ICS 03.060
A 11
备案号：

JR

中华人民共和国金融行业标准

JR/T 0122—2014

非金融机构支付业务设施技术要求

Technical requirements of non-financial institutions payment service facilities

2014-11-24 发布　　2014-11-24 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、上海市信息安全测评认证中心、银行卡检测中心、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）、中国信息安全测评中心、国家应用软件产品质量监督检验中心（北京软件产品质量检测检验中心）、信息产业信息安全测评中心、中金金融认证中心有限公司、中国电子科技集团公司信息化工程总体研究中心、支付宝（中国）网络技术有限公司、银联商务有限公司、拉卡拉支付有限公司、北京通融通信息技术有限公司、快钱支付清算信息有限公司、上海汇付数据服务有限公司、上海盛付通电子商务有限公司、钱袋网（北京）信息技术有限公司、联通支付有限公司、深圳市财付通科技有限公司等。

本标准主要起草人：潘润红、杜宁、邬向阳、李兴锋、吴晓光、陈实博、王磊磊、聂丽琴、唐立军、田洁、王翠、高天游、赵春华、郝晓花、王妍娟、付小康、陆碧波、李红曼、张奇、扈浩、布宁、吴迪、严妍、刘思蓉、甘杰夫、刘力凤、蒋朝阳、马国照、张瑞秀、刘文光、白智勇、周悦、王威、赵小帆、郑丽娜、孔昊、李宏达、陆嘉琪、金铭彦、刘健、张益、董晶晶、杜磊、李海滨、王睿超、段超、张金凤、熊军、吴祥富、高磊、宋铮、郭宇、孔嘉俊、罗文兵、唐刚、杨天识、漆添虎、潘莹、侯龙、王雅杰、张进、李鹏、牛跃华、王雄、唐凌、林志伟、王华锋、方海峰、张健、戴维、冷杉、程伟、冯建盟、林勇、刘锦祥、叶飞、王庆、罗旭、任震、赵传飞等。

引　言

为促进支付服务市场健康发展，规范非金融机构支付服务行为，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》、《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）及《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）等相关法律法规的规定，制定《非金融机构支付业务设施技术要求》。本标准的评估对象为从事非金融机构支付服务的非金融机构支付企业，包括申请或已获得《支付业务许可证》的非金融机构。

《非金融机构支付业务设施技术要求》包括基本要求和增强要求两部分；增强要求在本标准中做出了具体的规定。

本标准根据现有技术的发展水平，提出和规定了非金融机构支付业务设施技术认证相应级别的最低要求，即基本要求，基本要求包括技术标准符合性和系统安全性要求。达到本标准的可以实现系统的基本技术符合和相对安全。

非金融机构支付业务设施技术要求

1 范围

本标准规定了非金融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。

本标准适用于中华人民共和国境内的非金融支付机构。

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 8567-2006 计算机软件文档编制规范

GB/T 9385-2008 计算机软件需求规格说明

GB/T 9386-2008 计算机软件测试文档编制规范

GB/T 12406-2008 表示货币和资金的代码

JR/T 0025.7-2013 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

CNAS-CC02 产品、过程和服务认证机构要求

会计档案管理办法 财会字〔1998〕32号文印发

3 术语和定义

下列术语和定义适用于本文件。

3.1

非金融机构支付服务 non-financial institutions payment services

非金融机构在收付款人之间作为中介机构提供下列部分或全部货币资金转移服务：

a) 互联网支付；

b) 移动电话支付；

c) 固定电话支付；

d) 数字电视支付；

e) 预付卡发行与受理；

f) 银行卡收单；

g) 中国人民银行确定的其他支付服务。

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行为。

3.3

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行为。

3.4

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，使用IC卡或网络实现支付交易的行为。

注：数字电视支付业务不涉及IC卡的发行和管理。

3.5

预付卡 prepaid cards

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。

3.6

记名预付卡 registered prepaid cards

预付卡业务处理系统中记载持卡人身份信息的预付卡。

3.7

不记名预付卡 anonymous prepaid cards

预付卡业务处理系统中不记载持卡人身份信息的预付卡。

3.8

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。

3.9

一般支付 general payment

在支付过程中，支付指令需要由付款方在支付服务方授权，并且支付成功后即可结算的支付行为。

注：客户在支付服务方进行身份认证、交易认证、支付工具确认等，并且支付服务方不对交易双方提供交易担保。

3.10

担保支付 guarantee payment

在支付过程中，由支付服务方为支付的双方提供交易担保，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。

3.11

协议支付 agreement payment

在客户信任商户能够保障自己资金安全的前提下，客户、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，而无需通过客户另行授权即可完成付款的支付行为。

3.12

订单撤销 order cancellation

客户因业务需要，在支付业务未完成前，取消订单的过程。

3.13

基本要求 basic requirement

对非金融机构支付业务设施的基础性技术要求。

3.14

增强要求 enhancement requirement

对非金融机构支付业务设施的增强性技术要求。

注：考虑到非金融机构支付业务设施的实际技术应用现状，也考虑到金融行业对于业务的规范化要求，以及将来的发展需要，对未来一段时间内行业的发展水平进行合理的预估，提出增强要求。增强要求高于当前的平均水平，使得技术规范能够在比较长的一段时间内适用。

3.15

外包服务 outsourcing services

企业根据自身的需要将运营工作中的某一项或是所有项分包出去，由专业的组织或机构进行运作。

注：此处外包服务包括基础设施运维服务、应用系统运维服务和安全管理服务等。

3.16

基础设施运维服务 infrastructure maintenance services

对IT基础设施进行监视、日常维护和维修保障，包括网络系统、主机系统、存储/备份系统、安全系统等。

3.17

应用系统运维服务 application system maintenance services

对应用系统进行维护及改进。

3.18

安全管理服务 security management services

对IT环境涉及的网络、应用系统的安全进行管理，包括安全保护、安全监控等服务。

3.19

退款 refund

商户因商品退回或服务取消，商户向支付服务方提交单笔（批量）退款请求行为。

3.20

退货 returned purchase

商户应持卡人要求，对持卡人已经扣款的消费交易，发起退货并将已完成交易款项退还持卡人原扣款账户的过程。

3.21

消费撤销 consuming cancellation

特约商户由于自身原因对持卡人已经联机结算的交易，于当日当批内主动发起的对消费交易的取消。

3.22

长款 cash overflow

资金结算时发现的有待查明原因的现金溢余。

3.23

短款 cash shortage

资金结算时发现的有待查明原因的现金短缺。

3.24

委托交易 trading commission

获得用户授权、建立交易发起渠道、用户手机号码、银行卡账户等交易要素之间绑定关系的交易。

3.25

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商品或服务订单金额向发卡行索取日后付款的承诺。

3.26

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。

3.27

预授权完成 pre-authorization completion

持卡人对已批准的预授权交易，在预授权有效期内以实时发送结算通知报文形式作支付结算。

3.28

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，将已扣款项退还持卡人原扣款账户的过程。

3.29

运营人员 operating personnel

具有审核、确认等权限的管理人员。

3.30

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。

3.31

圈存 load

增加卡中电子现金余额的过程。

3.32

圈提 unload

减少卡中电子现金余额至零的过程。

3.33

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，应该取消其处理结果。

3.34

交易查询 trading inquiry

商户向支付服务方发起查询单笔（批量）业务状态请求的过程。

3.35

委托结算 settlement commission

由商户发起，委托支付服务方把资金结算到其指定的一个或多个账户。

4 等级划分

非金融机构支付业务设施技术认证分为二级：一级和二级。一级覆盖本技术规范的基本要求，二级覆盖本技术规范的基本要求和增强要求。

本标准对于非金融机构将支付业务设施相关运维外包给第三方服务机构的情况提出了附加要求。

5 评判原则

5.1 客观性原则

应以非金融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。

5.2 公正性原则

应依据国家法律法规和认可规范，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。其认证活动不受任何外来压力和商业因素的影响和干扰。

5.3 科学性原则

应以科学思想为指导，以事实为依据。

5.4 审慎性原则

应对可能存在的风险予以充分考量。

6 互联网支付技术要求

6.1 功能要求

6.1.1 客户管理

6.1.1.1 客户信息登记及管理

应实现客户注册、客户信息的编辑等功能。

6.1.1.2 商业银行管理

应实现商业银行的接入、信息修改和删除等功能。

6.1.1.3 客户证书管理

应实现电子证书的申请、发放、更新、作废等服务。

6.1.1.4 客户审核

应实现客户注册信息的审核、确认开通及关键信息修改审核等功能。

6.1.2 账户管理

6.1.2.1 客户支付账户管理

应实现客户支付账户的开户、修改、状态设置等功能；客户支付账户状态至少应包括正常、冻结、注销等。

增强要求为：应实现客户账户的开户、修改、冻结/解冻、销户等功能。

6.1.2.2 客户支付账户管理审核

应实现客户支付账户信息的审核、确认等服务。

6.1.2.3 客户支付账户查询

应实现客户支付账户设置、交易等信息的查询功能。

6.1.2.4 客户支付账户资金审核

应实现当客户支付账户资金转移、交易、结算时，进行资金的审核和确认等。

6.1.3 交易处理

6.1.3.1 一般支付

应实现客户一般支付交易功能。

增强要求为：报文设计符合附录A中A.2.1的报文结构设计要求；

交易模型及流程设计符合附录B中B.2.1的要求。

6.1.3.2 担保支付

应实现客户担保支付交易功能。
增强要求为：报文设计符合附录A中A.2.2的报文结构设计要求；
交易模型及流程设计符合附录B中B.2.2的要求。

6.1.3.3 协议支付

应实现客户协议支付交易功能。
增强要求为：报文设计符合附录A中A.2.3、A.2.7的报文结构设计要求；
交易模型及流程设计符合附录B中B.2.3的要求。

6.1.3.4 订单撤销

应实现客户撤销订单功能，如果支付已经完成，则拒绝响应撤销订单请求。
增强要求为：报文设计符合附录A中A.2.4的报文结构设计要求；
交易模型及流程设计符合附录B中B.2.4的要求。

6.1.3.5 转账

应实现不同客户支付账户之间的相互转账功能。

6.1.3.6 充值

应实现客户支付账户的充值或预存现金。

6.1.3.7 提现

应实现将资金从客户支付账户转账到银行账户的服务。

6.1.3.8 积分查询

应实现客户积分信息的查询功能。

6.1.3.9 积分兑换

应实现客户积分兑换服务。

6.1.3.10 积分兑换撤销

应实现撤销客户积分兑换，且撤销后积分退还客户服务。

6.1.3.11 交易纠纷处理

应实现客户交易的投诉、处理、确认、撤销等。

6.1.3.12 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的功能，且能实现浏览交易明细。
增强要求为：报文设计符合附录A中A.2.5、A.2.6的报文结构设计要求；
交易模型及流程设计符合附录B中B.2.5的要求。

6.1.3.13 交易明细下载

应实现交易明细信息下载到指定终端。

6.1.3.14 邀请其他人代付

应实现邀请他人进行支付。

6.1.4 资金结算

应实现支付服务方与客户之间的资金结算功能。

增强要求为：报文设计符合附录A中A.2.8、A.2.9的报文结构设计要求；

交易模型及流程设计符合附录B中B.2.6的要求。

6.1.5 对账处理

6.1.5.1 商户发送对账请求

应实现商户提交对账申请，支付服务方提供对账信息的服务。

6.1.5.2 商户下载对账文件

应实现商户对账文件的查询、浏览和下载等。

6.1.6 差错处理

6.1.6.1 调账处理

应实现对资金结算时发现的有待查明原因的现金溢余或短缺等情况进行调账等服务并进行记录。

6.1.6.2 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。

支付服务方将部分或全部已扣款项退还给客户（个人或企业买方）的原扣款账户，原扣款账户不能接收退款的，退款到付款人其他账户。

增强要求为：报文设计符合附录A中A.2.10的报文结构设计要求；

交易模型及流程设计符合附录B中B.2.7.1的要求。

6.1.6.3 批量退款

应实现对已发生的多笔交易同时进行退款申请、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给客户（个人或企业买方）的原扣款账户，原扣款账户不能接收退款的，退款到付款人其他账户。

增强要求为：报文设计符合附录A中A.2.11的报文结构设计要求；

交易模型及流程设计符合附录B中B.2.7.2的要求。

6.1.7 统计报表

6.1.7.1 业务类报表

应实现对一段时间内业务操作（客户注册、商户开通、支付、结算、转账、提现等操作）的查询统计功能。

6.1.7.2 运行管理类报表

应实现对一段时间内运行管理情况（资产、监控、安全事件等）的查询统计，第三方支付公司可以根据自身的情况将“一段时间”细化为“月季年”。

6.1.8 运营管理

6.1.8.1 运营人员权限管理

应实现对此类人员权限的增加、删除、修改或审核等功能。

6.1.8.2 提现管理

应实现对提现操作进行管理，如提现规则设置、提现审核确认等措施。

6.1.8.3 提现财务处理

应实现对提交的提现申请进行财务处理。

6.1.8.4 退款风控处理

应实现对退款操作进行风险处理，如采用退款风险识别、退款审核确认等措施。

6.1.8.5 退款财务处理

应实现对退款申请进行财务处理。

6.2 风险监控要求

6.2.1 账户风险管理

应对客户进行实名认证。

6.2.2 交易监控

6.2.2.1 监控规则管理

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

6.2.2.2 当日交易查询

应实现当日交易信息的查询功能。

6.2.2.3 历史交易查询

应实现历史交易信息的查询功能。

6.2.2.4 实时交易监控

应实现交易监控规则的设置，以实现对实时交易的监控，并对违反规则的交易提供查询、处理、风险控制等服务。

增强要求为：建立账户与交易监控系统，对支付交易全过程实施7*24小时监控。

6.2.2.5 可疑交易处理

应实现可疑交易处理规则的设置，以实现对可疑交易的查询、分析处理等服务。

6.2.2.6 交易事件报警

应实现对违反规则的交易事件进行报警，并提供事件的查询统计。

6.2.2.7 支付限额管理

应根据用户使用的不同身份认证方式设置支付限额，以保护用户的资金安全。

6.2.2.8 单笔交易限额

应设置单笔交易限额。

6.2.2.9 当日累计交易限额

应设置当日累计交易限额。

6.2.3 交易审核

6.2.3.1 系统自动审核

应实现交易审核规则的设置，系统根据交易规则自动进行交易审核，并提供交易审核记录。

6.2.3.2 人工审核

应确保在相关管理制度中完整、明确的定义需要人工审核的交易类型，实现人工审核规则的设置，并保存人工审核的记录。

6.2.4 风控规则

6.2.4.1 风控规则管理

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

6.2.4.2 黑名单

应实现黑名单的管理功能，并对黑名单中客户的交易进行风险监控。

6.2.4.3 风险识别

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。

6.2.4.4 事件管理

应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，并保留事件的记录。

6.2.4.5 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报表功能。

6.2.5 商户风险管理

6.2.5.1 商户资质审核

应对商户资质进行审核。严格限制发展具有风险的商户。审核内容包括：

a) 营业执照、税务登记证、组织机构代码证，法人代表或商户负责人身份证等；
b) 商户网站域名应可以正常访问，网站信息应定时更新；
c) 应取得 ICP 证或有 ICP 备案；
d) 网站内容。

应提示特约商户定期审核网站，杜绝非法链接。

6.2.5.2 商户签约

应与合作商户签订相关协议。

6.3 性能要求

支付业务设施性能基本要求见表1。

表1 互联网支付性能检测基本要求列表

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	比对性能需求表高峰时段并发数	<=80%	100%	>=99%	>=30分钟

6.4 安全性要求

6.4.1 网络安全性要求

6.4.1.1 结构安全

6.4.1.1.1 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。

增强要求为：应保证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。

6.4.1.1.2 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。

6.4.1.1.3 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。

6.4.1.1.4 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。

6.4.1.1.5 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，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

6.4.1.1.6 QoS 保证

宜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。

增强要求为：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。

6.4.1.2 网络访问控制

6.4.1.2.1 网络域安全隔离和限制

应在网络边界部署访问控制设备，启用访问控制功能。

6.4.1.2.2 地址转换和绑定

重要网段应采取技术手段防止地址欺骗。

6.4.1.2.3 内容过滤

应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP等协议命令级的控制。

6.4.1.2.4 访问控制

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。

应按用户和系统之间的访问控制规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。

6.4.1.2.5 流量控制

应限制网络最大流量数及网络连接数。

6.4.1.2.6 会话控制

应在会话处于非活跃一定时间或会话结束后终止网络连接。

6.4.1.2.7 远程拨号访问控制和记录

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。

6.4.1.3 网络安全审计

6.4.1.3.1 日志信息

应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。

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。

6.4.1.3.2 网络系统故障分析

应对网络系统故障进行分析，查找原因并形成故障知识库。

6.4.1.3.3 网络对象操作审计

应能够根据记录数据进行分析，并生成审计报表。

6.4.1.3.4 日志权限和保护

应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

6.4.1.3.5 审计工具

应具备日志审计工具，对日志进行记录、分析和报告。

增强要求为：应定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，当存储空间被耗尽时，终止可审计事件的发生；

应根据信息系统的统一安全策略，实现集中审计，时钟宜采用多模方式授时。并应安排专人负责时间服务器，防止被恶意篡改。

6.4.1.4 边界完整性检查

应能够对非授权设备私自连接到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

应能够对内部网络用户私自连接到外部网络的行为进行检查,准确定出位置,并对其进行有效阻断。

增强要求为：对非法外联和非法接入行为进行检测并阻断的同时，应通过报警方式通知管理员。

6.4.1.5 网络入侵防范

6.4.1.5.1 网络 ARP 欺骗攻击

应能够有效的防范网络ARP欺骗攻击。

6.4.1.5.2 信息窃取

应采用防范信息窃取的措施。

6.4.1.5.3 DoS/DDoS 攻击

应具有防DoS/DDoS攻击设备或技术手段。

6.4.1.5.4 网络入侵防范机制

应在网络边界处监视以下攻击行为：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提供报警。

增强要求为：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。

6.4.1.6 恶意代码防范

6.4.1.6.1 恶意代码防范措施

应在网络边界处对恶意代码进行检测和清除。

增强要求为：应在系统边界中对恶意代码进行检测和清除。

6.4.1.6.2 定时更新

应维护恶意代码库的升级，检测系统的更新。

6.4.1.7 网络设备防护

6.4.1.7.1 设备登录设置

应对登录网络设备的用户进行身份鉴别。

网络设备用户的标识应唯一。

主要网络设备宜对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。

增强要求为：主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别，网络设备用户的身份鉴别信息至少应有一种是不可伪造的。

6.4.1.7.2 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。

6.4.1.7.3 登录地址限制

应对网络设备的管理员登录地址进行限制。

6.4.1.7.4 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。

6.4.1.7.5 设备用户设置策略

应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

6.4.1.7.6 权限分离

应实现设备特权用户的权限分离。

6.4.1.7.7 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。

6.4.1.8 网络安全管理

6.4.1.8.1 网络设备运维手册

应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面做出规定。

应保证所有与外部系统的连接均得到授权和批准。

应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

6.4.1.8.2 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。

6.4.1.8.3 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进行及时的修补。

6.4.1.8.4 网络数据传输加密

当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

6.4.1.9 网络相关人员安全管理

6.4.1.9.1 网络安全管理人员配备

应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作。

6.4.1.9.2 网络安全管理人员责任划分规则

应制定文件明确网络安全管理岗位的职责、分工和技能要求。

6.4.1.9.3 网络安全关键岗位人员管理

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

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。

6.4.2 主机安全性要求

6.4.2.1 身份鉴别

6.4.2.1.1 系统与应用管理员用户设置

应对登录操作系统和数据库系统的用户进行身份标识和鉴别。

应为操作系统和数据库系统的不同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。

增强要求为：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，并且身份鉴别信息至少有一种是不可伪造的。

6.4.2.1.2 系统与应用管理员口令安全性

操作系统和数据库系统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。

6.4.2.1.3 登录策略

应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

6.4.2.2 访问控制

6.4.2.2.1 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。

应实现操作系统和数据库系统特权用户的权限分离。

增强要求为：在系统对用户进行身份鉴别时，系统与用户之间应能够建立一条安全的信息传输路径；在用户对系统进行访问时，系统与用户之间应能够建立一条安全的信息传输路径。

6.4.2.2.2 主机信任关系

应避免不必要的主机信任关系。

6.4.2.2.3 默认过期用户

应及时删除多余的、过期的用户，避免共享用户的存在。

应严格限制默认用户的访问权限，重命名系统默认用户，修改这些用户的默认口令。

6.4.2.3 安全审计

6.4.2.3.1 日志信息

审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。

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。

增强要求为：应能够根据信息系统的统一安全策略，实现集中审计。

6.4.2.3.2 日志权限和保护

应保护审计记录，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。

增强要求为：应保护审计进程，避免受到未预期的中断。

6.4.2.3.3 系统信息分析

应能够根据记录数据进行分析，并生成审计报表。

6.4.2.4 系统保护

6.4.2.4.1 系统备份

应具有系统备份或系统重要文件备份。

6.4.2.4.2 故障恢复策略

应具备各种主机故障恢复策略。

6.4.2.4.3 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。

6.4.2.4.4 主机安全加固

应对主机进行安全加固。

6.4.2.5 剩余信息保护

应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。

应确保系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

6.4.2.6 入侵防范

6.4.2.6.1 入侵防范记录

宜能够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、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

宜能够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具有恢复的措施。

增强要求为：应能够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、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

应能够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具有恢复的措施。

6.4.2.6.2 关闭服务和端口

应关闭系统不必要的服务和端口。

6.4.2.6.3 最小安装原则

操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

6.4.2.7 恶意代码防范

6.4.2.7.1 防范软件安装部署

应至少在生产系统中的服务器安装防恶意代码软件。

6.4.2.7.2 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。

6.4.2.7.3 防范软件统一管理

应支持防范软件的统一管理。

6.4.2.8 资源控制

6.4.2.8.1 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。
应根据安全策略设置登录终端的操作超时锁定。

6.4.2.8.2 资源监控和预警

应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。
应限制单个用户对系统资源的最大或最小使用限度。
应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

6.4.2.9 主机安全管理

6.4.2.9.1 主机运维手册

应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面做出具体规定。

6.4.2.9.2 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。

6.4.2.9.3 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，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。

6.4.2.9.4 操作日志管理

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，严禁进行未经授权的操作。

应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

6.4.2.10 主机相关人员安全管理

6.4.2.10.1 主机安全管理人员配备

应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则。

6.4.2.10.2 主机安全管理人员责任划分规则

应制定文件明确主机管理岗位的职责、分工和技能要求。

6.4.2.10.3 主机安全关键岗位人员管理

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

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。

6.4.3 应用安全性要求

6.4.3.1 身份鉴别

6.4.3.1.1 系统与普通用户设置

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，提供系统管理员和普通用户的设置功能。

6.4.3.1.2 系统与普通用户口令安全性

系统与普通用户口令应具有一定的复杂度。

6.4.3.1.3 登录访问安全策略

应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

增强要求为：应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别，其中一种是不可伪造的。

6.4.3.1.4 非法访问警示和记录

应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

6.4.3.1.5 客户端鉴别信息安全

客户端鉴别信息应不被窃取和冒用。

6.4.3.1.6 口令有效期限制

应提示客户定期修改口令。

应限制系统管理用户的口令有效期。

6.4.3.1.7 限制认证会话时间

应对客户端认证会话时间进行限制。

6.4.3.1.8 身份标识唯一性

应提供用户身份标识唯一性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身份标识，身份鉴别信息不易被冒用。

应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

6.4.3.1.9 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。

6.4.3.2 WEB 页面安全

6.4.3.2.1 登录防穷举

应提供登录防穷举的措施，如图片验证码等。

6.4.3.2.2 安全控件

登录应使用安全控件，并提供第三方检测机构的检测报告。

6.4.3.2.3 使用数字证书

应使用服务器证书，并在整个生命周期保障令牌的安全。

6.4.3.2.4 独立的支付密码

应提供独立的支付密码和健全的密码找回机制。

6.4.3.2.5 网站页面注入防范

网站页面应采取防范SQL注入、Path注入和LDAP注入等风险的措施。

6.4.3.2.6 网站页面跨站脚本攻击防范

网站页面应采取防范跨站脚本攻击风险的措施。

6.4.3.2.7 网站页面源代码暴露防范

网站页面应采取防范源代码暴露的措施。

6.4.3.2.8 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。

6.4.3.2.9 网站页面防篡改措施

应采取网站页面防篡改措施。

6.4.3.2.10 网站页面防钓鱼

网站页面应提供防钓鱼网站的防伪信息验证。

6.4.3.3 访问控制

6.4.3.3.1 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，并严格限制默认用户的访问权限。

应授予不同用户为完成各自承担任务所需的最小权限，并在它们之间形成互相制约的关系。

6.4.3.3.2 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、客体及它们之间的操作。

6.4.3.3.3 业务操作日志

应具有所有业务操作日志。

6.4.3.3.4 关键数据操作控制

应严格控制用户对关键数据的操作，宜按照“双人控制”原则进行访问或操作权限分配。关键数据如：敏感数据、重要业务数据、系统管理数据等。

6.4.3.3.5 异常中断防护

用户访问异常中断后，应具有防护手段，保证数据不丢失。

6.4.3.3.6 数据库安全配置

应具有数据库安全配置手册，并对数据库进行安全配置。

6.4.3.4 安全审计

6.4.3.4.1 日志信息

审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

6.4.3.4.2 日志权限和保护

应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录。

6.4.3.4.3 系统信息查询与分析

应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

6.4.3.4.4 对象操作审计

应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。

6.4.3.4.5 审计工具

应具备日志审计工具，对日志进行记录、分析和报告。

增强要求为：应根据系统统一安全策略，提供集中审计接口。

6.4.3.4.6 事件报警

应具有交易事件报警功能。

6.4.3.5 剩余信息保护

应对无用的过期信息、文档进行完整删除。

增强要求为：应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

6.4.3.6 资源控制

6.4.3.6.1 连接控制

应能够根据业务需求，对系统的最大并发会话连接数进行限制。

应能够对一个时间段内可能的并发会话连接数进行限制。

6.4.3.6.2 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。

应能够对单个帐户的多重并发会话进行限制。

6.4.3.6.3 进程资源分配

应能够对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额。

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。

6.4.3.6.4 资源监测预警

应能够对系统服务水平降低到预先规定的最小值进行检查和报警。

6.4.3.7 应用容错

6.4.3.7.1 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或长度符合系统设定要求。

6.4.3.7.2 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。

增强要求为：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。

6.4.3.7.3 故障机制

发生故障后，系统应能够及时恢复。

6.4.3.7.4 回退机制

应提供回退功能，当故障发生后，能够及时回退到故障发生前的状态。

6.4.3.8 报文完整性

通信报文应采用密码技术保证通讯过程中交易数据的完整性。

6.4.3.9 报文保密性

在通讯时采用安全通道或对报文中敏感信息进行加密。

6.4.3.10 抗抵赖

6.4.3.10.1 原发和接收证据

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。

6.4.3.10.2 可信时间戳服务

增强要求为：本地时间应从国家权威时间源采时，保证时间的同一性；
应采用国家认可的可信时间戳服务；
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。

6.4.3.11 编码安全

6.4.3.11.1 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。
增强要求为：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。

6.4.3.11.2 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。

6.4.3.11.3 编码规范约束

应按照编码规范进行编码，具有编码规范约束制度。

6.4.3.11.4 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。

6.4.3.11.5 版本管理

应具有代码版本管理制度。

6.4.3.12 电子认证应用

6.4.3.12.1 第三方电子认证机构证书

在对外业务（非内部业务）处理过程中，应使用经过认证的第三方电子认证证书。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，可以使用自建证书（非第三方电子认证证书）。在条件允许的情况下，建议对所有业务使用经过认证的第三方电子认证证书。

6.4.3.12.2 关键业务电子认证技术应用

关键业务应使用电子认证技术。在条件允许的情况下，建议在所有业务均使用经过认证的第三方电子认证技术。

6.4.3.12.3 电子签名有效性

应使用有效的电子签名。在对外业务（非内部业务）处理过程中，应使用经过第三方认证的电子签名体系。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，可以使用自建的电子签名体系（非第三方认证的电子签名体系）。在条件允许的情况下，建议对所有业务使用经过认证的第三方电子签名体系。

6.4.3.12.4 服务器证书私钥保护

应对所持有的服务器证书私钥进行有效保护。

6.4.4 数据安全性要求

6.4.4.1 数据保护

6.4.4.1.1 客户身份信息保护

应按规定妥善保管客户身份基本信息，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。

6.4.4.1.2 支付业务信息保护

应按规定妥善保管支付业务信息，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。

6.4.4.1.3 会计档案信息保护

应按规定妥善保管会计档案，支付机构对会计档案的保管期限适用《会计档案管理办法》（财会字〔1998〕32号文印发）相关规定。

6.4.4.2 数据完整性

6.4.4.2.1 重要数据更改机制

应制定重要数据更改流程和管理制度。

6.4.4.2.2 数据备份记录

应具备数据备份记录。

6.4.4.2.3 保障传输过程中的数据完整性

应能够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。

6.4.4.2.4 备份数据定期恢复

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。

6.4.4.3 交易数据以及客户数据的安全性

6.4.4.3.1 数据物理存储安全

应具备高可用性的数据物理存储环境。

6.4.4.3.2 客户身份认证信息存储安全

应不允许保存非必须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、卡片有效期、个人标识码、银行卡交易密码、指纹、CVN、CVN2等敏感信息）。

应对客户的其他敏感信息，如卡号、户名、开户手机、贷记卡有效期、电子邮箱等信息采取保护措施，防止未经授权擅自对个人信息进行查看、篡改、泄露和破坏。宜采用加密存储、部分屏蔽显示等技术。

6.4.4.3.3 终端信息采集设备硬加密措施或其它防伪手段

如果使用终端信息采集设备则应采取硬加密措施，否则要使用其它手段达到防伪目的。

6.4.4.3.4 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。

6.4.4.3.5 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。

6.4.4.3.6 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。

增强要求为：应避免使用标准的哈希算法。

6.4.4.3.7 数据访问控制

应具备重要数据的访问控制措施。

6.4.4.3.8 在线的存储备份

应具备实时在线的存储备份设施。

6.4.4.3.9 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，应指明备份数据的备份方式（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。

6.4.4.3.10 本地备份

应提供本地数据备份。

应具有同机房数据备份设施。

6.4.4.3.11 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。

6.4.4.3.12 备份数据的恢复

应具有备份数据恢复操作手册，并提供恢复功能。

6.4.4.3.13 数据销毁制度和记录

应具有数据销毁制度和相关记录。

6.4.4.3.14 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。

6.4.5 运维安全性要求

6.4.5.1 环境管理

6.4.5.1.1 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。

6.4.5.1.2 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。

6.4.5.1.3 办公环境的保密性措施

应加强对办公环境的保密性管理，规范办公环境人员行为，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档文件等。

6.4.5.1.4 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做出规定。

增强要求为：开发、测试和运行设施应分离，以减少未授权访问或改变运行系统的风险。

6.4.5.1.5 机房进出登记表

应具有机房进出登记表。

6.4.5.2 介质管理

6.4.5.2.1 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，并实行存储环境专人管理。

6.4.5.2.2 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、维护和销毁等方面做出规定。

6.4.5.2.3 维修或销毁介质之前清除敏感数据

应对送出维修以及销毁等进行严格的管理，对送出维修或销毁的介质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。

