ICS 03.060
A 11

JR

中华人民共和国金融行业标准

JR/T 0122—2018
代替 JR/T 0122—2014

非银行支付机构支付业务设施技术要求

Technical requirements of non-bank payment institutions payment service facilities

2018－10－29 发布　　2018－10－29 实施

中国人民银行　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准代替JR/T 0122—2014《非金融机构支付业务设施技术要求》，与JR/T 0122—2014相比主要变化如下：

——为确保本标准的针对性和适用性，将本标准名称变更为《非银行支付机构支付业务设施技术要求》；

——将互联网支付、数字电视支付和固定电话支付的功能要求合并成网络支付功能要求，以对应《非银行支付机构网络支付业务管理办法》（中国人民银行公告〔2015〕第43号）的相关要求（见第7章）；

——增加了商户管理类、支付账户分类管理类、争议投诉处理类以及支付标记化管理类等要求（见7.1）；

——增加了特约商户管理类要求（见7.2.1）；

——增加了客户风险管理类、支付账户风险管理、商户风险管理类等要求（见8.1）；

——增加了当年累计交易限额、当日累计交易限次、异常行为监控、账户资金监控要求（见8.1.4）；

——增加了风险及反洗钱管理制度类要求（见8.1.6、8.2.3、8.3.3）；

——增加了自建机房的物理安全要求（见10.1）；

——增加了主机对象审计、应用操作审计要求（见10.3、10.4）；

——修订了网络域安全隔离和限制、内容过滤、网络对象审计等要求（见10.2）；

——修订了访问控制范围等要求（见10.3）；

——修改了应用安全中可信时间戳服务、支付安全策略、日志信息等要求（见10.4）；

——修订了应急恢复预案、定期业务连续性演练、定期业务连续性培训等要求（见10.7）；

——增加了个人信息保护、数据使用等要求（见10.5）；

——增加了运维安全文档管理要求（见10.6.5）；

——删除了文档要求（见2014版6.5、7.5、8.5、9.5、10.5）；

——删除外包附加要求（见2014版第11章）；

——增加了条码支付功能、风控、安全等方面的要求（见7、8、10章）；

——增加了移动支付功能、风控、安全等方面的要求（见7、8、10章）；

——增加了SM系列算法的使用要求（见第10章）。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准起草单位：中国人民银行科技司、北京中金国盛认证有限公司、中国信息安全认证中心、中国金融电子化公司、银行卡检测中心、上海市信息安全测评认证中心、中金金融认证中心有限公司、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、北京软件产品质量检测检验中心（国家应用软件产品质量监督检验中心）、中电科技（北京）有限公司、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、支付宝（中国）网络技术有限公司、银联商务股份有限公司、财付通支付科技有限公司、网银在线（北京）科技有限公司。

本标准主要起草人：李伟、安荔荔、潘润红、邬向阳、李兴锋、聂丽琴、赵春华、高天游、王翠、王鹏飞、裴倩如、李红曼、焦莉纳、唐立军、牛跃华、林春、马鸣、刘欣、王妍娟、夏采莲、高祖康、陆嘉琪、王凯阳、赵亮、于泉、冯云、张益、宋铮、何韡、吴永强、马志斌。

本标准于2014年11月24日首次发布，本次为第一次修订。

引　言

为规范非银行支付机构支付服务行为，防范支付风险，保护当事人的合法权益，根据《中华人民共和国标准化法》、《中华人民共和国认证认可条例》（中华人民共和国国务院令第390号）、《非金融机构支付服务管理办法》（中国人民银行令〔2010〕第2号）、《非金融机构支付服务管理办法实施细则》（中国人民银行公告〔2010〕第17号）、《非金融机构支付服务业务系统检测认证管理规定》（中国人民银行公告〔2011〕第14号）、《支付机构预付卡业务管理办法》（中国人民银行公告〔2012〕第12号）、《非银行支付机构网络支付业务管理办法》（中国人民银行公告〔2015〕第43号）等相关法律法规及管理办法，制定本标准。

本标准是JR/T 0123—2018《非银行支付机构支付业务设施检测规范》的制定依据。凡涉及密码应用的部分，根据国家密码主管部门的相关要求制定并执行。

非银行支付机构支付业务设施技术要求

1 范围

本标准规定了非银行支付机构支付业务设施的技术标准符合性和系统安全性相应级别的基本要求和增强要求，为非银行支付机构支付业务设施认证、检测提供了依据。

本标准适用于中华人民共和国境内的非银行支付机构。如无支付业务类型的特别说明，本标准条款适用于全部支付业务范围。

注：支付业务设施包括支付业务处理系统、网络通信系统以及容纳以上系统的专用机房。

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 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918（所有部分） 信息安全技术 SM2椭圆曲线公钥密码算法

GM/T 0054—2018 信息系统密码应用基本要求

JR/T 0025.7—2018 中国金融集成电路（IC）卡规范 第7部分：借记贷记应用安全规范

中国人民银行.非银行支付机构网络支付业务管理办法（中国人民银行公告〔2015〕第43号），2016-07-01.

中国人民银行.中国人民银行关于印发《条码支付业务规范（试行）》的通知（银发〔2017〕296号），2017-12-25.

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络支付业务 online payment service

收款人或付款人通过计算机、移动终端等电子设备，依托公共网络信息系统远程发起支付指令，且付款人电子设备不与收款人特定专属设备交互，由非银行支付机构为收付款人提供货币资金转移服务的活动。

注：网络支付业务范围包括互联网支付、移动电话支付、数字电视支付、固定电话支付。

3.2

互联网支付 internet payment

依托互联网实现收付款方之间货币资金转移的支付方式。

3.3

移动终端 mobile device

具有移动通讯能力的终端设备。

注：移动终端包括手机、PDA等，在本标准中主要指手机。

3.4

移动电话支付 mobile payment

允许用户使用移动终端对所消费的商品或服务进行账务支付的一种支付方式。

注：移动电话支付主要分为近场支付和远程支付两种。

3.5

近场支付 proximity payment

移动终端通过实体受理终端在交易现场以联机或脱机方式完成交易处理的支付方式。

3.6

远程支付 remote payment

移动终端通过无线通信网络接入直接与后台服务器进行交互完成交易处理的支付方式。

3.7

固定电话支付 fixed telephone payment

电话通过语音IVR方式，使用电话线路发出支付指令，实现货币支付与资金转移的支付方式。

3.8

数字电视支付 digital TV payment

依托交互机顶盒等数字电视支付终端发起的实现货币支付与资金转移的支付方式。

3.9

预付卡 prepaid card

发卡机构以特定载体和形式发行的、可在发卡机构之外购买商品或服务的预付价值。

注：预付卡分为记名预付卡和不记名预付卡。

3.10

记名预付卡 registered prepaid card

预付卡业务处理系统中记载持卡人身份信息的预付卡。

3.11

不记名预付卡 anonymous prepaid card

预付卡业务处理系统中不记载持卡人身份信息的预付卡。

3.12

银行卡收单 bank card acceptance

收单机构与特约商户签订银行卡受理协议，在特约商户按约定受理银行卡并与持卡人达成交易后，为特约商户提供交易资金结算服务的行为。

3.13

条码支付 bar code payment

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。

3.14

客户 customer

购买或使用非银行支付机构提供的支付服务的组织或个人。

注：客户包含个人客户和企业客户。

3.15

一般支付 general payment

付款方使用支付指令支付成功后即可结算的支付行为。

3.16

担保支付 guarantee payment

在支付过程中，由支付服务方为支付双方提供交易担保，付款方进行支付确认后，由支付服务方把款项结算给收款方的支付行为。

3.17

协议支付 agreement payment

在付款方信任商户能够保障自己资金安全的前提下，付款方、商户、支付服务方事先签订协议，在后续支付过程中，商户根据协议直接向支付服务方发起扣款请求，而无需通过付款方另行授权即可完成付款的支付行为。

3.18

消费撤销 consuming cancellation

商户对持卡人已经联机结算的交易，于当日当批内发起的对消费交易的取消。

3.19

预授权 pre-authorization

担保支付或其他需预先冻结一笔资金的交易，即根据持卡人需支付的金额向发卡行索取日后付款的承诺。

3.20

预授权撤销 pre-authorization cancellation

对已成功的预授权交易，在结算前使用预授权撤销交易，请求发卡方取消付款承诺。

3.21

预授权完成 pre-authorization completion

在预授权有效期内，持卡人以实时发送结算通知报文的形式对已批准的预授权交易作支付结算。

3.22

预授权完成撤销 the cancellation of pre-authorization completion

因预授权交易的商品退回或服务取消，将已扣款项退还至持卡人原扣款账户的过程。

3.23

运营人员 operating personnel

具有审核、确认等权限的管理人员。

3.24

数据库 database

存储在一个或多个计算机文件中的相关数据集合。

3.25

圈存 load

增加卡中电子现金余额的过程。

3.26

圈提 unload

通过受理终端，将电子现金账户中的资金划入预先与电子现金账户绑定的借记卡或信用卡账户（或额度）的过程。

3.27

冲正交易 reversal transaction

由报文的发送方发起，用于通知接收方，先前的一笔授权类或金融类交易没有按预定流程完成，应取消其处理结果的过程。

3.28

交易查询 trading inquiry

客户向支付服务方发起查询单笔（批量）业务状态请求的过程。

4 缩略语

下列缩略语适用于本文件。

ARQC：授权请求密文（Authorization Request Cryptogram）

ARPC：授权响应密文（Authorization Response Cryptogram）

IVR：互动式语音应答（Interactive Voice Response）

MAC：报文认证码（Message Authentication Code）

TAC：终端行为代码（Terminal Action Code）

TSP：标记服务提供方（Token Service Provider）

TR：标记服务请求方（Token Requestor）

5 等级划分

非银行支付机构支付业务设施技术认证分为两级：一级和二级。一级覆盖本标准的基本要求，二级覆盖本标准的基本要求和增强要求。

6 评判原则

6.1 客观性原则

应以非银行支付机构支付业务设施提供者的实际业务或事项为依据进行确认、审查和报告，如实地反映符合确认和审查的各项检查要素，保证审查信息的真实可靠，内容完整。

6.2 公正性原则

应依据国家法律法规、认可规范、认可准则CNAS—CC02及其他有关规定的要求，建立完整的质量体系，并严格按照质量体系开展认证活动。认证活动不受任何外来压力和商业因素的影响和干扰。

