理、存储，均适用本标准。

第二章　基本要求

2.1　支付信息定义

支付信息是指银联卡上记录的账户信息、基于银联卡开展支付业务的网络支付账户信息、身份鉴别信息、支付业务涉及的必要个人信息和其他支付相关信息。包括但不限于:

2.1.1 银联卡上记录的账户信息

包括银联卡卡号、卡片有效期、磁道信息（含芯片等效磁道信息）、卡片验证码（CVN 及 CVN2）等，以及基于上述信息产生的支付标记。

2.1.2 基于银联卡开展支付业务的网络支付账户信息

包括网络支付账户、用户注册名、用户登录名、用户 ID 等，以及基于上述信息的支付标记。

2.1.3 身份鉴别信息

包括个人标识代码(PIN)，网络支付业务中的登录密码、手势密码、查询密码、支付密码、动态口令、短信验证码、密码提示问题答案，指纹、虹膜、人脸等个人生物特征信息，预付卡支付密码等。

2.1.4 支付业务涉及的必要个人信息

包括但不限于姓名、身份证和护照等证件类识别标识、手机号码、固定电话号码、电子邮箱、工作及家庭地址以及支付业务中采集或产生的其他个人信息。

2.1.5 其他支付相关信息

机构或商户名称、机构或商户编码、批量制卡文件、加密密钥、终端编码、终端序列号、设备标识、支付应用软件标识、IP 地址、交易位置信息等。

2.2 支付信息分级

按照支付信息对完成支付交易和信息主体资金安全的影响程度，分为敏感支付信息、重要支付信息和一般支付信息。

2.2.1 敏感支付信息

指作为支付要素能够直接完成交易，且一旦泄漏将对信息主体的资金安全造成严重影响的支付信息，包括但不限于卡片有效期、磁道信息（含芯片等效磁道信息）、卡片验证码（CVN 及 CVN2）、个人标识代码（PIN）、网络支付密码、预付卡支付密码以及用于身份鉴别的个人生物特征信息。

2.2.2 重要支付信息

指通过关联其他支付要素会对完成交易或信息主体的资金安全造成一定影响的支付信息，包括但不限于银联卡卡号、支付标记、网络支付业务中的支付账户、登录密码和查询密码、证件类识别标识、手机号码、固定电话号码、动态口令、短信验证码、密码提示问题答案、批量制卡文件、加密密钥、设备标识、IP 地址、交易位置信息以及其他可能对完成交易造成一定影响的个人信息。

2.2.3 一般支付信息

指对完成交易或信息主体的资金安全影响较小或无影响的支付信息，包括但不限于网络支付用户注册名和登录名、用户 ID、姓名、电子邮箱、工作及家庭地址、终端编码、终端序列号、支付应用软件标识以及支付业务中采集或产生的

其他个人信息。

2.3 支付信息保护基本要求

根据“业务必须”、“最小化”和“明示同意”原则，严格控制支付信息的采集、存储和使用。

2.3.1 敏感支付信息保护

2.3.1.1 不得在受理终端、支付应用软件、应用系统、日志文件等存储非本机构的敏感支付信息。

2.3.1.2 敏感支付信息仅用于完成银联卡交易，不得用于除此之外的任何其他用途。

2.3.2 重要支付信息保护

2.3.2.1 严格控制卡号、证件类识别标识、手机号码等重要支付信息的使用和存储。

2.3.2.2 重要支付信息的使用和存储仅限以下业务需要：业务处理，清分与清算，差错处理，业务对账，交易查询与分析，案件协查，风险管理与监控，以及根据法律法规要求使用和存储的业务场景。

2.3.3 一般支付信息保护

一般支付信息的采集、存储和使用应获得信息主体明示同意，并严格控制在信息主体授权的范围内。

第三章 组织管理

3.1 组织架构

3.1.1 设置支付信息安全管理委员会

3.1.1.1 应设置支付信息安全管理委员会，委员会成员应至少涵盖本机构研发、测试、运维、风控、清算等与支付信息安全管理相关部门和具体负责人。

3.1.1.2 支付信息安全管理委员会职责应包括但不限于：规划和建设支付信息安全管理机制、审批支付信息安全管理制度和流程、管理支付信息安全管理岗位职责和权限、推动支付信息安全管理制度落实、统筹支付信息安全事件应急处理。

3.1.2 明确支付信息安全责任人

3.1.2.1 应通过正式书面授权指定支付信息安全责任人。

3.1.2.2 支付信息安全责任人职责应包括但不限于：统筹支付信息安全合规评估工作，开展支付信息安全事件先期处理、后续跟踪和损失处理等，配合相关调查和评估鉴定。

3.1.3 设置支付信息安全管理岗位

应设置支付信息安全管理岗位，其职责包括但不限于：制订和维护支付信息安全管理制度与流程、对本机构银联卡支付信息的使用进行管理监督及内部审计、对外部合作方[3]和服务提供商[4]的支付信息安全管理进行监督、对银联卡支付信息安全事件进行分析处理。

3.2 人员管理

3.2.1 人员录用

3.2.1.1 录用员工之前，需进行必要的背景调查，包括但不限于犯罪记录、简历核实、专业资格等，确保员工未从事或参与过危害持卡人支付信息安全或其他信息泄漏事件。

3.2.1.2 应与所有可访问支付信息的员工签署保密协议，或在劳动合同中设置保密条款。

3.2.1.3 应与所有可访问支付信息的员工签订支付信息

3 外部合作方是指与本机构开展支付业务合作的直接参与方。

4 服务提供商是指为本机构提供支付业务相关服务的间接参与方。

安全责任承诺书。承诺书至少应包含员工岗位的支付信息安全责任、义务及相关惩罚措施等内容。

3.2.2 人员培训

3.2.2.1 员工上岗前应及时安排其参加支付信息安全培训，培训内容包括但不限于支付信息安全管理制度、管理规定及操作流程、支付信息安全意识等相关内容，并保留原始培训记录。

3.2.2.2 应至少每年开展一次支付信息安全相关的培训或宣贯，提升员工的银联卡支付信息安全防护意识和技能，确保员工了解各自岗位职责、本岗位可访问支付信息的安全等级，以及违反安全规定可能导致的后果及惩罚措施，并保留相关记录至少 2 年。