6.4.5.2.4 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。

6.4.5.2.5 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。

6.4.5.3 设备管理

6.4.5.3.1 设备管理的责任人员或部门

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。

6.4.5.3.2 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管理。

6.4.5.3.3 设备选型、采购、发放等的审批控制

应建立基于申报、审批和专人负责的设备安全管理制度，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。

6.4.5.3.4 设备配置标准化

应建立标准化的设备配置文档。

6.4.5.3.5 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，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。

6.4.5.3.6 设备的操作日志

应具有完整的设备操作日志。

6.4.5.3.7 设备使用管理文档

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。

6.4.5.3.8 设备标识

应对设备进行分类和标识。

6.4.5.4 人员管理

6.4.5.4.1 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。

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

6.4.5.4.2 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。

应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。

6.4.5.4.3 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。

6.4.5.4.4 安全意识教育和培训

应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训。

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。

应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训。

应对安全教育和培训的情况和结果进行记录并归档保存。

6.4.5.4.5 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。

6.4.5.4.6 职责分离

关键岗位人员应职责分离。

6.4.5.5 监控管理

6.4.5.5.1 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、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。

6.4.5.5.2 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。

6.4.5.5.3 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。

6.4.5.5.4 异常处理机制

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。

应按重要程度进行分级报警，并且重要报警要能以某种方式（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，采取必要措施。

6.4.5.5.5 资源监控

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

6.4.5.6 变更管理

6.4.5.6.1 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须经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。

6.4.5.6.2 变更方案

应确认系统中要发生的变更，并制定变更方案，变更内容中应有变更失败后的回退方案等。

6.4.5.6.3 重要系统变更的通知

重要系统变更前，应通知相关单位、部门和人员。

6.4.5.6.4 重要系统变更的实施

应记录变更实施过程，并妥善保存所有文档和记录。

6.4.5.7 安全事件处置

6.4.5.7.1 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。

6.4.5.7.2 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。

6.4.5.7.3 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，过程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。

6.4.5.8 应急预案管理

6.4.5.8.1 制定不同事件的应急预案

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。

6.4.5.8.2 相关人员应急预案培训

应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。

6.4.5.8.3 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。对应急预案演练中暴露出的问题进行总结并及时整改。

6.4.6 业务连续性要求

6.4.6.1 业务连续性需求分析

6.4.6.1.1 业务中断影响分析

应进行业务中断影响分析。

6.4.6.1.2 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。

6.4.6.2 业务连续性技术环境

6.4.6.2.1 备份机房

应具备同城应用级备份。

6.4.6.2.2 网络双链路

应具备双链路。

6.4.6.2.3 网络设备和服务器备份

应具有同城应用级备份设施。

6.4.6.2.4 高可靠的磁盘阵列

应使用高可靠的磁盘阵列。

6.4.6.2.5 远程数据库备份

应具备远程备份数据库。

6.4.6.3 业务连续性管理

6.4.6.3.1 业务连续性管理制度

应具备业务连续性管理制度。

6.4.6.3.2 应急响应流程

应具备应急响应流程。

6.4.6.3.3 恢复预案

应具备不同场景恢复预案，同时具备应用级恢复预案。

6.4.6.3.4 数据备份和恢复制度

应具备数据备份和恢复管理制度。

6.4.6.4 备份和恢复管理

6.4.6.4.1 备份数据范围和备份频率

应具备备份数据范围和备份频率清单。

6.4.6.4.2 备份和恢复手册

应具备数据备份和恢复手册。

6.4.6.4.3 备份记录和定期恢复测试记录

应具备备份记录和定期恢复测试记录。

6.4.6.4.4 定期数据备份恢复性测试

应进行定期数据备份恢复性测试。

6.4.6.5 日常维护

6.4.6.5.1 每年业务连续性演练

应每年进行业务连续性演练，包括主备机房的切换演练，演练需提供记录。

6.4.6.5.2 定期业务连续性培训

应定期进行业务连续性培训并具有培训记录。

6.5 文档要求

6.5.1 用户文档

6.5.1.1 用户手册

用户手册应描述手工操作该软件的用户应如何安装和使用一个软件系统。它还包括软件操作的一些特别的方面，诸如，关于特定岗位或任务的指令等。用户手册是为由用户操作的软件而开发的，具有要求联机用户输入或解释输出显示的用户界面。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

6.5.1.2 操作手册

操作手册应提供操作指定的设备所需的信息。本手册侧重设备自身，而不是运行在其上的特定的软件。操作手册主要针对一些新开发的设备、专用设备、无现成的商用操作手册或其他操作手册可用的其他的设备。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

6.5.2 开发文档

6.5.2.1 需求说明书

需求说明书应从以下几方面描述一个建议的系统：说明它能满足用户什么需要，它与现有系统或过程的关系，以及它的使用方式等。需求说明书旨在需方、开发方、支持方和用户代理之间对所建议的系

统的运行机理取得共识。取决于使用的目的，需求说明书可专注于向开发者表述用户的需求，或专注于向用户或其他感兴趣的对象表达开发者的思路。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

6.5.2.2 需求分析文档

需求分析文档应描述对计算机软件系统的需求，及确保每个需求得以满足所使用的方法。需求分析文档应涉及该系统外部接口的需求。

宜符合GB/T 8567和GB/T 9385要求。

增强要求为：应符合GB/T 8567和GB/T 9385要求。

6.5.2.3 总体设计方案

总体设计方案应描述系统或子系统的系统级或子系统级设计与体系结构设计。总体设计方案还要用《概要设计文档》和《数据库设计文档》加以补充。总体设计方案连同相关的概要和数据库设计文档是构成进一步系统实现的基础。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

6.5.2.4 数据库设计文档

数据库设计文档应描述数据库的设计。数据库可由用户或计算机程序通过数据库管理系统加以访问。数据库设计文档还描述了存取或操纵数据所使用的软件配置项。数据库设计文档是实现数据库及相关软件配置项的基础。它向需方提供了设计的可视性，为软件支持提供了所需要的信息。数据库设计文档是否单独成册或与详细设计文档合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

6.5.2.5 概要设计文档

概要设计文档应描述计算机软件系统的设计。它描述了系统级设计决策、系统体系结构设计，概要设计和数据库设计是否单独成册抑或与详细设计合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

6.5.2.6 详细设计文档

详细设计文档应描述计算机软件系统的设计。它描述了子系统级设计决策、系统体系结构设计和实现该软件所需的详细设计。概要设计和数据库设计是否单独成册抑或与详细设计合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

6.5.2.7 工程实施方案

工程实施方案应描述开发者实施软件开发工作的计划，包括新开发、修改、重用、再工程、维护和由软件产品引起的其他所有的活动。工程实施方案是向需求方提供了解和监督软件开发过程、所使用的方法、每项活动的途径、项目的安排、组织及资源的一种手段。

6.5.3 管理文档

6.5.3.1 测试报告

测试报告应是对计算机软件、软件系统或子系统，或与软件相关项目执行合格性测试的记录。通过测试报告，需方能够评估所执行的合格性测试及其测试结果。

宜符合GB/T 8567和GB/T 9386要求。

增强要求为：应符合GB/T 8567和GB/T 9386要求。

6.5.3.2 系统运维手册

系统运维手册应是对系统运维管理中用到的环境、资产、介质、设备等进行维护、升级、漏洞扫描等操作的详细描述。

6.5.3.3 系统应急手册

应根据不同的事件，制定应急预案，形成系统应急手册。

6.5.3.4 运维管理制度

运维管理制度应包含但不限于机房管理制度、介质管理制度、设备管理制度、人员管理制度、监控巡检管理制度、变更管理制度、安全事件处理制度等。

6.5.3.5 安全管理制度

安全管理制度应是对负责安全管理机构的设置与人员等资源的配备描述，以及保证其正常实施安全管理工作的管理制度。

6.5.3.6 安全审计报告

应由专业审计人员根据有关的法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并做出相应评价报告。

7 预付卡发行与受理技术要求

7.1 功能要求

7.1.1 账户管理

应实现客户支付账户的开户、修改、状态设置等功能。

记名预付卡，应当在预付卡核心业务处理系统中记载购卡人/单位经办人的有效身份证件信息、预付卡卡号、金额等信息。

办理一次性金额1万元以上不记名预付卡充值业务时，应当在预付卡核心业务处理系统中记载持卡人的有效身份证件信息、预付卡卡号、金额等信息。

增强要求为：应实现客户账户的开户、修改、冻结/解冻、销户等功能。

7.1.2 特约商户管理

7.1.2.1 商户提交资质材料

在特约商户申请首次、业务变更、解冻、退出等情况下，应对特约商户提交的资质材料进行审核。应提示特约商户定期审核网站，杜绝非法链接。

7.1.2.2 商户信息查询

应具有商户信息的查询功能。

7.1.2.3 商户终端管理

应对商户控制平台或POS机等进行管理。

7.1.2.4 商户受理业务管理

应具有商户受理业务的增加、修改和取消功能。

7.1.2.5 商户信息维护

应具有商户信息的增加、修改和删除功能。

7.1.2.6 商户冻结、解冻

在特约商户申请首次、业务变更、解冻、退出等情况下，应暂停商户交易和重新恢复商户交易的功能。

7.1.2.7 商户退出

在特约商户申请首次、业务变更、解冻、退出等情况下，应能够永久停止商户交易的功能。

7.1.3 卡片管理

7.1.3.1 制卡

应具有制卡基本功能，如新增制卡、制卡文件生成等。

7.1.3.2 卡片发行

应具有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。

7.1.3.3 卡片激活

新卡应激活后才能使用。

7.1.3.4 充值

应可以对卡片进行充值，并在充值失败时进行自动撤销。

应可以通过现金、银行转账方式对卡片进行充值。

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。

7.1.3.5 卡片有效期延长

应能对卡片有效期进行延长，可以指定延长期限。

7.1.3.6 更换

应具有卡片更换功能，在卡片丢失或不可使用时可更换新卡。

7.1.3.7 密码修改

应可以对卡片密码进行修改。

7.1.3.8 卡片冻结/解冻

应可以根据需要对卡片资金进行冻结/解冻。

7.1.3.9 卡片挂失/解挂

应可以根据需要对卡片进行挂失/解挂。

7.1.3.10 锁卡/解锁

应可以对卡片功能进行锁卡/解锁。

7.1.3.11 退卡

应可以退卡返回资金。

7.1.3.12 销卡

应可以对卡片进行注销回收。

7.1.4 密钥和证书管理

7.1.4.1 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。

7.1.4.2 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。

7.1.4.3 IC卡密钥管理

应对IC卡卡片密钥进行有效的管理和控制。

7.1.4.4 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。

7.1.4.5 IC卡证书管理

应对IC卡卡片公钥证书进行有效的管理和控制。

7.1.5 交易处理

7.1.5.1 联机消费

应实现预付卡联机消费功能。

7.1.5.2 联机消费撤销

应实现预付卡联机消费撤销功能。

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。

7.1.5.3 联机余额查询

应实现预付卡联机余额查询功能。

7.1.5.4 退货

应实现退货功能，无法退回的，发卡机构应当将资金退回至持卡人提供的同一发卡机构的同类预付卡。预付卡接受退货后的卡内资金余额不得超过规定限额。

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，完成退货交易并打印凭证。

7.1.5.5 冲正交易

应有效实现冲正交易功能。

7.1.5.6 异常卡交易

应有效实现对各种异常卡交易的处理功能。

7.1.5.7 现金充值

应能够通过柜台或自助终端等方式使用现金进行充值交易。

7.1.5.8 指定账户圈存

应实现指定账户圈存功能。

7.1.5.9 非指定账户圈存

应实现非指定账户圈存功能。

7.1.5.10 IC卡脚本通知

应实现向IC卡发送脚本通知指令功能。

7.1.5.11 圈提

应实现圈提交易功能。

7.1.5.12 脱机消费

应实现IC卡脱机消费功能。

7.1.5.13 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。

7.1.5.14 脱机余额查询

应实现脱机余额查询的功能。

7.1.5.15 交易查询

应具有在受理平台和终端上进行交易查询的功能。

7.1.6 资金结算

应具有商户资金结算功能。

7.1.7 对账处理

7.1.7.1 发送对账请求

应允许商户发送对账请求。

7.1.7.2 生成对账文件

应具有生成对账文件功能。

7.1.8 差错处理

应实现对长款/短款资金的记录、调账等服务。

7.1.9 统计报表

7.1.9.1 业务类报表

应实现对一段时间内业务操作（如客户注册、商户开通、卡片发行、交易、结算等操作）的查询统计。

7.1.9.2 运行管理类报表

应实现对一段时间内运行管理情况（资产、监控、安全事件等）的查询统计，第三方支付公司可以根据自身的情况将“一段时间”细化为“月季年”。

7.2 风险监控要求

7.2.1 联机交易风险管理

7.2.1.1 联机交易 ARQC/ARPC 验证

应能够进行联机交易的ARQC/ARPC验证。

7.2.1.2 联机报文 MAC 验证

应对联机交易报文进行MAC验证。

7.2.1.3 卡片状态控制

应对卡片各种状态进行控制。

7.2.1.4 单笔消费限额

相关风控制度中应对单笔消费限额进行规定。

系统应对单笔消费限额进行设置，并可对其正确识别、记录、响应。

7.2.1.5 当日累计消费限额

相关风控制度中应对当日累计消费额度进行规定。

系统应对当日累计消费额度进行设置，并可对其正确识别、记录、响应。

7.2.1.6 当日累计消费次数限制

相关风控制度中应对当日累计消费次数进行规定。

系统应对当日累计消费次数进行设置，并可对其正确识别、记录、响应。

7.2.1.7 单笔充值金额最大值

相关风控制度中应对预付卡单笔充值金额最大值进行规定。

系统应对预付卡单笔充值金额最大值进行设置，并可对其正确识别、记录、响应。

预付卡充值后，资金余额不得超过预付卡账户余额限额设置。

预付卡只能通过现金、银行转账方式进行充值。

7.2.1.8 账户余额限额

相关风控制度中应对预付卡账户余额最大值进行规定。

系统应对预付卡账户余额最大值进行设置，并可对其正确识别、记录、响应。

应对预付卡账户余额最大值进行限制，并符合国家法律法规及人民银行相关规定。

7.2.1.9 大额消费商户交易监控

相关风控制度中应对大额消费商户交易进行规定。

系统应能够对大额消费商户交易进行设置并根据设置触发风控规则，并提供相关交易监控、记录、查询等功能。

7.2.1.10 密码错误情况下的交易请求

相关风控制度中应对预付卡联机交易密码错误以及多次密码错误后的处理进行规定。

系统应对预付卡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。

多次密码错误后，系统应按风控制度规定冻结卡片。

7.2.1.11 非法卡号交易

相关风控制度中应对预付卡非法卡号交易及处理进行规定。

系统应对预付卡非法卡号交易进行正确识别、记录，并拒绝交易请求。

7.2.1.12 卡片有效期检查

相关风控制度中应对预付卡卡片有效期及其检查进行规定。

系统应能对预付卡卡片有效期进行设置。

预付卡联机交易时，应检查卡片有效期，并在系统中记录并拒绝过期卡片的交易请求。

7.2.1.13 无磁无密交易

相关风控制度中应对预付卡无磁无密交易进行详细规定与严格控制。

系统应对预付卡无磁无密交易进行正确识别、记录和查询。

7.2.2 脱机交易风险管理

7.2.2.1 TAC 验证

脱机交易中，应进行TAC验证。

7.2.2.2 MAC 验证

脱机交易中，应进行MAC验证。

7.2.3 终端风险管理

7.2.3.1 POS 机申请、参数设置、程序灌装、使用、更换、维护、撤销的管理

支付机构应提供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。

支付机构应提供商户申请、使用、更换、维护、撤销POS机的详细记录。

7.2.3.2 POS 机密钥和参数的安全管理

支付机构应提供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。

7.2.3.3 控制移动 POS 机的安装

支付机构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。

7.2.3.4 终端安全检测报告

使用的终端应有安全检测报告，报告内容要能反映终端的安全状况。

7.2.3.5 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，报告内容要能反映终端的安全状况。

7.2.3.6 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，防止不法份子窃取账户信息，并保留巡查记录，包括终端巡检制度、巡检内容、巡检记录等。

7.2.3.7 实名认证

宜对客户进行实名认证。

增强要求为：应对客户身份进行实名认证。

7.3 性能要求

支付业务设施性能基本要求见表2。

表2 预付卡发行与受理性能检测基本要求列表

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	比对性能需求表高峰时段并发数	<=80%	100%	>=99%	>=30分钟

7.4 安全性要求

7.4.1 网络安全性要求

7.4.1.1 结构安全

7.4.1.1.1 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。

增强要求为：应保证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。

7.4.1.1.2 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。

7.4.1.1.3 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。

7.4.1.1.4 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。

7.4.1.1.5 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，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

7.4.1.1.6 QoS 保证

宜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。

增强要求为：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。

7.4.1.2 网络访问控制

7.4.1.2.1 网络域安全隔离和限制

应在网络边界部署访问控制设备，启用访问控制功能。

7.4.1.2.2 地址转换和绑定

重要网段应采取技术手段防止地址欺骗。

7.4.1.2.3 内容过滤

应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP等协议命令级的控制。

7.4.1.2.4 访问控制

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。

应按用户和系统之间的访问控制规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。

7.4.1.2.5 流量控制

应限制网络最大流量数及网络连接数。

7.4.1.2.6 会话控制

应在会话处于非活跃一定时间或会话结束后终止网络连接。

7.4.1.2.7 远程拨号访问控制和记录

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。

7.4.1.3 网络安全审计

7.4.1.3.1 日志信息

应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。

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。

7.4.1.3.2 网络系统故障分析

应对网络系统故障进行分析，查找原因并形成故障知识库。

7.4.1.3.3 网络对象操作审计

应能够根据记录数据进行分析，并生成审计报表。

7.4.1.3.4 日志权限和保护

应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

7.4.1.3.5 审计工具

应具备日志审计工具，对日志进行记录、分析和报告。

增强要求为：应定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，当存储空间被耗尽时，终止可审计事件的发生；

应根据信息系统的统一安全策略，实现集中审计，时钟宜采用多模方式授时。并应专人负责时间服务器，防止被恶意篡改。

7.4.1.4 边界完整性检查

应能够对非授权设备私自连接到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

应能够对内部网络用户私自连接到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

增强要求为：对非法外联和非法接入行为进行检测并阻断的同时，应通过报警方式通知管理员。

7.4.1.5 网络入侵防范

7.4.1.5.1 网络 ARP 欺骗攻击

应能够有效的防范网络ARP欺骗攻击。

7.4.1.5.2 信息窃取

应采用防范信息窃取的措施。

7.4.1.5.3 DoS/DDoS 攻击

应具有防DoS/DDoS攻击设备或技术手段。

7.4.1.5.4 网络入侵防范机制

应在网络边界处监视以下攻击行为：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提供报警。

增强要求为：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，应记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警及自动采取相应动作。

7.4.1.6 恶意代码防范

7.4.1.6.1 恶意代码防范措施

应在系统网络中对恶意代码进行检测和清除。

7.4.1.6.2 定时更新

应维护恶意代码库的升级，检测系统的更新。

7.4.1.7 网络设备防护

7.4.1.7.1 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，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

主要网络设备宜对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。

增强要求为：主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别，网络设备用户的身份鉴别信息至少应有一种是不可伪造的。

7.4.1.7.2 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。

7.4.1.7.3 登录地址限制

应对网络设备的管理员登录地址进行限制。

7.4.1.7.4 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。

7.4.1.7.5 设备用户设置策略

网络设备用户的标识应唯一，杜绝用户共享行为。

7.4.1.7.6 权限分离

应实现设备特权用户的权限分离。

7.4.1.7.7 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。

7.4.1.8 网络安全管理

7.4.1.8.1 网络设备运维手册

应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面做出规定。

应保证所有与外部系统的连接均得到授权和批准。

应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

7.4.1.8.2 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。

7.4.1.8.3 漏洞扫描

应定期对网络系统进行漏洞扫描，并保留扫描结果，对发现的网络系统安全漏洞进行及时的修补。

7.4.1.8.4 网络数据传输加密

当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

7.4.1.9 网络相关人员安全管理

7.4.1.9.1 网络安全管理人员配备

应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作。

7.4.1.9.2 网络安全管理人员责任划分规则

应制定文件明确网络安全管理岗位的职责、分工和技能要求。

7.4.1.9.3 网络安全关键岗位人员管理

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

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。

7.4.2 主机安全性要求

7.4.2.1 身份鉴别

7.4.2.1.1 系统与应用管理员用户设置

应对登录操作系统和数据库系统的用户进行身份标识和鉴别。

应为操作系统和数据库系统的不同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。

增强要求为：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， 并且身份鉴别信息至少有一种是不可伪造的。

7.4.2.1.2 系统与应用管理员口令安全性

操作系统和数据库系统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。

7.4.2.1.3 登录策略

应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

7.4.2.2 访问控制

7.4.2.2.1 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。

应实现操作系统和数据库系统特权用户的权限分离。

增强要求为：在系统对用户进行身份鉴别时，系统与用户之间应能够建立一条安全的信息传输路径；在用户对系统进行访问时，系统与用户之间应能够建立一条安全的信息传输路径。

7.4.2.2.2 主机信任关系

应避免不必要的主机信任关系。

7.4.2.2.3 默认过期用户

应及时删除多余的、过期的用户，避免共享用户的存在。

应严格限制默认用户的访问权限，重命名系统默认用户，修改这些用户的默认口令。

7.4.2.3 安全审计

7.4.2.3.1 日志信息

审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。

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。

增强要求为：应能够根据信息系统的统一安全策略，实现集中审计。

7.4.2.3.2 日志权限和保护

应保护审计记录，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。

增强要求为：应保护审计进程，避免受到未预期的中断。

7.4.2.3.3 系统信息分析

应能够根据记录数据进行分析，并生成审计报表。

7.4.2.4 系统保护

7.4.2.4.1 系统备份

应具有系统备份或系统重要文件备份。

7.4.2.4.2 故障恢复策略

应具备各种主机故障恢复策略。

7.4.2.4.3 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。

7.4.2.4.4 主机安全加固

应对主机进行安全加固并提供相关记录。

7.4.2.5 剩余信息保护

应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。

应确保系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

7.4.2.6 入侵防范

7.4.2.6.1 入侵防范记录

宜能够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、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

宜能够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具有恢复的措施。

增强要求为：应能够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、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

应能够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具有恢复的措施。

7.4.2.6.2 关闭服务和端口

应关闭系统不必要的服务和端口。

7.4.2.6.3 最小安装原则

操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

7.4.2.7 恶意代码防范

7.4.2.7.1 防范软件安装部署

应至少在生产系统中的服务器安装防恶意代码软件。

7.4.2.7.2 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。

7.4.2.7.3 防范软件统一管理

应支持防范软件的统一管理。

7.4.2.8 资源控制

7.4.2.8.1 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。

应根据安全策略设置登录终端的操作超时锁定。

7.4.2.8.2 资源监控和预警

应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。

应限制单个用户对系统资源的最大或最小使用限度。

应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

7.4.2.9 主机安全管理

7.4.2.9.1 主机运维手册

应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面做出具体规定。

7.4.2.9.2 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。

7.4.2.9.3 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，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。

7.4.2.9.4 操作日志管理

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，严禁进行未经授权的操作。

应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

7.4.2.10 主机相关人员安全管理

7.4.2.10.1 主机安全管理人员配备

应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则。

7.4.2.10.2 主机安全管理人员责任划分规则

应制定文件明确主机管理岗位的职责、分工和技能要求。

7.4.2.10.3 主机安全关键岗位人员管理

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

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。

7.4.3 应用安全性要求

7.4.3.1 身份鉴别

7.4.3.1.1 系统与普通用户设置

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，提供系统管理员和普通用户的设置功能。

7.4.3.1.2 系统与普通用户口令安全性

系统与普通用户口令应具有一定的复杂度。

7.4.3.1.3 登录访问安全策略

应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

增强要求为：应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别，其中一种是不可伪造的。

7.4.3.1.4 非法访问警示和记录

应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

7.4.3.1.5 客户端鉴别信息安全

客户端鉴别信息应不被窃取和冒用。

7.4.3.1.6 口令有效期限制

应提示客户定期修改口令。

应限制系统管理用户的口令有效期。

7.4.3.1.7 限制认证会话时间

应对客户端认证会话时间进行限制。

7.4.3.1.8 身份标识唯一性

应提供用户身份标识唯一性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身份标识，身份鉴别信息不易被冒用。

应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

7.4.3.1.9 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。

7.4.3.2 WEB 页面安全

7.4.3.2.1 登录防穷举

应提供登录防穷举的措施，如图片验证码等。

如预付卡系统为内部使用，不对互联网用户提供服务，该项不适用。

7.4.3.2.2 安全控件

登录应使用安全控件。

如预付卡系统为内部使用，不对互联网用户提供服务，该项不适用。

7.4.3.2.3 使用数字证书

应使用服务器证书，并在整个生命周期保障令牌的安全。
如预付卡系统为内部使用，不对互联网用户提供服务，该项不适用。

7.4.3.2.4 独立的支付密码

应提供独立的支付密码和健全的密码找回机制。
如预付卡系统为内部使用，不对互联网用户提供服务，该项不适用。

7.4.3.2.5 网站页面注入防范

网站页面应采取防范SQL注入、Path注入和LDAP注入等风险的措施。

7.4.3.2.6 网站页面跨站脚本攻击防范

网站页面应采取防范跨站脚本攻击风险的措施。

7.4.3.2.7 网站页面源代码暴露防范

网站页面应采取防范源代码暴露的措施。

7.4.3.2.8 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。

7.4.3.2.9 网站页面防篡改措施

应采取网站页面防篡改措施。
如预付卡系统为内部使用，不对互联网用户提供服务，该项不适用。

7.4.3.2.10 网站页面防钓鱼

网站页面应提供防钓鱼网站的防伪信息验证。
如预付卡系统为内部使用，不对互联网用户提供服务，该项不适用。

7.4.3.3 访问控制

7.4.3.3.1 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，并严格限制默认用户的访问权限。
应授予不同用户为完成各自承担任务所需的最小权限，并在它们之间形成互相制约的关系。

7.4.3.3.2 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、客体及它们之间的操作。

7.4.3.3.3 业务操作日志

应具有所有业务操作日志。

7.4.3.3.4 关键数据操作控制

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

7.4.3.3.5 异常中断防护

用户访问异常中断后，应具有防护手段，保证数据不丢失。

7.4.3.3.6 数据库安全配置

应具有数据库安全配置手册，并对数据库进行安全配置。

7.4.3.4 安全审计

7.4.3.4.1 日志信息

审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

7.4.3.4.2 日志权限和保护

应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录。

7.4.3.4.3 系统信息查询与分析

应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

7.4.3.4.4 对象操作审计

应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。

7.4.3.4.5 审计工具

应具备日志审计工具，对日志进行记录、分析和报告。

增强要求为：应根据系统统一安全策略，提供集中审计接口。

7.4.3.4.6 事件报警

应具有交易事件报警功能。

7.4.3.5 剩余信息保护

应对无用的过期信息、文档进行完整删除。

增强要求为：应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

7.4.3.6 资源控制

7.4.3.6.1 连接控制

应能够根据业务需求，对系统的最大并发会话连接数进行限制。

应能够对一个时间段内可能的并发会话连接数进行限制。

7.4.3.6.2 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。

应能够对单个帐户的多重并发会话进行限制。

7.4.3.6.3 进程资源分配

应能够对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额。

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。

7.4.3.6.4 资源监测预警

应能够对系统服务水平降低到预先规定的最小值进行检查和报警。

7.4.3.7 应用容错

7.4.3.7.1 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或长度符合系统设定要求。

7.4.3.7.2 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。

增强要求为：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。

7.4.3.7.3 故障机制

发生故障后，系统应能够及时恢复。

7.4.3.7.4 回退机制

应提供回退功能，当故障发生后，能够及时回退到故障发生前的状态。

7.4.3.8 报文完整性

通信报文应采用密码技术保证通讯过程中交易数据的完整性。

7.4.3.9 报文保密性

在通讯时采用安全通道或对报文中敏感信息进行加密。

7.4.3.10 抗抵赖

7.4.3.10.1 原发和接收证据

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。

7.4.3.10.2 可信时间戳服务

增强要求为：本地时间应从国家权威时间源采时，保证时间的同一性；

应采用国家认可的可信时间戳服务；

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。

7.4.3.11 编码安全

7.4.3.11.1 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。

增强要求为：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。

7.4.3.11.2 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。

7.4.3.11.3 编码规范约束

应按照编码规范进行编码，具有编码规范约束制度。

7.4.3.11.4 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。

7.4.3.11.5 版本管理

应具有代码版本管理制度。

7.4.3.12 电子认证应用

7.4.3.12.1 第三方电子认证机构证书

在对外业务（非内部业务）处理过程中，应使用经过认证的第三方电子认证证书。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，可以使用自建证书（非第三方电子认证证书）。在条件允许的情况下，建议对所有业务使用经过认证的第三方电子认证证书。

7.4.3.12.2 关键业务电子认证技术应用

关键业务应使用电子认证技术。在条件允许的情况下，建议在所有业务均使用经过认证的第三方电子认证技术。

7.4.3.12.3 电子签名有效性

应使用有效的电子签名。在对外业务（非内部业务）处理过程中，应使用经过第三方认证的电子签名体系。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，可以使用自建的电子签名体系（非第三方认证的电子签名体系）。在条件允许的情况下，建议对所有业务使用经过认证的第三方电子签名体系。