6.3 科学性原则

应以科学思想为指导，以事实为依据。

6.4 审慎性原则

应对可能存在的风险予以充分考量。

7 功能要求

7.1 网络支付功能要求

7.1.1 客户管理

7.1.1.1 客户信息登记及管理

应实现客户注册、客户信息编辑等功能。

7.1.1.2 客户审核

应实现客户注册信息审核、确认开通审核及关键信息修改审核等功能。

7.1.1.3 客户状态管理

客户状态应至少包括正常、冻结、注销等。
冻结应实现暂停客户交易和重新恢复客户交易的功能。
注销应实现永久停止客户交易的功能。

7.1.1.4 客户查询

应实现客户信息的查询功能。

7.1.1.5 客户证书管理

宜实现客户的电子证书的申请、发放、更新、作废等功能。

7.1.1.6 客户业务管理

应实现客户业务的增加、修改和取消等功能。

7.1.1.7 终端设备关联

宜实现将用户账户与移动终端设备相关联的功能。
宜实现将用户账户与配合终端设备使用来辨识用户的载体（如手机号码）相关联的功能。
宜实现移动支付开通确认的功能。

7.1.2 支付账户管理

7.1.2.1 客户支付账户信息登记及分类管理

应实现客户支付账户的开户、修改等功能。
应实现支付账户分类管理的功能。

7.1.2.2 客户支付账户审核

应实现客户支付账户信息审核、确认开通审核及关键信息修改审核等功能。

7.1.2.3 客户支付账户状态管理

客户支付账户状态应至少包括正常、冻结、注销等。
冻结应实现暂停客户支付账户交易和重新恢复客户支付账户交易的功能。
注销应实现永久停止客户支付账户交易的功能。

7.1.2.4 客户支付账户查询

应实现客户支付账户信息查询的功能。

7.1.2.5 银行卡关联

应实现将客户账户与银行卡相关联的功能，且仅关联其名下的实名银行卡账户，未关联的银行卡不应用于支付。

开展条码支付业务，应实现客户用于生成条码的银行账户或支付账户、身份证件号码、手机号码的关联管理。

7.1.3 商户管理

7.1.3.1 商户信息登记及管理

应实现商户注册、商户信息编辑等功能。

7.1.3.2 商户审核

应实现商户注册信息审核、确认开通审核及关键信息修改审核等功能。

7.1.3.3 商户状态管理

商户状态应至少包括正常、冻结、注销等。
冻结应实现暂停商户交易和重新恢复商户交易的功能。
注销应实现永久停止商户交易的功能。

7.1.3.4 商户查询

应实现商户信息查询的功能。

7.1.3.5 商户证书管理

应提供商户的电子证书的申请、发放、更新、作废等服务。

7.1.3.6 商户业务管理

应实现商户业务的增加、修改和取消等功能。

7.1.4 交易处理

7.1.4.1 一般支付

应实现客户一般支付交易的功能。
开展条码支付业务，应提供收款扫码功能或付款扫码功能。

7.1.4.2 担保支付

应实现客户担保支付交易的功能。

7.1.4.3 协议支付

应实现客户协议支付交易的功能。

7.1.4.4 转账

应实现不同账户之间相互转账的功能。

7.1.4.5 充值

应实现将资金从客户银行账户转账至本人支付账户的功能。

7.1.4.6 提现

应实现将资金从客户支付账户转账到本人银行账户的功能。

7.1.4.7 交易明细查询

应实现按照时间、交易类型或者客户等交易明细信息进行查询，且能实现浏览交易明细的功能。
应提供至少近1年的交易信息查询服务。

7.1.4.8 交易明细下载

应实现交易明细信息下载的功能。
应提供至少近1年的交易明细下载服务。

7.1.4.9 邀请他人代付

应实现邀请他人代为支付的功能。

7.1.5 对账处理

7.1.5.1 发送对账请求

应提供商户提交对账申请的服务。

当商户提交对账申请时，支付服务方应提供对账信息的服务。

7.1.5.2 生成对账文件

应实现商户对账文件的查询、浏览或下载等功能。

7.1.6 差错处理

7.1.6.1 单笔退款

应实现对已发生的单笔交易进行退款申请、确认、审核、退款等功能。
支付服务方应将部分或全部已扣款项退还至客户的原扣款账户。

7.1.6.2 批量退款

应实现对已发生的多笔交易进行退款申请、确认、审核、退款等功能。
支付服务方应将部分或全部已扣款项退还至客户的原扣款账户。

7.1.6.3 对账差错处理

应实现对账文件出错、对账结果不平等差错情况的处理流程。

7.1.6.4 差错交易查询

应实现对各种差错交易查询的功能。

7.1.7 资金结算

7.1.7.1 客户结算

应提供支付服务方与客户之间的资金结算服务。

7.1.7.2 商户结算

应提供支付服务方与商户之间的资金结算服务。

7.1.8 运营及接入管理

7.1.8.1 外部接入管理

应提供外部机构的接入、审核、信息修改和删除等服务。

7.1.8.2 统计报表

应实现对一段时间内的业务操作（如客户注册、商户开通、支付、结算等操作）进行查询统计的功能。

支付服务方可根据自身的情况将“一段时间”细化为“月、季、年”等。

7.1.8.3 运营人员权限管理

应实现运营人员权限的增加、删除、修改或审核等功能。

7.1.9 争议投诉处理

7.1.9.1 交易差错处理

应建立健全差错争议处理制度，配备专业部门和人员据实、准确、及时地处理交易差错。

7.1.9.2 纠纷投诉处理

应建立健全纠纷投诉处理制度，配备专业部门和人员据实、准确、及时地处理客户投诉。

7.1.10 移动近场支付交易

7.1.10.1 联机消费

应实现移动终端联机消费的功能。

交易信息至少应包括：直接提供商品或服务的商户名称、类别和代码，受理终端类型和代码，交易时间和地点、交易金额、交易类型和渠道、交易发起方式等。

开展条码支付业务，应提供收款扫码功能。

7.1.10.2 联机消费撤销

应实现移动终端联机消费撤销的功能。

应提供原交易的凭证，按业务要求输入有关数据，收到响应后，完成消费撤销交易并提供凭证。

7.1.10.3 联机余额查询

应实现移动终端联机余额查询的功能。

7.1.10.4 退货

应实现退货的功能。

7.1.10.5 预授权

应实现预授权的功能。

7.1.10.6 预授权撤销

应实现预授权撤销的功能。

7.1.10.7 预授权完成

应实现预授权完成的功能。

7.1.10.8 预授权完成撤销

应实现预授权完成撤销的功能。

7.1.10.9 指定账户圈存

应实现指定账户圈存的功能。

7.1.10.10 非指定账户圈存

应实现非指定账户圈存的功能。

7.1.10.11 圈提

应实现圈提交易的功能。

7.1.10.12 脱机消费

应实现移动终端的脱机消费功能。

7.1.10.13 脱机消费文件处理

应实现对脱机消费文件进行处理的功能。

7.1.10.14 脱机余额查询

应实现脱机余额查询的功能。

7.1.10.15 冲正交易

应实现冲正交易的功能。

7.1.10.16 异常交易确认

交易请求出现异常时，应实现异常确认功能。对于转账、充值等交易请求，在出现异常时以确认通知报文确认原交易。

7.1.10.17 异常处理存储转发机制

应实现异常处理存储转发机制。

当冲正发送方不能发送冲正通知或未能收到接收方对冲正的应答时，将冲正通知报文存放在存储转发队列中存储转发；当确认发送方不能发送确认通知或未能收到对确认的应答时，将确认通知报文存放在存储转发队列中存储转发。

冲正通知和确认通知不应跨越清算日。

7.1.10.18 IC卡参数下载

应实现IC卡参数下载的功能。

7.1.11 固定电话支付语音IVR管理

7.1.11.1 电话语音密码

固定电话支付应实现电话语音预留密码设置的功能，应实现将客户支付账户与预留密码相关联的功能。

7.1.11.2 按键输入

固定电话支付应实现使用语音IVR将按键输入转换为相应指令的功能。

7.1.11.3 电话回拨

固定电话支付应实现使用语音IVR回拨到指定电话终端的功能。

7.1.12 支付标记化应用

应采用支付标记化技术，对具有金融交易功能的银行账户、非银行支付机构支付账户的编码、银行卡卡号等信息进行脱敏处理。

应支持基于支付标记化技术的交易处理。

7.2 预付卡发行与受理功能要求

7.2.1 特约商户管理

7.2.1.1 商户信息登记及管理

应实现商户注册、信息编辑、审核等功能。

7.2.1.2 商户交易状态管理

商户交易状态应至少包括正常、冻结、注销等。

冻结应实现暂停商户交易和重新恢复商户交易的功能。

注销应实现永久停止商户交易的功能。

7.2.1.3 商户信息查询

应实现商户信息查询的功能。

7.2.1.4 商户终端管理

应对商户控制平台或POS机等终端进行管理。

7.2.2 终端机具信息管理

7.2.2.1 机具申领和报废控制

应具有机具的申领和报废的控制策略，用于控制申领和报废过程。

7.2.2.2 机具信息维护

应能对机具信息（如机具编号、对应商户名称、商户编号等）进行维护。

7.2.2.3 机具信息查询

应能对机具信息（如机具编号、对应商户名称、商户编号等）进行查询。

7.2.3 卡片管理

7.2.3.1 制卡

应实现制卡的基本功能，如新增制卡、制卡文件生成等。

7.2.3.2 卡片发行

应实现对发行的新卡信息进行管理的功能，如售卡、卡片登记等。采用银行转账等非现金结算方式购买预付卡，系统应记载付款人银行账户名称和账号、收款人银行账户名称和账号、转账金额等信息。不应使用信用卡购买预付卡。

单位一次性购买预付卡5000元以上，个人一次性购买预付卡5万元以上的，应通过银行转账等非现金结算方式购买，不应使用现金。

个人或单位购买记名预付卡或一次性购买不记名预付卡1万元以上的，应使用实名并提供有效身份证件。

7.2.3.3 卡片激活

新卡应激活后才能使用。

7.2.3.4 卡片有效期延长

应实现对不记名预付卡有效期进行延长的功能，并可指定延长期限。
不记名预付卡有效期不应低于3年。记名预付卡不应设置有效期。

7.2.3.5 更换

应提供卡片更换的服务，在卡片丢失或不可使用时更换新卡。

7.2.3.6 密码修改

应实现对记名卡片密码进行修改的功能。

7.2.3.7 卡片冻结/解冻

应实现根据需要对卡片资金进行冻结/解冻的功能。

7.2.3.8 卡片挂失/解挂

应实现根据需要对记名预付卡进行挂失/解挂的功能。

7.2.3.9 赎回

应提供退卡赎回资金的服务。
记名预付卡办理赎回应在购卡3个月后，赎回时资金应原路退回。

7.2.3.10 销卡

应对卡片进行注销回收。

7.2.4 密钥和证书管理

7.2.4.1 认证中心公钥管理

应对认证中心下发的公钥进行有效的管理和控制。

7.2.4.2 发卡机构密钥管理

应对发卡机构密钥进行有效的管理和控制。

7.2.4.3 IC卡密钥管理

应对IC卡密钥进行有效的管理和控制。

7.2.4.4 发卡机构证书管理

应对发卡机构公钥证书进行有效的管理和控制。

7.2.4.5 IC卡证书管理

应对IC卡公钥证书进行有效的管理和控制。

7.2.5 交易处理

7.2.5.1 联机消费

应实现联机消费的功能。

交易信息至少应包括：直接提供商品或服务的商户名称、类别和代码，受理终端（网络支付接口）类型和代码，交易时间和地点（网络特约商户的网络地址）、交易金额、交易类型和渠道、交易发起方式等。网络特约商户的交易信息还应包括商品订单号和网络交易平台名称。