3.2.3 人员转岗或离职

3.2.3.1 员工岗位调动或离职时，应立即变更、冻结或删除离岗员工对支付信息所有访问权限。

3.2.3.2 员工岗位调动或离职时，应立即取回相关身份证件、钥匙等物品以及机构提供的软硬件设备。

3.2.3.3 员工岗位调动或离职时，应办理严格的调离手续，并要求其履行保密义务。

3.2.4 违规人员管理

应对违反支付信息安全管理规定并造成敏感支付信息泄漏事件的员工进行处罚，情节严重的应向相关监管部门报送违规员工个人信息并标明报送原因；涉嫌违法犯罪的，应及时报告公安机关。

3.2.5 外部人员管理

3.2.5.1 外部人员物理访问受控区域前，应先提出书面

申请，批准后由专人全程陪同，并登记备案。

3.2.5.2 应采取有效措施（如临时工牌等），识别和区分外部人员和内部员工。

3.2.5.3 外部人员离场时，应及时回收临时工牌或其他类似凭证。

3.2.5.4 外部人员接入网络访问系统前，应先提出书面申请，批准后由专人开设账号、分配权限，并登记备案。

3.2.5.5 外部人员完成系统访问后，应及时终止其所有的访问权限并删除相应账号。

3.2.5.6 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得非授权获取和变更支付信息。

3.3 岗位权限管理

应严格执行支付信息安全相关的权限管理，确保支付信息安全核心工作落实到岗位，责任落实到人。包括但不限于:

3.3.1 管理和控制对支付信息的访问权限;

3.3.2 监控所有对机构内部支付信息的访问活动;

3.3.3 检查和监督支付信息安全管理规定的落实;

3.3.4 及时处理突发支付信息安全事件等。

第四章 安全管理策略

4.1 安全管理策略制定与发布

4.1.1 应根据本标准中的各项规定，提出支付信息安全管理策略，包括建立支付信息安全日常管理及操作流程、内部检查及监督、应急处理流程和预案等内部控制建设策略，以及有效的外部风险防范策略。

4.1.2 支付信息安全策略应处于受控状态并通过正式流

程予以有效发布并实施。

4.2 内控制度建设策略

应根据本标准中的各项规定，建立支付信息安全管理制度体系，以明确支付信息安全管理工作职责、规范相关工作流程。各机构支付信息安全管理制度体系的管理范畴应涵盖本机构、外部合作方、服务提供商等。

4.2.1 建立支付信息安全日常管理及操作流程

4.2.1.1 应对支付信息的采集、传输、存储、使用、销毁等环节提出具体安全管理工作要求。

4.2.1.2 明确各岗位在支付信息安全管理方面的操作流程。

4.2.2 建立支付信息安全内部检查及监督机制

建立支付信息安全内部检查机制和工作流程，及时发现管理漏洞，确保支付信息安全。包括但不限于:

4.2.2.1 建立支付信息安全日常检查机制和工作流程;

4.2.2.2 定期评估支付信息安全管理方面存在的不足;

4.2.2.3 根据安全管理实际，及时对检查机制和工作流程进行调整。

4.2.2.4 建立内部日常管理监督机制（如用户登录日志及操作日志审核），确保落实支付信息安全管理的各项要求。

4.2.3 建立应急处理流程和预案

4.2.3.1 应建立支付信息安全事件应急处理流程和典型场景的有效应急预案。

4.2.3.2 每年至少进行一次应急演练，对应急演练中暴露出来的问题及时进行总结和整改，并保留相关演练记录。

4.3 外部风险防范策略

对于涉及支付信息处理的外部合作方及服务提供商，应建立支付信息安全管理机制，明确其支付信息保护要求及责任，防范因外部因素引发的支付信息泄漏风险。包括但不限于:

4.3.1 在建立合作关系前应考察其支付信息安全管理能力，要求其提供遵从本标准的证明材料，并保留相关记录;

4.3.2 在合作协议或合同中要求其持续遵从本标准，并明确其应承担的支付信息安全管理责任;

4.3.3 发生支付信息泄漏事件后，协调其配合监管部门或中国银联风险管理委员会授权的第三方专业化检测机构开展泄漏原因及范围调查。

第五章　支付信息访问控制管理

5.1　基本要求

5.1.1 权限管理

5.1.1.1 根据“业务必须”和“最小化”原则，严格控制访问和使用支付信息，任何人都只能访问其开展业务所必需的支付信息，且只能够获得访问支付信息所必要的最小权限。防止未经授权擅自对支付信息进行查看、篡改和破坏。

5.1.1.2 应根据“双人控制”原则，对敏感支付信息的访问权限进行分配。

5.1.1.3 涉及支付信息处理的系统，其默认用户权限应为“拒绝所有访问”。

5.1.2 身份验证

5.1.2.1 应至少采用下列一种因素验证访问支付信息的人员身份:

根据用户知道的身份证明信息进行身份验证（如登录密码等）;

根据用户持有的身份证明信息进行身份验证（如智能卡、动态口令（OTP）、短信验证码等）;

根据用户特有的身份证明信息进行身份验证（如指纹等个人生物特征信息）。

5.1.2.2 通过远程方式访问支付信息，应至少采用双因素验证。

5.2 访问控制要求

5.2.1 用户账号管理

用户账号包括但不限于涉及支付信息处理的应用系统的用户名、远程访问支付信息时相关 VPN 登录名等。

5.2.1.1 应建立用户账号管理制度，明确用户账号创建、修改、冻结、解冻、删除的审批、操作等流程的管理要求。

5.2.1.2 应分配唯一的用户账号给每个有权访问支付信息的系统用户。

5.2.1.3 在添加、修改、删除用户账号或操作权限前，应履行严格的审批手续。

5.2.1.4 对于连续 90 天未使用的账号，应删除该账号或冻结其权限。

5.2.1.5 用户间不得共用同一个访问账号。

5.2.1.6 立即清除过期用户账号（包含超过允许使用期限的账号、已经使用完成的开发/测试账号等）及访问权限。

5.2.2 用户密码管理

应对可访问支付信息的应用系统用户密码管理采取下列措施，降低用户密码遭窃取或泄漏的风险:

5.2.2.1 应对不同用户账号设置不同的初始密码;

5.2.2.2 用户首次登录系统时，应强制要求其更改初始密码，且更改后密码不得与最近四次密码相同;

5.2.2.3 用户密码长度不得少于 8 位，应由至少包括数字和字符的组合共同组成，不得设置简单密码;

5.2.2.4 系统应强制要求用户每 90 天至少更改一次登录密码，否则应予以登录限制;