7.4.3.12.4 服务器证书私钥保护

应对所持有的服务器证书私钥进行有效保护。

7.4.3.13 脱机数据认证

7.4.3.13.1 密钥和证书

应符合JR/T 0025.7-2013，第5.1条中的规定，产生符合业务要求的密钥和证书。

7.4.3.13.2 静态数据认证

脱机交易应采用静态数据认证方式。

7.4.3.13.3 动态数据认证

脱机交易应采用动态数据认证方式。

7.4.3.14 应用密文和发卡机构认证

7.4.3.14.1 应用密文产生

应符合JR/T 0025.7-2013，第6.1条中的规定，产生符合业务要求的应用密文。

7.4.3.14.2 发卡机构认证

发卡机构认证过程应符合JR/T 0025.7-2013，第6.2条中的规定。

7.4.3.14.3 密钥管理

密钥管理应符合JR/T 0025.7-2013，第6.3条中的规定。

7.4.3.15 安全报文

7.4.3.15.1 报文格式

报文格式应符合JR/T 0025.7-2013，第7.1条中的规定。

7.4.3.15.2 报文完整性验证

应对报文完整性进行验证。

7.4.3.15.3 报文私密性

应保证报文私密性。

7.4.3.15.4 密钥管理

应对密钥进行安全管理。

7.4.3.16 卡片安全

7.4.3.16.1 共存应用

如支持多应用，则应保证多应用安全共存。

7.4.3.16.2 密钥的独立性

应符合JR/T 0025.7-2013，第8.2条中的规定，保证密钥的独立性。

7.4.3.16.3 卡片内部安全体系

应符合JR/T 0025.7-2013，第8.3条中的规定，建立卡片内部安全体系。

7.4.3.16.4 卡片中密钥的种类

应符合JR/T 0025.7-2013，第8.4条中的规定，对卡片中不同应用密钥进行分类。

7.4.3.17 终端安全

7.4.3.17.1 终端数据安全性要求

终端数据安全性应符合JR/T 0025.7-2013，第9.1条中的规定。

7.4.3.17.2 终端设备安全性要求

应提供金融行业检测机构安全检测报告。

7.4.3.17.3 终端密钥管理要求

应提供金融行业检测机构安全检测报告。

7.4.3.18 密钥管理体系

7.4.3.18.1 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。

7.4.3.18.2 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。

7.4.3.18.3 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。

7.4.3.19 安全机制

7.4.3.19.1 对称加密机制

对称加解密应符合JR/T 0025.7-2013，第11.1条中的规定。

7.4.3.19.2 非对称加密机制

非对称加解密应符合JR/T 0025.7-2013，第11.2条中的规定。

7.4.3.20 认可的算法

7.4.3.20.1 对称加密算法

应符合JR/T 0025.7-2013，第12.1条中的规定，使用认可的对称加密算法。

7.4.3.20.2 非对称加密算法

应符合JR/T 0025.7-2013，第12.2条中的规定，使用认可的非对称加密算法。

7.4.3.20.3 哈希算法

应符合JR/T 0025.7-2013，第12.3条中的规定，使用认可的哈希算法。

7.4.4 数据安全性要求

7.4.4.1 数据保护

7.4.4.1.1 客户身份信息保护

应按规定妥善保管客户身份基本信息，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。

7.4.4.1.2 支付业务信息保护

应按规定妥善保管支付业务信息（办理预付卡发行、受理、使用、充值和赎回等业务活动获得和产生的相关信息）。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。

7.4.4.1.3 会计档案信息保护

应按规定妥善保管会计档案，支付机构对会计档案的保管期限适用《会计档案管理办法》（财会字〔1998〕32号文印发）相关规定。

7.4.4.2 数据完整性

7.4.4.2.1 重要数据更改机制

应制定重要数据更改流程和管理制度。

7.4.4.2.2 数据备份记录

应具备数据备份记录。

7.4.4.2.3 保障传输过程中的数据完整性

应能够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。

7.4.4.2.4 备份数据定期恢复

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。

7.4.4.3 交易数据以及客户数据的安全性

7.4.4.3.1 数据物理存储安全

应具备高可用性的数据物理存储环境。

7.4.4.3.2 客户身份认证信息存储安全

应不允许保存非必须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、卡片有效期、个人标识码、银行卡交易密码、指纹、CVN、CVN2等敏感信息）。

应对客户的其他敏感信息，如卡号、户名、开户手机、贷记卡有效期、电子邮箱等信息采取保护措施，防止未经授权擅自对个人信息进行查看、篡改、泄露和破坏。宜采用加密存储、部分屏蔽显示等技术。

7.4.4.3.3 终端信息采集设备硬加密措施或其它防伪手段

如果使用终端信息采集设备则应采取硬加密措施，否则要使用其它手段达到防伪目的。

7.4.4.3.4 同一安全级别和可信赖的系统之间信息传输

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。

7.4.4.3.5 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。

7.4.4.3.6 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。

增强要求为：应避免使用标准的哈希算法。

7.4.4.3.7 数据访问控制

应具备重要数据的访问控制措施。

7.4.4.3.8 在线的存储备份

应具备实时在线的存储备份设施。

7.4.4.3.9 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，应指明备份数据的备份方式（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。

7.4.4.3.10 本地备份

应提供本地数据备份。

应具有同机房数据备份设施。

7.4.4.3.11 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。

7.4.4.3.12 备份数据的恢复

应具有备份数据恢复操作手册，并提供恢复功能。

7.4.4.3.13 数据销毁制度和记录

应具有数据销毁制度和相关记录。

7.4.4.3.14 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。

7.4.5 运维安全性要求

7.4.5.1 环境管理

7.4.5.1.1 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。

7.4.5.1.2 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。

7.4.5.1.3 办公环境的保密性措施

应加强对办公环境的保密性管理，规范办公环境人员行为，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档文件等。

7.4.5.1.4 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做出规定。

增强要求为：开发、测试和运行设施应分离，以减少未授权访问或改变运行系统的风险。

7.4.5.1.5 机房进出登记表

应具有机房进出登记表。

7.4.5.2 介质管理

7.4.5.2.1 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，并实行存储环境专人管理。

7.4.5.2.2 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、维护和销毁等方面做出规定。

7.4.5.2.3 维修或销毁介质之前清除敏感数据

应对送出维修以及销毁等进行严格的管理，对送出维修或销毁的介质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。

7.4.5.2.4 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。

7.4.5.2.5 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。

7.4.5.3 设备管理

7.4.5.3.1 设备管理的责任人员或部门

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。

7.4.5.3.2 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管理。

7.4.5.3.3 设备选型、采购、发放等的审批控制

应建立基于申报、审批和专人负责的设备安全管理制度，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。

7.4.5.3.4 设备配置标准化

应建立标准化的设备配置文档。

7.4.5.3.5 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，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。

7.4.5.3.6 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。

7.4.5.3.7 设备使用管理文档

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。

7.4.5.3.8 设备标识

应对设备进行分类和标识。

7.4.5.4 人员管理

7.4.5.4.1 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。

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

7.4.5.4.2 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。

应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。

7.4.5.4.3 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。

7.4.5.4.4 安全意识教育和培训

应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训。

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

应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训。

应对安全教育和培训的情况和结果进行记录并归档保存。

7.4.5.4.5 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。

7.4.5.4.6 职责分离

关键岗位人员应职责分离。

7.4.5.5 监控管理

7.4.5.5.1 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、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。

7.4.5.5.2 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。

7.4.5.5.3 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。

7.4.5.5.4 异常处理机制

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。

7.4.5.5.5 资源监控

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

7.4.5.6 变更管理

7.4.5.6.1 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须经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。

7.4.5.6.2 变更方案

应确认系统中要发生的变更，并制定变更方案，变更内容中应有变更失败后的回退方案等。

7.4.5.6.3 重要系统变更的通知

重要系统变更前，应通知相关单位、部门和人员。

7.4.5.6.4 重要系统变更的实施

应记录变更实施过程，并妥善保存所有文档和记录。

7.4.5.7 安全事件处置

7.4.5.7.1 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。

7.4.5.7.2 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。

7.4.5.7.3 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，过程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。

7.4.5.8 应急预案管理

7.4.5.8.1 制定不同事件的应急预案

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。

7.4.5.8.2 相关人员应急预案培训

应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。

7.4.5.8.3 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。对应急预案演练中暴露出的问题进行总结并及时整改。

7.4.6 业务连续性要求

7.4.6.1 业务连续性需求分析

7.4.6.1.1 业务中断影响分析

应进行业务中断影响分析。

7.4.6.1.2 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。

7.4.6.2 业务连续性技术环境

7.4.6.2.1 备份机房

应具备同城应用级备份。

7.4.6.2.2 网络双链路

应具备双链路。

7.4.6.2.3 网络设备和服务器备份

应具有同城应用级备份设施。

7.4.6.2.4 高可靠的磁盘阵列

应使用高可靠的磁盘阵列。

7.4.6.2.5 远程数据库备份

应具备远程备份数据库。

7.4.6.3 业务连续性管理

7.4.6.3.1 业务连续性管理制度

应具备业务连续性管理制度。

7.4.6.3.2 应急响应流程

应具备应急响应流程。

7.4.6.3.3 恢复预案

应具备不同场景恢复预案，同时具备应用级恢复预案。

7.4.6.3.4 数据备份和恢复制度

应具备数据备份和恢复管理制度。

7.4.6.4 备份和恢复管理

7.4.6.4.1 备份数据范围和备份频率

应具备备份数据范围和备份频率清单。

7.4.6.4.2 备份和恢复手册

应具备数据备份和恢复手册。

7.4.6.4.3 备份记录和定期恢复测试记录

应具备备份记录和定期恢复测试记录。

7.4.6.4.4 定期数据备份恢复性测试

应进行定期数据备份恢复性测试。

7.4.6.5 日常维护

7.4.6.5.1 每年业务连续性演练

应每年进行业务连续性演练。

7.4.6.5.2 定期业务连续性培训

应每年进行业务连续性演练，包括主备机房的切换演练，演练需提供记录。

7.5 文档要求

7.5.1 用户文档

7.5.1.1 用户手册

用户手册应描述手工操作该软件的用户应如何安装和使用一个软件系统。它还包括软件操作的一些特别的方面，诸如，关于特定岗位或任务的指令等。用户手册是为由用户操作的软件而开发的，具有要求联机用户输入或解释输出显示的用户界面。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

7.5.1.2 操作手册

操作手册应提供操作指定的设备所需的信息。本手册侧重设备自身，而不是运行在其上的特定的软件。操作手册主要针对一些新开发的设备、专用设备、无现成的商用操作手册或其他操作手册可用的其他的设备。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

7.5.2 开发文档

7.5.2.1 需求说明书

需求说明书应从以下几方面描述一个建议的系统：说明它能满足用户什么需要，它与现有系统或过程的关系，以及它的使用方式等。需求说明书旨在需方、开发方、支持方和用户代理之间对所建议的系统的运行机理取得共识。取决于使用的目的，需求说明书可专注于向开发者表述用户的需求，或专注于向用户或其他感兴趣的对象表达开发者的思路。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

7.5.2.2 需求分析文档

需求分析文档应描述对计算机软件系统的需求，及确保每个需求得以满足所使用的方法。需求分析文档应涉及该系统外部接口的需求。

宜符合GB/T 8567和GB/T 9385要求。

增强要求为：应符合GB/T 8567和GB/T 9385要求。

7.5.2.3 总体设计方案

总体设计方案应描述系统或子系统的系统级或子系统级设计与体系结构设计。总体设计方案还要用《概要设计文档》和《数据库设计文档》加以补充。总体设计方案连同相关的概要和数据库设计文档是构成进一步系统实现的基础。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

7.5.2.4 数据库设计文档

数据库设计文档应描述数据库的设计。数据库可由用户或计算机程序通过数据库管理系统加以访问。数据库设计文档还描述了存取或操纵数据所使用的软件配置项。数据库设计文档是实现数据库及相关软件配置项的基础。它向需方提供了设计的可视性，为软件支持提供了所需要的信息。数据库设计文档是否单独成册或与详细设计文档合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

7.5.2.5 概要设计文档

概要设计文档应描述计算机软件系统的设计。它描述了系统级设计决策、系统体系结构设计，概要设计和数据库设计是否单独成册抑或与详细设计合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

7.5.2.6 详细设计文档

详细设计文档应描述计算机软件系统的设计。它描述了子系统级设计决策、系统体系结构设计和实现该软件所需的详细设计。概要设计和数据库设计是否单独成册抑或与详细设计合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

7.5.2.7 工程实施方案

工程实施方案应描述开发者实施软件开发工作的计划，包括新开发、修改、重用、再工程、维护和由软件产品引起的其他所有的活动。工程实施方案是向需求方提供了解和监督软件开发过程、所使用的方法、每项活动的途径、项目的安排、组织及资源的一种手段。

7.5.3 管理文档

7.5.3.1 测试报告

测试报告应是对计算机软件、软件系统或子系统，或与软件相关项目执行合格性测试的记录。通过测试报告，需方能够评估所执行的合格性测试及其测试结果。

宜符合GB/T 8567和GB/T 9386要求。

增强要求为：应符合GB/T 8567和GB/T 9386要求。

7.5.3.2 系统运维手册

系统运维手册应是对系统运维管理中用到的环境、资产、介质、设备等进行维护、升级、漏洞扫描等操作的详细描述。

7.5.3.3 系统应急手册

应根据不同的事件，制定应急预案，形成系统应急手册。

7.5.3.4 运维管理制度

运维管理制度应包含但不限于机房管理制度、介质管理制度、设备管理制度、人员管理制度、监控巡检管理制度、变更管理制度、安全事件处理制度等。

7.5.3.5 安全管理制度

安全管理制度应是对负责安全管理机构的设置与人员等资源的配备描述，以及保证其正常实施安全管理工作的管理制度。

7.5.3.6 安全审计报告

应由专业审计人员根据有关的法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并做出相应评价报告。

8 银行卡收单技术要求

8.1 功能要求

8.1.1 特约商户管理

8.1.1.1 商户提交资质材料

应实现商户资质等信息的录入、审核等功能。在特约商户申请首次、业务变更、解冻、退出等情况下，应对特约商户提交的资质材料进行审核，并定期复核。

8.1.1.2 黑名单检查及管理

应具有交易过程中黑名单检查、日常黑名单管理的功能。

8.1.1.3 商户信息查询

应具有商户信息的查询功能。

8.1.1.4 商户操作员管理

应对商户控制平台或POS机等的操作员进行管理。

8.1.1.5 商户受理业务管理

应具有商户受理业务的增加、修改和取消功能。

8.1.1.6 商户信息维护

应具有商户信息的增加、修改和删除功能。

8.1.1.7 商户冻结、解冻

应具有暂停商户交易和重新恢复商户交易的功能。

8.1.1.8 商户退出

应能够永久停止商户交易的功能。

8.1.2 终端机具信息管理

8.1.2.1 机具申领和报废控制

应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。

8.1.2.2 机具信息维护

应能够对机具的编号、对应商户名称、商户编号进行维护。

8.1.2.3 机具信息查询

应能够对机具信息（例如：编号、对应商户名称、商户编号）进行查询。

8.1.3 密钥管理

8.1.3.1 密钥生成

应具有密钥生成流程及控制。

8.1.3.2 密钥分发

应具有密钥分发流程及控制。

8.1.3.3 密钥使用

应具有密钥使用控制流程及控制。

8.1.3.4 密钥存储

应具有密钥存储规定及控制。

8.1.3.5 密钥更新

应具有密钥更新流程及控制。

8.1.3.6 密钥销毁

应具有密钥销毁流程及控制。

8.1.4 交易处理

8.1.4.1 消费

应实现POS等消费功能。

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当包括商品订单号和网络交易平台名称。

8.1.4.2 消费撤销

应实现消费撤销功能。

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打印凭证。

8.1.4.3 余额查询

应实现银行卡余额查询的功能。

8.1.4.4 预授权

应实现预授权功能。

8.1.4.5 预授权撤销

应实现预授权撤销功能。

8.1.4.6 预授权完成

应实现预授权完成功能。

8.1.4.7 预授权完成撤销

应实现预授权完成撤销功能。

8.1.4.8 追加预授权

应实现追加预授权功能。

8.1.4.9 退货

应实现退货功能。

应提供原消费交易的凭证，按业务要求在POS上输入有关数据，收到响应后，完成退货交易并打印凭证。

8.1.4.10 指定账户圈存

应实现指定账户圈存功能。

8.1.4.11 非指定账户圈存

应实现非指定账户圈存功能。

8.1.4.12 现金充值

应能够通过柜台或自助终端等方式使用现金进行充值交易。

8.1.4.13 圈提

应实现圈提交易功能，应在金融终端上联机进行。

8.1.4.14 脱机消费

应实现IC卡脱机消费功能。

8.1.4.15 IC卡参数下载

应实现IC卡参数下载功能。

8.1.4.16 交易明细查询

应实现在受理平台和终端上的历史交易明细查询的功能。

8.1.4.17 冲正交易

应具有在受理平台或终端上的冲正交易的功能。

8.1.5 资金结算

8.1.5.1 银行清算

应能够根据银行的要求正确完成与银行之间的清算。

8.1.5.2 商户结算

应具有商户资金结算功能。

8.1.6 对账处理

8.1.6.1 发送对账请求

应允许商户发送对账请求。

8.1.6.2 报文设计

增强要求为：报文设计符合附录 C 中 C.1 的报文结构设计要求。

8.1.6.3 下载对账文件

应具有商户下载对账文件。

8.1.7 差错处理

8.1.7.1 拒付管理

应具有对于拒付交易的查询、删除等功能。

8.1.7.2 单笔退款

应具有针对单笔交易的退款功能。

支付服务方应将部分或全部已扣款项退还给客户（个人或企业买方）的原扣款账户，原扣款账户不能接收退款的，退款到付款人其他账户。

8.1.7.3 批量退款

应具有差错处理过程中针对批量交易的退款功能。

支付服务方应将部分或全部已扣款项退还给客户（个人或企业买方）的原扣款账户，原扣款账户不能接收退款的，退款到付款人其他账户。

8.1.7.4 差错交易查询

应具有对各种差错交易的查询功能。

8.1.7.5 对账差错处理

应具有对账文件出错，对账结果不平等的处理流程。

8.1.7.6 报文设计

增强要求为：报文设计符合附录C中C.2的报文结构设计要求。

8.1.8 统计报表

8.1.8.1 业务类报表

应具有与收单业务有关的各种业务类型以及相关的业务规模等统计功能。

8.1.8.2 运行管理类报表

应实现一段时间内运行管理情况（如客户注册、商户开通、卡片发行、交易、结算等操作）的查询统计。第三方支付公司可以根据自身的情况将“一段时间”细化为“月季年”。

8.2 风险监控要求

8.2.1 交易管理

8.2.1.1 联机交易 ARQC/ARPC 验证

应能够进行联机交易的ARQC/ARPC验证。

8.2.1.2 联机报文 MAC 验证

联机交易的报文的MAC验证失败后应有记录。

8.2.1.3 黑名单管理

使用黑名单内的卡片交易应有记录并触发风控规则。

8.2.1.4 单笔消费限额

超过单笔消费限额的交易应有记录并触发风控规则。

8.2.1.5 大额消费商户交易监控

对于大额消费商户的交易应有记录并触发风控规则。

8.2.1.6 可疑交易处理

应实现可疑交易处理规则的设置，以实现对可疑交易的查询、分析、处理等服务。

8.2.1.7 无磁无密交易

对于无磁无密的交易，在风险监控系统上应有记录。

8.2.2 收单风险管理

8.2.2.1 商户资质审核

收单机构应对商户资质进行审核，实行实名制管理，严格审核特约商户的营业执照等证明文件，以及法定代表人或负责人有效身份证件等申请材料。特约商户为自然人的，收单机构应当审核其有效身份证件。特约商户使用单位银行结算账户作为收单银行结算账户的，收单机构还应当审核其合法拥有该账户的证明文件。

应具有明确的审核流程和标准，明确资质审核权限，审核人员不得兼岗。

8.2.2.2 商户签约

收单机构在与商户合作时，应签订协议，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。

应当建立资金结算风险管理制度，包含资金结算、移机、套现、侧录等。

8.2.2.3 特约商户日常风险管理

应向商户发放风险提示信息，给商户风险培训。应提示特约商户定期审核网站，杜绝非法链接。

8.2.2.4 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。

8.2.2.5 特约商户强制冻结、解冻、解约

遇到问题后，能够强制冻结、解冻商户，甚至和商户解约。

8.2.2.6 可疑商户信息共享

可疑商户的信息要在收单机构间共享。

8.2.2.7 风险事件报送

当出现风险事件时应向上级部门或者主管部门报送。

8.2.3 终端风险管理

8.2.3.1 POS 机申请、参数设置、程序灌装、使用、更换、维护、撤销、回收的管理

POS机的管理应有明确的流程。

8.2.3.2 POS 机密钥和参数的安全管理

对POS机密钥和参数有严格的管理要求。POS终端密钥应严格按照“一机一密”安全规范进行管理，POS终端密钥应符合双倍长密钥算法规范。

8.2.3.3 控制移动 POS 机的安装

移动POS机的安装要严格限制，详细登记。

8.2.3.4 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，报告内容要能反映终端的安全状况；应有终端入网检测报告，报告内容要能明确POS签购单打印格式和要素。

8.2.3.5 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，报告内容要能反映密码键盘的安全状况。

8.2.3.6 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，防止不法份子窃取账户信息，并保留巡查记录。

8.2.4 风控规则

8.2.4.1 风控规则管理

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

8.2.4.2 风险识别

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。

8.2.4.3 风险事件管理

应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，并保留事件的记录。

8.2.4.4 风险报表

应提供一段时间内的风险事件报表，可以根据自身的情况将“一段时间”细化为“月季年”。

8.3 性能要求

支付业务设施性能基本要求见表3。

表3 银行卡收单性能检测基本要求列表

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	比对性能需求表高峰时段并发数	<=80%	100％	>=99%	>=30分钟

8.4 安全性要求

8.4.1 网络安全性要求

8.4.1.1 结构安全

8.4.1.1.1 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。

增强要求为：应保证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。

8.4.1.1.2 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。

8.4.1.1.3 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。

8.4.1.1.4 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。

8.4.1.1.5 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，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

8.4.1.1.6 QoS 保证

宜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。

增强要求为：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。

8.4.1.2 网络访问控制

8.4.1.2.1 网络域安全隔离和限制

应在网络边界部署访问控制设备，启用访问控制功能。

8.4.1.2.2 地址转换和绑定

重要网段应采取技术手段防止地址欺骗。

8.4.1.2.3 内容过滤

应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP 等协议命令级的控制。

8.4.1.2.4 访问控制

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。

应按用户和系统之间的访问控制规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。

8.4.1.2.5 流量控制

应限制网络最大流量数及网络连接数。

8.4.1.2.6 会话控制

应在会话处于非活跃一定时间或会话结束后终止网络连接。

8.4.1.2.7 远程拨号访问控制和记录

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。

8.4.1.3 网络安全审计

8.4.1.3.1 日志信息

应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。

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。

8.4.1.3.2 网络系统故障分析

应对网络系统故障进行分析，查找原因并形成故障知识库。

8.4.1.3.3 网络对象操作审计

应能够根据记录数据进行分析，并生成审计报表。

8.4.1.3.4 日志权限和保护

应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

8.4.1.3.5 审计工具

应具备日志审计工具，对日志进行记录、分析和报告。

增强要求为：应定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，当存储空间被耗尽时，终止可审计事件的发生；

应根据信息系统的统一安全策略，实现集中审计。时钟宜采用多模方式授时。并应专人负责时间服务器，防止被恶意篡改。

8.4.1.4 边界完整性检查

应能够对非授权设备私自连接到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

应能够对内部网络用户私自连接到外部网络的行为进行检查,准确定出位置,并对其进行有效阻断。

增强要求为：对非法外联和非法接入行为进行检测并阻断的同时，应通过报警方式通知管理员。

8.4.1.5 网络入侵防范

8.4.1.5.1 网络 ARP 欺骗攻击

应能够有效的防范网络 ARP 欺骗攻击。

8.4.1.5.2 信息窃取

应采用防范信息窃取的措施。

8.4.1.5.3 DoS/DDoS 攻击

应具有防 DoS/DDoS 攻击设备或技术手段。

8.4.1.5.4 网络入侵防范机制

应在网络边界处监视以下攻击行为：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提供报警。

增强要求为：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，应记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警及自动采取相应动作。

8.4.1.6 恶意代码防范

8.4.1.6.1 恶意代码防范措施

应在网络边界处对恶意代码进行检测和清除。

增强要求为：应在系统网络中对恶意代码进行检测和清除。

8.4.1.6.2 定时更新

应维护恶意代码库的升级，检测系统的更新。

8.4.1.7 网络设备防护

8.4.1.7.1 设备登录设置

应对登录网络设备的用户进行身份鉴别。

网络设备用户的标识应唯一。

主要网络设备宜对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。

增强要求为：主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别，网络设备用户的身份鉴别信息至少应有一种是不可伪造的。

8.4.1.7.2 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。

8.4.1.7.3 登录地址限制

应对网络设备的管理员登录地址进行限制。

8.4.1.7.4 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。

8.4.1.7.5 设备用户设置策略

应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

8.4.1.7.6 权限分离

应实现设备特权用户的权限分离。

8.4.1.7.7 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。

8.4.1.8 网络安全管理

8.4.1.8.1 网络设备运维手册

应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面做出规定。

应保证所有与外部系统的连接均得到授权和批准。

应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

8.4.1.8.2 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。

8.4.1.8.3 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进行及时的修补。

8.4.1.8.4 网络数据传输加密

当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

8.4.1.9 网络相关人员安全管理

8.4.1.9.1 网络安全管理人员配备

应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作。

8.4.1.9.2 网络安全管理人员责任划分规则

应制定文件明确网络安全管理岗位的职责、分工和技能要求。

8.4.1.9.3 网络安全关键岗位人员管理

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

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。

8.4.2 主机安全性要求

8.4.2.1 身份鉴别

8.4.2.1.1 系统与应用管理员用户设置

应对登录操作系统和数据库系统的用户进行身份标识和鉴别。

应为操作系统和数据库系统的不同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。

增强要求为：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，并且身份鉴别信息至少有一种是不可伪造的。

8.4.2.1.2 系统与应用管理员口令安全性

操作系统和数据库系统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。

8.4.2.1.3 登录策略

应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

8.4.2.2 访问控制

8.4.2.2.1 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。

应实现操作系统和数据库系统特权用户的权限分离。

增强要求为：在系统对用户进行身份鉴别时，系统与用户之间应能够建立一条安全的信息传输路径；

在用户对系统进行访问时，系统与用户之间应能够建立一条安全的信息传输路径。

8.4.2.2.2 主机信任关系

应避免不必要的主机信任关系。

8.4.2.2.3 默认过期用户

应及时删除多余的、过期的用户，避免共享用户的存在。

应严格限制默认用户的访问权限，重命名系统默认用户，修改这些用户的默认口令。

8.4.2.3 安全审计

8.4.2.3.1 日志信息

审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。

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。

增强要求为：应能够根据信息系统的统一安全策略，实现集中审计。

8.4.2.3.2 日志权限和保护

应保护审计记录，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。

增强要求为：应保护审计进程，避免受到未预期的中断。

8.4.2.3.3 系统信息分析

应能够根据记录数据进行分析，并生成审计报表。

8.4.2.4 系统保护

8.4.2.4.1 系统备份

应具有系统备份或系统重要文件备份。

8.4.2.4.2 故障恢复策略

应具备各种主机故障恢复策略。

8.4.2.4.3 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。

8.4.2.4.4 主机安全加固

应对主机进行安全加固。

8.4.2.5 剩余信息保护

应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。

应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

8.4.2.6 入侵防范

8.4.2.6.1 入侵防范记录

宜能够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、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

宜能够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具有恢复的措施。

增强要求为：应能够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、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

应能够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具有恢复的措施。

8.4.2.6.2 关闭服务和端口

应关闭系统不必要的服务和端口。

8.4.2.6.3 最小安装原则

操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

8.4.2.7 恶意代码防范

8.4.2.7.1 防范软件安装部署

应至少在生产系统中的服务器安装防恶意代码软件。

8.4.2.7.2 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。

8.4.2.7.3 防范软件统一管理

应支持防范软件的统一管理。

8.4.2.8 资源控制

8.4.2.8.1 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。

应根据安全策略设置登录终端的操作超时锁定。

8.4.2.8.2 资源监控和预警

应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。

应限制单个用户对系统资源的最大或最小使用限度。

应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

8.4.2.9 主机安全管理

8.4.2.9.1 主机运维手册

应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面做出具体规定。

8.4.2.9.2 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。

8.4.2.9.3 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，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。

8.4.2.9.4 操作日志管理

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，严禁进行未经授权的操作。

应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

8.4.2.10 主机相关人员安全管理

8.4.2.10.1 主机安全管理人员配备

应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则。

8.4.2.10.2 主机安全管理人员责任划分规则

应制定文件明确主机管理岗位的职责、分工和技能要求。

8.4.2.10.3 主机安全关键岗位人员管理

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

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。

8.4.3 应用安全性要求

8.4.3.1 身份鉴别

8.4.3.1.1 系统与普通用户设置

应提供专用的登录控制模板对登录用户进行身份标识和鉴别，提供系统管理员和普通用户的设置功能。

8.4.3.1.2 系统与普通用户口令安全性

系统与普通用户口令应具有一定的复杂度。

8.4.3.1.3 登录访问安全策略

应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

增强要求为：应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别，其中一种是不可伪造的。

8.4.3.1.4 非法访问警示和记录

应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

8.4.3.1.5 客户端鉴别信息安全

客户端鉴别信息应不被窃取和冒用。

8.4.3.1.6 口令有效期限制

应提示客户定期修改口令。

应限制系统管理用户的口令有效期。

8.4.3.1.7 限制认证会话时间

应对客户端认证会话时间进行限制。

8.4.3.1.8 身份标识唯一性

应提供用户身份标识唯一性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身份标识，身份鉴别信息不易被冒用。

应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

8.4.3.1.9 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。

8.4.3.2 WEB 页面安全

8.4.3.2.1 登录防穷举

应提供登录防穷举的措施，如图片验证码等。如收单系统为内部使用，不对互联网用户提供服务，该项不适用。

8.4.3.2.2 安全控件

登录应使用安全控件。如收单系统为内部使用，不对互联网用户提供服务，该项不适用。

8.4.3.2.3 使用数字证书

应使用服务器证书，并在整个生命周期保障令牌的安全。
如收单系统为内部使用，不对互联网用户提供服务，该项不适用。

8.4.3.2.4 独立的支付密码

应提供独立的支付密码和健全的密码找回机制。如收单系统为内部使用，不对互联网用户提供服务，该项不适用。

8.4.3.2.5 网站页面注入防范

网站页面应采取防范SQL注入、Path注入和LDAP注入等风险的措施。

8.4.3.2.6 网站页面跨站脚本攻击防范

网站页面应采取防范跨站脚本攻击风险的措施。

8.4.3.2.7 网站页面源代码暴露防范

网站页面应采取防范源代码暴露的措施。

8.4.3.2.8 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。

8.4.3.2.9 网站页面防篡改措施

应采取网站页面防篡改措施。如收单系统为内部使用，不对互联网用户提供服务，该项不适用。

8.4.3.2.10 网站页面防钓鱼

网站页面应提供防钓鱼网站的防伪信息验证。如收单系统为内部使用，不对互联网用户提供服务，该项不适用。

8.4.3.3 访问控制

8.4.3.3.1 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，并严格限制默认用户的访问权限。

应授予不同用户为完成各自承担任务所需的最小权限，并在它们之间形成互相制约的关系。

8.4.3.3.2 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、客体及它们之间的操作。

8.4.3.3.3 业务操作日志

应具有所有业务操作日志。

8.4.3.3.4 关键数据操作控制

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

8.4.3.3.5 异常中断防护

用户访问异常中断后，应具有防护手段，保证数据不丢失。

8.4.3.3.6 数据库安全配置

应具有数据库安全配置手册，并对数据库进行安全配置。

8.4.3.4 安全审计

8.4.3.4.1 日志信息

审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

8.4.3.4.2 日志权限和保护

应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录。

8.4.3.4.3 系统信息查询与分析

应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

8.4.3.4.4 对象操作审计

应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。

8.4.3.4.5 审计工具

应具备日志审计工具，对日志进行记录、分析和报告。

增强要求为：应根据系统统一安全策略，提供集中审计接口。

8.4.3.4.6 事件报警

应具有交易事件报警功能。

8.4.3.5 剩余信息保护

应对无用的过期信息、文档进行完整删除。

增强要求为：应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

8.4.3.6 资源控制

8.4.3.6.1 连接控制

应能够根据业务需求，对系统的最大并发会话连接数进行限制。

应能够对一个时间段内可能的并发会话连接数进行限制。

8.4.3.6.2 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。

应能够对单个帐户的多重并发会话进行限制。

8.4.3.6.3 进程资源分配

应能够对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额。

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。

8.4.3.6.4 资源监测预警

应能够对系统服务水平降低到预先规定的最小值进行检查和报警。

8.4.3.7 应用容错

8.4.3.7.1 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或长度符合系统设定要求。

8.4.3.7.2 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。

增强要求为：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。

8.4.3.7.3 故障机制

发生故障后，系统应能够及时恢复。

8.4.3.7.4 回退机制

应提供回退功能，当故障发生后，能够及时回退到故障发生前的状态。

8.4.3.8 报文完整性

通信报文应采用密码技术保证通讯过程中交易数据的完整性。

8.4.3.9 报文保密性

在通讯时采用安全通道或对报文中敏感信息进行加密。

8.4.3.10 抗抵赖

8.4.3.10.1 原发和接收证据

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。

8.4.3.10.2 可信时间戳服务

增强要求为：本地时间应从国家权威时间源采时，保证时间的同一性；
应采用国家认可的可信时间戳服务；
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。