开展条码支付业务，应提供收款扫码功能或付款扫码功能。

7.2.5.2 联机消费撤销

应实现联机消费撤销的功能。

应提供原交易的凭证，按业务要求输入有关数据，收到响应后，完成消费撤销交易并提供凭证。

7.2.5.3 联机余额查询

应实现联机余额查询的功能。

7.2.5.4 退货

应实现退货的功能。

应提供原消费交易的凭证，按业务要求在受理终端输入有关数据，收到响应后，完成退货交易并提供凭证。

货款无法退回原卡的，发卡机构应将资金退回至持卡人提供的同一发卡机构的同类预付卡。预付卡接受退款后的卡内资金余额不应超过规定限额。

7.2.5.5 充值

应实现对卡片进行充值，并在充值失败时进行自动撤销的功能。

应可通过现金、银行转账等方式对卡片进行充值，不应使用信用卡为预付卡充值。

同时获准办理“互联网支付”业务的发卡机构，应可通过持卡人在本发卡机构开立的实名网络支付账户进行充值。

办理一次性金额5000元以上预付卡充值业务的，不应使用现金。

7.2.5.6 指定账户圈存

应实现指定账户圈存的功能。

7.2.5.7 非指定账户圈存

应实现非指定账户圈存的功能。

7.2.5.8 圈提

应实现圈提交易的功能。

7.2.5.9 脱机消费

应实现脱机消费的功能。

7.2.5.10 脱机消费文件处理

应实现对脱机消费文件进行处理的功能。

7.2.5.11 脱机余额查询

应实现脱机余额查询的功能。

7.2.5.12 交易明细查询

应实现在受理平台和终端上进行交易明细查询的功能。

7.2.5.13 冲正交易

应实现冲正交易的功能。

7.2.5.14 异常卡交易

应实现对各种异常卡交易的处理功能。

7.2.5.15 IC卡脚本通知

应实现向IC卡发送脚本通知指令的功能。

7.2.5.16 资金结算

应提供支付服务方与客户之间资金结算的服务。

7.2.6 对账处理

7.2.6.1 发送对账请求

应提供商户提交对账申请的服务。

当商户提交对账申请时，支付服务方应提供对账信息的服务。

7.2.6.2 生成对账文件

应实现商户对账文件的查询、浏览或下载等功能。

7.2.7 差错处理

7.2.7.1 单笔/批量退款

应实现单笔/批量交易退款的功能。

支付服务方应将部分或全部已扣款项退还至个人或企业客户的原扣款账户，原扣款账户不能接收退款的，退款到付款方其他账户。

7.2.7.2 差错交易查询

应实现对各种差错交易查询的功能。

7.2.7.3 对账差错处理

应实现对账文件出错、对账结果不平等差错情况的处理流程。

7.2.8 运营管理

7.2.8.1 统计报表

应实现对一段时间内的业务操作（如客户注册、商户开通、支付、结算等操作）进行查询统计的功能。

支付服务方可根据自身的情况将“一段时间”细化为“月、季、年”等。

7.2.8.2 运营人员权限管理

应实现运营人员权限的增加、删除、修改和审核等功能。

7.2.9 条码支付客户管理

7.2.9.1 客户信息登记及管理

应实现客户注册、客户信息编辑等功能。

7.2.9.2 客户审核

应实现客户注册信息审核、确认开通审核及关键信息修改审核等功能。

7.2.9.3 客户状态管理

客户状态应至少包括正常、冻结、注销等。

冻结应实现暂停客户交易和重新恢复客户交易的功能。

注销应实现永久停止客户交易的功能。

7.2.9.4 客户查询

应实现客户信息的查询功能。

7.2.9.5 客户证书管理

宜实现客户的电子证书的申请、发放、更新、作废等功能。

7.2.9.6 客户业务管理

应实现客户业务的增加、修改和取消等功能。

7.2.9.7 终端设备关联

宜实现将用户账户与移动终端设备。

宜实现将用户账户与配合终端设备使用可用来辨识用户的载体（如手机号码）相关联的功能。

宜实现移动支付开通确认的功能。

7.2.9.8 预付卡关联

应实现将客户账户与预付卡相关联的功能，且只能关联不记名预付卡或同名的记名预付卡。

应将客户用于生成条码的预付卡账户、身份证件号码、手机号码进行关联管理。

7.3 银行卡收单功能要求

7.3.1 特约商户管理

7.3.1.1 商户信息登记及管理

应实现商户注册、信息编辑、审核等功能。

7.3.1.2 商户交易状态管理

商户交易状态应至少包括正常、冻结、注销等。
冻结应实现暂停商户交易和重新恢复商户交易的功能。
注销应实现永久停止商户交易的功能。

7.3.1.3 商户信息查询

应实现商户信息查询的功能。

7.3.1.4 商户受理业务管理

应实现商户受理业务的增加、修改和取消等功能。

7.3.1.5 商户终端管理

应对商户控制平台或POS机等终端进行管理。

7.3.2 终端机具信息管理

7.3.2.1 机具申领和报废控制

应具有机具的申领和报废的控制策略，用于控制申领和报废过程。

7.3.2.2 机具信息维护

应能对机具信息（如机具编号、对应商户名称、商户编号等）进行维护。

7.3.2.3 机具信息查询

应能对机具信息（如机具编号、对应商户名称、商户编号等）进行查询。

7.3.3 密钥管理

7.3.3.1 密钥生成

应对密钥生成进行有效的管理和控制。

7.3.3.2 密钥分发

应对密钥分发进行有效的管理和控制。

7.3.3.3 密钥使用

应对密钥使用进行有效的管理和控制。

7.3.3.4 密钥存储

应对密钥存储进行有效的管理和控制。

7.3.3.5 密钥更新

应对密钥更新进行有效的管理和控制。

7.3.3.6 密钥销毁

应对密钥销毁进行有效的管理和控制。

7.3.4 交易处理

7.3.4.1 联机消费

应实现联机消费的功能。

交易信息至少应包括：直接提供商品或服务的商户名称、类别和代码，受理终端类型和代码，交易时间和地点、交易金额、交易类型和渠道、交易发起方式等。

开展条码支付业务，应提供收款扫码功能。

7.3.4.2 联机消费撤销

应实现联机消费撤销的功能。

应提供原交易的凭证，按业务要求输入有关数据，收到响应后，完成消费撤销交易并提供凭证。

7.3.4.3 联机余额查询

应实现联机余额查询的功能。

7.3.4.4 退货

应实现退货的功能。

应提供原消费交易的凭证，按业务要求输入有关数据，收到响应后，完成退货交易并提供凭证。

7.3.4.5 指定账户圈存

应实现指定账户圈存的功能。

7.3.4.6 非指定账户圈存

应实现非指定账户圈存的功能。

7.3.4.7 圈提

应实现圈提交易的功能。

7.3.4.8 脱机消费

应实现脱机消费的功能。

7.3.4.9 脱机消费文件处理

应实现对脱机消费文件进行处理的功能。

7.3.4.10 脱机余额查询

应实现脱机余额查询的功能。

7.3.4.11 交易明细查询

应实现在受理平台和终端上进行交易明细查询的功能。

7.3.4.12 冲正交易

应实现冲正交易的功能。

7.3.4.13 IC卡参数下载

应实现IC卡参数下载的功能。

7.3.4.14 预授权

应实现预授权的功能。

7.3.4.15 预授权撤销

应实现预授权撤销的功能。

7.3.4.16 预授权完成

应实现预授权完成的功能。

7.3.4.17 预授权完成撤销

应实现预授权完成撤销的功能。

7.3.4.18 追加预授权

应实现追加预授权的功能。

7.3.5 资金结算

7.3.5.1 商户结算

应实现商户资金结算的功能。

7.3.5.2 银行清算

应能根据银行的要求正确完成与银行之间的清算。

7.3.6 对账处理

7.3.6.1 发送对账请求

应提供商户提交对账申请的服务。

当商户提交对账申请时，支付服务方提供对账信息的服务。

7.3.6.2 生成对账文件

应实现商户对账文件的查询、浏览或下载等功能。

7.3.7 差错处理

7.3.7.1 单笔退款

应实现单笔交易退款的功能。

支付服务方应将部分或全部已扣款项退还至个人或企业客户的原扣款账户，原扣款账户不能接收退款的，退款至付款方其他账户。

7.3.7.2 批量退款

应实现差错处理过程中批量交易退款的功能。

支付服务方应将部分或全部已扣款项退还至个人或企业客户的原扣款账户，原扣款账户不能接收退款的，退款至付款方其他账户。

7.3.7.3 差错交易查询

应实现对各种差错交易查询的功能。

7.3.7.4 对账差错处理

应实现对账文件出错、对账结果不平等差错情况的处理流程。

7.3.8 运营管理

7.3.8.1 统计报表

应实现对一段时间内的业务操作（如客户注册、商户开通、支付、结算等操作）进行查询统计的功能。

支付服务方可根据自身的情况将“一段时间”细化为“月、季、年”等。

7.3.8.2 运营人员权限管理

应实现运营人员权限的增加、删除、修改和审核等功能。

8 风险监控及反洗钱要求

8.1 网络支付风险监控及反洗钱要求

8.1.1 客户风险管理

8.1.1.1 客户签约

应与客户签订相关协议，针对风险防范条款、客户身份基本信息的使用目的和范围、差错和争议处理、支付账户与支付账户之间或支付账户与银行账户之间的日累计转账限额和笔数等事项，明确双方权利义务。