5.2.2.5 应对密码进行加密保护，密码明文不得以任何形式出现;

5.2.2.6 修改或重置用户密码前必须对用户身份进行验证核实。

5.2.3 系统登录控制

5.2.3.1 对于可访问和处理支付信息的系统应启用系统登录控制，连续输错登录密码应对账户进行锁定，锁定时间应不低于 30 分钟或直至管理员予以解锁，连续尝试次数应不超过 6 次;

5.2.3.2 对于可访问和处理支付信息的系统，会话处于非活跃状态应及时结束会话自动退出，非活跃状态持续时间不应超过 15 分钟;

5.2.3.3 对于可访问和处理支付信息的系统，应启用单个账户并发登录控制。

5.3 远程访问控制

应严格控制通过远程网络对涉及支付信息处理的系统或设备进行访问,如确因业务需要而开放此功能的，应符合如下要求:

5.3.1 严格限制远程登录操作业务范围,实施严格的审

批程序，对超出业务范围的操作请求应予以拒绝;

5.3.2 加强对远程网络接入设备的管理，对接入设备进行限制，仅允许指定的设备接入;

5.3.3 仅在访问开始前激活远程登录端口或连接，访问结束后应及时关闭;

5.3.4 在进行远程登录操作时，不得将支付信息通过远程网络存储到本地硬盘及其他外部存储介质;

5.3.5 远程登录操作应采取加密措施或通过安全加密通道进行，防止身份鉴别信息在网络传输过程中被窃听;

5.3.6 建立远程登录操作监控和记录，至少包括：登录及操作时间、IP 地址、远程访问人员、工作内容、操作结果、持续时间，必要时由监督人签字确认。

5.4 无线和移动网络访问控制

业务过程中若使用无线或移动网络，应采取有效措施确保其安全性:

5.4.1 在网络拓扑图中明确标识出使用环境及节点;

5.4.2 无线和移动网络与生产网络之间部署防火墙，并开启有效的访问控制策略;

5.4.3 无线和移动设备的初始默认配置必须进行修改;

5.4.4 确保无法通过无线或移动设备以非授权方式直接访问处理、存储支付信息的生产系统。

5.5 用户配置文件管理

5.5.1 应严格管理记录有系统用户登录或注册信息控制参数的配置文件。

5.5.2 应有效控制配置文件的访问权限，除系统管理员外，不得向其他系统用户开放对配置文件的访问权限。

5.6 日志管理

5.6.1 系统应对所有用户访问支付信息等行为进行日志记录。

5.6.2 系统应对用户账号(包括具有 root 权限或管理员权限的账号）创建、删除、权限变更等操作进行日志记录。

5.6.3 系统应记录所有对日志文件的访问及对日志初始化、关闭或暂停等操作行为。采取有效措施（如部署日志监控软件、远程日志服务器等），防止日志被非法篡改或删除。

5.6.4 日志记录内容至少应包括用户 ID 或登录名、操作日期及时间、操作内容、操作是否成功等。

5.6.5 所有重要系统时钟时间应保持同步，以真实记录系统访问及操作情况。

5.6.6 日志记录应至少保存一年。

5.7 日志审计

5.7.1 应建立日志审计机制。

5.7.2 日志审计内容应包括但不限于:

所有执行安全功能的设备日志（如防火墙、IDS/IPS）以及安全事件;

所有用户访问支付信息的行为记录;

所有涉及支付信息处理系统的日志记录。

5.7.3 应每年至少对日志记录进行一次审计，将审计结果及时向本机构支付信息安全管理委员会或支付信息安全责任人进行报告，并妥善保管审计结果等记录文件。

5.8 数据库访问控制

5.8.1 仅允许数据库管理员直接访问或查询数据库。

5.8.2 其他用户对数据库的访问或查询应通过应用程序

完成。

5.8.3 应能够识别应用程序的数据库访问账号,并确保访问账号仅由这些应用程序使用。

第六章　支付信息生命周期安全管理

6.1　支付信息采集

6.1.1 支付信息生成

6.1.1.1　制卡文件要求

应保证制卡文件生成、存储、传输的安全，制卡文件使用完毕后应进行安全清除。

应设定制卡文件保存期限，定期检查并及时清除超过保存期限的制卡数据。

6.1.1.2　网络支付业务开通要求

通过绑定银联卡开通网络支付业务时，应对银联卡卡号、卡片验证码、卡片有效期等支付信息进行脱敏，支持基于支付标记化技术的交易处理，从源头控制信息泄漏风险。

二维码等条码生成时应不包含任何敏感支付信息并对生成的动态条码信息设置有效时限。

6.1.2 支付信息采集基本要求

6.1.2.1 采集支付信息应遵循“业务必须”和“最小化”原则，不得收集与所提供服务无关的支付信息。

6.1.2.2 采集支付信息必须经信息主体明示同意，并确保所采集信息来源的可追溯性。

6.1.3 受理终端采集敏感支付信息

6.1.3.1 商户终端、公共自助终端等受理终端应配备经银联技术安全认证的专用密码键盘对个人标识代码（PIN）

进行硬加密。

6.1.3.2 前置系统、主机系统应配备硬件加密机对个人标识代码（PIN）信息进行加密保护。

6.1.3.3 对个人标识代码（PIN）应采用双倍长密钥算法或等效安全强度的密钥算法加密保护。

6.1.3.4 从受理终端（包括但不限于个人支付终端、公共自助终端、商户终端）采集磁道信息（含芯片等效磁道信息）时应进行加密保护，包括但不限于使用加密芯片实现硬加密。

6.1.4 网络支付业务采集敏感支付信息

6.1.4.1 开展网络支付业务时，不得委托或授权无支付业务资质的外部合作方及服务提供商采集敏感支付信息。

6.1.4.2 通过互联网、移动设备、固定电话等支付渠道输入卡片有效期、CVN2、个人标识代码（PIN）、网络支付密码等敏感支付信息时，应通过强效加密等技术措施进行保护，包括但不限于使用安全控件、密码软键盘等。

6.1.4.3 应采取有效措施防止外部合作方及服务提供商获取、留存敏感支付信息。

6.2 支付信息传输

6.2.1 ATM 及 POS 交易报文安全要求

6.2.1.1 为保障交易报文信息的唯一性和可追溯性，对于 ATM 终端，各商业银行要在交易报文中包含终端编码。

6.2.1.2 为保障交易报文信息的唯一性和可追溯性，对于 POS 终端（含连接扫码设备的 POS 终端），各收单机构应在交易报文中包含受理机构编码、商户编码、终端编码、终端序列号、终端应用版本编号等信息。