8.4.3.11 编码安全

8.4.3.11.1 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。
增强要求为：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。

8.4.3.11.2 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。

8.4.3.11.3 编码规范约束

应按照编码规范进行编码，具有编码规范约束制度。

8.4.3.11.4 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。

8.4.3.11.5 版本管理

应具有代码版本管理制度。

8.4.3.12 电子认证应用

8.4.3.12.1 第三方电子认证机构证书

在对外业务（非内部业务）处理过程中，应使用经过认证的第三方电子认证证书。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，可以使用自建证书（非第三方电子认证证书）。在条件允许的情况下，建议对所有业务使用经过认证的第三方电子认证证书。

8.4.3.12.2 关键业务电子认证技术应用

关键业务应使用电子认证技术。在条件允许的情况下，建议在所有业务均使用经过认证的第三方电子认证技术。

8.4.3.12.3 电子签名有效性

应使用有效的电子签名。在对外业务（非内部业务）处理过程中，应使用经过第三方认证的电子签名体系。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，可以使用自建的电子签名体系（非第三方认证的电子签名体系）。在条件允许的情况下，建议对所有业务使用经过认证的第三方电子签名体系。

8.4.3.12.4 服务器证书私钥保护

应对所持有的服务器证书私钥进行有效保护。

8.4.3.13 脱机数据认证

8.4.3.13.1 密钥和证书

应符合JR/T 0025.7-2013，第5.1条中的规定，产生符合业务要求的密钥和证书。

8.4.3.13.2 静态数据认证

脱机交易应采用静态数据认证方式。

8.4.3.13.3 动态数据认证

脱机交易应采用动态数据认证方式。

8.4.3.14 安全报文

8.4.3.14.1 报文格式

应符合JR/T 0025.7-2013，第7.1条中的规定。

8.4.3.14.2 报文完整性验证

应对报文完整性进行验证。

8.4.3.14.3 报文私密性

应保证报文私密性。

8.4.3.14.4 密钥管理

应对密钥进行安全管理。

8.4.3.15 终端安全

8.4.3.15.1 终端数据安全性要求

终端数据安全性应符合JR/T 0025.7-2013，第9.1条中的规定。

8.4.3.15.2 终端设备安全性要求

应符合国家相关标准，并提供金融行业检测机构安全检测报告。

8.4.3.15.3 终端密钥管理要求

应符合国家相关标准，并提供金融行业检测机构安全检测报告。

8.4.3.16 安全机制

8.4.3.16.1 对称加密机制

对称加解密应符合JR/T 0025.7-2013，第11.1条中的规定。

8.4.3.16.2 非对称加密机制

非对称加解密应符合JR/T 0025.7-2013，第11.2条中的规定。

8.4.3.17 认可的算法

8.4.3.17.1 对称加密算法

应符合JR/T 0025.7-2013，第12.1条中的规定，使用认可的对称加密算法。

8.4.3.17.2 非对称加密算法

应符合JR/T 0025.7-2013，第12.2条中的规定，使用认可的非对称加密算法。

8.4.3.17.3 哈希算法

应符合JR/T 0025.7-2013，第12.3条中的规定，使用认可的哈希算法。

8.4.4 数据安全性要求

8.4.4.1 数据保护

8.4.4.1.1 客户身份信息保护

应当按规定妥善保管客户身份基本信息，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。

8.4.4.1.2 支付业务信息保护

应当按规定妥善保管支付业务信息，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。

8.4.4.1.3 会计档案信息保护

应当按规定妥善保管会计档案，支付机构对会计档案的保管期限适用《会计档案管理办法》（财会字〔1998〕32号文印发）相关规定。

8.4.4.2 数据完整性

8.4.4.2.1 重要数据更改机制

应制定重要数据更改流程和管理制度。

8.4.4.2.2 数据备份记录

应具备数据备份记录。

8.4.4.2.3 保障传输过程中的数据完整性

应能够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。

8.4.4.2.4 备份数据定期恢复

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。

8.4.4.3 交易数据以及客户数据的安全性

8.4.4.3.1 数据物理存储安全

应具备高可用性的数据物理存储环境。

8.4.4.3.2 客户身份认证信息存储安全

应不允许保存非必须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、卡片有效期、个人标识码、银行卡交易密码、指纹、CVN、CVN2等敏感信息）。

应对客户的其他敏感信息，如卡号、户名、开户手机、贷记卡有效期、电子邮箱等信息采取保护措施，防止未经授权擅自对个人信息进行查看、篡改、泄露和破坏。宜采用加密存储、部分屏蔽显示等技术。

8.4.4.3.3 终端信息采集设备硬加密措施或其它防伪手段

如果使用终端信息采集设备则应采取硬加密措施，否则要使用其它手段达到防伪目的。

8.4.4.3.4 同一安全级别和可信赖的系统之间信息传输

某一安全级别的系统应只能向同级别或更高级别可信赖的系统传输数据。

8.4.4.3.5 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。

8.4.4.3.6 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。

增强要求为：应避免使用标准的哈希算法。

8.4.4.3.7 数据访问控制

应具备重要数据的访问控制措施。

8.4.4.3.8 在线的存储备份

应具备实时在线的存储备份设施。

8.4.4.3.9 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，应指明备份数据的备份方式（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。

8.4.4.3.10 本地备份

应具有同机房数据备份设施。

8.4.4.3.11 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。

8.4.4.3.12 备份数据的恢复

应具有备份数据恢复操作手册，并提供恢复功能。

8.4.4.3.13 数据销毁制度和记录

应具有数据销毁制度和相关记录。

8.4.4.3.14 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。

8.4.5 运维安全性要求

8.4.5.1 环境管理

8.4.5.1.1 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。

8.4.5.1.2 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。

8.4.5.1.3 办公环境的保密性措施

应加强对办公环境的保密性管理，规范办公环境人员行为，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。

8.4.5.1.4 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做出规定。

增强要求为：开发、测试和运行设施应分离，以减少未授权访问或改变运行系统的风险。

8.4.5.1.5 机房进出登记表

应具有机房进出登记表。

8.4.5.2 介质管理

8.4.5.2.1 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，并实行存储环境专人管理。

8.4.5.2.2 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、维护和销毁等方面做出规定。

8.4.5.2.3 维修或销毁介质之前清除敏感数据

应对送出维修以及销毁等进行严格的管理，对送出维修或销毁的介质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。

8.4.5.2.4 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。

8.4.5.2.5 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。

8.4.5.3 设备管理

8.4.5.3.1 设备管理的责任人员或部门

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。

8.4.5.3.2 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管理。

8.4.5.3.3 设备选型、采购、发放等的审批控制

应建立基于申报、审批和专人负责的设备安全管理制度，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。

8.4.5.3.4 设备配置标准化

应建立标准化的设备配置文档。

8.4.5.3.5 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，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。

8.4.5.3.6 设备的操作日志

应具有完整的设备操作日志。

8.4.5.3.7 设备使用管理文档

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，建立相应的管理文档。

8.4.5.3.8 设备标识

应对设备进行分类和标识。

8.4.5.4 人员管理

8.4.5.4.1 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。

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

8.4.5.4.2 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。
应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。
应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。

8.4.5.4.3 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。

8.4.5.4.4 安全意识教育和培训

应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训。
应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反安全策略和规定的人员进行惩戒。
应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训。
应对安全教育和培训的情况和结果进行记录并归档保存。

8.4.5.4.5 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。

8.4.5.4.6 职责分离

关键岗位人员应职责分离。

8.4.5.5 监控管理

8.4.5.5.1 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、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。

8.4.5.5.2 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。

8.4.5.5.3 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。

8.4.5.5.4 异常处理机制

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。

8.4.5.5.5 资源监控

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

8.4.5.6 变更管理

8.4.5.6.1 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须经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。

8.4.5.6.2 变更方案

应确认系统中要发生的变更，并制定变更方案，变更内容中应有变更失败后的回退方案等。

8.4.5.6.3 重要系统变更的通知

重要系统变更前，应通知相关单位、部门和人员。

8.4.5.6.4 重要系统变更的实施

应记录变更实施过程，并妥善保存所有文档和记录。

8.4.5.7 安全事件处置

8.4.5.7.1 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。

8.4.5.7.2 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。

8.4.5.7.3 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，过程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。

8.4.5.8 应急预案管理

8.4.5.8.1 制定不同事件的应急预案

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。

8.4.5.8.2 相关人员应急预案培训

应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。

8.4.5.8.3 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。对应急预案演练中暴露出的问题进行总结并及时整改。

8.4.6 业务连续性要求

8.4.6.1 业务连续性需求分析

8.4.6.1.1 业务中断影响分析

应进行业务中断影响分析。

8.4.6.1.2 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。

8.4.6.2 业务连续性技术环境

8.4.6.2.1 备份机房

应具备同城应用级备份。

8.4.6.2.2 网络双链路

应具备双链路。

8.4.6.2.3 网络设备和服务器备份

应具备同城应用级备份设施。

8.4.6.2.4 高可靠的磁盘阵列

应使用高可靠的磁盘阵列。

8.4.6.2.5 远程数据库备份

应具备远程备份数据库。

8.4.6.3 业务连续性管理

8.4.6.3.1 业务连续性管理制度

应具备业务连续性管理制度。

8.4.6.3.2 应急响应流程

应具备应急响应流程。

8.4.6.3.3 恢复预案

应具备不同场景恢复预案，同时具备应用级恢复预案。

8.4.6.3.4 数据备份和恢复制度

应具备数据备份和恢复管理制度。

8.4.6.4 备份和恢复管理

8.4.6.4.1 备份数据范围和备份频率

应具备备份数据范围和备份频率清单。

8.4.6.4.2 备份和恢复手册

应具备数据备份和恢复手册。

8.4.6.4.3 备份记录和定期恢复测试记录

应具备备份记录和定期恢复测试记录。

8.4.6.4.4 定期数据备份恢复性测试

应进行定期数据备份恢复性测试。

8.4.6.5 日常维护

8.4.6.5.1 每年业务连续性演练

应每年进行业务连续性演练，包括主备机房的切换演练，演练需提供记录。

8.4.6.5.2 定期业务连续性培训

应定期进行业务连续性培训并具有培训记录。

8.5 文档要求

8.5.1 用户文档

8.5.1.1 用户手册

用户手册应描述手工操作该软件的用户应如何安装和使用一个软件系统。它还包括软件操作的一些特别的方面，诸如，关于特定岗位或任务的指令等。用户手册是为由用户操作的软件而开发的，具有要求联机用户输入或解释输出显示的用户界面。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

8.5.1.2 操作手册

操作手册应提供操作指定的设备所需的信息。本手册侧重设备自身，而不是运行在其上的特定的软件。操作手册主要针对一些新开发的设备、专用设备、无现成的商用操作手册或其他操作手册可用的其他的设备。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

8.5.2 开发文档

8.5.2.1 需求说明书

需求说明书应从以下几方面描述一个建议的系统：说明它能满足用户什么需要，它与现有系统或过程的关系，以及它的使用方式等。需求说明书旨在需方、开发方、支持方和用户代理之间对所建议的系

统的运行机理取得共识。取决于使用的目的，需求说明书可专注于向开发者表述用户的需求，或专注于向用户或其他感兴趣的对象表达开发者的思路。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

8.5.2.2 需求分析文档

需求分析文档应描述对计算机软件系统的需求，及确保每个需求得以满足所使用的方法。需求分析文档应涉及该系统外部接口的需求。

宜符合GB/T 8567和GB/T 9385要求。

增强要求为：应符合GB/T 8567和GB/T 9385要求。

8.5.2.3 总体设计方案

总体设计方案应描述系统或子系统的系统级或子系统级设计与体系结构设计。总体设计方案还要用《概要设计文档》和《数据库设计文档》加以补充。总体设计方案连同相关的概要和数据库设计文档是构成进一步系统实现的基础。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

8.5.2.4 数据库设计文档

数据库设计文档应描述数据库的设计。数据库可由用户或计算机程序通过数据库管理系统加以访问。数据库设计文档还描述了存取或操纵数据所使用的软件配置项。数据库设计文档是实现数据库及相关软件配置项的基础。它向需方提供了设计的可视性，为软件支持提供了所需要的信息。数据库设计文档是否单独成册或与详细设计文档合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

8.5.2.5 概要设计文档

概要设计文档应描述计算机软件系统的设计。它描述了系统级设计决策、系统体系结构设计，概要设计和数据库设计是否单独成册抑或与详细设计合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

8.5.2.6 详细设计文档

详细设计文档应描述计算机软件系统的设计。它描述了子系统级设计决策、系统体系结构设计和实现该软件所需的详细设计。概要设计和数据库设计是否单独成册抑或与详细设计合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

8.5.2.7 工程实施方案

工程实施方案应描述开发者实施软件开发工作的计划，包括新开发、修改、重用、再工程、维护和由软件产品引起的其他所有的活动。工程实施方案是向需求方提供了解和监督软件开发过程、所使用的方法、每项活动的途径、项目的安排、组织及资源的一种手段。

8.5.3 管理文档

8.5.3.1 测试报告

测试报告应是对计算机软件、软件系统或子系统，或与软件相关项目执行合格性测试的记录。通过测试报告，需方能够评估所执行的合格性测试及其测试结果。

宜符合GB/T 8567和GB/T 9386要求。

增强要求为：应符合GB/T 8567和GB/T 9386要求。

8.5.3.2 系统运维手册

系统运维手册应是对系统运维管理中用到的环境、资产、介质、设备等进行维护、升级、漏洞扫描等操作的详细描述。

8.5.3.3 系统应急手册

应根据不同的事件，制定应急预案，形成系统应急手册。

8.5.3.4 运维管理制度

运维管理制度应包含但不限于机房管理制度、介质管理制度、设备管理制度、人员管理制度、监控巡检管理制度、变更管理制度、安全事件处理制度等。

8.5.3.5 安全管理制度

安全管理制度应是对负责安全管理机构的设置与人员等资源的配备描述，以及保证其正常实施安全管理工作的管理制度。

8.5.3.6 安全审计报告

应由专业审计人员根据有关的法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并做出相应评价报告。

9 固定电话支付技术要求

9.1 功能要求

9.1.1 客户管理

9.1.1.1 客户信息登记及管理

应实现客户注册、客户信息的编辑等功能。

9.1.1.2 终端设备关联

应实现将客户支付账户与电话设备（如电话号码）相关联的功能，应实现固定电话支付开通确认的功能。

9.1.1.3 电话语音密码

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

9.1.1.4 商业银行管理

应实现商业银行的接入、信息修改和删除等功能。

9.1.1.5 客户证书管理

应实现电子证书的申请、发放、更新、作废等服务。

9.1.1.6 客户审核

应实现客户注册信息的审核、确认开通等功能。

9.1.2 账户管理

9.1.2.1 客户支付账户管理

应实现客户支付账户的开户、修改、状态设置等功能。
增强要求为：应实现客户支付账户的开户、修改、冻结/解冻、销户等功能。

9.1.2.2 客户支付账户管理审核

应实现客户支付账户信息的审核、确认等服务。

9.1.2.3 银行卡关联

应实现将客户支付账户与银行卡相关联的功能。

9.1.2.4 客户支付账户查询

应实现客户支付账户设置、交易等信息的查询功能。

9.1.2.5 客户支付账户资金审核

应实现当客户支付账户资金转移、交易、结算时，进行资金的审核和确认等。

9.1.3 语音 IVR 管理

9.1.3.1 IVR 登录

应实现IVR防穷举功能，可以采取会话结束、限制非法登录次数和登录连接超时自动退出等措施。

9.1.3.2 按键输入

应实现使用语音IVR将按键输入转换为相应的指令。

9.1.3.3 电话回拨

应实现使用语音IVR回拨到指定的电话终端。

9.1.3.4 用户信息保护

应实现固定电话支付用户的鉴别信息所在的存储空间在通话结束后应立即完全清除，并保证这些信息不存放在永久化设备中。

9.1.4 交易处理

9.1.4.1 一般支付

应实现客户一般支付交易。

9.1.4.2 担保支付

应实现客户担保支付交易。

9.1.4.3 协议支付

应实现客户协议支付交易。

9.1.4.4 订单撤销

应实现客户撤销订单功能；如果支付已经完成，则拒绝响应撤销订单请求。

9.1.4.5 转账

应实现不同客户支付账户之间相互转账。

9.1.4.6 充值

应实现客户支付账户的充值或预存现金。

9.1.4.7 提现

应实现从客户支付账户转账到银行账户服务。

9.1.4.8 积分查询

应实现客户积分信息的查询功能。

9.1.4.9 积分兑换

应实现客户积分兑换服务。

9.1.4.10 积分兑换撤销

应实现撤销客户积分兑换，且撤销后积分退还客户服务。

9.1.4.11 交易纠纷处理

应实现客户交易的投诉、处理、确认、撤销等。

9.1.4.12 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。

9.1.4.13 交易明细下载

应实现交易明细信息下载。

9.1.4.14 邀请其他人代付

应实现邀请他人进行支付。

9.1.5 资金结算

应实现支付服务方与客户之间的资金结算。

9.1.6 对账处理

9.1.6.1 商户发送对账请求

应实现商户提交对账申请，支付服务方提供对账信息的服务。

9.1.6.2 商户下载对账文件

应实现商户对账文件的查询、浏览和下载等。

9.1.7 差错处理

9.1.7.1 长款/短款处理

应实现对长款/短款资金的记录、调账等服务。

9.1.7.2 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、退款等服务。

支付服务方将部分或全部已扣款项退还给客户（个人或企业买方）的原扣款账户，原扣款账户不能接收退款的，退款到付款人其他账户。

9.1.7.3 批量退款

应实现对已发生的多笔交易同时进行退款申请、确认、审核、退款等服务。

支付服务方将部分或全部已扣款项退还给客户（个人或企业买方）的原扣款账户，原扣款账户不能接收退款的，退款到付款人其他账户。

9.1.8 统计报表

9.1.8.1 业务类报表

应实现对一段时间内业务操作（客户注册、商户开通、支付、结算、转账、提现等操作）的查询统计。

9.1.8.2 运行管理类报表

应实现对一段时间内运行管理情况（资产、监控、安全事件等）的查询统计，第三方支付公司可以根据自身的情况将“一段时间”细化为“月季年”。

9.1.9 运营管理

9.1.9.1 运营人员权限管理

应实现对此类人员权限的增加、删除、修改或审核等。

9.1.9.2 提现风控处理

应实现对提现操作进行风险处理，如采用提现风险识别、提现审核确认等措施。

9.1.9.3 提现财务处理

应实现对提交的提现申请进行财务处理。

9.1.9.4 退款风控处理

应实现对退款操作进行风险处理，如采用退款风险识别、退款审核确认等措施。

9.1.9.5 退款财务处理

应实现对退款申请进行财务处理。

9.2 风险监控要求

9.2.1 账户风险管理

宜对客户进行实名认证。

增强要求为：应对客户身份进行实名认证。

9.2.2 交易监控

9.2.2.1 监控规则管理

应确保在相关风险管理制度中完整、明确地定义各类（如实时、异常等）交易监控规则。

9.2.2.2 当日交易查询

应实现当日交易信息的查询功能。

9.2.2.3 历史交易查询

应实现历史交易信息的查询功能。

9.2.2.4 实时交易监控

应实现交易监控规则的设置，以实现对实时交易的监控，并对违反规则的交易提供查询、处理、风险控制等服务。

增强要求为：建立账户与交易监控系统，对支付交易全过程实施7*24小时监控。

9.2.2.5 可疑交易处理

应实现可疑交易处理规则的设置，以实现对可疑交易的查询、分析处理等服务。

9.2.2.6 交易事件报警

应实现对违反规则的交易事件进行报警，并提供事件的查询统计。

9.2.3 交易审核

9.2.3.1 系统自动审核

应实现交易审核规则的设置，系统根据交易规则自动进行交易审核，并提供交易审核记录。

9.2.3.2 人工审核

应确保在相关管理制度中完整、明确地定义需要人工审核的交易类型，实现人工审核规则的设置，并保存人工审核的记录。

9.2.4 风控规则

9.2.4.1 风控规则管理

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

9.2.4.2 黑名单

应实现黑名单的管理功能，并对黑名单中客户的交易进行风险监控。

9.2.4.3 风险识别

应确保在相关风险管理制度中完整、明确地定义各种风险类别。

9.2.4.4 事件管理

应确保在相关风险管理制度中完整、明确地定义各项风险事件处理规则，并保留事件的记录。

9.2.4.5 风险报表

应提供一段时间内的风险事件报表。

9.3 性能要求

支付业务设施性能基本要求见表4。

表4 固定电话支付性能检测基本要求列表

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	比对性能需求表高峰时段并发数	<=80%	100%	>=99%	>=30分钟

9.4 安全性要求

9.4.1 网络安全性要求

9.4.1.1 结构安全

9.4.1.1.1 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。

增强要求为：应保证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。

9.4.1.1.2 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。

9.4.1.1.3 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。

9.4.1.1.4 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。

9.4.1.1.5 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，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

9.4.1.1.6 QoS保证

宜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。

增强要求为：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。

9.4.1.2 网络访问控制

9.4.1.2.1 网络域安全隔离和限制

应在网络边界部署访问控制设备，启用访问控制功能。

9.4.1.2.2 地址转换和绑定

重要网段应采取技术手段防止地址欺骗。

9.4.1.2.3 内容过滤

应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP等协议命令级的控制。

9.4.1.2.4 访问控制

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。

应按用户和系统之间的访问控制规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。

9.4.1.2.5 流量控制

应限制网络最大流量数及网络连接数。

9.4.1.2.6 会话控制

应在会话处于非活跃一定时间或会话结束后终止网络连接。

9.4.1.2.7 远程拨号访问控制和记录

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。

9.4.1.3 网络安全审计

9.4.1.3.1 日志信息

应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。

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。

9.4.1.3.2 网络系统故障分析

应对网络系统故障进行分析，查找原因并形成故障知识库。

9.4.1.3.3 网络对象操作审计

应能够根据记录数据进行分析，并生成审计报表。

9.4.1.3.4 日志权限和保护

应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

9.4.1.3.5 审计工具

应具备日志审计工具，对日志进行记录、分析和报告。

增强要求为：应定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，当存储空间被耗尽时，终止可审计事件的发生；

应根据信息系统的统一安全策略，实现集中审计，时钟宜采用多模方式授时。并应专人负责时间服务器，防止被恶意篡改。

9.4.1.4 边界完整性检查

应能够对非授权设备私自连接到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

应能够对内部网络用户私自连接到外部网络的行为进行检查,准确定出位置,并对其进行有效阻断。

增强要求为：对非法外联和非法接入行为进行检测并阻断的同时，应通过报警方式通知管理员。

9.4.1.5 网络入侵防范

9.4.1.5.1 网络 ARP 欺骗攻击

应能够有效的防范网络ARP欺骗攻击。

9.4.1.5.2 信息窃取

应采用防范信息窃取的措施。

9.4.1.5.3 DoS/DDoS 攻击

应具有防DoS/DDoS攻击设备或技术手段。

9.4.1.5.4 网络入侵防范机制

应在网络边界处监视以下攻击行为：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提供报警。

增强要求为：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，应记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警及自动采取相应动作。

9.4.1.6 恶意代码防范

9.4.1.6.1 恶意代码防范措施

应在网络边界处对恶意代码进行检测和清除。

9.4.1.6.2 定时更新

应维护恶意代码库的升级和检测系统的更新。

9.4.1.7 网络设备防护

9.4.1.7.1 设备登录设置

应对登录网络设备的用户进行身份鉴别。

网络设备用户的标识应唯一。

主要网络设备宜对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。

增强要求为：主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别，网络设备用户的身份鉴别信息至少应有一种是不可伪造的。

9.4.1.7.2 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。

9.4.1.7.3 登录地址限制

应对网络设备的管理员登录地址进行限制。

9.4.1.7.4 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。

9.4.1.7.5 设备用户设置策略

应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

9.4.1.7.6 权限分离

应实现设备特权用户的权限分离。

9.4.1.7.7 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。

9.4.1.8 网络安全管理

9.4.1.8.1 网络设备运维手册

应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面做出规定。

应保证所有与外部系统的连接均得到授权和批准。

应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

9.4.1.8.2 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。

9.4.1.8.3 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进行及时的修补。

9.4.1.8.4 网络数据传输加密

当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

9.4.1.9 网络相关人员安全管理

9.4.1.9.1 网络安全管理人员配备

应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作。

9.4.1.9.2 网络安全管理人员责任划分规则

应制定文件明确网络安全管理岗位的职责、分工和技能要求。

9.4.1.9.3 网络安全关键岗位人员管理

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

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。

9.4.2 主机安全性要求

9.4.2.1 身份鉴别

9.4.2.1.1 系统与应用管理员用户设置

应对登录操作系统和数据库系统的用户进行身份标识和鉴别。

应为操作系统和数据库系统的不同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。

增强要求为：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， 并且身份鉴别信息至少有一种是不可伪造的。

9.4.2.1.2 系统与应用管理员口令安全性

操作系统和数据库系统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。

9.4.2.1.3 登录策略

应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

9.4.2.2 访问控制

9.4.2.2.1 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。

应实现操作系统和数据库系统特权用户的权限分离。

增强要求为：在系统对用户进行身份鉴别时，系统与用户之间应能够建立一条安全的信息传输路径；

在用户对系统进行访问时，系统与用户之间应能够建立一条安全的信息传输路径。

9.4.2.2.2 主机信任关系

应避免不必要的主机信任关系。

9.4.2.2.3 默认过期用户

应及时删除多余的、过期的用户，避免共享用户的存在。

应严格限制默认用户的访问权限，重命名系统默认用户，修改这些用户的默认口令。

9.4.2.3 安全审计

9.4.2.3.1 日志信息

审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。

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。

增强要求为：应能够根据信息系统的统一安全策略，实现集中审计。

9.4.2.3.2 日志权限和保护

应保护审计记录，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。

增强要求为：应保护审计进程，避免受到未预期的中断。

9.4.2.3.3 系统信息分析

应能够根据记录数据进行分析，并生成审计报表。

9.4.2.4 系统保护

9.4.2.4.1 系统备份

应具有系统备份或系统重要文件备份。

9.4.2.4.2 故障恢复策略

应具备各种主机故障恢复策略。

9.4.2.4.3 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。

9.4.2.4.4 主机安全加固

应对主机进行安全加固。

9.4.2.5 剩余信息保护

应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。

应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

9.4.2.6 入侵防范

9.4.2.6.1 入侵防范记录

宜能够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、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

宜能够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具有恢复的措施。

增强要求为：应能够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、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

应能够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具有恢复的措施。

9.4.2.6.2 关闭服务和端口

应关闭系统不必要的服务和端口。

9.4.2.6.3 最小安装原则

操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

9.4.2.7 恶意代码防范

9.4.2.7.1 防范软件安装部署

应至少在生产系统中的服务器安装防恶意代码软件。

9.4.2.7.2 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。

9.4.2.7.3 防范软件统一管理

应支持防范软件的统一管理。

9.4.2.8 资源控制

9.4.2.8.1 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。

应根据安全策略设置登录终端的操作超时锁定。

9.4.2.8.2 资源监控和预警

应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。

应限制单个用户对系统资源的最大或最小使用限度。

应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

9.4.2.9 主机安全管理

9.4.2.9.1 主机运维手册

应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面做出具体规定。

9.4.2.9.2 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。

9.4.2.9.3 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，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。

9.4.2.9.4 操作日志管理

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，严禁进行未经授权的操作。

应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

9.4.2.10 主机相关人员安全管理

9.4.2.10.1 主机安全管理人员配备

应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则。

9.4.2.10.2 主机安全管理人员责任划分规则

应制定文件明确主机管理岗位的职责、分工和技能要求。

9.4.2.10.3 主机安全关键岗位人员管理

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

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。

9.4.3 应用安全性要求

9.4.3.1 身份鉴别

9.4.3.1.1 系统与普通用户设置

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，提供系统管理员和普通用户的设置功能。

9.4.3.1.2 系统与普通用户口令安全性

系统与普通用户口令应具有一定的复杂度。

9.4.3.1.3 登录访问安全策略

宜对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

增强要求为：应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别，其中一种是不可伪造的。

9.4.3.1.4 非法访问警示和记录

应提供终端登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

9.4.3.1.5 客户端鉴别信息安全

客户端鉴别信息应不被窃取和冒用。

9.4.3.1.6 口令有效期限制

应限制口令的有效期限。

9.4.3.1.7 限制认证会话时间

应对客户端认证会话时间进行限制。

9.4.3.1.8 身份标识唯一性

应提供用户身份标识唯一性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身份标识，身份鉴别信息不易被冒用。

应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

9.4.3.1.9 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。

9.4.3.2 WEB 页面安全

9.4.3.2.1 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。

9.4.3.2.2 安全控件

登录应使用安全控件，且能有效防止重放攻击。

如系统为内部使用，不对互联网用户提供服务，该项不适用。

9.4.3.2.3 使用数字证书

应使用服务器证书。

如系统为内部使用，不对互联网用户提供服务，该项不适用。

9.4.3.2.4 独立的支付密码

应提供独立的支付密码和健全的密码找回机制。

如系统为内部使用，不对互联网用户提供服务，该项不适用。

9.4.3.2.5 网站页面注入防范

网站页面应采取防范SQL注入、Path注入和LDAP注入等风险的措施。

9.4.3.2.6 网站页面跨站脚本攻击防范

网站页面应采取防范跨站脚本攻击风险的措施。

9.4.3.2.7 网站页面源代码暴露防范

网站页面应采取防范源代码暴露的措施。

9.4.3.2.8 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。

9.4.3.2.9 网站页面防篡改措施

网站页面应采用页面防篡改措施。
如系统为内部使用，不对互联网用户提供服务，该项不适用。

9.4.3.2.10 网站页面防钓鱼

网站页面应提供防钓鱼网站的防伪信息验证。
如系统为内部使用，不对互联网用户提供服务，该项不适用。

9.4.3.3 访问控制

9.4.3.3.1 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。
应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成互相制约的关系。