8.1.1.2 实名认证

应自主或委托合作机构以面对面方式核实客户身份，或通过权威性的外部认证渠道对客户身份基本信息进行实名认证。

实名认证对客户身份基本信息的采集、存储、传输和使用应遵循最小化原则，并按要求留存客户有效身份证件影印件或复印件信息。

应根据外部认证渠道的数量对个人支付账户进行分类管理，应通过至少三个合法安全的外部渠道对企业支付账户进行多重交叉验证。

8.1.1.3 客户风险评级管理

应对客户进行综合性的风险评级，根据评级结果采取相应的风控措施。

应对客户的风险等级进行动态调整。

8.1.1.4 小额免密支付风险管理

经过客户授权，在风险可控条件下，对小额免密支付可适当简化身份验证流程，简化流程时应在商户端展现交易信息。

8.1.2 客户支付账户风险管理

8.1.2.1 支付账户关联管理

应根据客户身份对同一客户的不同支付账户进行关联管理。

同一个人在同一家非银行支付机构只能开立一个Ⅲ类账户。

8.1.2.2 支付账户资金管理

由预付卡转账至支付账户中的余额应单独管理。

支付账户不应透支。

8.1.2.3 支付账户风险管理

应建立联系电话号码、个人身份证号码与支付账户的对应关系。

自开户之日起6个月内无交易记录的账户，非银行支付机构应暂停其资金往来业务，仅保留非资金类功能。

8.1.3 商户风险管理

8.1.3.1 商户资质审核

应审核特约商户资质，方式包括但不限于查询统一社会信用代码等。

应对特约商户的法定代表人或负责人实行实名制管理。

应具有明确的审核流程和标准，明确资质审核岗位和权限。

8.1.3.2 商户签约

应与商户签订相关协议，就风险防范条款、商户身份基本信息的使用目的和范围、可受理的卡种类、开通的交易类型、结算账户的设置和变更、资金结算周期、结算手续费标准、差错和争议处理等事项，明确双方权利义务。

8.1.3.3 商户日常风险管理

应向商户发放风险提示信息，对商户进行风险培训。

8.1.4 交易监控

8.1.4.1 交易查询

应实现交易信息的查询功能。

8.1.4.2 交易监控模型

应利用历史交易数据分析、客户鉴别安全强度、客户行为建模、监测终端设备异常等手段，建立交易风险监控模型和系统。

8.1.4.3 当日累计交易限额

应根据客户的支付验证方式的安全级别设置当日累计交易限额，并对其正确识别、记录、响应。

应按约定限制支付账户与支付账户之间、支付账户与银行账户之间的日累计转账额度。

开展条码支付业务，应根据条码支付业务场景和客户的风险防范能力，设置当日累计交易限额。

8.1.4.4 当月累计交易限额

开展条码支付业务，应根据小微商户风险等级和条码支付业务场景，设置当月累计交易限额。

8.1.4.5 当年累计交易限额

应根据客户的账户等级设置当年累计交易限额，并对其正确识别、记录、响应。

8.1.4.6 当日累计转账限次

应按约定限制支付账户与支付账户之间、支付账户与银行账户之间的日累计转账次数。

8.1.4.7 异常行为监控

应利用 IP 地址、终端设备标识信息、浏览器缓存信息等对批量或高频登录等异常行为进行综合识别。

8.1.4.8 账户资金监控

应实现对客户账户资金异常转移、交易、结算的审核和确认等处理。

8.1.4.9 可疑事件处理

对于可疑事件应通过短信、电话、客户端软件等进行风险提示，并根据违反规则事件的风险级别采取调查核实、延迟结算、拒绝请求等处理措施。

8.1.4.10 事件报警

应实现对违反规则事件进行报警并提供事件的查询统计的功能。

8.1.4.11 黑名单

应实现黑名单管理功能，并对黑名单中客户的行为进行正确的识别、记录、响应。

8.1.5 移动近场支付交易风险管理

8.1.5.1 联机交易 ARQC/ARPC 验证

应能进行联机交易的ARQC/ARPC认证。

8.1.5.2 联机报文 MAC 验证

应对联机交易报文进行MAC验证。

8.1.5.3 脱机交易 TAC 验证

脱机交易中，应进行TAC验证。

8.1.5.4 脱机交易 MAC 验证

脱机交易中，应进行MAC验证。

8.1.5.5 密码错误情况下的交易请求

相关风控制度应对联机交易密码错误以及多次密码错误后的处理进行规定，系统应对联机交易密码错误情况进行正确识别、记录并拒绝交易请求，系统应按风控制度规定在多次密码错误后冻结卡片。

8.1.5.6 非法卡号交易

相关风控制度应对非法卡号交易及处理进行规定，系统应对非法卡号交易进行正确识别、记录，并拒绝交易请求。

8.1.6 风险及反洗钱管理制度

8.1.6.1 风控规则管理

应确保在相关风险管理制度中完整、明确的定义各种风险类别。

应确保在相关风险管理制度中完整、明确的定义各类（如实时、异常等）事件监控规则。

应确保在相关风险管理制度中完整、明确的定义各项风控规则的变更、审核和确认制度。

8.1.6.2 反洗钱管理制度和操作规程

应制定大额交易和可疑交易报告内部管理制度和操作规程，对大额交易和可疑交易报告工作作出统一要求，并对分支机构、附属机构大额交易和可疑交易报告制度的执行情况进行监督管理。

8.1.6.3 岗位设置

应设立专职的反洗钱岗位，配备专职人员负责大额交易和可疑交易报告工作，并提供必要的资源保障和信息支持。

8.1.6.4 事件管理与处置

应健全紧急止付和快速冻结机制并确保在相关风险管理制度中完整、明确的定义各项风险事件处理规则以及向上级部门和主管部门报送的机制，并保留事件记录。

8.1.6.5 风险报表

应提供一段时间内的风险事件报表，或提供查询一段时间内的风险事件的报表功能。

8.1.7 终端风险管理

8.1.7.1 终端使用生命周期的管理

应提供POS机管理制度，对POS机的管理流程进行详细规定，包括申请、参数设置、程序灌装、使用、更换、维护、撤销等。

应提供商户申请、使用、更换、维护、撤销POS机的详细记录。

开展条码支付业务，应提供终端管理制度，对终端管理流程进行详细规定，包括申请、使用、更换、维护、撤销等。

8.1.7.2 终端密钥和参数的安全管理

应提供POS机密钥和参数的管理制度，对POS机密钥和参数进行严格管理。

每台POS机应具有唯一的密钥加密密钥，并对其严格管理。

POS机密钥算法应符合双倍长密钥算法规范。

开展条码支付业务，应提供终端密钥和参数的管理制度，对终端密钥和参数进行严格管理。

8.1.7.3 控制移动 POS 机的安装

应在制度中详细规定移动POS机的安装和管理要求，对移动POS机的安装进行限制。

商户安装移动POS机，应进行详细登记，登记内容应包括移动POS机通信卡或通信模块编号及运营商信息等。

8.1.7.4 终端安全检测报告和终端入网检测报告

使用的终端应有安全检测报告，报告内容应能反映终端的安全状况。

应有终端入网检测报告，报告内容应能明确POS签购单打印格式和要素。

开展条码支付业务，使用的终端应具有安全认证证书。

8.1.7.5 密码键盘安全检测报告

使用的密码键盘应有安全检测报告，报告内容应能反映终端的安全状况。

8.1.7.6 终端监控管理

应建立对受理终端的日常监控巡查机制，重点检查终端是否被非法改装，防止不法分子窃取账户信息，并保留巡查记录，包括终端巡检制度、巡检内容、巡检记录等。

8.2 预付卡发行与受理风险监控及反洗钱要求

8.2.1 商户风险管理

8.2.1.1 商户资质审核

应审核特约商户资质，方式包括但不限于查询统一社会信用代码等。

应对特约商户的法定代表人或负责人实行实名制管理。

应具有明确的审核流程和标准，明确资质审核岗位和权限。

8.2.1.2 商户签约

应与特约商户签订协议，就可受理的预付卡种类、开通的交易类型、商户结算账户的设置和变更、资金结算周期、结算手续费标准、差错和争议处理等事项，明确双方的权利、义务和违约责任。

8.2.1.3 商户日常风险管理

应向特约商户发放风险提示信息，对特约商户进行风险培训。

应提示特约商户定期审核网站，杜绝非法链接。

8.2.1.4 合作的第三方机构的风险管理

应对合作的第三方机构进行风险提示和培训。

8.2.1.5 商户黑名单管理

应实现商户黑名单的管理功能，并对黑名单中的商户进行风险监控。

8.2.2 交易风险管理

8.2.2.1 联机报文 MAC 验证

应对联机交易报文进行MAC验证。

8.2.2.2 脱机交易 TAC 验证

脱机交易中，应进行TAC验证。

8.2.2.3 脱机交易 MAC 验证

脱机交易中，应进行MAC验证。

8.2.2.4 账户余额限额

系统应对预付卡账户余额最大值进行设置，并对其进行正确识别、记录、响应。

8.2.2.5 可疑交易处理

系统应实现可疑交易处理规则的设置，并对其进行正确识别、记录、响应，以实现对可疑交易的查询、分析、处理等服务。

8.2.2.6 密码错误情况下的交易请求

系统应实现对密码错误的交易请求进行正确识别、拒绝和记录。
系统应实现对卡片冻结的密码错误次数的设置，并对其进行正确识别、记录、响应。

8.2.2.7 卡片有效期检查

预付卡联机交易时,应检查非记名预付卡卡片有效期,并在系统中拒绝并记录过期卡片的交易请求。

8.2.2.8 当日累计交易限额

开展条码支付业务时，应根据条码支付业务场景和客户的风险防范能力，设置当日累计交易限额。

8.2.2.9 当月累计交易限额

开展条码支付业务时，应根据小微商户风险等级和条码支付业务场景，设置当月累计交易限额。

8.2.3 风险及反洗钱管理制度

8.2.3.1 风控规则管理

应确保在相关风险管理制度中完整、明确的定义各种风险类别。
应确保在相关风险管理制度中完整、明确的定义各类（如实时、异常等）事件监控规则。
应确保在相关风险管理制度中完整、明确的定义各项风控规则的变更、审核和确认制度。

8.2.3.2 反洗钱管理制度和操作规程

应制定大额交易和可疑交易报告内部管理制度和操作规程,对大额交易和可疑交易报告工作作出统一要求，并对分支机构、附属机构大额交易和可疑交易报告制度的执行情况进行监督管理。