6.2.2 网络支付交易报文安全要求

6.2.2.1 网络支付交易报文应包含设备标识[5]、IP 地址[6]、手机号码[7]、账户 ID（或哈希值）[8]，以保证交易报文的必要完整性。

6.2.2.2 网络支付交易报文应同时满足以下安全要求:

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;

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。

6.2.3 传输加密

6.2.3.1 在公共、开放网络上传输支付信息时，应对支付信息进行加密或通过加密通道传输。

6.2.3.2 采用加密通道传输时应符合以下要求:

使用强壮的安全协议，例如使用安全套接字层（SSL）或传输层安全（TLS）、互联网协议安全（IPSec）等。使用 SSL/TLS 协议时，应使用安全的版本，取消对存在安全隐患版本以及弱加密套件的支持。安全协议所使用密码算法应符合国家密码管理部门相关密码管理要求。

6.2.3.3 禁止通过未加密的电子邮件、即时通信工具等终端用户通讯方式，以及通过 FTP 等未加密的网络协议，传

5 参照相应规范采集能够有效识别设备的编码信息，可实现跨行共享，包括安卓设备的 IMEI、IOS 设备的 IDFV 以及 PC 设备的硬盘序列号。

6 IP 地址不能为内网 IP 地址或服务器 IP 地址，必须包含交易发起的源 IP 地址。

7 是指持卡人在发卡机构预留的手机号码。

8 根据不同业务情形是否具备手机号码和账户 ID，确定是否在交易报文中上送。

输未加密的卡号等支付信息。

6.2.4 跨境传输要求

因业务需要，确需向境外提供支付信息的，应符合国家法律法规和相关标准要求并进行安全评估，同时通过业务规则及协议等有效措施，要求境外的信息接收机构为所获得的支付信息保密。

6.3 支付信息存储

6.3.1 基本要求

6.3.1.1 境内开展支付业务、提供支付业务相关服务过程中，采集或产生的支付信息应在境内存储。

6.3.1.2 所有存储支付信息的系统、设备、介质必须使用物理安全保护措施，禁止未授权访问、读取、打印、截屏、复印、扫描等行为。

6.3.1.3 备份支付信息的介质必须保存在安全的位置，每年至少检查一次备份介质的安全性、完整性和可用性。

6.3.2 敏感支付信息存储要求

6.3.2.1 不得记录或存储非本机构的敏感支付信息，包括但不限于以下位置:

涉及支付信息处理的应用系统;

受理终端、支付应用软件、Web 应用等到服务器之间以及服务器与服务器之间的通信日志;

交易记录表、银行卡绑定关系表等数据库表。

6.3.2.2 对于本机构的敏感支付信息，应进行强效加密后存储，防范明文泄漏的风险。

6.3.2.3 个人生物特征信息应存储在本地安全环境范围内，存储时应采用技术措施处理后再进行存储，如仅存储个

人生物特征信息的摘要。

6.3.3 重要支付信息存储要求

6.3.3.1 当两种或两种以上重要支付信息组合、重要支付信息与一般支付信息组合构成交易授权的完整要素时，如银联卡卡号与证件类识别标识、手机号码的组合，应对系统中存储的以上全部或部分信息采取加密或屏蔽等措施。

6.3.3.2 登录密码、查询密码等密码类信息，应进行强效加密后存储，防范明文泄漏的风险。

6.4 支付信息使用

6.4.1 基本要求

6.4.1.1 使用支付信息时，不得超出已征得信息主体明示同意的使用范围。

6.4.1.2 因业务需要，确需超出上述使用范围使用支付信息的，应再次征得信息主体的明示同意。

6.4.2 生产数据使用管理

6.4.2.1 应遵循 “业务必须”及“最小化”原则，建立并实施生产数据提取和使用管理制度，按敏感程度明确支付信息分类、审批和记录机制。

6.4.2.2 为解决特定问题必须提取生产数据时，应提取必要范围的最小量数据，并对数据进行脱敏。

6.4.2.3 提取的数据应存储在指定的安全区域，并采取加密等必要措施进行保护。

6.4.2.4 在使用完毕后应立即按支付信息销毁流程安全清除。

6.4.3 开发测试时支付信息使用要求

6.4.3.1 采用专门用于测试的测试卡片进行开发测试，

真实支付信息不得用于开发测试。

6.4.3.2 严格分离开发环境、测试环境与生产环境。测试环境必须与外部网络物理隔离，否则必须配置防火墙，并开启有效的访问控制策略。

6.4.3.3 系统开发人员与运行维护人员之间禁止相互兼职或兼岗。

6.4.4 支付信息显示要求

在商户终端、公共自助终端等银联卡受理终端打印的交易凭条，以及网页、移动通讯设备或电子邮件中显示支付信息时，应遵循以下要求:

6.4.4.1 ATM 的打印凭条应遵循以下原则: 除吞没卡、转账交易的转入卡号之外，其他交易凭条所打印的卡号应至少隐去卡号校验位前 4 位的数字; 不得打印卡片有效期。

6.4.4.2 POS 及商户自助终端打印凭条应遵循以下原则: 除预授权交易外，其他交易打印凭条不得打印卡片有效期，打印的卡号应至少隐去除卡号前 6 位和最后 4 位的其他位数。

6.4.4.3 网页、移动通讯设备或电子邮件中显示卡号信息时应至少隐去除卡号前 6 位和最后 4 位的其他位数。

6.4.4.4 通过互联网、移动设备等渠道采集个人标识代码（PIN)、网络支付密码、登录密码等支付信息时，应采取屏蔽措施，确保支付信息不以明文形式显示。

6.4.4.5 对上述屏蔽的信息使用相同位数的同一特殊字符（*或#等）进行替换。

6.5 支付信息销毁

6.5.1 销毁登记制度

对于下列情形中超出使用期限，或已经使用完毕的支付

信息，均应建立严格的销毁登记制度:

因业务需要存储的已超出使用期限的卡号、证件类识别标识、手机号等支付信息;

报废设备或介质中存储的支付信息;

其他超过保存期限需销毁的支付信息。

6.5.2 支付信息的销毁要求

6.5.2.1 对于所有需销毁的支付信息，应在监督员在场情况下，及时妥善销毁，系统定期自动销毁的除外。

6.5.2.2 对于不同类别支付信息的销毁，应分别建立销毁登记记录，销毁记录至少应包括：使用人、用途、销毁方式与时间、销毁人签字、监督人签字等内容；对于系统定期自动销毁的信息，应通过系统日志等方式建立销毁记录。