9.4.3.3.2 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、客体及它们之间的操作。

9.4.3.3.3 业务操作日志

应具有所有业务操作日志。

9.4.3.3.4 关键数据操作控制

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

9.4.3.3.5 异常中断防护

用户访问异常中断后，应具有防护手段，保证数据不丢失。

9.4.3.3.6 数据库安全配置

应具有数据库安全配置手册，并对数据库进行安全配置。

9.4.3.4 安全审计

9.4.3.4.1 日志信息

审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

9.4.3.4.2 日志权限和保护

应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录。

9.4.3.4.3 系统信息查询与分析

应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

9.4.3.4.4 对象操作审计

应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。

9.4.3.4.5 审计工具

应具备日志审计工具，对日志进行记录、分析和报告。

增强要求为：应根据系统统一安全策略，提供集中审计接口。

9.4.3.4.6 事件报警

应具有交易事件报警功能。

9.4.3.5 剩余信息保护

应对无用的过期信息、文档进行完整删除。

增强要求为：应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

9.4.3.6 资源控制

9.4.3.6.1 连接控制

应能够根据业务需求，对系统的最大并发会话连接数进行限制。

应能够对一个时间段内可能的并发会话连接数进行限制。

9.4.3.6.2 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。

应能够对单个帐户的多重并发会话进行限制。

9.4.3.6.3 进程资源分配

应能够对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额。

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。

9.4.3.6.4 资源监测预警

应能够对系统服务水平降低到预先规定的最小值进行检查和报警。

9.4.3.7 应用容错

9.4.3.7.1 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或长度符合系统设定要求。

9.4.3.7.2 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。

增强要求为：应提供自动恢复功能，当故障发生时立即自动启动新的进程，恢复原来的工作状态。

9.4.3.7.3 故障机制

发生故障后，系统应能够及时恢复。

9.4.3.7.4 回退机制

应提供回退功能，当故障发生后，能够及时回退到故障发生前的状态。

9.4.3.8 报文完整性

通信报文应采用密码技术保证通讯过程中交易数据的完整性。

9.4.3.9 报文保密性

在通讯时采用安全通道或对报文中敏感信息进行加密。

9.4.3.10 抗抵赖

9.4.3.10.1 原发和接收证据

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。

9.4.3.10.2 可信时间戳服务

增强要求为：本地时间应从国家权威时间源采时，保证时间的同一性；
应采用国家认可的可信时间戳服务；
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。

9.4.3.11 编码安全

9.4.3.11.1 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。
增强要求为：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。

9.4.3.11.2 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。

9.4.3.11.3 编码规范约束

应按照编码规范进行编码，具有编码规范约束制度。

9.4.3.11.4 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。

9.4.3.11.5 版本管理

应具有代码版本管理制度。

9.4.3.12 电子认证应用

9.4.3.12.1 第三方电子认证机构证书

在对外业务（非内部业务）处理过程中，应使用经过认证的第三方电子认证证书。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，可以使用自建证书（非第三方电子认证证书）。在条件允许的情况下，建议对所有业务使用经过认证的第三方电子认证证书。

9.4.3.12.2 关键业务电子认证技术应用

关键业务应使用电子认证技术。在条件允许的情况下，建议在所有业务均使用经过认证的第三方电子认证技术。

9.4.3.12.3 电子签名有效性

应使用有效的电子签名。在对外业务（非内部业务）处理过程中，应使用经过第三方认证的电子签名体系。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，可以使用自建的电子签名体系（非第三方认证的电子签名体系）。在条件允许的情况下，建议对所有业务使用经过认证的第三方电子签名体系。

9.4.3.12.4 服务器证书私钥保护

应对所持有的服务器证书私钥进行有效保护。

9.4.4 数据安全性要求

9.4.4.1 数据保护

9.4.4.1.1 客户身份信息保护

应当按规定妥善保管客户身份基本信息，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。

9.4.4.1.2 支付业务信息保护

应当按规定妥善保管支付业务信息，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。

9.4.4.1.3 会计档案信息保护

应当按规定妥善保管会计档案，支付机构对会计档案的保管期限适用《会计档案管理办法》（财会字〔1998〕32号文印发）相关规定。

9.4.4.2 数据完整性

9.4.4.2.1 重要数据更改机制

应制定重要数据更改流程和管理制度。

9.4.4.2.2 终端设备关联保护

应采取措施保护电话终端设备和银行卡或客户支付账户的关联关系，防止未授权地修改此种关联关系。

9.4.4.2.3 数据备份记录

应具备数据备份记录。

9.4.4.2.4 保障传输过程中的数据完整性

应能够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。

9.4.4.2.5 备份数据定期恢复

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。

9.4.4.3 交易数据以及客户数据的安全性

9.4.4.3.1 数据物理存储安全

应具备高可用性的数据物理存储环境。

9.4.4.3.2 客户身份认证信息存储安全

应不允许保存非必须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、卡片有效期、个人标识码、银行卡交易密码、指纹、CVN、CVN2等敏感信息）。

应对客户的其他敏感信息，如卡号、户名、开户手机、贷记卡有效期、电子邮箱等信息采取保护措施，防止未经授权擅自对个人信息进行查看、篡改、泄露和破坏。宜采用加密存储、部分屏蔽显示等技术。

9.4.4.3.3 同一安全级别和可信赖的系统之间信息传输

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。

9.4.4.3.4 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。

9.4.4.3.5 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。

9.4.4.3.6 数据访问控制

应具备重要数据的访问控制措施。

9.4.4.3.7 在线的存储备份

应具备实时在线的存储备份设施。

9.4.4.3.8 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，应指明备份数据的备份方式（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。

9.4.4.3.9 本地备份

应提供本地数据备份。

9.4.4.3.10 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。

9.4.4.3.11 备份数据的恢复

应具有备份数据恢复操作手册，并提供恢复功能。

9.4.4.3.12 数据销毁制度和记录

应具有数据销毁制度和相关记录。

9.4.4.3.13 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。

9.4.5 运维安全性要求

9.4.5.1 环境管理

9.4.5.1.1 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。

9.4.5.1.2 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。

9.4.5.1.3 办公环境的保密性措施

应加强对办公环境的保密性管理，规范办公环境人员行为，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档文件等。

9.4.5.1.4 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做出规定。

增强要求为：开发、测试和运行设施应分离，以减少未授权访问或改变运行系统的风险。

9.4.5.1.5 机房进出登记表

应具有机房进出登记表。

9.4.5.2 介质管理

9.4.5.2.1 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，并实行存储环境专人管理。

9.4.5.2.2 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、维护和销毁等方面做出规定。

9.4.5.2.3 维修或销毁介质之前清除敏感数据

应对送出维修以及销毁等进行严格的管理，对送出维修或销毁的介质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。

9.4.5.2.4 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。

9.4.5.2.5 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。

9.4.5.3 设备管理

9.4.5.3.1 设备管理的责任人员或部门

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。

9.4.5.3.2 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管理。

9.4.5.3.3 设备选型、采购、发放等的审批控制

应建立基于申报、审批和专人负责的设备安全管理制度，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。

9.4.5.3.4 设备配置标准化

应建立标准化的设备配置文档。

9.4.5.3.5 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，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。

9.4.5.3.6 设备的操作日志

应具有完整的设备操作日志。

9.4.5.3.7 设备使用管理文档

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。

9.4.5.3.8 设备标识

应对设备进行分类和标识。

9.4.5.4 人员管理

9.4.5.4.1 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；应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

9.4.5.4.2 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。

应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。

9.4.5.4.3 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。

9.4.5.4.4 安全意识教育和培训

应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训。

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。

应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训。

应对安全教育和培训的情况和结果进行记录并归档保存。

9.4.5.4.5 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。

9.4.5.4.6 职责分离

关键岗位人员应职责分离。

9.4.5.5 监控管理

9.4.5.5.1 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、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。

9.4.5.5.2 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。

9.4.5.5.3 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。

9.4.5.5.4 异常处理机制

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。

9.4.5.5.5 资源监控

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

9.4.5.6 变更管理

9.4.5.6.1 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须经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。

9.4.5.6.2 变更方案

应确认系统中要发生的变更，并制定变更方案，变更内容中应有变更失败后的回退方案等。

9.4.5.6.3 重要系统变更的通知

重要系统变更前，应通知相关单位、部门和人员。

9.4.5.6.4 重要系统变更的实施

应记录变更实施过程，并妥善保存所有文档和记录。

9.4.5.7 安全事件处置

9.4.5.7.1 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。

9.4.5.7.2 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。

9.4.5.7.3 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，过程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。

9.4.5.8 应急预案管理

9.4.5.8.1 制定不同事件的应急预案

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。

9.4.5.8.2 相关人员应急预案培训

应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。

9.4.5.8.3 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。对应急预案演练中暴露出的问题进行总结并及时整改。

9.4.6 业务连续性要求

9.4.6.1 业务连续性需求分析

9.4.6.1.1 业务中断影响分析

应进行业务中断影响分析。

9.4.6.1.2 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。

9.4.6.2 业务连续性技术环境

9.4.6.2.1 备份机房

应具备同城应用级备份机房。

9.4.6.2.2 网络双链路

应具备双链路。

9.4.6.2.3 网络设备和服务器备份

应具有同城应用级备份设施。

9.4.6.2.4 高可靠的磁盘阵列

应适用高可靠的磁盘阵列。

9.4.6.2.5 远程数据库备份

应具备远程备份数据库。

9.4.6.3 业务连续性管理

9.4.6.3.1 业务连续性管理制度

应具备业务连续性管理制度。

9.4.6.3.2 应急响应流程

应具备应急响应流程。

9.4.6.3.3 恢复预案

应具备不同场景恢复预案，同时具备应用级恢复预案。

9.4.6.3.4 数据备份和恢复制度

应具备数据备份和恢复管理制度。

9.4.6.4 备份和恢复管理

9.4.6.4.1 备份数据范围和备份频率

应具备备份数据范围和备份频率清单。

9.4.6.4.2 备份和恢复手册

应具备数据备份和恢复手册。

9.4.6.4.3 备份记录和定期恢复测试记录

应具备备份记录和定期恢复测试记录。

9.4.6.4.4 定期数据备份恢复性测试

应进行定期数据备份恢复性测试。

9.4.6.5 日常维护

9.4.6.5.1 每年业务连续性演练

应每年进行业务连续性演练，包括主备机房的切换演练，演练需提供记录。

9.4.6.5.2 定期业务连续性培训

应定期进行业务连续性培训并具有培训记录。

9.5 文档要求

9.5.1 用户文档

9.5.1.1 用户手册

用户手册应描述手工操作该软件的用户应如何安装和使用一个软件系统。它还包括软件操作的一些特别的方面，诸如，关于特定岗位或任务的指令等。用户手册是为由用户操作的软件而开发的，具有要求联机用户输入或解释输出显示的用户界面。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

9.5.1.2 操作手册

操作手册应提供操作指定的设备所需的信息。本手册侧重设备自身，而不是运行在其上的特定的软件。操作手册主要针对一些新开发的设备、专用设备、无现成的商用操作手册或其他操作手册可用的其他的设备。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

9.5.2 开发文档

9.5.2.1 需求说明书

需求说明书应从以下几方面描述一个建议的系统：说明它能满足用户什么需要，它与现有系统或过程的关系，以及它的使用方式等。需求说明书旨在需方、开发方、支持方和用户代理之间对所建议的系统的运行机理取得共识。取决于使用的目的，需求说明书可专注于向开发者表述用户的需求，或专注于向用户或其他感兴趣的对象表达开发者的思路。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

9.5.2.2 需求分析文档

需求分析文档应描述对计算机软件系统的需求，及确保每个需求得以满足所使用的方法。需求分析文档应涉及该系统外部接口的需求。

宜符合GB/T 8567和GB/T 9385要求。

增强要求为：应符合GB/T 8567和GB/T 9385要求。

9.5.2.3 总体设计方案

总体设计方案应描述系统或子系统的系统级或子系统级设计与体系结构设计。总体设计方案还要用《概要设计文档》和《数据库设计文档》加以补充。总体设计方案连同相关的概要和数据库设计文档是构成进一步系统实现的基础。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

9.5.2.4 数据库设计文档

数据库设计文档应描述数据库的设计。数据库可由用户或计算机程序通过数据库管理系统加以访问。数据库设计文档还描述了存取或操纵数据所使用的软件配置项。数据库设计文档是实现数据库及相关软件配置项的基础。它向需方提供了设计的可视性，为软件支持提供了所需要的信息。数据库设计文档是否单独成册或与详细设计文档合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

9.5.2.5 概要设计文档

概要设计文档应描述计算机软件系统的设计。它描述了系统级设计决策、系统体系结构设计，概要设计和数据库设计是否单独成册抑或与详细设计合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

9.5.2.6 详细设计文档

详细设计文档应描述计算机软件系统的设计。它描述了子系统级设计决策、系统体系结构设计和实现该软件所需的详细设计。概要设计和数据库设计是否单独成册抑或与详细设计合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

9.5.2.7 工程实施方案

工程实施方案应描述开发者实施软件开发工作的计划，包括新开发、修改、重用、再工程、维护和由软件产品引起的其他所有的活动。工程实施方案是向需求方提供了解和监督软件开发过程、所使用的方法、每项活动的途径、项目的安排、组织及资源的一种手段。

9.5.3 管理文档

9.5.3.1 测试报告

测试报告应是对计算机软件、软件系统或子系统，或与软件相关项目执行合格性测试的记录。通过测试报告，需方能够评估所执行的合格性测试及其测试结果。

宜符合GB/T 8567和GB/T 9386要求。

增强要求为：应符合GB/T 8567和GB/T 9386要求。

9.5.3.2 系统运维手册

系统运维手册应是对系统运维管理中用到的环境、资产、介质、设备等进行维护、升级、漏洞扫描等操作的详细描述。

9.5.3.3 系统应急手册

应根据不同的事件，制定应急预案，形成系统应急手册。

9.5.3.4 运维管理制度

运维管理制度应包含但不限于机房管理制度、介质管理制度、设备管理制度、人员管理制度、监控巡检管理制度、变更管理制度、安全事件处理制度等。

9.5.3.5 安全管理制度

安全管理制度应是对负责安全管理机构的设置与人员等资源的配备描述，以及保证其正常实施安全管理工作的管理制度。

9.5.3.6 安全审计报告

应由专业审计人员根据有关的法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并做出相应评价报告。

10 数字电视支付技术要求

10.1 功能要求

10.1.1 客户管理

10.1.1.1 客户信息登记及管理

应实现客户注册、客户信息的编辑等功能。

10.1.1.2 商业银行管理

应实现商业银行的接入、信息修改和删除等功能。

10.1.1.3 客户证书管理

应实现电子证书的申请、发放、更新、作废等服务。

10.1.1.4 客户审核

应实现客户注册信息的审核、确认开通等功能。

10.1.2 账户管理

10.1.2.1 客户支付账户管理

应实现客户对其支付账户信息的创建、修改、状态设置等功能。
增强要求为：应实现客户账户的开户、修改、冻结/解冻、销户等功能。

10.1.2.2 客户支付账户管理审核

应实现客户支付账户信息的审核、确认等服务。

10.1.2.3 客户支付账户查询

应实现客户支付账户设置、交易等信息的查询功能。

10.1.2.4 客户支付账户资金审核

应实现当客户支付账户资金转移、交易、结算时，进行资金的审核和确认等。

10.1.3 交易处理

10.1.3.1 消费

应实现通过数字电视支付应用客户端进行电视购物、电视商务和视频服务等支付的交易。

10.1.3.2 消费撤销

应实现消费撤销功能。

10.1.3.3 转账

应实现两个客户支付账户之间资金划转的过程。

10.1.3.4 充值

应实现客户对其支付账户的充值或预存现金。

10.1.3.5 提现

应实现从支付账户转账到银行账户服务。

10.1.3.6 交易纠纷处理

应实现客户交易的投诉、处理、确认、撤销等。

10.1.3.7 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功能。

10.1.3.8 委托交易

应实现委托交易功能。

10.1.3.9 冲正交易

应实现冲正交易功能。

10.1.3.10 退货

应实现退货功能。

10.1.3.11 销账

应实现向行业商户进行扣费销账交易功能。

10.1.3.12 预授权

应实现预授权功能，发卡行将持卡人账户的预授权金额冻结，并给出授权号。

持卡人结账时应将根据持卡人实际的消费金额向发卡行请求资金结算。发卡行对持卡人账户按实际消费的金额进行扣账后，同时将预授权的金额进行解冻。

10.1.3.13 预授权撤销

应实现预授权撤销交易，预授权撤销交易应是对原始预授权交易的全额撤销。

发卡行在收到预授权撤销交易后，将持卡人预授权金额全额解冻。

10.1.3.14 预授权完成

应实现预授权完成功能。

10.1.3.15 预授权完成撤销

应实现预授权完成撤销交易。

发卡行批准的预授权完成撤销金额应即时地反映到该持卡人的账户上。

10.1.3.16 IC卡指定账户圈存

应实现银行卡账户向金融IC卡电子现金帐户进行资金转账的交易。

10.1.3.17 IC卡现金充值

应实现现金对金融IC卡电子现金帐户进行充值的交易。

10.1.3.18 IC卡脱机交易上传

应实现IC卡电子现金脱机交易结算数据批量上送和清算功能。

10.1.3.19 账单费用查询

应实现客户待缴账单费用查询。

10.1.4 资金结算

应实现非金融机构与客户之间的资金结算。

10.1.5 对账处理

10.1.5.1 客户发送对账请求

应实现客户提交对账申请，支付服务方提供对账信息的服务。

10.1.5.2 客户下载对账文件

应实现客户对账文件的查询、浏览和下载等。

10.1.6 差错处理

10.1.6.1 长款/短款处理

应实现对长款/短款资金的记录、调账等服务。

10.1.6.2 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、退款等服务。

支付服务方将部分或全部已扣款项退还给客户（个人或企业买方）的原扣款账户，原扣款账户不能接收退款的，退款到付款人其他账户。

10.1.6.3 批量退款

应实现对已发生的多笔交易同时进行退款申请、确认、审核、退款等服务。

支付服务方将部分或全部已扣款项退还给客户（个人或企业买方）的原扣款账户，原扣款账户不能接收退款的，退款到付款人其他账户。

10.1.7 统计报表

10.1.7.1 业务类报表

应实现对一段时间内业务操作（客户注册、商户开通、支付、结算、转账、提现等操作）的查询统计。

10.1.7.2 运行管理类报表

应实现对一段时间内运行管理情况（资产、监控、安全事件等）的查询统计，第三方支付公司可以根据自身的情况将“一段时间”细化为“月季年”。

10.2 风险监控要求

10.2.1 账户风险管理

增强要求为：应对客户身份进行实名认证。

10.2.2 交易监控

10.2.2.1 监控规则管理

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

10.2.2.2 当日交易查询

应实现当日交易信息的查询功能。

10.2.2.3 历史交易查询

应实现历史交易信息的查询功能。

10.2.2.4 实时交易监控

应实现交易监控规则的设置，以实现对实时交易的监控，并对违反规则的交易提供查询、处理、风险控制等服务。

增强要求为：建立账户与交易监控系统，对支付交易全过程实施7*24小时监控。

10.2.2.5 可疑交易处理

应实现可疑交易处理规则的设置，以实现对可疑交易的查询、分析、处理等服务。

10.2.2.6 交易事件报警

应实现对违反规则的交易事件进行报警，并提供事件的查询统计。

10.2.2.7 支付限额管理

应根据用户使用的不同身份认证方式设置支付限额，以保护用户的资金安全。

10.2.2.8 单笔交易限额

应设置单笔交易限额。

10.2.2.9 当日累计交易限额

应设置当日累计交易限额。

10.2.3 交易审核

10.2.3.1 系统自动审核

应实现交易审核规则的设置，系统根据交易规则自动进行交易审核，并提供交易审核记录。

10.2.3.2 人工审核

应确保在相关管理制度中完整、明确的定义需要人工审核的交易类型，实现人工审核规则的设置，并保存人工审核的记录。

10.2.4 风控规则

10.2.4.1 风控规则管理

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

10.2.4.2 黑名单

应实现黑名单的管理功能，并对黑名单中客户的交易进行风险监控。

10.2.4.3 风险识别

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。

10.2.4.4 事件管理

应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，并保留事件的记录。

10.2.4.5 风险报表

应提供一段时间内的风险事件报表。

10.3 性能要求

支付业务设施性能基本要求见表5。

表5 数字电视支付性能检测基本要求列表

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	比对性能需求表高峰时段并发数	<=80%	100％	>=99%	>=30分钟

10.4 安全性要求

10.4.1 网络安全性要求

10.4.1.1 结构安全

10.4.1.1.1 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。

增强要求为：应保证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。

10.4.1.1.2 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。

10.4.1.1.3 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。

10.4.1.1.4 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。

10.4.1.1.5 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，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

10.4.1.1.6 QoS 保证

宜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。

增强要求为：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。

10.4.1.2 网络访问控制

10.4.1.2.1 网络域安全隔离和限制

应在网络边界部署访问控制设备，启用访问控制功能。

10.4.1.2.2 地址转换和绑定

重要网段应采取技术手段防止地址欺骗。

10.4.1.2.3 内容过滤

应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP等协议命令级的控制。

10.4.1.2.4 访问控制

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。

应按用户和系统之间的访问控制规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。

10.4.1.2.5 流量控制

应限制网络最大流量数及网络连接数。

10.4.1.2.6 会话控制

应在会话处于非活跃一定时间或会话结束后终止网络连接。

10.4.1.2.7 远程拨号访问控制和记录

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。

10.4.1.3 网络安全审计

10.4.1.3.1 日志信息

应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。

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。

10.4.1.3.2 网络系统故障分析

应对网络系统故障进行分析，查找原因并形成故障知识库。

10.4.1.3.3 网络对象操作审计

应能够根据记录数据进行分析，并生成审计报表。

10.4.1.3.4 日志权限和保护

应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

10.4.1.3.5 审计工具

应具备日志审计工具，对日志进行记录、分析和报告。

增强要求为：应定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，当存储空间被耗尽时，终止可审计事件的发生；

应根据信息系统的统一安全策略，实现集中审计，时钟宜采用多模方式授时。并应专人负责时间服务器，防止被恶意篡改。

10.4.1.4 边界完整性检查

应能够对非授权设备私自连接到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

应能够对内部网络用户私自连接到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

增强要求为：对非法外联和非法接入行为进行检测并阻断的同时，应通过报警方式通知管理员。

10.4.1.5 网络入侵防范

10.4.1.5.1 网络 ARP 欺骗攻击

应能够有效的防范网络ARP欺骗攻击。

10.4.1.5.2 信息窃取

应采用防范信息窃取的措施。

10.4.1.5.3 DoS/DDoS 攻击

应具有防DoS/DDoS攻击设备或技术手段。

10.4.1.5.4 网络入侵防范机制

应在网络边界处监视以下攻击行为：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提供报警。

增强要求为：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，应记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警及自动采取相应动作。

10.4.1.6 恶意代码防范

10.4.1.6.1 恶意代码防范措施

应在网络边界处对恶意代码进行检测和清除。

增强要求为：应在系统网络中对恶意代码进行检测和清除。

10.4.1.6.2 定时更新

应维护恶意代码库的升级，检测系统的更新。

10.4.1.7 网络设备防护

10.4.1.7.1 设备登录设置

应对登录网络设备的用户进行身份鉴别。

网络设备用户的标识应唯一。

主要网络设备宜对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。

增强要求为：主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别，网络设备用户的身份鉴别信息至少应有一种是不可伪造的。

10.4.1.7.2 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。

10.4.1.7.3 登录地址限制

应对网络设备的管理员登录地址进行限制。

10.4.1.7.4 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。

10.4.1.7.5 设备用户设置策略

应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

10.4.1.7.6 权限分离

应实现设备特权用户的权限分离。

10.4.1.7.7 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。

10.4.1.8 网络安全管理

10.4.1.8.1 网络设备运维手册

应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面做出规定。

应保证所有与外部系统的连接均得到授权和批准。

应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

10.4.1.8.2 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。

10.4.1.8.3 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进行及时的修补。

10.4.1.8.4 网络数据传输加密

当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

10.4.1.9 网络相关人员安全管理

10.4.1.9.1 网络安全管理人员配备

应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作。

10.4.1.9.2 网络安全管理人员责任划分规则

应制定文件明确网络安全管理岗位的职责、分工和技能要求。

10.4.1.9.3 网络安全关键岗位人员管理

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

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。

10.4.2 主机安全性要求

10.4.2.1 身份鉴别

10.4.2.1.1 系统与应用管理员用户设置

应对登录操作系统和数据库系统的用户进行身份标识和鉴别。

应为操作系统和数据库系统的不同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。

增强要求为：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， 并且身份鉴别信息至少有一种是不可伪造的。

10.4.2.1.2 系统与应用管理员口令安全性

操作系统和数据库系统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。

10.4.2.1.3 登录策略

应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

10.4.2.2 访问控制

10.4.2.2.1 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。

应实现操作系统和数据库系统特权用户的权限分离。

增强要求为：在系统对用户进行身份鉴别时，系统与用户之间应能够建立一条安全的信息传输路径；在用户对系统进行访问时，系统与用户之间应能够建立一条安全的信息传输路径。

10.4.2.2.2 主机信任关系

应避免不必要的主机信任关系。

10.4.2.2.3 默认过期用户

应及时删除多余的、过期的用户，避免共享用户的存在。

应严格限制默认用户的访问权限，重命名系统默认用户，修改这些用户的默认口令。

10.4.2.3 安全审计

10.4.2.3.1 日志信息

审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。

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。

增强要求为：应能够根据信息系统的统一安全策略，实现集中审计。

10.4.2.3.2 日志权限和保护

应保护审计记录，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。

增强要求为：应保护审计进程，避免受到未预期的中断。

10.4.2.3.3 系统信息分析

应能够根据记录数据进行分析，并生成审计报表。

10.4.2.4 系统保护

10.4.2.4.1 系统备份

应具有系统备份或系统重要文件备份。

10.4.2.4.2 故障恢复策略

应具备各种主机故障恢复策略。

10.4.2.4.3 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。

10.4.2.4.4 主机安全加固

应对主机进行安全加固。

10.4.2.5 剩余信息保护

应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。

应确保系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

10.4.2.6 入侵防范

10.4.2.6.1 入侵防范记录

宜能够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、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

宜能够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具有恢复的措施。

增强要求为：应能够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、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

应能够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具有恢复的措施。

10.4.2.6.2 关闭服务和端口

应关闭系统不必要的服务和端口。

10.4.2.6.3 最小安装原则

操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

10.4.2.7 恶意代码防范

10.4.2.7.1 防范软件安装部署

应至少在生产系统中的服务器安装防恶意代码软件。

10.4.2.7.2 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。

10.4.2.7.3 防范软件统一管理

应支持防范软件的统一管理。

10.4.2.8 资源控制

10.4.2.8.1 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。

应根据安全策略设置登录终端的操作超时锁定。

10.4.2.8.2 资源监控和预警

应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。

应限制单个用户对系统资源的最大或最小使用限度。

应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

10.4.2.9 主机安全管理

10.4.2.9.1 主机运维手册

应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面做出具体规定。

10.4.2.9.2 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。

10.4.2.9.3 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，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。

10.4.2.9.4 操作日志管理

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，严禁进行未经授权的操作。

应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

10.4.2.10 主机相关人员安全管理

10.4.2.10.1 主机安全管理人员配备

应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则。

10.4.2.10.2 主机安全管理人员责任划分规则

应制定文件明确主机管理岗位的职责、分工和技能要求。

10.4.2.10.3 主机安全关键岗位人员管理

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

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。

10.4.3 应用安全性要求

10.4.3.1 身份鉴别

10.4.3.1.1 系统与普通用户设置

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，提供系统管理员和普通用户的设置功能。

10.4.3.1.2 系统与普通用户口令安全性

系统与普通用户口令应具有一定的复杂度。

10.4.3.1.3 登录访问安全策略

应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

增强要求为：应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别，其中一种是不可伪造的。

10.4.3.1.4 非法访问警示和记录

应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

10.4.3.1.5 客户端鉴别信息安全

客户端鉴别信息应不被窃取和冒用。

10.4.3.1.6 口令有效期限制

应提示客户定期修改口令。

应限制系统管理用户的口令有效期。

10.4.3.1.7 限制认证会话时间

应对客户端认证会话时间进行限制。

10.4.3.1.8 身份标识唯一性

应提供用户身份标识唯一性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身份标识，身份鉴别信息不易被冒用。

应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

10.4.3.1.9 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。

10.4.3.2 WEB 页面安全

10.4.3.2.1 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。

10.4.3.2.2 安全控件

登录应使用安全控件。

如系统为内部使用，不对互联网用户提供服务，该项不适用。

10.4.3.2.3 使用数字证书

WEB服务器应使用服务器数字证书。

如系统为内部使用，不对互联网用户提供服务，该项不适用。

10.4.3.2.4 独立的支付密码

应提供独立的支付密码和健全的密码找回机制。

如系统为内部使用，不对互联网用户提供服务，该项不适用。

10.4.3.2.5 网站页面注入防范

网站页面应采取防范SQL注入、Path注入和LDAP注入等风险的措施。

10.4.3.2.6 网站页面跨站脚本攻击防范

网站页面应采取防范跨站脚本攻击风险的措施。

10.4.3.2.7 网站页面源代码暴露防范

网站页面应采取防范源代码暴露的措施。

10.4.3.2.8 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。

10.4.3.2.9 网站页面防篡改措施

应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。

10.4.3.2.10 网站页面防钓鱼

网站页面应提供防钓鱼网站的防伪信息验证。
如系统为内部使用，不对互联网用户提供服务，该项不适用。

10.4.3.3 访问控制

10.4.3.3.1 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，并严格限制默认用户的访问权限。
应授予不同用户为完成各自承担任务所需的最小权限，并在它们之间形成互相制约的关系。

10.4.3.3.2 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、客体及它们之间的操作。

10.4.3.3.3 业务操作日志

应具有所有业务操作日志。

10.4.3.3.4 关键数据操作控制

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

10.4.3.3.5 异常中断防护

用户访问异常中断后，应具有防护手段，保证数据不丢失。

10.4.3.3.6 数据库安全配置

应具有数据库安全配置手册，并对数据库进行安全配置。

10.4.3.4 安全审计

10.4.3.4.1 日志信息

审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

10.4.3.4.2 日志权限和保护

应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录。

10.4.3.4.3 系统信息查询与分析

应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

10.4.3.4.4 对象操作审计

应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。

10.4.3.4.5 审计工具

应具备日志审计工具，对日志进行记录、分析和报告。
增强要求为：应根据系统统一安全策略，提供集中审计接口。

10.4.3.4.6 事件报警

应具有交易事件报警功能。

10.4.3.5 剩余信息保护

应对无用的过期信息、文档进行完整删除。

增强要求为：应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

10.4.3.6 资源控制

10.4.3.6.1 连接控制

应能够根据业务需求，对系统的最大并发会话连接数进行限制。

应能够对一个时间段内可能的并发会话连接数进行限制。

10.4.3.6.2 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。

应能够对单个帐户的多重并发会话进行限制。

10.4.3.6.3 进程资源分配

应能够对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额。

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。

10.4.3.6.4 资源监测预警

应能够对系统服务水平降低到预先规定的最小值进行检查和报警。

10.4.3.7 应用容错

10.4.3.7.1 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或长度符合系统设定要求。

10.4.3.7.2 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。

增强要求为：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。

10.4.3.7.3 故障机制

发生故障后，系统应能够及时恢复。

10.4.3.7.4 回退机制

应提供回退功能，当故障发生后，能够及时回退到故障发生前的状态。

10.4.3.8 报文完整性

通信报文应采用密码技术保证通讯过程中交易数据的完整性。

10.4.3.9 报文保密性

在通讯时采用安全通道或对报文中敏感信息进行加密。

10.4.3.10 抗抵赖

10.4.3.10.1 原发和接收证据

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。

10.4.3.10.2 可信时间戳服务

增强要求为：本地时间应从国家权威时间源采时，保证时间的同一性；
应采用国家认可的可信时间戳服务；
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。