8.2.3.3 岗位设置

应设立专职的反洗钱岗位，配备专职人员负责大额交易和可疑交易报告工作，并提供必要的资源保障和信息支持。

8.2.3.4 事件管理与处置

应健全紧急止付和快速冻结机制并确保在相关风险管理制度中完整、明确的定义各项风险事件处理规则以及向上级部门和主管部门报送的机制，并保留事件的记录。

8.2.3.5 风险报表

应提供一段时间内的风险事件报表，或提供查询一段时间内的风险事件的报表功能。

8.2.4 终端风险管理

8.2.4.1 终端使用生命周期管理

应提供POS机管理制度，对POS机的管理流程进行详细规定，包括申请、参数设置、程序灌装、使用、更换、维护、撤销等。

应提供商户申请、使用、更换、维护、撤销POS机的详细记录。

开展条码支付业务，应提供终端管理制度，对终端管理流程进行详细规定，包括申请、使用、更换、维护、撤销等。

8.2.4.2 终端密钥和参数的安全管理

应提供POS机密钥和参数的管理制度，对POS机密钥和参数进行严格管理。

每台POS机应具有唯一的密钥加密密钥，并对其严格管理。

POS机密钥算法应符合双倍长密钥算法规范。

开展条码支付业务，应提供终端密钥和参数的管理制度，对终端密钥和参数进行严格管理。

8.2.4.3 控制移动 POS 机的安装

应在制度中详细规定移动POS机的安装和管理要求，对移动POS机的安装的进行限制。

商户安装移动POS机，应进行详细登记，登记内容应包括移动POS机通信卡或通信模块编号及运营商信息等。

8.2.4.4 终端安全检测报告和终端入网检测报告

使用的终端应有安全检测报告，报告内容应能反映终端的安全状况。

应有终端入网检测报告，报告内容应能明确POS签购单打印格式和要素。

开展条码支付业务，使用的终端应具有安全认证证书。

8.2.4.5 密码键盘安全检测报告

使用的密码键盘应有安全检测报告，报告内容应能反映终端的安全状况。

8.2.4.6 终端监控管理

应建立对受理终端的日常监控巡查机制，重点检查终端是否被非法改装，防止不法分子窃取账户信息，并保留巡查记录，包括终端巡检制度、巡检内容、巡检记录等。

8.2.5 条码支付客户风险管理

8.2.5.1 客户签约

应与客户签订相关协议，就风险防范条款、客户身份基本信息的使用目的和范围、差错和争议处理、根据风险防范能力分级的条码支付限额等事项，明确双方权利义务。

8.2.5.2 实名认证

应自主或委托合作机构以面对面方式核实客户身份，或通过权威性的外部认证渠道对客户身份基本信息进行实名认证。

实名认证对客户身份基本信息的采集、存储、传输和使用应遵循最小化原则，并按要求留存客户有效身份证件影印件或复印件信息。

8.2.5.3 客户风险评级管理

应对客户进行风险防范能力分级。

8.2.5.4 小额免密支付风险管理

经过客户授权，在风险可控条件下，对小额免密支付可适当简化身份验证流程，简化流程时应在商户端展现交易信息。

8.3 银行卡收单风险监控及反洗钱要求

8.3.1 商户风险管理

8.3.1.1 商户资质审核

应审核特约商户资质，方式包括但不限于查询统一社会信用代码等。

应对特约商户的法定代表人或负责人实行实名制管理。

应具有明确的审核流程和标准，明确资质审核岗位和权限。

8.3.1.2 商户签约

应与特约商户签订协议，就可受理的银行卡种类、开通的交易类型、收单银行结算账户的设置和变更、资金结算周期、结算手续费标准、差错和争议处理等事项，明确双方的权利、义务和违约责任。

8.3.1.3 商户日常风险管理

应向特约商户发放风险提示信息，对特约商户进行风险培训。

应提示特约商户定期审核网站，杜绝非法链接。

不应为入网不满90日或者入网后连续正常交易不满30日的特约商户提供T+0资金结算服务。

8.3.1.4 合作的第三方机构的风险管理

应对合作的第三方机构进行风险提示和培训。

8.3.1.5 商户黑名单管理

应实现商户黑名单的管理功能，并对黑名单中的商户进行风险监控。

应在机构间实现商户黑名单的信息共享。

8.3.2 交易风险管理

8.3.2.1 联机交易 ARQC/ARPC 验证

应能进行联机交易的ARQC/ARPC验证。

8.3.2.2 联机报文 MAC 验证

应对联机交易报文进行MAC验证。

8.3.2.3 脱机交易 TAC 验证

脱机交易中，应进行TAC验证。

8.3.2.4 脱机交易 MAC 验证

脱机交易中，应进行MAC验证。

8.3.2.5 可疑交易处理

应实现可疑交易处理规则的设置，并对其进行正确识别、记录、响应，以实现对可疑交易的查询、分析、处理等服务。

8.3.2.6 卡片黑名单监控

应实现卡片黑名单的管理功能，对黑名单中的交易进行风险监控，并对其进行正确识别、记录、响应。

8.3.3 风险及反洗钱管理制度

8.3.3.1 风控规则管理

应确保在相关风险管理制度中完整、明确的定义各种风险类别。

应确保在相关风险管理制度中完整、明确的定义各类（如实时、异常等）事件监控规则。

应确保在相关风险管理制度中完整、明确的定义各项风控规则的变更、审核和确认制度。

8.3.3.2 反洗钱管理制度和操作规程

应制定大额交易和可疑交易报告内部管理制度和操作规程，对大额交易和可疑交易报告工作作出统一要求，并对分支机构、附属机构大额交易和可疑交易报告制度的执行情况进行监督管理。

8.3.3.3 岗位设置

应设立专职的反洗钱岗位，配备专职人员负责大额交易和可疑交易报告工作，并提供必要的资源保障和信息支持。

8.3.3.4 事件管理与处置

应健全紧急止付和快速冻结机制并确保在相关风险管理制度中完整、明确的定义各项风险事件处理规则以及向上级部门和主管部门报送的机制，并保留事件记录。

8.3.3.5 风险报表

应提供一段时间内的风险事件报表，或提供查询一段时间内的风险事件的报表功能。

8.3.4 终端风险管理

8.3.4.1 终端使用生命周期的管理

应提供POS机管理制度，对POS机的管理流程进行详细规定，包括申请、参数设置、程序灌装、使用、更换、维护、撤销等。

应提供商户申请、使用、更换、维护、撤销POS机的详细记录。

开展条码支付业务，应提供终端管理制度，对终端管理流程进行详细规定，包括申请、使用、更换、维护、撤销等。

8.3.4.2 终端密钥和参数的安全管理

应提供POS机密钥和参数的管理制度，对POS机密钥和参数进行严格管理。

每台POS机应具有唯一的密钥加密密钥，并对其严格管理。

POS机密钥算法应符合双倍长密钥算法规范。

开展条码支付业务，应提供终端密钥和参数的管理制度，对终端密钥和参数进行严格管理。

8.3.4.3 控制移动 POS 机的安装

应在制度中详细规定移动POS机的安装和管理要求，对移动POS机的安装进行限制。

商户安装移动POS机，应进行详细登记，登记内容应包括移动POS机通信卡或通信模块编号及运营商信息等。

8.3.4.4 终端安全检测报告和终端入网检测报告

使用的终端应有安全检测报告，报告内容应能反映终端的安全状况。

应有终端入网检测报告，报告内容应能明确POS签购单打印格式和要素。

开展条码支付业务，使用的终端应具有安全认证证书。

8.3.4.5 密码键盘安全检测报告

使用的密码键盘应有安全检测报告，报告内容应能反映终端的安全状况。

8.3.4.6 终端监控管理

应建立对受理终端的日常监控巡查机制，重点检查终端是否被非法改装，防止不法分子窃取账户信息，并保留巡查记录，包括终端巡检制度、巡检内容、巡检记录等。

9 性能要求

支付业务设施性能检测基本要求见表1。

表1 支付业务设施性能检测基本要求

策略	并发数	CPU平均利用率	并发成功率	交易成功率	测试时长
稳定并发	比对性能需求表中高峰时段并发数	<=80%	100％	>=99%	>=30分钟

10 安全性要求

10.1 物理安全[1)]

10.1.1 物理位置选择

1) 本条仅适用于自建机房的情况。

10.1.1.1 机房所在建筑物选择

机房应选择设在中华人民共和国境内具有防震、防风和防雨等能力的建筑中。

10.1.1.2 建筑物内机房位置选择

机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

10.1.2 物理访问控制

10.1.2.1 机房设置电子门禁系统

机房出入口应安排专人值守并宜配置电子门禁系统，控制、鉴别和记录进出的人员。

10.1.2.2 来访人员申请和审批

来访人员进入机房应经过申请和审批，并限制和监控来访人员的活动范围。

10.1.2.3 对机房划分区域进行管理

宜对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域。

10.1.2.4 重要区域设置第二道电子门禁系统

重要区域宜配置第二道电子门禁系统，控制、鉴别和记录进出的人员。

10.1.3 防盗窃和防破坏

10.1.3.1 设备放置

应将主要设备放置在机房内。

10.1.3.2 设备固定

应对设备或主要部件进行固定，并设置明显的不易除去的标记。

10.1.3.3 通信线缆铺设

应将通信线缆铺设在隐蔽处，可铺设在地下或管道中。

10.1.3.4 机房监控防入侵报警系统

应设置机房防盗报警系统或设置有专人值守的视频监控系统。

10.1.4 防雷击

10.1.4.1 安装避雷装置

机房建筑应设置避雷装置。

10.1.4.2 安装防雷装置

应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

10.1.4.3 交流电源地线

机房应设置交流电源地线。

10.1.5 防火

10.1.5.1 设置火灾自动消防系统

机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。

10.1.5.2 采用耐火的建筑材料

机房及相关的工作房间和辅助房间应采用具有耐火等级的建筑材料。

10.1.5.3 采用区域隔离防火措施

应对机房划分区域进行管理，区域和区域之间采用隔离防火措施。

10.1.6 防水和防潮

10.1.6.1 水管安装要求

水管安装不应穿过机房屋顶和活动地板下。

10.1.6.2 防雨水措施

应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

10.1.6.3 防水检测和报警

应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

10.1.7 防静电

10.1.7.1 接地防静电措施

设备应采用必要的接地防静电措施。

10.1.7.2 采用防静电地板

机房应采用防静电地板。

10.1.7.3 安装静电消除装置

应采用措施防止静电的产生，如采用静电消除器、佩戴防静电手环等。

10.1.8 温湿度控制

机房应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

10.1.9 电力供应

10.1.9.1 供电线路防护设备配置

应在机房供电线路上配置稳压器和过电压防护设备。

10.1.9.2 备用电力供应

应提供短期的备用电力供应，至少满足设备在断电情况下一定时间内的正常运行要求。

10.1.9.3 冗余或并行的电力电缆线路设置

应设置冗余或并行的电力电缆线路为计算机系统供电。

10.1.9.4 备用供电系统

应建立备用供电系统。

10.1.10 电磁防护

10.1.10.1 防止电磁干扰

应采用接地方式防止外界电磁干扰和设备寄生耦合干扰。

10.1.10.2 电源线和通信线缆隔离铺设

电源线和通信线缆应隔离铺设，避免互相干扰。

10.1.10.3 关键设备电磁屏蔽

应对关键设备实施电磁屏蔽。

10.2 网络安全性要求

10.2.1 结构安全

10.2.1.1 网络冗余和备份

应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要。

应保证网络各个部分的带宽满足业务高峰期需要。

增强要求：

应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

10.2.1.2 网络安全路由

应在业务终端与业务服务器之间进行路由控制，建立安全的访问路径。

10.2.1.3 网络安全防火墙

应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。

应具备完整清晰的物理边界。

10.2.1.4 网络拓扑结构

应绘制与当前运行情况相符的网络拓扑结构图。

10.2.1.5 IP 子网划分

应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，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。