6.5.2.3 不应只采用删除索引、删除文件系统的方式销毁设备或介质中存储的支付信息：相关设备或介质如还需继续使用，在被分配给其他使用者之前，应通过多次覆写方式安全地擦除信息，保证支付信息被删除或销毁后不能再被恢复或者以其它形式加以利用；相关设备或介质如不再使用，销毁时应采用不可恢复的方式，如消磁、焚烧、粉碎等。

6.5.2.4 对于存储在个人终端上的支付信息，当终端不再使用支付信息或信息主体主动要求删除时，除明确提示并征得信息主体明示同意的信息外，其他支付信息应通过卸载时随即删除、远程擦除等手段进行销毁，服务器端存储的支付信息也应删除。

6.6 密钥安全管理

6.6.1 管理制度

6.6.1.1 应制定完善的密钥管理制度，对各类密钥生成、

注入和启用、传输、保管、泄漏与重置、删除与销毁等生命周期流程制定专门的操作规程。

6.6.1.2 建立并履行严格的操作审批手续和登记制度。

6.6.2 密码算法

应根据业务和安全需要，选择安全的密码算法和密钥长度，所使用密码算法应符合国家密码管理部门相关密码管理要求。

6.6.3 加密设备

6.6.3.1 硬件加密设备应采用双机热备，避免单机故障造成密钥丢失，影响正常交易。

6.6.3.2 硬件加密设备应存放在带锁机柜中，机柜背板应固定，安放在严格进出管理的机房内。

6.6.3.3 应配备摄像系统监控对硬件加密设备的操作，但不得监控到注入内容。

6.6.3.4 硬件加密设备的上线、下线应有严格的审批手续和记录。

6.6.3.5 至少双人控制钥匙或密码来执行对硬件加密设备的操作，并根据不同的操作权限，设置不同的操作密码。

6.6.4 密钥管理

6.6.4.1 对称密钥管理

各机构应依照《银联卡密钥安全管理规则》(银联风管委〔2004〕2号)，对用于加密保护敏感支付信息的密钥实施严格管理，基本要求如下:

必须遵循随机或伪随机原则，使用硬件加密机生成密钥;

除加密机主密钥外的密钥，必须经上级密钥加密保护，以密文形式传输;

密钥必须保存在密码键盘或硬件加密机内，不得在其他介质中以明文形式显示;

在“双重控制”下，及时删除或销毁已失效、作废或泄漏的密钥。

6.6.4.2　非对称密钥管理

采用基于非对称密码体系的加解密、认证、签名等机制，应依照银联卡非对称密码算法使用及密钥管理相关规范，对用于加密保护敏感支付信息的密钥实施严格管理，基本要求如下:

公私密钥对应在安全计算环境内产生，应正确使用密钥管理规则以确保私钥的机密性和公私钥的完整性及真实性;

将私钥存储在安全密码设备中，以完整性受到保护的密钥组件的方式存储;

密钥周期结束或者已知或怀疑私钥已经泄漏时，应停止密钥对的使用，并实施物理控制和逻辑控制来防止密钥的非授权使用;

应以安全方式实现数字证书的申请和签发。

第七章　支付业务设施安全管理

7.1　网络和通信安全

7.1.1 基本要求

7.1.1.1 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。

7.1.1.2 所有接入互联网的系统都必须安装防火墙，阻止来自 Internet 网络的非法访问。防火墙应分别部署在互联网接入点与 DMZ 区之间、DMZ 区与内部网络之间。

7.1.1.3 当存储、处理支付信息的相关系统与本系统安全域之外的不可信网络之间存在网络连接时，应在系统与不可信网络之间部署防火墙。

7.1.1.4 在任何无线网络与存储、处理支付信息的相关系统之间部署边界防火墙。

7.1.1.5 应确保所有位置部署的防火墙开启有效的访问控制策略。

7.1.1.6 应在网络拓扑图中明确标识出所有支付信息流经的位置。

7.1.2 防火墙及路由器管理

7.1.2.1 建立防火墙及路由器的管理规范。

7.1.2.2 明确网络拓扑图中所有到支付信息处理相关系统的网络连接（包括无线网络连接）。

7.1.2.3 在网络拓扑图中体现与各业务合作机构的网络连接方式和业务情况。

7.1.2.4 明确业务必需的服务和端口清单，并保留审批记录。

7.1.2.5 所有允许从防火墙通过的传输协议都必须经过审批（包括 HTTP、SSL、SSH、VPN 等）。

7.1.2.6 如果允许 FTP 等风险较高的传输协议通过防火墙，应记录使用该协议的原因和已采取的安全措施。

7.1.2.7 每季度检查防火墙、路由器的规则配置并保留检查记录。

7.1.3 网络访问控制

7.1.3.1 限制通过互联网访问 DMZ 区 IP 的流量。

7.1.3.2 禁止通过互联网访问内部网络 IP 地址。

7.1.3.3 禁止内部网络到互联网的非授权访问。

7.1.3.4 将数据库放置于内部网络，通过防火墙与 DMZ 区隔离。

7.1.3.5 在所有可直接访问互联网的办公电脑及移动电脑上安装个人防火墙软件，防火墙软件应一直处于运行状态，用户无法禁用或修改其策略。

7.1.3.6 采取 IP 伪装技术防止内部网络地址被识别并暴露在互联网上。

7.1.3.7 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。审计记录应保留 6 个月以上。

7.2 设备和计算安全

7.2.1 设备安全管理

7.2.1.1 系统正式投产之前，应更改设备生产厂商提供的设备管理初始密码及相关安全参数（如设备初始管理口令等）。

7.2.1.2 对于无线网络设备，应更改厂商设定的无线网络安全密钥、SSID、管理口令等初始设置，并关闭 SSID 广播。

7.2.1.3 每台服务器只承担一项处于同一安全级别的主要功能（如 Web 服务器、数据库服务器应该分别部署在不同的设备上），且虚拟化系统也应视为一台独立服务器，部署前应禁用所有不必要的或不安全的服务和协议，并删除不必要的功能，如脚本、驱动程序或应用。

7.2.1.4 应维护所有涉及支付信息处理的软硬件设备列表及功能、用途等详细信息。

7.2.2 恶意代码防护

应对所有系统安装防病毒软件，以防范病毒、木马及恶意软件，具体要求包括:

7.2.2.1 所有运行 Windows 操作系统的主机应部署防病毒软件。

7.2.2.2 对于运行其他操作系统且未安装防病毒软件的主机，应定期评估其是否能够充分防范恶意代码攻击，并根据评估结果确认是否需要安装防病毒软件。

7.2.2.3 允许公共访问的服务器应部署防病毒软件或者采用其他恶意代码检测手段。

7.2.2.4 维护允许使用的软件列表并指定软件获取方式，严格限制下载和安装列表以外的软件。

7.2.2.5 应及时更新防病毒软件及病毒库，并定期对系统进行扫描，对扫描结果进行分析处理。

7.2.2.6 定期检查各系统防病毒软件运行及更新情况，并报告检查结果。

7.2.2.7 所有外部存储介质（软盘、光盘、移动硬盘和 U 盘等）在使用前，必须进行病毒扫描。

7.2.2.8 防病毒软件应一直处于保护状态，用户无法禁用防病毒软件或修改其策略。

7.2.3 安全补丁管理

7.2.3.1 应定期通过可信途径获取最新安全漏洞信息。

7.2.3.2 所有操作系统、应用系统均应及时安装厂商提供的安全补丁，重要安全补丁应在厂商发布 1 个月内安装，

其他安全补丁应在厂商发布 3 个月内安装。

7.2.3.3 在安装安全补丁之前，应通过相应测试，方能投产运行。

7.3 应用安全

7.3.1 安全开发流程

软件开发及应用时应满足以下基本要求:

7.3.1.1 在关键应用系统开发中，不能在程序代码中写入固定的口令或加解密密钥。

7.3.1.2 系统上线之前进行代码安全审计和渗透测试，识别可能的恶意代码和安全漏洞。

7.3.1.3 如应用系统使用开源软件，应对开源软件预先进行安全测试评估，使用其稳定版本，并安装最新的安全补丁。

7.3.2 变更管理

7.3.2.1 制定变更管理的流程，以及变更失败的应急方案及回退机制。

7.3.2.2 系统的所有变更必须遵循变更管理流程，并满足以下基本要求:

详尽记录变更流程，并及时更新相关文档;

变更流程由授权方进行审批签字方可执行;

执行变更之前进行功能测试，以确保变更不会影响系统的安全稳定运行;

变更下线的程序、相关配置文件、数据和日志文件应至少备份保存一年。

7.3.3 应用系统安全

7.3.3.1 境内开展支付业务或提供支付服务时，处理支

付交易或开展支付信息处理的应用系统及备份系统应部署在境内。

7.3.3.2 应建立互联网端口开放清单，重要服务器（如数据库服务器、日志服务器等）不得向互联网开放。

7.3.3.3 应用系统业务通信日志（至少包含报文解析日志和接口调用日志），应至少保存一年。

7.3.3.4 应建立统一支付业务接口管理制度，加强接入机构审核，明确支付接口使用范围和支付信息传输要求，确保接入机构将支付业务接口用于协议约定的业务范围和用途。

7.3.4 Web 安全

7.3.4.1 涉及支付信息的 Web 应用，应至少具备以下攻击的防范能力：暴力破解、重放攻击、注入攻击、跨站脚本攻击、网页仿冒、跨站请求伪造、越权等。

7.3.4.2 涉及支付信息的 Web 应用应使用安全可靠的加密通信方式，保障数据在传输中的安全，如 HTTPS 协议。

7.4 运维安全

7.4.1 物理安全

7.4.1.1 存储或处理支付信息的设备和介质应安装在安全的物理隔离区域，实行专人管理，并严格限制对这些设备和介质的物理访问。

7.4.1.2 安装有存储或处理支付信息设备的物理隔离区域应与其他业务、办公区域相隔离，并设置门禁系统，只有通过身份验证的人员才能进入。

7.4.1.3 物理隔离区域进出通道均应安装有效的录像监控设备，对人员、设备进出情况进行监控，监控应无死角；

监控录像资料至少保存 3 个月。

7.4.1.4 外部来访人员必须在获得审批授权并进行身份登记后方可进入物理隔离区域,登记记录至少保存一年。

7.4.1.5 存储或处理支付信息的相关设备必须在获得审批授权后方可移入或移出物理隔离区域。

7.4.2 安全配置管理

7.4.2.1 统一制定基于主机操作系统、网络设备、数据库、中间件等方面的安全配置规范，并按照安全配置规范对相关设备进行配置。

7.4.2.2 至少每半年对主机操作系统、网络设备、数据库、中间件等方面的配置文件进行核查，对不符合安全配置规范要求的进行整改。

7.4.2.3 对主机操作系统、防火墙、路由器、交换机的重要配置文件进行管理与监控，及时发现并处理未授权修改等问题，以确保重要配置文件的一致性。

7.4.3 例行检查

7.4.3.1 应每半年定期对系统安全状况进行检查测试，确保系统能够有效地识别和阻止来自外部的非法访问。

7.4.3.2 每季度测试无线访问点，对未经授权的无线访问点进行侦测并限制其访问内部网络。

7.4.4 漏洞扫描

应定期及在网络发生重大变更时，对系统进行漏洞扫描，具体包括:

7.4.4.1 至少每季度执行外部网络漏洞扫描，外部网络漏洞扫描应由中国银联授权的第三方专业化检测机构执行;

7.4.4.2 至少每季度执行内部网络漏洞扫描，内部网络

漏洞扫描可由机构或中国银联授权的第三方专业化检测机构执行;

7.4.4.3 在网络发生重大变更时应进行内部和外部网络漏洞扫描。网络重大变更应包括但不限于安装新的设备、网络拓扑结构调整、防火墙配置调整、应用系统升级等。

7.4.4.4 应根据需要重复执行漏洞扫描，以确保扫描发现的漏洞得到有效修复。

7.4.5 渗透测试

应定期及在系统发生重大变更时，对系统进行渗透测试，具体包括:

7.4.5.1 至少每年执行一次外部渗透测试，外部渗透测试应由中国银联授权的第三方专业化检测机构执行;

7.4.5.2 至少每年执行一次内部渗透测试，内部渗透测试可由机构或中国银联授权的第三方专业化检测机构执行;