10.4.3.11 编码安全

10.4.3.11.1 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。
增强要求为：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。

10.4.3.11.2 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。

10.4.3.11.3 编码规范约束

应按照编码规范进行编码，具有编码规范约束制度。

10.4.3.11.4 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。

10.4.3.11.5 版本管理

应具有代码版本管理制度。

10.4.3.12 电子认证应用

10.4.3.12.1 第三方电子认证机构证书

在对外业务（非内部业务）处理过程中，宜使用经过认证的第三方电子认证证书。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，可以使用自建证书（非第三方电子认证证书）。在条件允许的情况下，建议对所有业务使用经过认证的第三方电子认证证书。

10.4.3.12.2 关键业务电子认证技术应用

关键业务应使用电子认证技术。在条件允许的情况下，建议在所有业务均使用经过认证的第三方电子认证技术。

10.4.3.12.3 电子签名有效性

应使用有效的电子签名。在对外业务（非内部业务）处理过程中，宜使用经过第三方认证的电子签名体系。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，可以使用自建的电子签名体系（非第三方认证的电子签名体系）。在条件允许的情况下，建议对所有业务使用经过认证的第三方电子签名体系。

10.4.3.12.4 服务器证书私钥保护

应对所持有的服务器证书私钥进行有效保护。

10.4.3.13 终端安全

应使用指定的第三方中立测试机构安全检测通过的机顶盒或遥控器。

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。

10.4.4 数据安全性要求

10.4.4.1 数据保护

10.4.4.1.1 客户身份信息保护

应按规定妥善保管客户身份基本信息，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。

10.4.4.1.2 支付业务信息保护

应按规定妥善保管支付业务信息，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。

10.4.4.1.3 会计档案信息保护

应按规定妥善保管会计档案，支付机构对会计档案的保管期限适用《会计档案管理办法》（财会字〔1998〕32号文印发）相关规定。

10.4.4.2 数据完整性

10.4.4.2.1 重要数据更改机制

应制定重要数据更改流程和管理制度。

10.4.4.2.2 数据备份记录

应具备数据备份记录。

10.4.4.2.3 保障传输过程中的数据完整性

应能够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。

10.4.4.2.4 备份数据定期恢复

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。

10.4.4.3 交易数据以及客户数据的安全性

10.4.4.3.1 数据物理存储安全

应具备高可用性的数据物理存储环境。

10.4.4.3.2 客户身份认证信息存储安全

应不允许保存非必须的客户身份认证信息（如银行卡交易密码、指纹、银行卡磁道信息、CVN、CVN2等）。

应对客户的其他敏感信息，如卡号、户名、开户手机、贷记卡有效期、电子邮箱等信息采取保护措施，防止未经授权擅自对个人信息进行查看、篡改、泄露和破坏。宜采用加密存储、部分屏蔽显示等技术。

10.4.4.3.3 终端信息采集设备硬加密措施或其它防伪手段

如果使用终端信息采集设备则应采取硬加密措施，否则要使用其它手段达到防伪目的。

10.4.4.3.4 同一安全级别和可信赖的系统之间信息传输

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。

10.4.4.3.5 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。

10.4.4.3.6 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。

10.4.4.3.7 数据访问控制

应具备重要数据的访问控制措施。

10.4.4.3.8 在线的存储备份

应具备实时在线的存储备份设施。

10.4.4.3.9 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，应指明备份数据的备份方式（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。

10.4.4.3.10 本地备份

应提供本地数据备份。

应具有同机房数据备份设施。

10.4.4.3.11 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。

10.4.4.3.12 备份数据的恢复

应具有备份数据恢复操作手册，并提供恢复功能。

10.4.4.3.13 数据销毁制度和记录

应具有数据销毁制度和相关记录。

10.4.4.3.14 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。

10.4.5 运维安全性要求

10.4.5.1 环境管理

10.4.5.1.1 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。

10.4.5.1.2 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。

10.4.5.1.3 办公环境的保密性措施

应加强对办公环境的保密性管理，规范办公环境人员行为，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档文件等。

10.4.5.1.4 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做出规定。

增强要求为：开发、测试和运行设施应分离，以减少未授权访问或改变运行系统的风险。

10.4.5.1.5 机房进出登记表

应具有机房进出登记表。

10.4.5.2 介质管理

10.4.5.2.1 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，并实行存储环境专人管理。

10.4.5.2.2 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、维护和销毁等方面做出规定。

10.4.5.2.3 维修或销毁介质之前清除敏感数据

应对送出维修以及销毁等进行严格的管理，对送出维修或销毁的介质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。

10.4.5.2.4 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。

10.4.5.2.5 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。

10.4.5.3 设备管理

10.4.5.3.1 设备管理的责任人员或部门

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。

10.4.5.3.2 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管理。

10.4.5.3.3 设备选型、采购、发放等的审批控制

应建立基于申报、审批和专人负责的设备安全管理制度，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。

10.4.5.3.4 设备配置标准化

应建立标准化的设备配置文档。

10.4.5.3.5 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，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。

10.4.5.3.6 设备的操作日志

应具有完整的设备操作日志。

10.4.5.3.7 设备使用管理文档

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。

10.4.5.3.8 设备标识

应对设备进行分类和标识。

10.4.5.4 人员管理

10.4.5.4.1 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。

应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

10.4.5.4.2 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。

应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。

10.4.5.4.3 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。

10.4.5.4.4 安全意识教育和培训

应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训。

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。

应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训。

应对安全教育和培训的情况和结果进行记录并归档保存。

10.4.5.4.5 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。

10.4.5.4.6 职责分离

关键岗位人员应职责分离。

10.4.5.5 监控管理

10.4.5.5.1 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、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。

10.4.5.5.2 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。

10.4.5.5.3 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。

10.4.5.5.4 异常处理机制

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。

应按重要程度进行分级报警，并且重要报警要能以某种方式（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，采取必要措施。

10.4.5.5.5 资源监控

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

10.4.5.6 变更管理

10.4.5.6.1 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须经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。

10.4.5.6.2 变更方案

应确认系统中要发生的变更，并制定变更方案，变更内容中应有变更失败后的回退方案等。

10.4.5.6.3 重要系统变更的通知

重要系统变更前，应通知相关单位、部门和人员。

10.4.5.6.4 重要系统变更的实施

应记录变更实施过程，并妥善保存所有文档和记录。

10.4.5.7 安全事件处置

10.4.5.7.1 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。

10.4.5.7.2 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。

10.4.5.7.3 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，过程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。

10.4.5.8 应急预案管理

10.4.5.8.1 制定不同事件的应急预案

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。

10.4.5.8.2 相关人员应急预案培训

应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。

10.4.5.8.3 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。对应急预案演练中暴露出的问题进行总结并及时整改。

10.4.6 业务连续性要求

10.4.6.1 业务连续性需求分析

10.4.6.1.1 业务中断影响分析

应进行业务中断影响分析。

10.4.6.1.2 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。

10.4.6.2 业务连续性技术环境

10.4.6.2.1 备份机房

应具备同城应用级备份。

10.4.6.2.2 网络双链路

应具备双链路。

10.4.6.2.3 网络设备和服务器备份

应具有同城应用级备份设施。

10.4.6.2.4 高可靠的磁盘阵列

应使用高可靠的磁盘阵列。

10.4.6.2.5 远程数据库备份

应具备远程备份数据库。

10.4.6.3 业务连续性管理

10.4.6.3.1 业务连续性管理制度

应具备业务连续性管理制度。

10.4.6.3.2 应急响应流程

应具备应急响应流程。

10.4.6.3.3 恢复预案

应具备不同场景恢复预案，同时具备应用级恢复预案。

10.4.6.3.4 数据备份和恢复制度

应具备数据备份和恢复管理制度。

10.4.6.4 备份和恢复管理

10.4.6.4.1 备份数据范围和备份频率

应具备备份数据范围和备份频率清单。

10.4.6.4.2 备份和恢复手册

应具备数据备份和恢复手册。

10.4.6.4.3 备份记录和定期恢复测试记录

应具备备份记录和定期恢复测试记录。

10.4.6.4.4 定期数据备份恢复性测试

应进行定期数据备份恢复性测试。

10.4.6.5 日常维护

10.4.6.5.1 每年业务连续性演练

应每年进行业务连续性演练，包括主备机房的切换演练，演练需提供记录。

10.4.6.5.2 定期业务连续性培训

应定期进行业务连续性培训并具有培训记录。

10.5 文档要求

10.5.1 用户文档

10.5.1.1 用户手册

用户手册应描述手工操作该软件的用户应如何安装和使用一个软件系统。它还包括软件操作的一些特别的方面，诸如，关于特定岗位或任务的指令等。用户手册是为由用户操作的软件而开发的，具有要求联机用户输入或解释输出显示的用户界面。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

10.5.1.2 操作手册

操作手册应提供操作指定的设备所需的信息。本手册侧重设备自身，而不是运行在其上的特定的软件。操作手册主要针对一些新开发的设备、专用设备、无现成的商用操作手册或其他操作手册可用的其他的设备。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

10.5.2 开发文档

10.5.2.1 需求说明书

需求说明书应从以下几方面描述一个建议的系统：说明它能满足用户什么需要，它与现有系统或过程的关系，以及它的使用方式等。需求说明书旨在需方、开发方、支持方和用户代理之间对所建议的系统的运行机理取得共识。取决于使用的目的，需求说明书可专注于向开发者表述用户的需求，或专注于向用户或其他感兴趣的对象表达开发者的思路。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

10.5.2.2 需求分析文档

需求分析文档应描述对计算机软件系统的需求，及确保每个需求得以满足所使用的方法。需求分析文档应涉及该系统外部接口的需求。

宜符合GB/T 8567和GB/T 9385要求。

增强要求为：应符合GB/T 8567和GB/T 9385要求。

10.5.2.3 总体设计方案

总体设计方案应描述系统或子系统的系统级或子系统级设计与体系结构设计。总体设计方案还要用《概要设计文档》和《数据库设计文档》加以补充。总体设计方案连同相关的概要和数据库设计文档是构成进一步系统实现的基础。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

10.5.2.4 数据库设计文档

数据库设计文档应描述数据库的设计。数据库可由用户或计算机程序通过数据库管理系统加以访问。数据库设计文档还描述了存取或操纵数据所使用的软件配置项。数据库设计文档是实现数据库及相关软件配置项的基础。它向需方提供了设计的可视性，为软件支持提供了所需要的信息。数据库设计文档是否单独成册或与详细设计文档合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

10.5.2.5 概要设计文档

概要设计文档应描述计算机软件系统的设计。它描述了系统级设计决策、系统体系结构设计，概要设计和数据库设计是否单独成册抑或与详细设计合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

10.5.2.6 详细设计文档

详细设计文档应描述计算机软件系统的设计。它描述了子系统级设计决策、系统体系结构设计和实现该软件所需的详细设计。概要设计和数据库设计是否单独成册抑或与详细设计合为一份资料视情况繁简而定。

宜符合GB/T 8567要求。

增强要求为：应符合GB/T 8567要求。

10.5.2.7 工程实施方案

工程实施方案应描述开发者实施软件开发工作的计划，包括新开发、修改、重用、再工程、维护和由软件产品引起的其他所有的活动。工程实施方案是向需求方提供了解和监督软件开发过程、所使用的方法、每项活动的途径、项目的安排、组织及资源的一种手段。

10.5.3 管理文档

10.5.3.1 测试报告

测试报告应是对计算机软件、软件系统或子系统，或与软件相关项目执行合格性测试的记录。通过测试报告，需方能够评估所执行的合格性测试及其测试结果。

宜符合GB/T 8567和GB/T 9386要求。

增强要求为：应符合GB/T 8567和GB/T 9386要求。

10.5.3.2 系统运维手册

系统运维手册应是对系统运维管理中用到的环境、资产、介质、设备等进行维护、升级、漏洞扫描等操作的详细描述。

10.5.3.3 系统应急手册

应根据不同的事件，制定应急预案，形成系统应急手册。

10.5.3.4 运维管理制度

运维管理制度应包含但不限于机房管理制度、介质管理制度、设备管理制度、人员管理制度、监控巡检管理制度、变更管理制度、安全事件处理制度等。

10.5.3.5 安全管理制度

安全管理制度应是对负责安全管理机构的设置与人员等资源的配备描述，以及保证其正常实施安全管理工作的管理制度。

10.5.3.6 安全审计报告

应由专业审计人员根据有关的法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并做出相应评价报告。

11 外包附加要求

11.1 基本要求

11.1.1 外包服务的外包内容

应明确外包程度及具体内容。

11.1.2 安全保密协议

应在合同中设定安全保密条款或单独签署安全保密协议。

安全保密条款或单独签署安全保密协议应明确各方的权利、义务及责任和争议解决办法，以保障托管数据的安全、可靠。

11.1.3 风险评估

应评估业务外包相关风险。

应在合同中设定条款要求外包商风险处置的合同义务和要求。

应有外包风险的控制和报告程序。

应指定或授权专门的部门或人员负责对外包服务进行管理和监督，定期评估外包商的运营状况，定期审查合同条款的履行情况。

应符合监管要求和准则。

应制订对外包的控制制度、事件报告程序和应急计划。

11.1.4 外包商资质

应确定外包行为前应对外包商的经验和能力、硬件资源、财务状况、资金构成、人员构成、主管部门审批等资质进行评估。

应确定外包行为前应对外包商的运维管理制度评估。

应确定外包行为前应进行外包模式调查，并对风险进行评估。

11.1.5 外包合同

应明确规定有关各方的权利和义务。

应明确外包商最低的服务水平。

应规定保守信息资源机密。

应规定争议解决办法。

11.1.6 控制和监督

应定期监视和评审由第三方提供的服务、报告和记录，审核也应定期执行。

应定期评估外包商的财务状况。

应定期审查合同条款的履行。

11.1.7 外包交付

应制订详细的外包交付清单，并对外包相关人员进行业务培训，保障顺利交付外包内容。

11.2 增强要求

外包商应建立质量管理体系和安全管理体系。

附 录 A
（规范性附录）
基于 Internet 网上支付的报文结构及要素

A.1 数据元属性说明

数据元属性的具体含义为：

a) 中文名称：数据元的中文名称，在一定语境下名称应保持唯一。

b) 标识符：它是各数据元的唯一标识，具体的命名方式，遵从了如下一项或多项规则。

1) 使用英式英语词汇；

2) 当命名元素时，遵循大多数语法的典型（字符）约束条件，即：

(1) 所有名称以字母开头；

(2) 第一个字符后面的字符可以是字母或数字字符。

3) 使用 camel 惯例：

(1) 元素和属性的名称可以由包含字母与数字的多个单词复合而成；

(2) 首字母大写；

(3) 词与词之间不留空格。

c) 数据格式：数据元值的类型、长度及数据格式的表示形式，数据类型及数据格式的具体表示如下：

1) a：字母字符；

2) n：数字字符；

3) m：任意字符；

4) s：特殊字符；

5) CCYYMMDDhhmmssmsμsns：“CCYY”表示年份，“MM”表示月份，“DD”表示日期，“hh”表示小时，“mm”表示分钟，“ss”表示秒，“ms”表示毫秒，“μs”表示微秒，“ns”表示纳秒，上述符号可视具体实际情况组合使用，如 an 表示数字字母字符；ans 表示数字字母及特殊字符。

示例如下所示：

例1：a10　　表示定长为10的字母字符。

例2：n5　　表示定长为5的数字字符。

例3：nMax(20)　　表示最长为20个数字字符。

例4：a1n2　　表示为1个字母与2个数字字符的组合。

d) 值域：由数据格式决定，数据元允许值的集合。

e) 说明：数据元含义描述。

A.2 业务部分的主要数据项

A.2.1 一般支付

A.2.1.1 一般支付请求

一般支付请求的主要数据项见表 A.1。

表 A.1　一般支付请求

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
订单号	OrderID	ansMAX(50)	无	用于识别一笔交易对应的商户订单号。	可选
交易币种	TrxCurrencyCode	a3	无	交易的币种代码，见 GB/T 12406。	必填
交易金额	TrxAmount	nMAX(16)	无	交易的金额，最小单位为分。例如 123.45 表示为 12345。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	商户提交交易请求的日期时间。	必填
订单有效期	OrderValidPeriod	a1+n3	无	订单保持有效的时间，缺省为支付服务方约定有效期。 第 1 位：表示有效期类型，y-年，m-月，d-天，h-小时，m-分钟； 第 2-4 位：表示有效期时间。	可选
通知类型	NoticeType	n1	1～3	用于描述交易结果信息的通知方式： 1 - 浏览器重定向； 2 - 服务器点对点通讯； 3 - 两种方式均支持。	可选
页面通知地址	PageCallBackURL	ansMAX(2048)	无	支付服务方通过客户浏览器传送交易结果的商户页面 URL。默认为支付服务方约定的地址。	可选
后台通知地址	ServerCallBackURL	ansMAX(2048)	无	描述支付服务方传送交易结果到商户 URL 地址。	可选
通知应答方式	ResponseType	n1	0～1	用于描述支付通知应答的方式。默认为不需要应答。 0 - 不需要应答，收到以 HTTP 协议响应码 200 则认为通知成功，其他为通知失败； 1 - 需要应答，收到应答信息表示通知成功，否则触发重发。	可选
用户设备标识	UserDeviceID	mMAX(200)	无	用于描述订单付款方的设备信息，可以是 IP 地址、MAC 地址、浏览器信息等。	可选
付款方手续	PayerFee	nMAX(16)	无	付款方支付的手续费。	可选

中文名称	标识符	数据格式	值域	说明	备注
费					
收款方手续费	PayeeFee	nMAX(16)	无	收款方支付的手续费。	可选
商品类别	ProductCatalog	n2	无	商品的分类： 00 - 实物类； 01 - 虚拟类； 02 - 服务类； ……。	必填
订单描述	OrderDesc	mMAX(100)	无	订单的简要描述，用于支付页面提示。	必填
订单备注	OrderMemo	mMAX(500)	无	订单的备注信息。	可选
客户标识	CustomerID	mMAX(50)	无	订单提交人的客户标识，如客户姓名、编号、电话号码，手机号码等。	可选
收款方账号	PayeeAccountID	nMAX(34)	无	收款方的账号。	可选
收款方名称	PayeeName	mMAX(50)	无	收款方的姓名。	可选
收货人标识	ConsigneeID	mMAX(50)	无	收货人的身份标识，如收货人会员号，收货人姓名、收货人电话号码、手机号码等。由使用方自行定义显示在订单上收货人栏位上的信息。	可选
收货人地址	ConsigneeAddress	mMAX(200)	无	显示在订单上收货人电子邮件栏位上的信息。	可选
收货人邮编	ConsigneePostcode	nMAX(10)	无	显示在订单上收货人邮编栏位上的信息。	可选
收货人电话	ConsigneePhoneNumber	nsMAX(22)	无	显示在订单上收货人电话栏位上的信息。	可选
收货人电子邮件地址	ConsigneeEmail	ansMAX(100)	无	显示在订单上收货人电子邮件栏位上的信息。	可选

A.2.1.2 一般支付响应

一般支付相应的主要数据项见表 A.2。

表 A.2 一般支付响应

中文名称	标识符	数据格式	值域	说明	备注
处理状态	ProcessStatus	n1	0～1	用于处理服务器是否接受请求的标志： 0 - 拒绝/失败； 1 - 接受/成功。	必填
交易错误码	TrxErrorCode	n6	无	用于表示交易结果错误的代码。	失败时填写

中文名称	标识符	数据格式	值域	说明	备注
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息,可以中文或英文等。	可选
支付地址	PaymentURL	ansMAX(2048)	无	支付地址。	成功时必填
付款方名称	PayerName	mMAX(50)	无	付款方的姓名。	必填

A.2.1.3 一般支付结果通知

一般支付结果通知的主要数据项见表 A.3。

表 A.3 一般支付结果通知

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
订单号	OrderID	ansMAX(50)	无	用于识别一笔交易对应的商户订单号。	可选
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	商户提交交易请求的日期时间。	必填
支付服务方流水号	TrxID	anMAX(60)	无	支付服务方产生的交易流水号。	成功时填入
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方支付成功的日期时间。	成功时填入
交易状态	TrxStatus	n1	无	交易状态： 0 - 未处理； 1 - 成功； 2 - 失败； 3 - 状态未明； ……。	必填
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
通知类型	NoticeType	n1	1～3	用于描述交易结果信息的通知方式： 1 - 浏览器重定向； 2 - 服务器点对点通讯； 3 - 两种方式均支持。	必填

中文名称	标识符	数据格式	值域	说明	备注
通知应答方式	ResponseType	n1	0～1	用于描述支付通知应答的方式。默认为不需要应答。 0 - 不需要应答，收到以 HTTP 协议响应码 200 则认为通知成功，其他为通知失败； 1 - 需要应答，收到应答信息表示通知成功，否则触发重发。	必填
用户设备标识	UserDeviceID	mMAX(200)	无	用于描述订单付款方的设备信息，可以是 IP 地址、MAC 地址、浏览器信息等。	可选
付款方手续费	PayerFee	nMAX(16)	无	付款方支付的手续费。	可选
收款方手续费	PayeeFee	nMAX(16)	无	收款方支付的手续费。	可选
付款方发卡/账户机构标识	PayerAccountIssuerID	anMAX(20)	无	付款方发卡行或付款方开户行标识代码。如果报文的接收方为支付服务方则为必填项。	可选
卡类型/卡类别	PayerCardType	an6	无	付款方的卡类型。	可选
付款方卡号	PayerCardNo	nMAX(19)	无	付款方支付时使用的卡号。如果报文的接收方为支付服务方则为必填项，与付款方账号二选一。	可选
付款方账号	PayerAccountID	nMAX(34)	无	付款方支付时使用的账号。如果报文的接收方为支付服务方则为必填项，与付款方卡号二选一。	可选
记账日期	AccountingDate	n8	CCYYMMDD	商户与支付服务方之间应转移资金的账务日期（商户入账的记账日期）。商户对账时，可以按照支付服务方返回的记账日期进行对账。	必填
实际交易币种	TrxRealCurrencyCode	a3	无	实际交易的币种代码。	必填
实际交易金额	TrxRealAmount	nMAX(16)	无	实际发生的交易金额，最小单位为分。例如 123.45 表示为 12345。	必填
付款方名称	PayerName	mMAX(50)	无	付款方的姓名。	必填
付款方证件类型	PayerIDType	n2	无	付款方的证件类型。如客户通过非银行结算账户支付且报文的接收方为支付服务方则为必填项。	可选
付款方证件号码	PayerID	anMAX(30)	无	付款方的证件号码。 如客户通过非银行结算账户支付且报文的接收方为支付服务方则为必填项。	可选

中文名称	标识符	数据格式	值域	说明	备注
收款方名称	PayeeName	mMAX(50)	无	收款方的姓名。如果报文的接收方为支付服务方则为必填项。	可选
收款方发卡/账户机构标识	PayeeAccountIssuerID	anMAX(20)	无	收款方发卡行或收款方开户行标识代码。如果报文的接收方为支付服务方则为必填项。	可选

A.2.1.4 一般支付结果通知响应

一般支付结果通知响应的主要数据项见表 A.4。

表 A.4 一般支付结果通知响应

中文名称	标识符	数据格式	值域	说明	备注
处理状态	ProcessStatus	n1	0～1	用于处理服务器是否接受请求的标志： 0 - 拒绝/失败； 1 - 接受/成功。	必填
注：如果收到的请求报文中ResponseType的值为“不需要应答”，则服务器不会收到相应的响应报文。					

A.2.2 担保支付

A.2.2.1 担保支付请求

担保支付只用于一般支付的担保。担保支付请求的主要数据项见表A.5。

表 A.5 担保支付请求

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
订单号	OrderID	ansMAX(50)	无	用于识别一笔交易对应的商户订单号。	可选
交易币种	TrxCurrencyCode	a3	无	交易的币种代码，GB/T 12406。	必填
交易金额	TrxAmount	nMAX(16)	无	交易的金额，最小单位为分。例如 123.45 表示为 12345。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	商户提交交易请求的日期时间。	必填
订单有效期	OrderValidPeriod	a1 + n3	无	订单保持有效的时间，缺省为支付服务方约定有效期。 第 1 位：表示有效期类型，y-年，m-月，d-天，h-小时，m-分钟； 第 2-4 位：表示有效期时间。	可选
通知类型	NoticeType	n1	1～3	用于描述接收交易结果信息的通知方式： 1 - 浏览器重定向； 2 - 服务器点对点通讯；	可选

中文名称	标识符	数据格式	值域	说明	备注
				3 - 两种方式均支持。	
页面通知地址	PageCallBackURL	ansMAX(2048)	无	支付服务方通过客户浏览器传送交易结果的商户页面 URL。默认为支付服务方约定的地址。	可选
后台通知地址	ServerCallBackURL	ansMAX(2048)	无	描述支付服务方传送交易结果到商户 URL 地址。	可选
通知应答方式	ResponseType	n1	0～1	用于描述支付通知应答的方式。默认为不需要应答。 0 - 不需要应答，收到以 HTTP 协议响应码 200 则认为通知成功，其他为通知失败； 1 - 需要应答，收到应答信息表示通知成功，否则触发重发。	可选
用户设备标识	UserDeviceID	mMAX(200)	无	用于描述订单付款方的设备信息，可以是 IP 地址、MAC 地址、浏览器信息等。	可选
付款方手续费	PayerFee	nMAX(16)	无	付款方支付的手续费。	可选
收款方手续费	PayeeFee	nMAX(16)	无	收款方支付的手续费。	可选
商品类别	ProductCatalog	n2	无	商品的分类： 00 - 实物类； 01 - 虚拟类； 02 - 服务类； ……。	必填
订单描述	OrderDesc	mMAX(100)	无	订单的简要描述，用于支付页面提示。	必填
订单备注	OrderMemo	mMAX(500)	无	订单的备注信息，用于支付页面提示。	可选
客户标识	CustomerID	mMAX(50)	无	订单提交人的客户标识，如客户姓名、编号、电话号码，手机号码等。	可选
收款方账号	PayeeAccountID	nMAX(34)	无	收款方的账号或卡号，明文或密文。	可选
收款方名称	PayeeName	mMAX(50)	无	收款方的姓名。	可选
担保标志	EscrowFlag	n1	0～1	支付担保的标志： 0 - 不担保； 1 - 担保。	必填
收货人标识	ConsigneeID	mMAX(50)	无	收货人的身份标识，如收货人会员号，收货人姓名、收货人电话	可选

中文名称	标识符	数据格式	值域	说明	备注
				号码、手机号码等。由使用方自行定义显示在订单上收货人栏位上的信息。	
收货人地址	ConsigneeAddress	mMAX(200)	无	显示在订单上收货人电子邮件栏位上的信息。	可选
收货人邮编	ConsigneePostcode	nMAX(10)	无	显示在订单上收货人邮编栏位上的信息。	可选
收货人电话	ConsigneePhoneNumber	nsMAX(22)	无	显示在订单上收货人电话栏位上的信息。	可选
收货人电子邮件地址	ConsigneeEmail	ansMAX(100)	无	显示在订单上收货人电子邮件栏位上的信息。	可选

A.2.2.2 担保支付响应

见A.2.1.2一般支付响应。

A.2.2.3 担保支付结果通知

见A.2.1.3一般支付结果通知。

A.2.2.4 担保支付结果通知响应

见A.2.1.4一般支付结果通知响应。

A.2.3 协议支付

A.2.3.1 协议支付请求

协议支付请求的主要数据项见表 A.6。

表 A.6 协议支付请求

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
订单号	OrderID	ansMAX(50)	无	用于识别一笔交易对应的商户订单号。	可选
交易币种	TrxCurrencyCode	a3	无	交易的币种代码，见 GB/T 12406。	必填
交易金额	TrxAmount	nMAX(16)	无	交易的金额，最小单位为分。例如 123.45 表示为 12345。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	商户提交交易请求的日期时间。	必填
订单有效期	OrderValidPeriod	a1 + n3	无	订单保持有效的时间，缺省为支付服务方约定有效期。	可选

中文名称	标识符	数据格式	值域	说明	备注
				第 1 位：表示有效期类型，y-年，m-月，d-天，h-小时，m-分钟； 第 2-4 位：表示有效期时间。	
通知类型	NoticeType	n1	1～3	用于描述接收交易结果信息的通知方式： 1 - 浏览器重定向； 2 - 服务器点对点通讯； 3 - 两种方式均支持。	可选
页面通知地址	PageCallBackURL	ansMAX(2048)	无	支付服务方通过客户浏览器传送交易结果的商户页面 URL。默认为支付服务方约定的地址。	可选
后台通知地址	ServerCallBackURL	ansMAX(2048)	无	描述支付服务方传送交易结果到商户 URL 地址。	可选
通知应答方式	ResponseType	n1	0～1	用于描述支付通知应答的方式。默认为不需要应答。 0 - 不需要应答，收到以 HTTP 协议响应码 200 则认为通知成功，其他为通知失败； 1 - 需要应答，收到应答信息表示通知成功，否则触发重发。	可选
用户设备标识	UserDeviceID	mMAX(200)	无	用于描述订单付款方的设备信息，可以是 IP 地址、MAC 地址、浏览器信息等。	可选
付款方手续费	PayerFee	nMAX(16)	无	付款方支付的手续费。	可选
收款方手续费	PayeeFee	nMAX(16)	无	收款方支付的手续费。	可选
商品类别	ProductCatalog	n2	无	商品的分类： 00 - 实物类； 01 - 虚拟类； 02 - 服务类； ……。	必填
订单描述	OrderDesc	mMAX(100)	无	订单的简要描述，用于支付页面提示。	必填
订单备注	OrderMemo	mMAX(500)	无	订单的备注信息，用于支付页面提示。	可选
客户标识	CustomerID	mMAX(50)	无	订单提交人的客户标识，如客户姓名、编号、电话号码，手机号码等。	可选
收款方账号	PayeeAccountID	nMAX(34)	无	收款方的账号或卡号，明文或密文。	可选