10.2.2 网络访问控制

10.2.2.1 网络域安全隔离和限制

应在网络边界和区域之间，根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。

10.2.2.2 内容过滤

应在关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制。

10.2.2.3 访问控制

应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。
应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。
应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。

10.2.2.4 会话控制

应在会话处于非活跃状态一定时间后或会话结束后终止网络连接。

10.2.2.5 远程访问控制

应通过技术手段控制管理用户对服务器进行远程访问，如使用VPN等技术。

10.2.3 网络安全审计

10.2.3.1 日志信息

应对网络系统中的网络设备运行状况、网络流量、用户行为和重要安全事件等进行日志记录。
应确保记录的留存时间符合法律法规要求。

10.2.3.2 日志权限和保护

应对日志记录进行保护，避免受到未预期的删除、修改或覆盖等。

10.2.3.3 审计工具

宜具备日志审计工具，提供对日志记录数据进行统计、查询、分析及生成审计报表的功能。

10.2.3.4 网络对象审计

应在网络边界、重要网络节点进行安全审计，审计范围应覆盖每个用户。
审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。
应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
审计记录应至少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。
应确保审计记录的留存时间符合法律法规要求。
宜保护审计进程，避免受到未预期的中断。
应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
增强要求：
应根据系统统一安全策略，实现集中审计。

应保护审计进程，避免受到未预期的中断。

10.2.4 边界完整性检查

应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信。

应定期检查违反规定无线上网及其他违反网络安全策略的行为。

应能对非授权设备私自连接到内部网络的行为进行检查，并对其进行有效阻断。

应能对内部网络用户私自连接到外部网络的行为进行检查，并对其进行有效阻断。

应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络。

增强要求：

对非法外联和非法接入行为进行检测并阻断的同时，应以报警方式通知管理员。

10.2.5 网络入侵防范

应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。

应在关键网络节点处检测和限制从内部发起的网络攻击行为。

应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击的检测和分析。

当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应报警。

增强要求：

应在系统网络中监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。

当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应报警并自动采取相应措施。

10.2.6 恶意代码防范

10.2.6.1 恶意代码防范措施

应在关键网络节点处对恶意代码进行检测和清除。

10.2.6.2 定时更新

应定时更新升级恶意代码库及检测系统。

10.2.7 网络设备防护

10.2.7.1 设备登录设置

应对登录网络设备的用户进行身份鉴别。

应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和网络登录连接超时自动退出等措施。

主要网络设备宜采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现。

增强要求：

主要网络设备应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现。

10.2.7.2 设备登录口令安全性

身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

10.2.7.3 登录地址限制

应对登录网络设备的源地址进行限制。

10.2.7.4 远程管理安全

当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

10.2.7.5 设备用户设置

网络设备用户的标识应唯一，及时删除或停用多余的、过期的账户，避免共享账户的存在。
应重命名或删除默认账户，修改默认账户的默认口令。

10.2.7.6 权限分离

应实现设备特权用户的权限分离。

10.2.7.7 最小化服务

应实现设备的最小服务配置，并对配置文件进行定期离线备份。

10.2.8 网络安全管理

10.2.8.1 定期补丁安装

应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份。

10.2.8.2 漏洞扫描

应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞及时进行修补。

10.3 主机安全性要求

10.3.1 身份鉴别

10.3.1.1 系统与应用管理员用户设置

应对登录的管理用户进行身份标识和鉴别。
应为不同管理用户分配不同的用户名，确保用户名具有唯一性。
宜采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。
增强要求：
应设置鉴别警示信息，描述未授权访问可能导致的后果。
应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，且其中至少一种鉴别技术应使用动态口令、密码技术或生物技术来实现。

10.3.1.2 系统与应用管理员口令安全性

管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

10.3.1.3 登录策略

应提供登录失败处理功能，应采取结束会话、限制非法登录次数和登录连接超时自动退出等措施。

10.3.2 访问控制

10.3.2.1 访问控制范围

应启用访问控制功能，依据安全策略控制用户对资源的访问。

应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

应实现不同特权用户的权限分离。

应能建立一条安全的信息传输路径，对设备进行管理。

10.3.2.2 主机信任关系

应避免不必要的主机信任关系。

10.3.2.3 默认过期账户

应及时删除多余的、过期的账户，避免共享账户的存在。

应严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令。

10.3.3 安全审计

10.3.3.1 日志信息

应对用户行为、系统资源的异常使用和重要系统命令的使用等进行日志记录。

应确保日志记录的留存时间符合法律法规要求。

10.3.3.2 日志权限和保护

应保护日志记录，避免受到未预期的删除、修改或覆盖等。

10.3.3.3 审计工具

宜具备日志审计工具，提供对日志记录数据进行统计、查询、分析及生成审计报表的功能。

10.3.3.4 主机对象审计

审计范围应覆盖到服务器和重要客户端上的每个用户。

审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。

审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。

应确保审计记录的留存时间符合法律法规要求。

应能根据记录数据进行分析，并生成审计报表。

应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

宜保护审计进程，避免受到未预期的中断。

增强要求：

应能根据信息系统的统一安全策略，实现集中审计。

应保护审计进程，避免受到未预期的中断。

10.3.4 系统保护

10.3.4.1 系统备份

应具有系统备份或系统重要文件备份。

10.3.4.2 磁盘空间安全

应对主机磁盘空间进行合理规划，确保磁盘空间使用安全。

10.3.4.3 主机安全加固

应对主机进行安全加固。

10.3.5 入侵防范

10.3.5.1 入侵防范记录

应能检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击类型、攻击目的、攻击时间，并在发生严重入侵事件时报警。

宜能对重要程序的完整性进行检测，并在检测到完整性受到破坏后，采取恢复的措施。

增强要求：

应能对系统程序、应用程序和重要配置文件/参数进行可信执行验证，并在检测到其完整性受到破坏时采取恢复措施。

10.3.5.2 关闭服务和端口

应关闭系统不必要的服务和端口。

10.3.5.3 最小安装原则

应遵循最小安装的原则，仅安装需要的组件和应用程序。

10.3.6 恶意代码防范

10.3.6.1 防范软件安装部署

应至少在生产系统的服务器中安装防恶意代码软件。

10.3.6.2 病毒库定时更新

应及时更新防恶意代码软件版本和恶意代码库。

10.3.6.3 防范软件统一管理

宜支持防范软件的统一管理。

10.3.7 连接控制

应通过设定终端接入方式、网络地址范围等条件限制终端登录。

10.3.8 主机安全管理

10.3.8.1 漏洞扫描

应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。

10.3.8.2 系统补丁

应具有主机系统补丁安装方案或制度，并根据方案或制度及时更新系统补丁。在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。

10.3.8.3 系统操作管理

应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，不应进行未经授权的操作。

10.4 应用安全性要求

10.4.1 身份鉴别

10.4.1.1 系统与普通用户设置

应提供系统管理员和普通用户的设置功能。

应提供专用的登录控制模块对登录用户进行身份标识和鉴别。

内部管理应用宜采用两种或两种以上的身份鉴别方式。

10.4.1.2 登录口令安全性

系统管理员与普通用户口令应具有一定的复杂度。

应强制用户首次登录时修改初始口令。

宜提示用户定期修改口令。

宜限制系统管理用户的口令有效期。

应对输入的登录口令进行安全保护，防范被窃取。

如系统为内部使用，不对互联网用户提供服务，该项不适用。

短信验证方式不应作为用户登录的唯一验证方式。

10.4.1.3 支付密码安全性

应提供独立的支付密码和健全的密码重置机制。

应严格限制使用初始支付密码并提示客户及时修改，建立支付密码复杂度系统校验机制，避免支付密码过于简单或与客户个人信息（如出生日期、证件号码、手机号码等）相似度过高。

客户输入支付密码时，客户端不应明文显示。

应在重置支付密码等关键操作时提供多种身份验证方式保障支付安全，并以短信、邮件等方式告知用户。

10.4.1.4 支付安全策略

支付前应按照《非银行支付机构网络支付业务管理办法》、《条码支付业务规范（试行）》对用户身份进行鉴别。

身份鉴别可组合选用下列三种要素，对客户支付交易进行验证：

——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。

用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全。

使用数字证书、电子签名作为身份鉴别要素的，应优先使用SM系列算法，并符合GM/T 0054—2018的相关规定，具体算法定义见GB/T 32918、GB/T 32905、GB/T 32907（下同）。

应采用技术手段对私钥信息进行保护。

10.4.1.5 非法访问控制策略

应提供登录失败处理功能，应采取结束会话、限制非法登录次数和登录连接超时自动退出等措施，并根据安全策略配置相关参数。

应对非法访问进行警示和记录。

10.4.1.6 身份标识唯一性

应提供用户身份标识唯一性检查功能，保证应用系统中不存在重复用户身份标识。

10.4.1.7 及时清除鉴别信息

会话结束后应及时清除客户端鉴别信息。

10.4.2 WEB 应用安全

10.4.2.1 登录防穷举

应提供登录防穷举的措施，如图片验证码等。

如系统为内部使用，不对互联网用户提供服务，该项不适用。

10.4.2.2 网站页面注入防范

应采取防范SQL注入、Path注入和LDAP注入等风险的措施。

10.4.2.3 网站页面跨站脚本攻击防范

应采取防范跨站脚本攻击风险的措施。

10.4.2.4 网站页面源代码暴露防范

应采取防范源代码暴露的措施。

10.4.2.5 网站页面黑客挂马防范

应采取防范网站页面黑客挂马的机制和措施。

如系统为内部使用，不对互联网用户提供服务，该项不适用。

10.4.2.6 网站页面防篡改措施

宜采取网站页面防篡改措施。

如系统为内部使用，不对互联网用户提供服务，该项不适用。

10.4.2.7 网站页面防钓鱼

宜提供防钓鱼的防伪信息验证。

如系统为内部使用，不对互联网用户提供服务，该项不适用。

10.4.2.8 漏洞扫描

应定期进行漏洞扫描，对发现的WEB应用、中间件等安全漏洞及时进行修补。

10.4.3 访问控制

10.4.3.1 访问权限设置

应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问。

应由授权主体配置访问控制策略，并严格限制默认账户的访问权限。
应授予不同用户为完成各自承担任务所需的最小权限，并在权限之间形成互相制约的关系。
应及时删除或停用多余、过期的账户，避免共享账户的存在。