7.4.5.3 在系统发生重大变更时应进行内部或外部渗透测试，系统重大变更包括但不限于操作系统升级、应用系统升级、网络拓扑变更、Web 服务器变更等。

7.4.5.4 应根据需要重复执行渗透测试，以确保测试发现的漏洞得到有效修复。

7.4.6 网络入侵检测

7.4.6.1 应采用入侵检测技术对网络数据传输进行实时监控。

7.4.6.2 对重要服务器的攻击行为，应能够记录攻击的源 IP、攻击的类型、攻击的目标、攻击的时间，并及时报警以阻止入侵行为。

7.4.7 监控管理

7.4.7.1 应对通信线路、网络设备、主机和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存。

7.4.7.2 应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

第八章　受理终端及支付应用软件安全

8.1　受理终端安全管理

8.1.1　技术标准符合性

受理终端应符合《银联卡受理终端安全规范》及其他相关规定的要求，且需通过中国银联授权的第三方专业化检测机构检测并获得安全认证，以确保受理终端采集支付信息时的安全性。

8.1.2　终端信息处理安全

受理终端及支付应用软件仅限于保存当前交易批次内用于交易清分所必需的基本信息要素，并在该批次结束后及时予以清除。

8.1.3　终端业务权限

应根据《银联卡受理终端业务准入管理办法》相关规定，加强对预授权、预授权完成撤销、消费撤销、联机退货等功能开通的审批和交易监控，记录并管理终端与交易权限的匹配关系，以确保支付信息处理的合理性和风险事件的可控性。

8.1.4　终端程序管理

8.1.4.1 应保障终端程序安全、稳定、完整、有效地执行交易流程。

8.1.4.2 应确保终端程序功能与开通业务类型要求一致。

8.1.4.3 应采取措施防止未经授权私自篡改终端程序、窃取支付信息等违规行为，确保终端程序具备抵御恶意破坏等黑客攻击的能力。

8.1.5 终端注册管理

应采用终端入网签名、唯一性标识等技术措施，确保终端注册信息真实可靠，交易可追溯到每一台终端。

8.1.6 终端设备管理

8.1.6.1 应加强受理终端选型、采购、验收等环节的安全管理，确保受理终端的技术标准符合性。

8.1.6.2 应加强受理终端出入库记录，并建立完整的库存台账。

8.1.6.3 应建立并维护受理终端清单（包含终端型号、序列号、布放位置等信息），持续开展终端抽巡检工作，确保布放的终端与合格样品的一致性，防范终端被非法改装风险。

8.1.7 终端密钥管理

应指定专人管理受理终端密钥和相关参数，确保不同的受理终端使用不同的终端主密钥并定期更换。

8.2 支付应用软件安全管理

8.2.1 技术标准符合性

支付应用软件应符合《银联卡支付应用软件安全规范》的要求，且需通过中国银联授权的第三方专业化检测机构检测并获得安全认证，以确保支付应用软件采集支付信息时的安全性。

8.2.2 支付应用软件完整性

8.3.2.1 支付应用软件应采用防逆向工程保护措施，如支付应用软件采取代码化指令、反调试、代码混淆等技术手段，防范攻击者对支付应用软件的反编译分析。

8.3.2.2 应对支付应用软件进行签名，标识支付应用软件的来源和发布者，保证客户所下载的支付应用软件来源于所信任的机构。

8.2.3 支付信息处理安全

8.2.3.1 支付应用软件应提供自定义软键盘，支持键位随机布局；输入支付密码时，应提供即时加密功能；完成身份鉴别后应及时清除缓存，防止信息泄漏。

8.2.3.2 应提供防截屏功能，防止在显示支付信息、付款条码等内容时，被恶意程序窃取。

8.2.3.3 支付应用软件业务逻辑应能够防范跨账户越权操作、业务欺骗等风险，确保响应报文仅包含必要的支付信息。

8.2.3.4 支付应用软件仅限于保存当前交易批次内用于交易清分所必需的基本信息要素，并在该批次结束后及时予以清除。

8.2.4 支付应用软件运行安全

8.3.4.1 支付应用软件在运行过程中产生的本地数据应进行安全存储，设置合理的访问控制权限。

8.3.4.2 支付应用软件运行时输出的调试信息，不能包含敏感支付信息。

8.3.4.3 支付应用软件应能监测并向后台系统反馈网络支付环境安全状况。

第九章　安全策略维护与持续改进

9.1　支付信息安全合规评估要求

9.1.1 评估范围

所有涉及支付信息采集、传输、存储、使用等环节及可能影响支付信息安全的业务处理系统及技术支撑环境。

9.1.2 自评估要求

涉及支付信息采集、传输、存储、使用等环节的支付业务直接参与方应每年根据本标准开展支付信息安全自评估，并保留自评估相关记录；同时，通过合作协议等方式要求提供专业化服务的间接参与方每年开展支付信息安全自评估，并保留相关记录。

9.1.3 外部评估要求

9.1.3.1　直接参与方

涉及支付信息采集、传输、存储、使用等环节的支付业务直接参与方需每年聘请中国银联风险管理委员会授权的第三方专业化检测机构开展外部合规评估，包括但不限于：

信息安全等级保护级别为三级及以下的发卡机构；

基于银联卡的支付账户发行方；

从事银联卡收单业务的收单机构；基于银联卡的二维码应用服务方；

在自有Web应用或支付应用软件采集支付信息的银联卡收单特约商户、达到《银联卡收单业务账户信息安全合规评估管理暂行规定》规定的外部合规评估条件的银联卡收单特约商户。

对于上述机构，如已通过外部合规评估可不再开展自评

估。

9.1.3.2　间接参与方

直接参与方开展外部合规评估时，评估范围应包含间接参与方提供的涉及支付信息处理的服务。如直接参与方提供了间接参与方的外部合规评估材料，可不再评估相关服务。

9.2　支付信息安全相关审计要求

9.2.1 在日常专项审计和检查等基础上，每年至少开展两次支付信息安全管理相关的内部或外部全面审计，并保留相关记录。

9.2.2 审计内容应至少包括支付信息安全策略的科学性、组织架构及岗位设置的合理性、员工对支付信息安全管理要求和职责的熟悉程度、内控制度和外部风险防范策略的有效性、交易及支付信息保护要求的准确性、支付业务设施的安全性等。