中文名称	标识符	数据格式	值域	说明	备注
收款方名称	PayeeName	mMAX(50)	无	收款方的姓名。	可选
收货人标识	ConsigneeID	mMAX(50)	无	收货人的身份标识，如收货人会员号，收货人姓名、收货人电话号码、手机号码等。由使用方自行定义显示在订单上收货人栏位上的信息。	可选
收货人地址	ConsigneeAddress	mMAX(200)	无	显示在订单上收货人电子邮件栏位上的信息。	可选
收货人邮编	ConsigneePostcode	nMAX(10)	无	显示在订单上收货人邮编栏位上的信息。	可选
收货人电话	ConsigneePhoneNumber	nsMAX(22)	无	显示在订单上收货人电话栏位上的信息。	可选
收货人电子邮件地址	ConsigneeEmail	ansMAX(100)	无	显示在订单上收货人电子邮件栏位上的信息。	可选

A.2.3.2 协议支付响应

见A.2.1.2一般支付响应。

A.2.3.3 协议支付结果通知

见A.2.1.3一般支付结果通知。

A.2.3.4 协议支付结果通知响应

见A.2.1.4一般支付结果通知响应。

A.2.4 订单撤销

A.2.4.1 订单撤销请求

订单撤销请求的主要数据项见表 A.7。

表 A.7 订单撤销请求

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	商户交易流水号
原请求日期时间	OrigRequestDateTime	n14	CCYYMMDDhhmmss	原交易的请求日期时间。	必填
原商户交易流水号	OrigRequestID	ansMAX(50)	无	原交易的商户交易流水号。	必填
订单号	OrderID	ansMAX(50)	无	用于识别一笔交易对应的商户订单号。	可选

中文名称	标识符	数据格式	值域	说明	备注
原交易金额	OrigTrxAmount	nMAX(16)	无	原交易的金额，以分为单位。	可选
后台通知地址	ServerCallBackURL	ansMAX(2048)	无	描述支付服务方传送交易结果到商户 URL 地址。	可选

A.2.4.2 订单撤销响应

订单撤销响应的主要数据项见表 A.8。

表 A.8 订单撤销响应

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	商户交易流水号
交易状态	TrxStatus	n1	无	交易状态： 0 - 未处理； 1 - 成功； 2 - 失败； 3 - 状态未明； ……。	必填
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
原交易金额	OrigTrxAmount	nMAX(16)	无	原交易的金额，以分为单位。	可选
原请求日期时间	OrigRequestDateTime	n14	CCYYMMDDhhmmss	商户提交交易请求的日期时间。	可选
原商户交易流水号	OrigRequestID	ansMAX(50)	无	商户提交的原始交易的商户交易流水号。	必填
原交易状态	OrigTrxStatus	n1	无	描述原交易的状态。取值同交易状态。	表示订单撤销请求指令的结果
原交易错误码	OrigTrxErrorCode	n6	无	描述原交易的错误码。	失败时填写
原交易结果信息	OrigTrxResultMsg	mMAX(100)	无	描述原请求的交易结果信息。	可选

A.2.5 单笔查询

A.2.5.1 单笔查询请求

单笔查询请求的主要数据项见表 A.9。

表 A.9　单笔查询请求

中文名称	标识符	数据格式	值域	说明	备注
原请求日期时间	OrigRequestDateTime	n14	CCYYMMDDhhmmss	原交易的请求日期时间。	必填
原商户交易流水号	OrigRequestID	ansMAX(50)	无	原交易的商户交易流水号。	必填

A.2.5.2　单笔查询响应

单笔查询响应的主要数据项见表 A.10。

表 A.10　单笔查询响应

中文名称	标识符	数据格式	值域	说明	备注
交易码	TrxCode	n2	无	标识一笔交易的交易类型的代码。	必填
记账日期	AccountingDate	n8	CCYYMMDD	交易的记账日期。	可选
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方支付成功的日期时间。	必填
支付服务方流水号	TrxId	anMAX(60)	无	支付服务方产生的交易流水号。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	交易请求的日期时间。	必填
商户交易流水号	RequestID	ansMAX(50)	无	商户交易请求号。	必填
交易金额	TrxAmount	nMAX(16)	无	交易的金额，最小单位为分。	必填
交易状态	TrxStatus	n1	无	交易状态： 0 - 未处理； 1 - 成功； 2 - 失败； 3 - 状态未明； ……。	必填
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
授权码	ApprovalCode	anMAX(6)	无	“预授权成功”填写授权码，其他交易填空。	可选

中文名称	标识符	数据格式	值域	说明	备注
商户协议号	MerchantAgreementID	nMAX(50)	无	商户用来唯一标识扣款协议的编号。	可选
支付服务方协议号	AgreementID	nMAX(50)	无	支付服务方用来唯一标识扣款协议的编号。	可选
收款方账号	PayeeAccountID	nMAX(34)	无	收款方的账号。 填写委托结算收款方的账号。	可选
已退款次数	RefundCount	n1	无	原交易的退款次数。	可选
已退款金额	RefundAmount	nMAX(16)	无	原交易的退款金额。	可选

A.2.6 批量查询

A.2.6.1 批量查询请求

批量查询请求的主要数据项见表 A.11。

表 A.11 批量查询请求

中文名称	标识符	数据格式	值域	说明	备注
起始日期时间	StartDateTime	n14	CCYYMMDDhhmmss	查询交易的起始日期时间。	必填
终止日期时间	EndDateTime	n14	CCYYMMDDhhmmss	查询交易的终止日期时间。	必填

A.2.6.2 批量查询响应

批量查询响应的主要数据项见表 A.12。

表 A.12 批量查询响应

中文名称	标识符	数据格式	值域	说明	备注
处理状态	ProcessStatus	n1	0～1	用于处理服务器是否接受请求的标志： 0 - 拒绝/失败； 1 - 接受/成功。	必填
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
记录数	RecordCount	nMAX(4)	无	查询返回交易结果的数量。	必填
交易列表	TrxList			每一条交易记录的标记，允许重复。	必填

A.2.6.3 交易列表

交易列表的主要数据项见表 A.13。

表 A.13　交易列表

中文名称	标识符	数据格式	值域	说明	备注
记录序号	SeqNo	nMAX(6)	无	收款信息序列号，每个批次从“1”开始计数。	必填
交易码	TrxCode	n2	无	标识一笔交易的交易类型的代码。	必填
记账日期	AccountingDate	n8	CCYYMMDD	交易的记账日期。	可选
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方支付成功的日期时间。	必填
支付服务方流水号	TrxId	anMAX(60)	无	支付服务方产生的交易流水号。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	交易请求的日期时间。	必填
商户交易流水号	RequestID	ansMAX(50)	无	商户交易请求号。	必填
交易金额	TrxAmount	nMAX(16)	无	交易的金额，最小单位为分。例如 123.45 表示为 12345。	必填
交易状态	TrxStatus	n1	无	交易状态： 0 - 未处理； 1 - 成功； 2 - 失败； 3 - 状态未明； ……。	必填
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
授权码	ApprovalCode	anMAX(6)	无	“预授权成功”填写授权码，其他交易填空。	可选
商户协议号	MerchantAgreementID	nMAX(50)	无	商户用来唯一标识扣款协议的编号。	可选
支付服务方协议号	AgreementID	nMAX(50)	无	支付服务方用来唯一标识扣款协议的编号。	可选
收款方账号	PayeeAccountID	nMAX(34)	无	收款方的账号。 填写委托结算收款方的账号。	可选
已退款次数	RefundCount	n1	无	用于描述一笔交易的累计退款次数。	可选
已退款金额	RefundAmount	nMAX(16)	无	用于描述一笔交易的累计退款金额。	可选

A.2.7　协议支付签约/解约

A.2.7.1 协议支付签约/解约请求

协议支付签约/解约请求的主要数据项见表 A.14。

表 A.14 协议支付签约/解约请求

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
签约/解约标志	AgreementFlag	n1	0～1	签约/解约的标志： 0 - 解约； 1 - 签约。	必填
商户协议号	MerchantAgreementID	nMAX(50)	无	商户用来唯一标识扣款协议的编号。	必填
客户标识	CustomerID	mMAX(50)	无	签约用户的客户标识，如客户姓名、编号、电话号码，手机号码等。	可选
协议业务类型	AgreementType	mMAX(60)	无	协议的业务种类，由支付平台约定。	必填
通知类型	NoticeType	n1	1～3	用于描述交易结果信息的通知方式： 1 - 浏览器重定向； 2 - 服务器点对点通讯； 3 - 两种方式均支持。	必填
页面通知地址	PageCallBackURL	ansMAX(2048)	无	支付服务方通过客户浏览器传送交易结果的商户页面 URL。 默认为支付服务方约定的地址。	可选
后台通知地址	ServerCallBackURL	ansMAX(2048)	无	描述支付服务方传送交易结果到商户 URL 地址。	可选
通知应答方式	ResponseType	n1	0～1	用于描述交易通知应答的方式。 默认为不需要应答。 0 - 不需要应答，收到以 HTTP 协议响应码 200 则认为通知成功，其他为通知失败； 1 - 需要应答，收到应答信息表示通知成功，否则触发重发。	必填
用户设备标识	UserDeviceID	mMAX(200)	无	用于描述订单付款方的设备信息，可以是 IP 地址、MAC 地址、浏览器信息等。	可选

A.2.7.2 协议支付签约/解约响应

协议支付签约/解约响应的主要数据项见表 A.15。

表 A.15　协议支付签约/解约响应

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
处理状态	ProcessStatus	n1	0～1	用于表示处理服务器是否接受请求的标志： 0 - 拒绝/失败； 1 - 接受/成功。	必填
签约/解约标志	AgreementFlag	n1	0～1	签约/解约的标志： 0 - 解约； 1 - 签约。	必填
商户协议号	MerchantAgreementID	nMAX(50)	无	商户用来唯一标识扣款协议的编号。	必填
客户标识	CustomerID	mMAX(50)	无	签约用户的客户标识，如客户姓名、编号、电话号码，手机号码等。	必填
协议业务类型	AgreementType	mMAX(60)	无	协议的业务种类，由支付平台约定。	必填
支付服务方流水号	TrxID	anMAX(60)	无	签约时支付服务方的处理流水号。	成功时填入
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	签约时支付服务方的处理日期时间。	成功时填入
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
通知类型	NoticeType	n1	1～3	用于描述交易结果信息的通知方式： 1 - 浏览器重定向； 2 - 服务器点对点通讯； 3 - 两种方式均支持。	必填
通知应答方式	ResponseType	n1	0～1	用于描述支付通知应答的方式。默认为不需要应答。 0 - 不需要应答,收到以HTTP协议响应码200则认为通知成功，其他为通知失败； 1 - 需要应答，收到应答信	必填

中文名称	标识符	数据格式	值域	说明	备注
				息表示通知成功，否则触发重发。	
用户设备标识	UserDeviceID	mMAX(200)	无	用于描述订单付款方的设备信息，可以是 IP 地址、MAC 地址、浏览器信息等。	可选
付款方账户类型	PayerAccountType	n1	0～1	付款方的账户类型： 0 - 银行结算账户； 1 - 非银行结算账户。	可选
付款方账号	PayerAccountID	nMAX(34)	无	用户签约的账号。	可选
付款方名称	PayerName	mMAX(50)	无	用户的姓名。	可选
付款方电话	PayerPhoneNumber	ansMAX(22)	无	用户签约的账号预留的联系电话。	可选
付款方电子邮件地址	PayerEmail	ansMAX(100)	无	用户签约的账号预留的电子邮件地址。	可选
付款方邮编	PayerPostalCode	anMAX(10)	无	用户签约的账号预留的邮政编码。	可选
付款方地址	PayerAddress	mMAX(200)	无	用户签约的账号预留的联系地址。	可选

A.2.7.3 签约结果通知

签约结果通知的主要数据项见表 A.16。

表 A.16 签约结果通知

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
交易状态	TrxStatus	n1	无	交易状态： 0 - 未处理； 1 - 成功； 2 - 失败； 3 - 状态未明； ……。	必填
签约/解约标志	AgreementFlag	n1	0～1	签约/解约的标志： 0 - 解约； 1 - 签约。	必填
商户协议号	MerchantAgreementID	nMAX(50)	无	商户用来唯一标识扣款协议的编号。	必填
支付服务方协议号	AgreementID	nMAX(50)	无	支付服务方用来唯一标识扣款协议的编号。	必填
客户编号	CustomerID	mMAX(20)	无	签约用户的客户编号，如电话	必填

中文名称	标识符	数据格式	值域	说明	备注
				号码，手机号码等。	
协议业务类型	AgreementType	mMAX(60)	无	协议的业务种类，由支付平台约定。	必填
支付服务方流水号	TrxID	anMAX(60)	无	签约时支付服务方的处理流水号。	成功时填入
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	签约时支付服务方的处理日期时间。	成功时填入
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
通知类型	NoticeType	n1	1～3	用于描述交易结果信息的通知方式： 1 - 浏览器重定向； 2 - 服务器点对点通讯； 3 - 两种方式均支持。	必填
通知应答方式	ResponseType	n1	0～1	用于描述交易通知应答的方式。默认为不需要应答。 0 - 不需要应答，收到以HTTP 协议响应码 200 则认为通知成功，其他为通知失败； 1 - 需要应答，收到应答信息表示通知成功，否则触发重发。	必填
用户设备标识	UserDeviceID	mMAX(200)	无	用于描述订单付款方的设备信息，可以是 IP 地址、MAC 地址、浏览器信息等。	可选
付款方账户类型	PayerAccountType	n1	0～1	付款方的账户类型： 0 - 银行结算账户； 1 - 非银行结算账户。	可选
付款方账号	PayerAccountID	nMAX(34)	无	用户签约的账号。	可选
付款方名称	PayerName	mMAX(50)	无	用户的姓名。	可选
付款方电话	PayerPhoneNumber	ansMAX(22)	无	用户签约的账号预留的联系电话。	可选
付款方电子邮件地址	PayerEmail	ansMAX(100)	无	用户签约的账号预留的电子邮件地址。	可选
付款方邮编	PayerPostalCode	anMAX(10)	无	用户签约的账号预留的邮政编码。	可选
付款方地址	PayerAddress	mMAX(200)	无	用户签约的账号预留的联系地址。	可选

A.2.7.4 签约结果通知响应

见A.2.1.4一般支付结果通知响应。

A.2.8 单笔委托结算

A.2.8.1 单笔委托结算请求

单笔委托结算请求的主要数据项见表A.17。

表A.17 单笔委托结算请求

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
交易币种	TrxCurrencyCode	a3	无	交易的币种代码，见GB/T 12406。	必填
交易金额	TrxAmount	nMAX(16)	无	交易的金额，最小单位为分。例如123.45表示为12345。 填写委托结算的金额。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	商户提交交易请求的日期时间。 填写商户委托结算的日期时间。	必填
订单描述	OrderDesc	mMAX(100)	无	填写打款描述信息。	必填
收款方账号	PayeeAccountID	nMAX(34)	无	收款方的账号。 填写委托结算收款方的账号。	必填
收款方名称	PayeeName	mMAX(50)	无	收款方的姓名。	可选
收款方发卡/账户机构标识	PayeeAccountIssuerID	anMAX(20)	无	收款方发卡/账户机构标识。	必填
收款方发卡/账户机构名称	PayeeAccountIssuerNm	mMAX(200)	无	收款方发卡行或收款方开户行名在工商部门注册的名称。	可选
收款方发卡/账户机构地址	PayeeAccountIssuerAdd	mMAX(200)	无	收款方发卡行或收款方开户行地址。	可选
收款方电话	PayeePhone	ansMAX(22)	无	付款方的联系电话。 填写委托结算收款方的联系电话。	可选
收款方电子邮件地址	PayeeEmail	ansMAX(100)	无	委托结算收款方的电子邮件地址。	可选
通知类型	NoticeType	n1	1～3	用于描述交易结果信息的通知方式：	必填

中文名称	标识符	数据格式	值域	说明	备注
				1 - 浏览器重定向； 2 - 服务器点对点通讯； 3 - 两种方式均支持。	
页面通知地址	PageCallBackURL	ansMAX(2048)		支付服务方通过客户浏览器传送交易结果的商户页面 URL。 默认为支付服务方约定的地址。	可选
后台通知地址	ServerCallBackURL	ansMAX(2048)	无	描述支付服务方传送交易结果到商户 URL 地址。	可选
通知应答方式	ResponseType	n1	0～1	用于描述支付通知应答的方式。 默认为不需要应答。 0 - 不需要应答，收到以 HTTP 协议响应码 200 则认为通知成功，其他为通知失败； 1 - 需要应答，收到应答信息表示通知成功，否则触发重发。	必填
用户设备标识	UserDeviceID	mMAX(200)	无	用于描述订单付款方的设备信息，可以是 IP 地址、MAC 地址、浏览器信息等。	必填
付款方手续费	PayerFee	nMAX(16)	无	付款方支付的手续费。	可选
收款方手续费	PayeeFee	nMAX(16)	无	收款方支付的手续费。	可选

A.2.8.2 单笔委托结算响应

单笔委托结算响应的主要数据项见表 A.18。

表 A.18 单笔委托结算响应

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
交易币种	TrxCurrencyCode	a3	无	按照请求填写。	必填
交易金额	TrxAmount	nMAX(16)	无	按照请求填写。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	按照请求填写。	必填
支付服务方流水号	TrxID	anMAX(60)	无	支付服务方产生的交易流水号。	成功时填入
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方支付成功的日期时间。	成功时填入
交易状态	TrxStatus	n1	无	交易状态：	必填

中文名称	标识符	数据格式	值域	说明	备注
				0 - 未处理； 1 - 成功； 2 - 失败； 3 - 状态未明； ……。	
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
通知类型	NoticeType	n1	1～3	用于描述交易结果信息的通知方式： 1 - 浏览器重定向； 2 - 服务器点对点通讯； 3 - 两种方式均支持。	必填

A.2.9 批量委托结算

A.2.9.1 批量委托结算请求

批量委托结算请求的主要数据项见表 A.19。

表 A.19 批量委托结算请求

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
交易币种	TrxCurrencyCode	a3	无	用于填写委托结算的币种代码，见 GB/T 12406。	必填
汇总金额	TotalAmount	nMAX(16)	无	填写委托结算的总金额，应和明细中的金额累计相等。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	商户提交交易请求的日期时间。 填写商户委托结算的日期时间。	必填
通知类型	NoticeType	n1	1～3	用于描述交易结果信息的通知方式： 1 - 浏览器重定向； 2 - 服务器点对点通讯； 3 - 两种方式均支持。	必填
页面通知地址	PageCallBackURL	ansMAX(2048)	无	支付服务方通过客户浏览器传送交易结果的商户页面 URL。 默认为支付服务方约定的地址。	可选
后台通知地址	ServerCallBackURL	ansMAX(2048)	无	描述支付服务方传送交易结果到商户 URL 地址。	可选

中文名称	标识符	数据格式	值域	说明	备注
通知应答方式	ResponseType	n1	0～1	用于描述支付通知应答的方式。默认为不需要应答。 0 - 不需要应答，收到以 HTTP 协议响应码 200 则认为通知成功，其他为通知失败； 1 - 需要应答，收到应答信息表示通知成功，否则触发重发。	必填
用户设备标识	UserDeviceID	mMAX(200)	无	用于描述订单付款方的设备信息，可以是 IP 地址、MAC 地址、浏览器信息等。	可选
记录数	RecordCount	nMAX(6)	无	委托结算明细的笔数。	必填
收款信息列表	PayeeDetail	见附录 A.2.9.2	见附录 A.2.9.2	每个收款信息都以 PayeeDetail 作为标记，内嵌具体收款信息。 该信息允许重复。	必填

A.2.9.2 收款信息列表

收款信息列表见表A.20。

表 A.20 收款信息列表

中文名称	标识符	数据格式	值域	说明	备注
记录序号	SeqNo	nMAX(6)	无	收款信息序列号，每个批次从“1”开始计数。	必填
交易金额	TrxAmount	nMAX(16)	无	填写结算给收款方的金额。	必填
收款方账号	PayeeAccountID	nMAX(34)	无	填写委托结算收款方的账号。	必填
收款方名称	PayeeName	mMAX(50)	无	收款方的姓名。	可选
收款方发卡/账户机构标识	PayeeAccountIssuerID	anMAX(20)	无	收款方发卡/账户机构标识。	必填
收款方发卡/账户机构名称	PayeeAccountIssuerNm	mMAX(200)	无	收款方发卡行或收款方开户行在工商部门注册的名称。	可选
收款方发卡/账户机构地址	PayeeAccountIssuerAdd	mMAX(200)	无	收款方发卡行或收款方开户行地址。	可选
收款方电话	PayeePhone	ansMAX(22)	无	委托结算收款方的联系电话。	可选
收款方电子邮件地址	PayeeEmail	ansMAX(100)	无	委托结算收款方的电子邮件地址。	可选

A.2.9.3 批量委托结算响应

批量委托结算响应的主要数据项见表 A.21。

表 A.21　批量委托结算响应

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
交易币种	TrxCurrencyCode	a3	无	按照委托结算请求填写。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	按照委托结算请求填写。	必填
支付服务方流水号	TrxID	anMAX(60)	无	支付服务方产生的交易流水号。	成功时填入
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方支付成功的日期时间。	成功时填入
处理状态	ProcessStatus	n1	0～1	用于表示处理服务器是否接受请求的标志： 0 - 拒绝/失败； 1 - 接受/成功。	必填
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
通知类型	NoticeType	n1	1～3	用于描述交易结果信息的通知方式： 1 - 浏览器重定向； 2 - 服务器点对点通讯； 3 - 两种方式均支持。	必填

A.2.9.4　批量委托结算结果通知

批量委托结算结果通知的主要数据项见表 A.22。

表 A.22　批量委托结算结果通知

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	商户交易流水号
交易币种	TrxCurrencyCode	a3	无	按照请求填写。	必填
汇总金额	TotalAmount	nMAX(16)	无	按照实际交易成功的金额填写。	必填

中文名称	标识符	数据格式	值域	说明	备注
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	按照请求填写。	必填
支付服务方流水号	TrxID	anMAX(60)	无	支付服务方产生的交易流水号。	成功时填入
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方支付成功的日期时间。	成功时填入
交易状态	TrxStatus	n1	无	交易状态： 0 - 未处理； 1 - 成功； 2 - 失败； 3 - 状态未明； ……。	必填
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
通知类型	NoticeType	n1	1～3	用于描述交易结果信息的通知方式： 1 - 浏览器重定向； 2 - 服务器点对点通讯； 3 - 两种方式均支持。	必填
通知应答方式	ResponseType	n1	0～1	用于描述支付通知应答的方式。默认为不需要应答。 0 - 不需要应答，收到以 HTTP 协议响应码 200 则认为通知成功，其他为通知失败； 1 - 需要应答，收到应答信息表示通知成功，否则触发重发。	必填
记账日期	AccountingDate	n8	CCYYMMDD	商户与支付服务方之间应转移资金的账务日期。 商户对账时，可以按照支付服务方返回的记账日期进行对账。	必填
记录数	RecordCount	nMAX(6)	无	委托结算明细的笔数。	必填
收款信息状态列表	PayeeDetailStatus			每个收款信息都以 PayeeDetailStatus 作为标记，内嵌具体收款信息的处理状态。该信息允许重复。	必填

A.2.9.5 收款信息状态列表

收款信息状态的主要数据项见表 A.23。

表 A.23　收款信息状态列表

中文名称	标识符	数据格式	值域	说明	备注
记录序号	SeqNo	nMAX(6)	无	收款信息序列号，每个批次从“1”开始计数。	必填
交易金额	TrxAmount	nMAX(16)	无	填写结算给收款方的金额。	必填
收款方账号	PayeeAccountID	nMAX(34)	无	收款方的账号。 填写委托结算收款方的账号。	必填
交易状态	TrxStatus	n1	无	交易状态： 0 - 未处理； 1 - 成功； 2 - 失败； 3 - 状态未明； ……。	必填
交易错误码	TrxErrorCode	n6	无	描述本打款记录的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	描述本打款记录的信息，可以中文或英文等。	可选

A.2.9.6　批量委托结算结果通知响应

见A.2.1.4一般支付结果通知响应。

A.2.10　单笔退款

A.2.10.1　单笔退款请求

单笔退款请求的主要数据项见表 A.24。

表 A.24　单笔退款请求

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	按照本退款请求的日期时间填写。	必填
交易金额	TrxAmount	nMAX(16)	无	请求退款的金额。	必填
原商户交易流水号	OrigRequestID	ansMAX(50)	无	原交易的商户交易流水号。	必填
原记账日期	OrigAccountingDate	n8	CCYYMMDD	填写原请求的记账日期。	可选
原请求日期时间	OrigRequestDateTime	n14	CCYYMMDDhhmmss	原交易的请求日期时间。	必填
原支付服务	OrigTrxID	anMAX(60)	无	原交易的支付服务方流水号。	必填

中文名称	标识符	数据格式	值域	说明	备注
方流水号					
原交易日期时间	OrigTrxDateTime	n14	CCYYMMDDhhmmss	原交易的交易日期时间。	必填
后台通知地址	ServerCallBackURL	ansMAX(2048)	无	描述支付服务方传送交易结果到商户 URL 地址。	可选
注：“原交易日期时间、原支付服务方流水号”与“原请求日期时间、原商户交易流水号”可以2选1。					

A.2.10.2 单笔退款响应

单笔退款响应的主要数据项见表 A.25。

表 A.25 单笔退款响应

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	按照单笔退款请求填写。	必填
交易状态	TrxStatus	n1	无	交易状态： 0 - 未处理； 1 - 成功； 2 - 失败； 3 - 状态未明； ……。	必填
交易金额	TrxAmount	nMAX(16)	无	按照请求回填。	必填
支付服务方流水号	TrxID	anMAX(60)	无	退款交易的交易流水号。	成功时填入
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	退款交易的日期时间。	成功时填入
原交易日期时间	OrigTrxDateTime	n14	CCYYMMDDhhmmss	原交易的交易日期时间。	必填
原支付服务方流水号	OrigTrxID	anMAX(60)	无	原交易的支付服务方流水号。	必填
原请求日期时间	OrigRequestDateTime	n14	CCYYMMDDhhmmss	原交易的请求日期时间。	必填
原商户交易流水号	OrigRequestID	ansMAX(50)	无	原交易的商户交易流水号。	必填
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填

中文名称	标识符	数据格式	值域	说明	备注
					写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
记账日期	AccountingDate	n8	CCYYMMDD	退款交易的记账日期。	成功时填入
已退款次数	RefundCount	n1	无	原交易的累计退款次数。	可选
已退款金额	RefundAmount	nMAX(16)	无	原交易的累计退款金额。	可选

A.2.11 批量退款

A.2.11.1 批量退款请求

批量退款请求的主要数据项见表 A.26。

表 A.26 批量退款请求

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	按照本退款请求的日期时间填写。	必填
后台通知地址	ServerCallBackURL	ansMAX(2048)	无	描述支付服务方传送交易结果到商户 URL 地址。	可选
记录数	RecordCount	nMAX(6)	无	批量退款笔数。	必填
汇总金额	RefundAmount	nMAX(16)	无	批量退款的总金额，应和退款明细的累计金额一致。	必填
退款交易列表	RefundList			每一条退款记录的标记，允许重复。	必填

A.2.11.2 退款交易列表

退款交易列表的主要数据项见表 A.27。

表 A.27 退款交易列表

中文名称	标识符	数据格式	值域	说明	备注
记录序号	SeqNo	nMAX(6)	无	退款记录序号，每个批次从“1”开始计数。	退款请求序号
交易金额	TrxAmount	nMAX(16)	无	退款金额不能超过交易的金额。	必填
原记账日期	OrigAccountingDate	n8	CCYYMMDD	填写原交易的记账日期。	可选
原交易日期时间	OrigTrxDateTime	n14	CCYYMMDDhhmmss	原交易的交易日期时间。	必填
原支付服务方	OrigTrxID	anMAX(60)	无	原交易的支付服务方流水号。	必填

中文名称	标识符	数据格式	值域	说明	备注
流水号					
原请求日期时间	OrigRequestDateTime	n14	CCYYMMDDhhmmss	原交易的请求日期时间。	必填
原商户交易流水号	OrigRequestID	ansMAX(50)	无	商户提交的原始交易的商户交易流水号。	必填
订单备注	OrderMemo	mMAX(500)	无	退款原因。	可选

A.2.11.3 批量退款响应

批量退款响应的主要数据项见表 A.28。

表 A.28 批量退款响应

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	按照批量退款请求填写。	必填
处理状态	ProcessStatus	n1	0～1	用于处理服务器是否接受请求的标志： 0 - 拒绝/失败； 1 - 接受/成功。	必填
支付服务方流水号	TrxID	anMAX(60)	无	支付服务方产生的交易流水号（针对退款批次本身的）。	成功时填入
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方交易成功的日期时间（针对退款批次本身的）。	成功时填入
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选

A.2.11.4 批量退款结果通知

批量退款通知的主要数据项见表 A.29。

表 A.29 批量退款结果通知

中文名称	标识符	数据格式	值域	说明	备注
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	必填
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	按照批量退款请求填写。	必填
交易状态	TrxStatus	n1	无	交易状态： 0 - 未处理； 1 - 成功；	必填

中文名称	标识符	数据格式	值域	说明	备注
				2 - 失败； 3 - 状态未明； ……。	
支付服务方流水号	TrxID	anMAX(60)	无	支付服务方产生的交易流水号（针对退款批次本身的）。	成功时填入
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方交易成功的日期时间（针对退款批次本身的）。	成功时填入
汇总金额	TotalAmount	nMAX(16)	无	按照实际交易成功的金额填写。	必填
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
通知应答方式	ResponseType	n1	0～1	用于描述交易通知应答的方式。默认为不需要应答。 0 - 不需要应答，收到以 HTTP 协议响应码 200 则认为通知成功，其他为通知失败； 1 - 需要应答，收到应答信息表示通知成功，否则触发重发。	可选
记录数	RecordCount	nMAX(6)	无	批量退款笔数。	必填
退款结果列表	RefundResultList	见表 A.30	见表 A.30	每一条退款结果的记录标记，允许重复。	必填

A.2.11.5 退款结果列表

退款结果列表的主要数据项见表 A.30。

表 A.30 退款结果列表

中文名称	标识符	数据格式	值域	说明	备注
记录序号	SeqNo	nMAX(6)	无	退款记录序号，每个批次从“1”开始计数。	退款请求序号
原记账日期	OrigAccountingDate	n8	CCYYMMDD	填写原交易的记账日期。	可选
原支付服务方流水号	OrigTrxID	anMAX(60)	无	原交易的支付服务方流水号。	必填
交易状态	TrxStatus	n1	无	交易状态： 0 - 未处理； 1 - 成功； 2 - 失败；	必填

中文名称	标识符	数据格式	值域	说明	备注
				3 - 状态未明； ……。	
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	失败时填写
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	可选
记账日期	AccountingDate	n8	CCYYMMDD	本退款交易的记账日期。	成功时填入
支付服务方流水号	TrxID	anMAX(60)	无	本退款交易的交易流水号。	成功时填入
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	本退款交易的日期时间。	成功时填入
已退款次数	RefundCount	n1	无	用于描述一笔交易的累计退款次数。	必填
已退款金额	RefundAmount	nMAX(16)	无	用于描述一笔交易的累计退款金额。	必填