10.4.3.2 自主访问控制范围

访问控制的覆盖范围应包括与资源访问相关的主体、客体及主体客体之间的操作。

10.4.3.3 业务操作日志

应具有所有业务操作日志。

10.4.3.4 关键数据操作控制

应严格控制用户对关键数据的操作。
关键数据包括敏感数据、重要业务数据、系统管理数据等。

10.4.4 安全审计

10.4.4.1 日志信息

应对业务系统和管理系统的用户行为、支付标记化行为、系统资源的异常使用和重要系统命令的使用等进行日志记录。
如使用支付标记化技术，日志应可查询支付标记化行为。

10.4.4.2 日志权限和保护

应对日志记录进行保护，避免受到未预期的删除、修改或覆盖等。
宜保证无法单独中断日志进程。

10.4.4.3 审计工具

宜具备日志审计工具，提供对日志记录数据进行统计、查询、分析及生成审计报表的功能。

10.4.4.4 应用操作审计

应提供覆盖到应用系统每个用户的安全审计功能。
审计内容应包括用户重要行为和异常行为等系统内重要的安全相关事件。
审计记录应至少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。
宜保护审计进程，避免受到未预期的中断。
增强要求：
应根据系统的统一安全策略，实现集中审计。
应保护审计进程，避免受到未预期的中断。

10.4.5 剩余信息保护

应对无用的过期信息、文档进行完整删除。
增强要求：
在存有鉴别信息的存储空间被释放或重新分配之前，应保证鉴别信息得到完整清除。
在存有敏感数据的存储空间被释放或重新分配之前，应保证敏感数据得到完整清除。

10.4.6 资源控制

10.4.6.1 连接控制

宜能根据业务需求，对系统的最大并发会话连接数进行限制。

宜能对一个时间段内可能的并发会话连接数进行限制。

10.4.6.2 会话控制

当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。

应能对单个账户的多重并发会话进行限制。

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，防止未授权访问。

应用审计日志宜记录暴力破解会话令牌的事件。

10.4.6.3 进程资源分配

应提供服务优先级设定功能，并在安装后根据安全策略设定访问用户或请求进程的优先级，根据优先级分配系统资源。

10.4.7 应用容错

10.4.7.1 数据有效性校验

应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式及长度符合系统设定要求。

10.4.7.2 容错机制

应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

增强要求：

应提供自动恢复功能，当故障发生时恢复原来的工作状态，如自动启动新的进程。

10.4.8 抗抵赖

10.4.8.1 原发和接收证据

增强要求：

应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能。

应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

应对数据原发行为和数据接收行为进行数字签名，数字签名应优先使用SM系列算法，并符合GM/T 0054—2018的相关规定。

10.4.8.2 时间同步机制

系统时间应由系统范围内唯一确定的时钟产生，本地时间宜从国家权威时间源采时，保证时间的同一性。

增强要求：

本地时间应从国家权威时间源采时，保证时间的同一性。

应采用可信时间戳服务，优先采用SM系列算法，并符合GM/T 0054—2018的相关规定。

应安全保存时间戳及相关信息，确保数据的可审计性，实现系统数据处理的抗抵赖性。

10.4.9 编码安全

10.4.9.1 源代码审查

应对源代码进行安全性审查，提供源代码审查报告。

增强要求：

应通过自动化工具（如弱点扫描工具、静态代码审查工具等）对应用程序进行检查。

10.4.9.2 插件安全性审查

应对插件进行安全性审查，提供插件审查报告。

10.4.9.3 编码规范约束

应具有编码规范约束制度，按照编码规范进行编码。

10.4.9.4 源代码管理

应具有源代码管理制度，具有源代码管理记录。在每次源代码变更时，需填写变更备注信息。

10.4.10 电子认证应用

10.4.10.1 数字证书

在外部业务处理过程中，应使用第三方电子认证服务生成的数字证书或经国家有关管理部门许可的电子认证服务生成的数字证书。

在内部业务（仅涉及本机构内人员或设备的业务）处理过程中，可使用自建的电子认证服务生成的数字证书。

电子认证应优先使用SM系列算法，并符合GM/T 0054—2018的相关规定。

10.4.10.2 电子认证

应使用有效的电子认证。在外部关键业务处理过程中（包含但不限于支付、转账等），应使用经过国家有关管理部门许可的电子认证服务。

电子认证应优先使用SM系列算法，并符合GM/T 0054—2018的相关规定。

10.4.10.3 电子认证证书私钥保护

应对所持有的电子认证证书私钥进行有效保护。

10.4.11 脱机数据认证

10.4.11.1 密钥和证书

应符合JR/T 0025.7—2018中5.2的规定，生成符合业务要求的密钥和证书。

适用于移动电话支付、预付卡发行与受理和银行卡收单业务。

10.4.11.2 数据认证

脱机交易应采用静态数据认证、动态数据认证或复合动态数据认证的方式。

适用于移动电话支付、预付卡发行与受理和银行卡收单业务。

10.4.12 应用密文和发卡机构认证

10.4.12.1 应用密文产生

应符合JR/T 0025.7—2018中6.2的规定，生成符合业务要求的应用密文。
适用于移动电话支付和预付卡发行与受理业务。

10.4.12.2 发卡机构认证

发卡机构认证过程应符合JR/T 0025.7—2018中6.3的规定。
适用于移动电话支付和预付卡发行与受理业务。

10.4.12.3 密钥管理

密钥管理应符合JR/T 0025.7—2018中6.4的规定。
适用于移动电话支付和预付卡发行与受理业务。

10.4.13 安全报文

10.4.13.1 报文格式

报文格式应符合JR/T 0025.7—2018中7.2的规定。
适用于移动电话支付、预付卡发行与受理和银行卡收单业务。

10.4.13.2 报文完整性验证

应对报文完整性进行验证。
适用于移动电话支付、预付卡发行与受理和银行卡收单业务。

10.4.13.3 报文私密性

应保证报文私密性。
适用于移动电话支付、预付卡发行与受理和银行卡收单业务。

10.4.13.4 密钥管理

应对密钥进行安全管理。
适用于移动电话支付、预付卡发行与受理和银行卡收单业务。

10.4.14 卡片安全

10.4.14.1 共存应用

如支持多应用，应保证多应用安全共存。
适用于移动电话支付和预付卡发行与受理业务。

10.4.14.2 密钥的独立性

应符合JR/T 0025.7—2018中8.2的规定，保证密钥的独立性。
适用于移动电话支付和预付卡发行与受理业务。

10.4.14.3 卡片内部安全体系

应符合JR/T 0025.7—2018中8.3的规定，建立卡片内部安全体系。
适用于移动电话支付和预付卡发行与受理业务。

10.4.14.4 卡片中密钥的种类

应符合JR/T 0025.7—2018中8.4的规定，对卡片中不同应用密钥进行分类。

适用于移动电话支付和预付卡发行与受理业务。

10.4.15 终端安全

10.4.15.1 终端数据安全性要求

应符合JR/T 0025.7—2018中9.1的规定。

适用于移动电话支付、预付卡发行与受理和银行卡收单业务。

10.4.15.2 终端设备安全性要求

应符合国家相关标准的规定，并提供金融行业检测机构出具的安全检测报告。

数字电视支付中使用的机顶盒应经过第三方测试机构安全检测。机顶盒和相关IC卡应能防范通过物理攻击的手段获取设备内的敏感信息。

10.4.15.3 终端密钥管理要求

应符合国家相关标准的规定，并提供金融行业检测机构出具的安全检测报告。

10.4.16 密钥管理体系

10.4.16.1 认证中心公钥管理

应对认证中心下发的公钥进行有效的管理和控制。

适用于预付卡发行与受理业务。

10.4.16.2 发卡机构公钥管理

应对发卡机构公钥进行有效的管理和控制。

适用于预付卡发行与受理业务。

10.4.16.3 发卡机构对称密钥管理

应对发卡机构对称密钥进行有效的管理和控制。

适用于预付卡发行与受理业务。

10.4.17 条码支付

10.4.17.1 条码生成

应使用支付标记化技术对支付账号等信息进行脱敏处理。

应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，严格设置条码及条码生成因子的使用有效期。

10.4.17.2 收款扫码的条码生成

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。

应采用加密方式生成条码，应优先使用SM系列算法，并符合GM/T 0054—2018的相关规定。

对于服务器端生成、由移动终端批量获取的条码生成方式，后台服务器应对客户端软件进行有效识别，保存的条码应与移动终端的唯一标识信息绑定，防止受到未授权的访问。应优先使用SM系列算法对客户端软件进行有效识别，并符合GM/T 0054—2018的相关规定。

对于通过生成因子加密动态生成条码的方式，移动终端客户端软件应从后台服务器获取条码生成因子，条码生成因子应与移动终端的唯一标识信息绑定，防止生成因子受到未授权的访问。

10.4.17.3 付款扫码的条码生成

采用显码设备展示条码时，条码应加密、动态生成，宜实时加密生成或从后台服务器获取，并具有展示周期。

采用静态条码时，条码应由后台服务器加密生成。

应优先使用SM系列算法，并符合GM/T 0054—2018的相关规定。

10.4.17.4 条码码制

条码应使用符合国家标准的码制。

10.4.17.5 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。

应对条码的完整性、真实性进行校验，校验应优先使用SM系列算法，并符合GM/T 0054—2018的相关规定。

应防范病毒、木马等恶意代码，保障交易的安全性。

10.4.17.6 条码内容安全

应对条码中包含的网址等信息进行校验，对非法地址进行拦截。

10.4.17.7 交易确认

采用付款扫码支付方式时，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，由付款人发起支付指令，交易信息应至少包含收款人名称、金额。

采用收款扫码支付方式时，应在商户端展现交易信息，但不应包含付款人支付敏感信息。如在移动终端进行身份验证，应在移动终端上展现交易信息。

10.4.17.8 条码交易防重放

应防范交易报文重放攻击。

10.4.17.9 条码支付移动客户端安全

当客户端检测到移动终端交易出现异常时宜向用户提示出错信息。

客户端软件程序配置文件被篡改后，应采取相应的安全检测和预警措施。

客户端软件宜采取反逆向工程保护措施。

宜具有条码支付移动客户端软件认证证书。

10.5 数据安全性要求

10.5.1 数据保护

10.5.1.1 敏感信息安全管理制度

应制定敏感信息安全管理制度，明确支付敏感信息保护的相关要求，严禁从业人员非法存储、窃取、泄露、买卖支付敏感信息。

应明确规定严禁留存非本机构的支付敏感信息（包括银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等），确有必要留存的应取得客户本人及账户管理机构的授权。