9.3　安全策略持续改进

9.3.1 每年根据支付信息安全合规评估结果和审计情况，并在业务、系统或外部环境发生重大变更时，调整支付信息安全管理策略，并确保得到有效执行。

9.3.2 每年在支付信息安全管理策略调整后，应加强员工支付信息安全培训，确保所有涉及支付信息的员工熟悉最新的支付信息安全管理要求和保护责任。

9.3.3 每年定期维护外部合作方及服务提供商列表、合作协议，并监控其对本标准的遵从状态，持续改进外部风险防范策略。

第十章　附则

本标准经银联风险管理委员会审议通过后，自发布之日起实施。《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）同时废止。

附录

术语表

支付信息

本标准所指的支付信息，包括但不限于银联卡上记录的账户信息、基于银联卡开展支付业务的网络支付账户信息、身份鉴别信息、支付业务涉及的必要个人信息和其他支付相关信息。

敏感支付信息

作为支付要素能够直接完成交易且一旦泄漏将对信息主体的资金安全造成严重影响的支付信息，包括卡片有效期、磁道信息(含芯片等效磁道信息)、卡片验证码(CVN及CVN2)、个人标识代码（PIN）、网络支付密码以及用于身份鉴别的个人生物特征信息等。

二维码应用服务方

加入二维码支付业务并提供移动应用的主体机构。

收单专业化服务机构

从事商户拓展与服务，终端布放与维护，交易接入服务，渠道接入服务等的专业化机构。

聚合技术服务商

通过开展“聚合支付”服务，为商户提供融合多个支付渠道、一站式资金结算和对账等综合支付解决方案的机构。

云服务提供商

获得互联网资源协作服务业务经营许可的企业，利用架设在数据中心之上的设备和资源，通过互联网或其他网络以

随时获取、按需使用、随时扩展、协作共享等方式，为用户提供数据存储、互联网应用开发环境、互联网应用部署和运行管理等服务。

银联卡交易

是指直接或间接通过银联卡卡号等相关信息，基于银联卡进行业务（权限）开通、信息验证、货币支付与资金转移等业务处理的（行为）过程，包括但不限于:

直接通过卡号等银联卡相关信息完成的交易。例如：银联卡刷卡交易、银联卡插卡交易、银联卡挥卡交易、移动设备（如智能手机、智能手环等）挥卡交易、银联卡无卡交易等;

间接通过卡号等银联卡相关信息完成的交易。例如：账户绑定、实名验证、快捷支付、扫码支付等。

银行卡卡号

即卡号，用于标识银行卡所有者及卡片唯一性的号码，由发卡行标识代码、个人账户标识和校验位组成。

个人标识代码

是在联机交易中识别持卡人身份合法性的数据信息。本标准中个人标识代码主要限定在发卡机构与持卡人约定的交易密码，不包含支付平台自身的客户鉴别信息，如登录密码、支付密码、生物特征信息等。

登录密码

用户登录到商户平台、支付平台所使用的用于身份鉴别的密码信息，一般与登录用户名共同使用。

支付密码

用户在商户平台、支付平台等进行网络支付交易时提供

的用于完成身份鉴别的密码信息。

个人生物特征信息

生物特征信息是指人的生理特征或行为特征，例如指纹、虹膜等信息，可用来进行个人身份的鉴定。

卡片有效期

发卡机构规定的卡片有效使用时间，印制在卡片的正面左下方位置，超过该时间后，卡片将停止使用。

卡片验证码

CVN 是对磁条信息合法性进行验证的代码，通常写入磁道中; CVN2 是非面对面交易中验证交易者是否持有卡片的代码，通常位于卡片背面。

磁道信息

一磁、二磁和三磁定义的必备或可选的数据元。磁道信息可以在物理卡的磁条上，也可以被包含在集成电路或者其他媒介上。

支付标记

银行卡卡号、卡片有效期等支付信息的替代值，在支付交易中用支付标记替换原始支付信息，不影响交易处理，增强了交易安全性。

动态口令

也称动态密码，由令牌种子与其他数据，通过特定算法运算生成的一次性口令。

短信验证码

也称短信动态密码，是身份认证系统以手机短信形式发送到客户手机上的随机数，也是一种手机动态口令形式，客户在登录或者交易认证时输入，从而确保系统身份认证的安

全性。

证件类识别标识

由国家法定有权部门颁发，能够唯一确定客户的且具有法律效力的标识。

明示同意

信息主体通过书面声明或主动做出肯定性动作，对其支付信息进行特定处理做出明确授权的行为。

双人控制

利用两个或多个人共同协调操作以保护敏感支付信息，确保任何一个人均不能单独访问、使用敏感支付信息。

双重控制

单个人员不能控制保护项的过程。

DMZ

设置在内部网络和外部公共网络（如 Internet）之间的缓冲带，一般用于对外提供必须公开的服务器设施。

IP

一种网络层协议，包含地址信息和部分控制信息，数据包根据这些信息被路由，IP 是互联网协议集中最重要的网络层协议。

IPSEC

一系列由互联网工程工作组（IETF）正式制定的，基于 IP 网络（包括 Intranet、Extranet 和 Internet）的开放性 IP 安全标准，通过对所有 IP 数据包进行加密和认证以确保 IP 通信安全。

SSL

一种国际标准的加密及身份认证通信协议，能在浏览器

和服务器之间建立一条安全的、可信任的通讯通道，确保数据保密性、完整性和相互鉴定。

TLS

安全套接层协议层(SSL)的后继协议，保障两个相互通信应用之间数据的机密性和完整性。

VPN

通过对网络数据的封包和加密传输，在公用网络上传输私有数据，达到私有网络的安全级别。

硬加密

硬加密是指终端配备专用密码键盘（密码输入模块与加密模块无缝连接，且密码键盘具备“开机自毁”功能），使用专用密码键盘中的加密芯片进行加密。

银联卡受理终端

银联卡受理终端是指通过读取或输入银联卡相关信息，发起交易并提示操作方交易完成的专用设备及其终端程序。包括个人支付终端、公共支付终端、商户终端等。

支付应用软件

支付应用软件是为完成存储、处理或传输持卡人授权或结算数据的应用软件，包括但不限于手机支付客户端、商户插件以及商用支付终端、个人支付终端、自助终端中的应用程序和配套后台服务器中的涉及支付业务处理的应用程序等。

强效加密

使用经过行业测试和认可的加密算法和密钥长度，对数据进行加密保护的方法。包括但不限于 AES（128 位和更高）、TDES/TDEA（最少三倍长的密钥）、RSA（2048 位和更高）、

ECC（224 位和更高）以及 DSA/D-H（2048/224 位和更高）、SM2（256 位）、SM4（128 位）。