增强要求：

应制定支付标记化安全管理制度，明确TR不得留存账户敏感信息。TR存储Token时，应对Token实施有效的安全保护。

10.5.1.2 敏感信息安全审计

每年应至少开展两次支付敏感信息安全的内部审计，并形成报告存档备查。

10.5.1.3 信息保存期限

应按规定妥善保管客户身份基本信息，非银行支付机构对客户身份信息的保管期限自业务关系结束当年起至少保存5年。

应按规定妥善保管支付业务信息，非银行支付机构对支付业务信息的保管期限自业务关系结束当年起至少保存5年。

10.5.2 数据完整性

10.5.2.1 重要数据更改机制

应制定重要数据更改流程和管理制度。

10.5.2.2 保障传输过程中的数据完整性

应能检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

完整性校验应优先使用SM系列算法，并符合GM/T 0054—2018的相关规定。

10.5.3 交易数据以及客户数据的安全性

10.5.3.1 数据物理存储安全

应具备高可靠性的数据物理存储环境。

10.5.3.2 客户身份认证信息存储安全

应明确规定严禁保存非必需的客户身份认证信息（如银行卡磁道信息或芯片信息、卡片验证码、银行卡交易密码、指纹、CVN、CVN2、非本机构的网络支付交易密码等敏感信息）。

应对客户的其他敏感信息，如口令、身份证号、卡号、手机号、经授权的贷记卡有效期、电子邮箱、身份证影印件等信息，采取加密等保护措施，显示时应进行屏蔽处理，防止未经授权擅自对个人信息进行查看、篡改和泄露。

数据加密应优先使用SM系列算法，并符合GM/T 0054—2018的相关规定。

10.5.3.3 个人信息保护

应仅采集和保存业务必需的用户个人信息。

应仅允许授权的访问和使用用户个人信息。

应在修改个人信息等关键操作时提供多种身份验证方式保障个人信息安全，并以短信、邮件等方式

告知用户。

10.5.3.4 同一安全级别和可信赖的系统之间信息传输

应保证某一安全级别的系统只能向同级别或更高级别可信赖的系统传输数据。

10.5.3.5 加密传输

应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性。

数据加密传输应优先采用SM系列算法，并符合GM/T 0054—2018的相关规定。

10.5.3.6 加密存储

应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。

数据加密存储应优先采用SM系列算法，并符合GM/T 0054—2018的相关规定。

10.5.3.7 数据访问控制

应采取重要数据的访问控制措施。

10.5.3.8 在线的存储备份

应具备实时在线的存储备份设施。

10.5.3.9 数据备份机制

应根据数据的重要性和数据对系统运行的影响，制定数据的备份和恢复策略，指明备份数据的备份范围、备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期、放置场所、文件命名规则、介质替换频率和数据传输方法等。

应具备数据备份记录。

10.5.3.10 本地备份

应提供本地数据备份。

应具备同机房数据备份设施。

10.5.3.11 异地备份

应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地。

10.5.3.12 备份数据的恢复

应具有备份数据恢复操作手册。

应定期随机抽取备份数据进行解压、还原，检查其内容有效性。

10.5.3.13 数据销毁

应具有数据销毁制度和相关记录，并实现有效的数据销毁功能。

10.5.3.14 数据使用

开发环境和测试环境应与实际运行环境物理分离。开发环境不应使用生产数据，测试环境使用的生产数据应进行脱敏处理。

10.6 运维安全性要求

10.6.1 环境管理

10.6.1.1 机房基本设施定期维护

应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理。

应对机房的温度、湿度、防火、防盗、供电、线路、整洁等进行规范化管理。

10.6.1.2 机房的出入管理制度化和文档化

应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机和关机等工作进行管理。

10.6.1.3 办公环境的保密性措施

应加强对办公环境的保密性管理，规范办公人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸质文件等。

10.6.1.4 机房安全管理制度

应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。

增强要求：

开发、测试和运行设施应分离，以降低未授权访问或改变运行系统的风险。

10.6.1.5 机房进出登记表

应具有机房进出登记表。

10.6.2 介质管理

10.6.2.1 介质的存放环境保护措施

应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存放环境专人管理。

10.6.2.2 介质的使用管理文档化

应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定。

10.6.2.3 介质的维修或销毁

应对送出维修以及销毁的介质进行严格的管理，应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁。

10.6.2.4 介质管理记录

应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点。

10.6.2.5 介质的分类与标识

应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

10.6.3 设备管理

10.6.3.1 设备管理的责任部门或人员

应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员进行管理。

10.6.3.2 设施、设备定期维护

应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护。

10.6.3.3 设备管理制度

应建立基于申报、审批和专人负责的设备管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。

10.6.3.4 设备配置标准化

应建立标准化的设备配置文档。

10.6.3.5 设备的操作规程

应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。

10.6.3.6 设备的操作日志

应具有完整的设备操作日志，至少应包括操作人员、操作时间、操作类型及操作结果等信息。

10.6.3.7 设备标识

应对设备进行分类和标识。

10.6.4 人员管理

10.6.4.1 人员录用

应指定或授权专门的部门或人员负责人员录用。

应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核。

应签署保密协议，保密协议应覆盖人员在职、离职等相关要求。

10.6.4.2 安全管理岗位设置

应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权。

应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。

应设立网络管理员、主机管理员、数据库管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。

10.6.4.3 安全管理人员配备

应配备一定数量的网络管理员、主机管理员、数据库管理员、安全管理员等。

应配备专职的安全管理人员，不可兼任。

应划分各管理员角色，明确各个角色的权限、责任和风险，权限设定应遵循最小授权原则。

10.6.4.4 人员转岗、离岗

应严格规范人员离岗过程，及时终止离岗员工的所有访问权限。

人员离岗时，应取回其持有的各种身份证件、钥匙、徽章、机构提供的软硬件设备等。

应办理严格的调离手续，关键岗位人员离岗应承诺调离后的保密义务后方可离开。

10.6.4.5 人员考核

应定期对各个岗位的人员进行安全技能及安全认知的考核。

应对关键岗位的人员进行全面、严格的安全审查和技能考核。

应对考核结果进行记录并保存。

10.6.4.6 安全意识教育和培训

应对各类人员进行安全意识教育，对信息安全基础知识、岗位操作规程、岗位技能和相关安全技术等内容进行培训。

应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒。

应对定期开展安全教育和培训进行书面规定，对不同岗位制定不同的培训计划。

应对安全教育、培训的情况和结果进行记录并归档保存。

10.6.4.7 外部人员访问管理

应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案。

对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。

10.6.4.8 职责分离

关键岗位人员应职责分离。

应根据职责划分运维人员操作权限。

应明确规定敏感信息管理的相关岗位和人员管理责任，分离不相容岗位并控制信息操作权限，规定敏感信息操作流程和规范。

10.6.5 文档管理

10.6.5.1 文档编写要求

文档描述应与实际系统相符合。

10.6.5.2 文档版本控制

文档应进行版本控制管理与编号管理。

10.6.5.3 文档格式要求

文档格式应统一规范，易于浏览。

10.6.6 监控管理

10.6.6.1 主要网络设备的各项指标监控情况

应对通信线路、网络设备的运行状况等进行监测和报警，形成记录并妥善保存。

10.6.6.2 主要服务器的各项指标监控情况

应对主机的运行状况、用户行为等进行监测和报警，形成记录并妥善保存。
运行状况应包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。
应能对系统的服务水平降低到预先规定的最小值进行监测和报警。

10.6.6.3 应用运行各项指标监控情况

应对应用软件的运行状况进行监测和报警，形成记录并妥善保存。
应能对系统的服务水平降低到预先规定的最小值进行监测和报警。

10.6.6.4 异常处理机制

应按重要程度进行分级报警，并且重要报警应能以某种方式（短信、邮件等）主动通知相关人员及时处置。此外，还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。

10.6.6.5 资源监控

增强要求：
资源的使用应加以监控、调整，并应做出对于未来容量要求的预测，以确保拥有所需的系统性能。

10.6.7 变更管理

10.6.7.1 变更制度化管理

应建立变更管理制度。制定变更控制的申报和审批文件化程序，对变更影响进行分析并文档化。
系统发生变更前，向主管领导申请，变更申请和变更方案应经过评审、审批、测试后方可实施变更，并在实施后将变更情况向相关人员通告。
变更方案应有变更失败后的回退策略等。

10.6.7.2 变更实施

应记录变更实施过程，并妥善保存所有文档和记录。

10.6.8 安全事件处置

10.6.8.1 安全事件识别、报警和分析

应能对网络和主机中发生的各类安全事件进行识别、报警和分析。

10.6.8.2 安全事件报告和处置

应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责。
应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等。

10.6.8.3 安全事件的分类和分级

应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分。

10.6.8.4 安全事件记录和采取的措施

应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，上述过程中形成的所有文件和记录均应妥善保存。

对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。

10.6.9 内部审计管理

10.6.9.1 内部审计制度

应制定信息系统安全内部审计制度，规定审计职责、审计内容、审计周期、审计问题处理机制。

应明确规定敏感信息的内部监督机制、安全事件处置机制和安全审计机制，严禁从业人员非法存储、窃取、泄露、买卖支付敏感信息。

10.6.9.2 内部审计

按制度开展内部审计工作，记录审计内容。

通报审计结果，总结问题，制定整改计划，并进行记录。

宜每年至少进行一次全面系统的第三方安全审计，并作出相应评价报告。

10.7 业务连续性要求

10.7.1 业务连续性需求分析

10.7.1.1 业务中断影响分析

应定期进行业务中断影响分析。

10.7.1.2 灾难恢复时间目标和恢复点目标

应具备灾难恢复时间目标和恢复点目标。系统应支持RPO和RTO的设置。

10.7.2 业务连续性技术环境

10.7.2.1 备份机房

应具备应用级备份机房。

10.7.2.2 关键链路冗余设计

应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障。

应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

主机房互联网接入应具备双链路。

10.7.2.3 高可靠的磁盘存储

应使用高可靠的磁盘存储。

10.7.3 业务连续性管理

10.7.3.1 业务连续性管理制度

应具备业务连续性管理制度。

10.7.3.2 应急响应流程

应具备应急响应流程。

10.7.3.3 应急恢复预案

应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容。

应具备不同场景的恢复预案，同时具备应用级恢复预案。

10.7.4 日常维护

10.7.4.1 定期演练

应制定演练计划，根据不同的应急恢复内容，确定演练的周期，至少每年一次。

应每年进行业务连续性演练，包括主备机房的切换演练，并保存演练记录。

应对演练中暴露出的问题进行总结并及时整改。

10.7.4.2 定期培训

应定期进行应急预案和业务连续性培训并具有培训记录。应至少每年举办一次。

参 考 文 献

[1] GB/T 8567—2006 计算机软件文档编制规范
[2] GB/T 9385—2008 计算机软件需求规格说明规范
[3] GB/T 9386—2008 计算机软件测试文档编制规范
[4] GB/T 12406—2008 表示货币和资金的代码
[5] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求
[6] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南
[7] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
[8] GB/T 27065—2015 合格评定 产品、过程和服务认证机构要求
[9] JR/T 0149—2016 中国金融移动支付 支付标记化技术规范