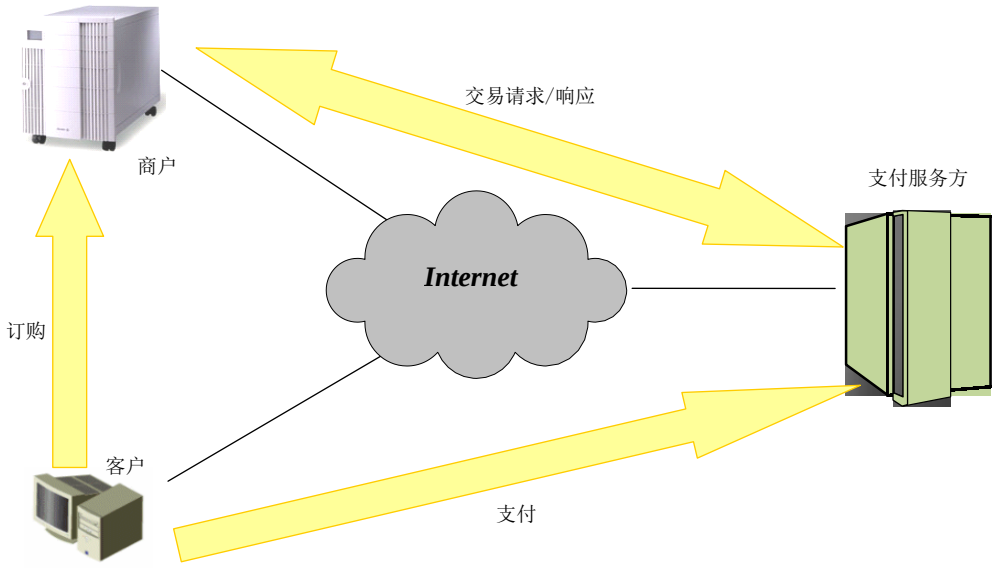
A.2.11.6 批量退款结果通知响应

见A.2.1.4一般支付结果通知响应。

附 录 B
（规范性附录）
基于 Internet 网上支付的交易模型及流程

B.1 总体结构

在基于Internet的电子支付过程中，主要涉及如下角色：客户、商户、支付服务方，总体结构示意见图B.1。



图B.1 基于 Internet 的电子支付过程总体结构

客户是支付过程中，购买商品或服务的个人或企业；商户是支付过程中，提供商品或服务的个人或企业，或者给买卖双方提供撮合的交易平台；支付服务方是支付过程中，给客户及商户提供支付结算服务的机构，视不同情况，可为银行或非金融支付服务组织。具体而言，如果客户通过银行直接完成支付，则支付服务方为银行；如果客户通过非金融支付服务组织转银行完成支付，对商户而言非金融支付服务组织为支付服务方，对银行而言非金融支付服务组织为商户，银行为支付服务方。

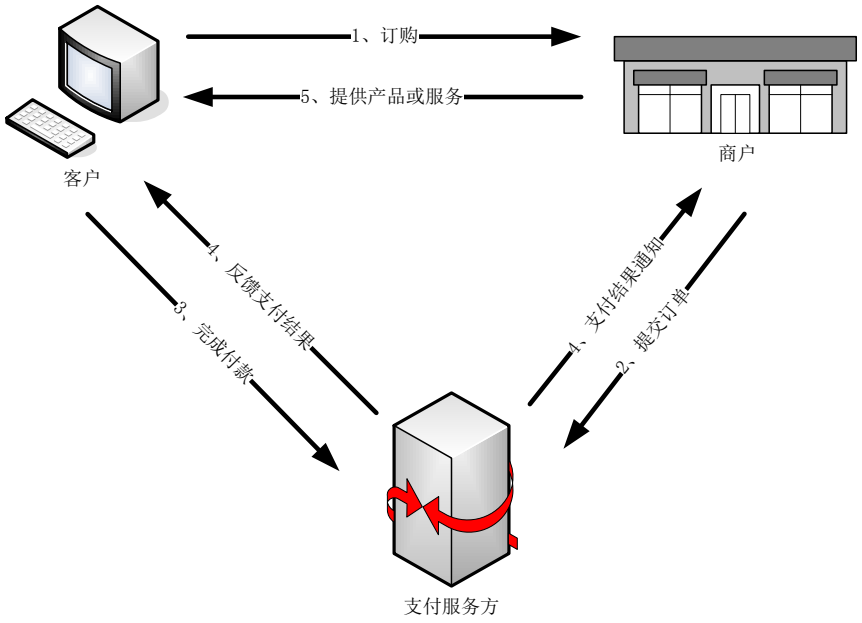
例如：客户通过浏览器访问商户的网站，选择商品并结账；商户记录客户的订单，按照支付服务方的格式组织报文并提交；客户在支付服务方完成付款过程；支付服务方把支付结果通知商户的网站；商户为客户提供商品/服务。

B.2 交易类型及流程

B.2.1 一般支付

B.2.1.1 交易模型

一般支付交易模型见图B.2。



图B.2　一般支付交易模型

B.2.1.2　交易流程

一般支付交易流程如下：

a）　客户在商户网站等选购货物；

b）　商户提交订单，并送给支付服务方；

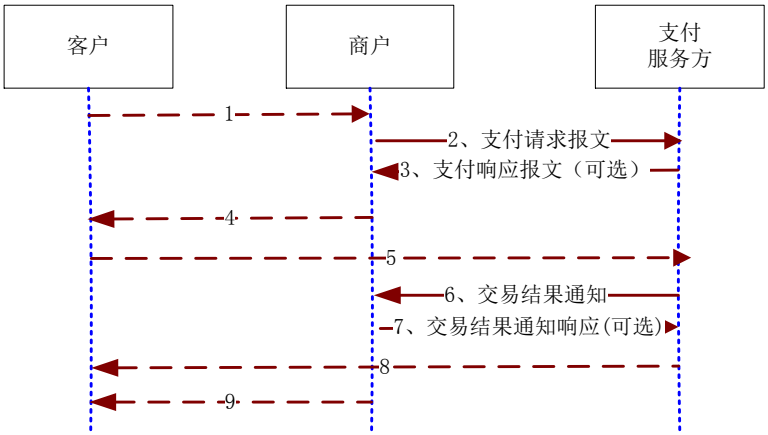
c）　客户在支付服务方完成卡、密码等信息输入，完成付款；

d）　支付服务方将支付结果通知反馈客户和商户；

e）　商户收到通知后提供产品或服务。

B.2.1.3　信息交互过程

一般支付的信息交互过程见图B.3。



图B.3　一般支付信息交互过程

注：在信息交互过程中，实线表示支付服务方和商户之间的交互报文，其他交互的报文用虚线表示（以下图同理）。

1） 客户浏览商户网站购物，订购产品或服务；
2） 商户按照支付服务方的支付请求接口组织报文，并送给支付服务方；
3） 支付服务方返回支付请求响应（可选）；
4） 商户把客户浏览器引导到支付服务方支付页面；
5） 客户确认支付款项、输入身份验证信息并确认付款；
6） 支付服务方完成扣款，并按照约定的交易结果通知接口组织报文，通知商户；
7） 商户返回交易结果通知的响应（可选）；
8） 支付服务方返回交易结果给客户并把客户引导到商户；
9） 商户提示客户付款成功信息，并提供相应的产品或服务。

B.2.1.4 报文

商户与支付服务方之间涉及报文：

a） 一般支付请求报文；
b） 一般支付响应报文；
c） 一般支付结果通知报文；
d） 一般支付结果通知响应报文。

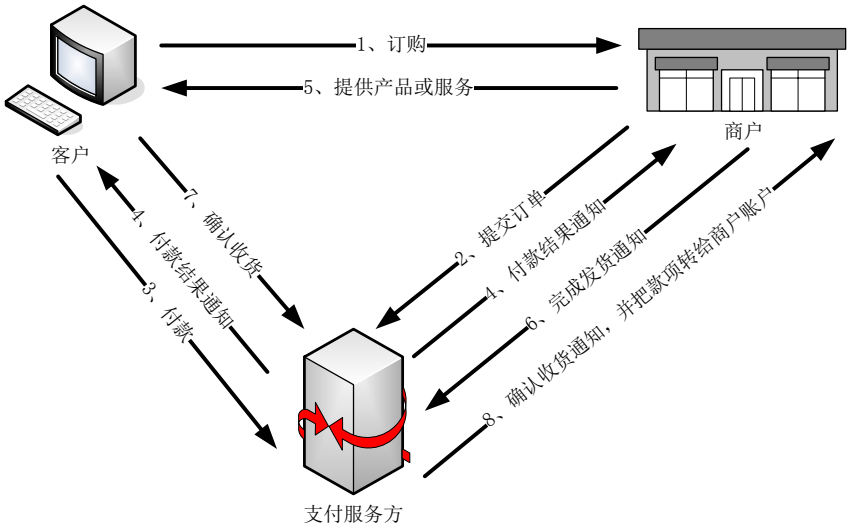
注1：一般支付有两种实现方式：一种是商户通过客户浏览器重新定向方式把报文发送给支付服务方；另外一种是商户服务器通过直连模式把报文送给支付服务方，支付服务方接收后产生一个新的 URL 请求返回给商户，商户服务器把客户重新定向到该 URL。

注2：一般支付请求与一般支付结果通知报文是两个独立的报文。支付请求发出后，并不能立即收到交易结果通知报文，需要客户完成付款操作后才能收到支付结果报文。一般支付响应报文、一般支付结果通知响应报文是报文接收方立即返回的报文，一般支付响应报文、一般支付结果通知响应报文可以根据具体情况选择采用。

B.2.2 担保支付

B.2.2.1 交易模型

担保支付交易模型见图B.4。



图B.4 担保支付交易模型

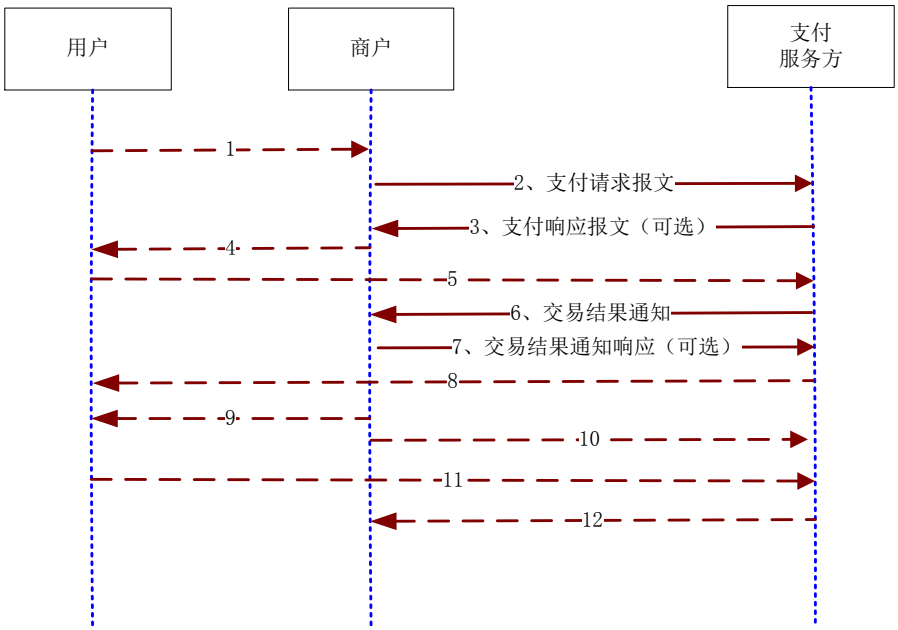
B.2.2.2 交易流程

担保支付交易流程如下：

a) 客户在商户网站等选购货物，并使用担保支付；
b) 商户提交订单，发送给支付服务方；
c) 客户在支付服务方验证身份信息，并确认付款；
d) 付款完成后支付服务方发送支付结果通知给商户和客户；
e) 商户（或商户交易平台上的卖家）提供相应的产品或服务；
f) 商户通知支付服务方完成发货（一般需要上传发货凭证等信息）；
g) 买家收到货后在支付服务方确认收货；
h) 支付服务方将款项转入商户账户或在订单中指定的收款账户，并向商户发送买家确认收货的通知。

B.2.2.3 信息交互过程

担保支付的信息交互过程见图B.5。



图B.5 担保支付信息交互过程

1) 客户在商户网站等选购货物，并使用担保支付；
2) 商户提交订单，送给支付服务方；
3) 支付平台返回支付响应报文给商户（可选）；
4) 商户把客户浏览器引导到支付服务方支付页面；
5) 客户在支付平台验证身份信息，并确认付款；
6) 付款成功后支付平台发送交易结果通知给商户；
7) 商户返回交易结果通知响应给支付平台（可选）；
8) 支付服务方返回交易结果给客户并把客户引导到商户；
9) 商户提示客户付款成功，并且商户（或商户交易平台上的卖家）提供产品或服务处理；
10) 商户上传发货单等，通知支付平台完成发货；

11）买家收到货后在支付服务方确认收货；
12）支付平台发送买家确认收到货通知给商户，并把款项划到商户在订单中约定的收款账户。

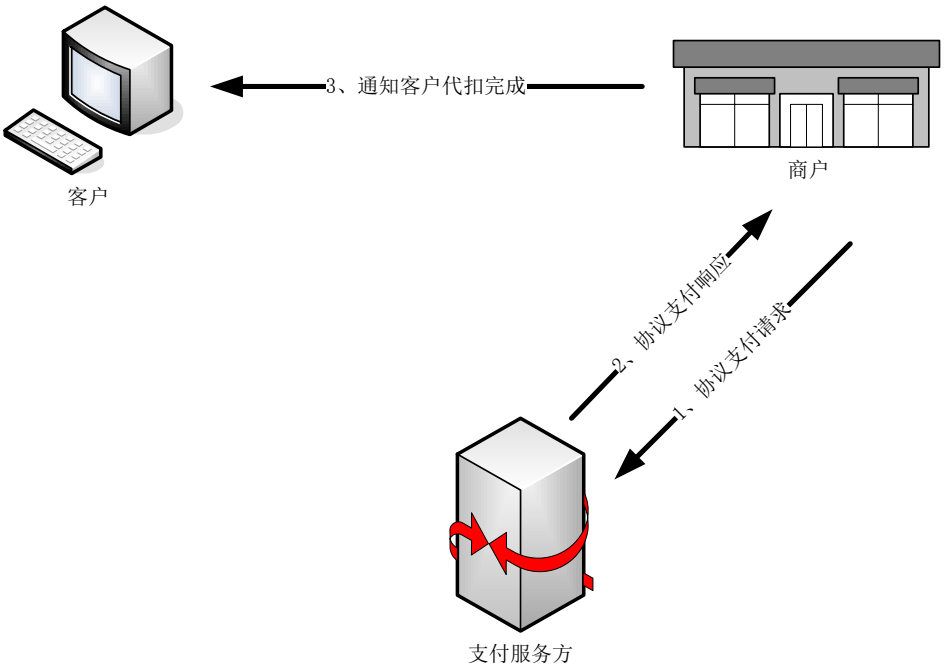
B.2.2.4 报文

商户与支付服务方之间涉及报文：
a） 担保支付请求报文；
b） 担保支付响应报文；
c） 担保支付结果通知报文；
d） 担保支付结果通知响应报文。

B.2.3 协议支付

B.2.3.1 交易模型

协议支付交易模型见图B.6。



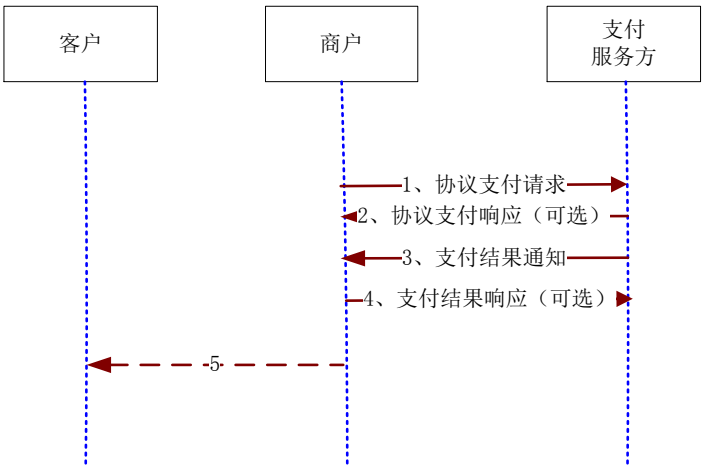
图B.6 协议支付交易模型

B.2.3.2 交易流程

协议支付交易流程如下：
a） 商户获取客户订单并根据客户信息获取客户签订的协议支付号，向支付服务方发起代扣请求；
b） 支付服务方根据协议号扣款，并把处理结果反馈给商户；
c） 商户通知客户代扣完成。

B.2.3.3 信息交互过程

协议支付的信息交互过程见图B.7。



图B.7　协议支付信息交互过程

1）　商户发起协议支付请求；
2）　支付服务方返回协议支付响应（可选）；
3）　支付服务返回支付结果通知；
4）　商户返回支付结果响应（可选）；
5）　商户通知客户代扣完成。

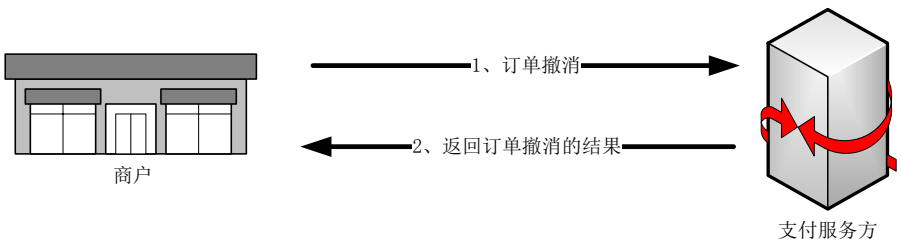
B.2.3.4　报文

商户与支付服务方之间涉及报文：
a）　协议支付请求报文；
b）　协议支付响应报文；
c）　协议支付结果通知报文；
d）　协议支付结果通知响应报文。

B.2.4　订单撤销

B.2.4.1　交易模型

订单撤销交易模型见图B.8。



图B.8　订单撤销交易模型

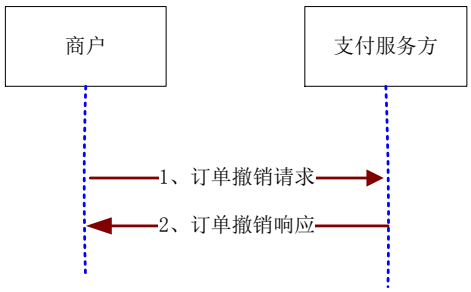
B.2.4.2　交易流程

订单撤销交易流程如下：
a）　商户发起订单撤销的请求；

b) 支付服务方检索支付记录的状态，并进行处理。如果未支付则把支付请求撤销，并返回给商户订单撤销请求成功的信息；否则返回商户订单撤销请求失败的信息。

B.2.4.3 信息交互过程

订单撤销的信息交互过程见图B.9。



图B.9 订单撤销信息交互过程

1) 商户发起订单撤销请求；
2) 支付服务方返回订单撤销响应。

B.2.4.4 报文

商户与支付服务方之间涉及报文：

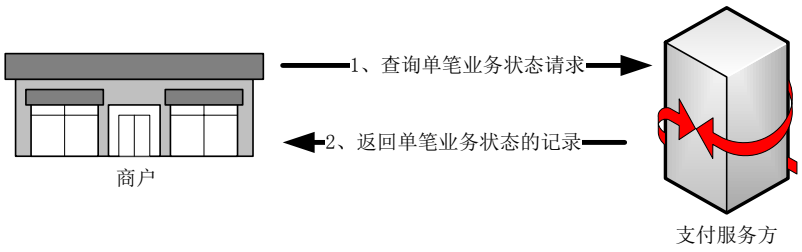
a) 订单撤销请求报文；
b) 订单撤销响应报文。

B.2.5 交易查询

B.2.5.1 单笔查询

B.2.5.1.1 交易模型

单笔查询交易模型见图B.10。



图B.10 单笔查询交易模型

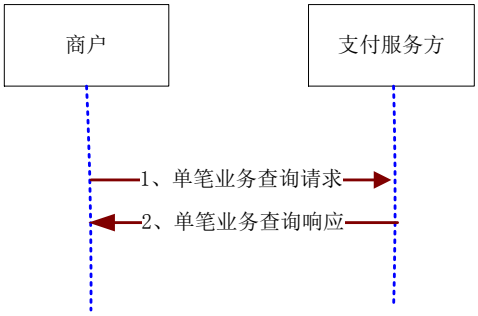
B.2.5.1.2 交易流程

单笔查询交易流程如下：

a) 商户发起查询单笔业务状态的请求；
b) 支付服务方检索业务处理记录的状态并把结果返回给商户。

B.2.5.1.3 信息交互过程

单笔查询的信息交互过程见图B.11。



图B.11　单笔查询信息交互过程

1）　商户向支付服务方发起单笔业务查询请求；
2）　支付服务方向商户回应单笔业务查询响应。

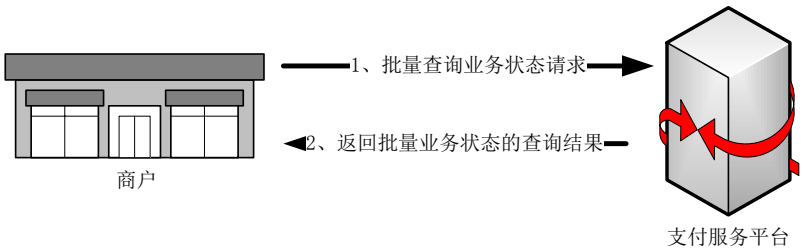
B.2.5.1.4　报文

商户与支付服务方之间涉及报文：
a）　单笔查询请求报文；
b）　单笔查询响应报文。

B.2.5.2　批量查询

B.2.5.2.1　交易模型

批量查询交易模型见图B.12。



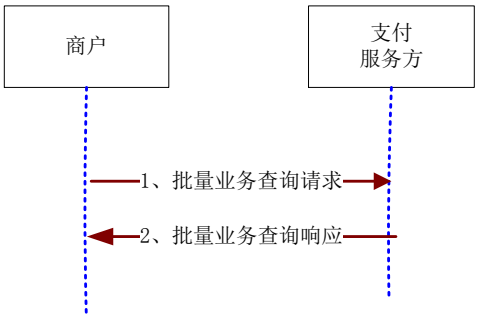
图B.12　批量查询交易模型

B.2.5.2.2　交易流程

批量查询交易流程如下：
a）　商户发起查询按照时间区间查询一批业务记录状态的请求；
b）　支付服务方按照时间区间、时间区间类型（支付时间区间或订单时间区间）检索满足条件的支付状态，返回给商户。

B.2.5.2.3　信息交互过程

批量查询的信息交互过程见图B.13。



图B.13　批量查询信息交互过程

1）　商户向支付服务方发起批量业务查询请求；
2）　支付服务方向商户回应批量业务查询响应。

B.2.5.2.4　报文

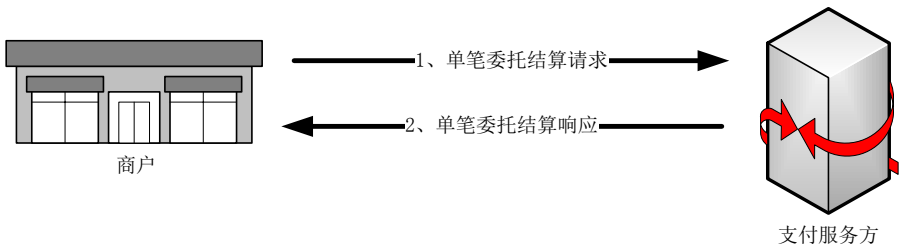
商户与支付服务方之间涉及报文：
a）　批量查询请求报文；
b）　批量查询响应报文。

B.2.6　委托结算

B.2.6.1　单笔委托结算

B.2.6.1.1　交易模型

单笔委托结算交易模型见图B.14。



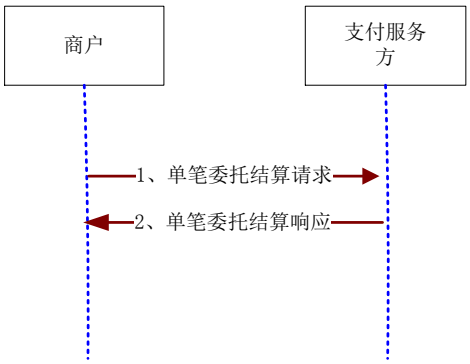
图B.14　单笔委托结算交易模型

B.2.6.1.2　交易流程

单笔委托结算交易流程如下：
a）　商户向支付服务方提交委托结算请求；
b）　支付服务方验证扣减商户的资金、把款项打给请求指定银行，并通知商户委托结算成功；

B.2.6.1.3　交互过程

单笔委托结算的信息交互过程见图B.15。



图B.15　单笔委托结算信息交互过程

1）　商户向支付服务方发送单笔委托结算请求；
2）　支付服务方返回单笔委托结算响应。

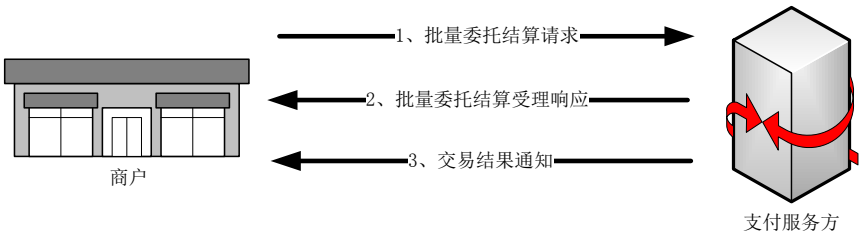
B.2.6.1.4　报文

商户与支付服务方之间涉及报文：
a）　单笔委托结算请求报文；
b）　单笔委托结算响应报文。

B.2.6.2　批量委托结算

B.2.6.2.1　交易模型

批量委托结算交易模型见图B.16。



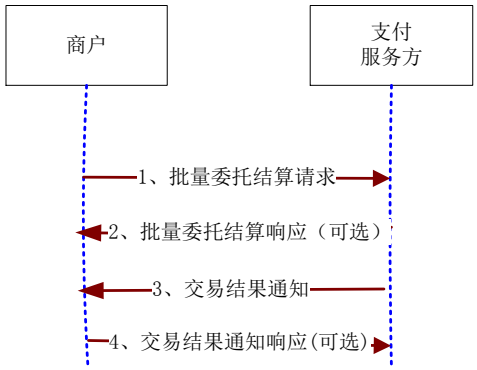
图B.16　批量委托结算交易模型

B.2.6.2.2　交易流程

批量委托结算交易流程如下：
a）　商户准备需要委托结算的账户、金额列表，向支付服务方提交委托结算请求；
b）　支付服务方验证扣减商户的资金，返回委托结算请求已受理；
c）　支付服务方完成资金转账，并返回委托结算状态。

B.2.6.2.3　信息交互过程

批量委托结算的信息交互过程见图B.17。



图B.17　批量委托结算信息交互过程

1）　商户向支付服务方发送批量委托结算请求报文；
2）　支付服务方给商户返回批量委托结算响应报文（可选）；
3）　支付服务方向商户发送交易结果通知报文；
4）　商户给支付服务方返回交易结果响应报文（可选）。

B.2.6.2.4　报文

商户与支付服务方之间涉及报文：

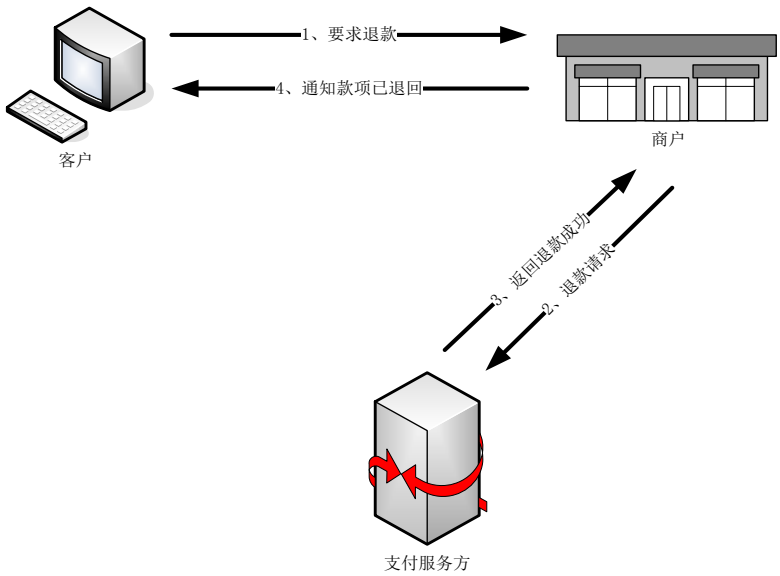
a）　批量委托结算请求报文；
b）　批量委托结算响应报文；
c）　批量委托结算结果通知报文；
d）　批量委托结算结果通知响应报文。

B.2.7　退款

B.2.7.1　单笔退款

B.2.7.1.1　交易模型

单笔退款交易模型见图B.18。



图B.18　单笔退款交易模型

B.2.7.1.2　交易流程

单笔退款交易流程如下：

a)　客户要求退款；

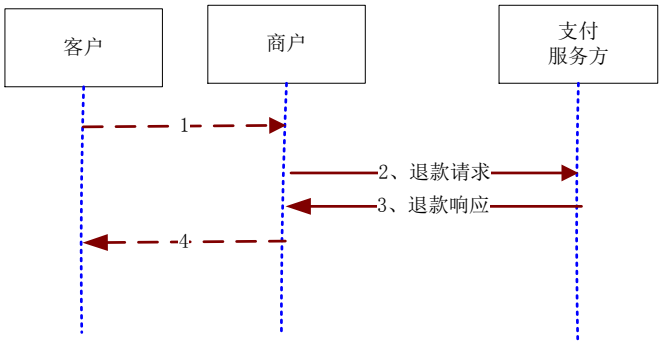
b)　商户同意客户退款，收到退回的货物后，生成退款请求，并送给支付服务方；

c)　支付服务方返回商户退款成功信息；

d)　商户通过电子邮件、电话等方式通知客户款项已退回客户账户。

B.2.7.1.3　信息交互过程

单笔退款的信息交互过程见图B.19。



图B.19　单笔退款信息交互过程

1)　客户向商户提出退款要求；

2)　商户录入退款信息，并向支付服务方发送退款请求报文；

3)　返回商户退款成功信息；

4)　商户通知客户退款成功。

B.2.7.1.4　报文

商户与支付服务方之间涉及报文：

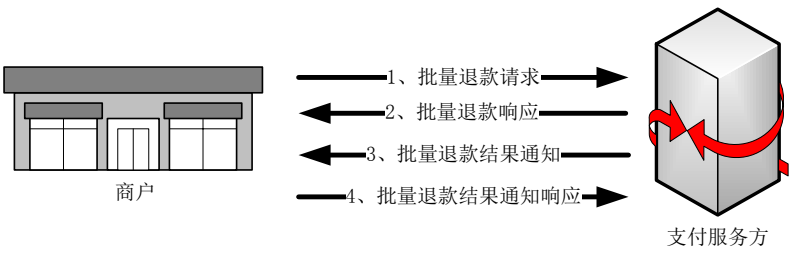
a)　单笔退款请求报文；

b)　单笔退款响应报文。

B.2.7.2　批量退款

B.2.7.2.1　交易模型

批量退款交易模型见图B.20。



图B.20　批量退款交易模型

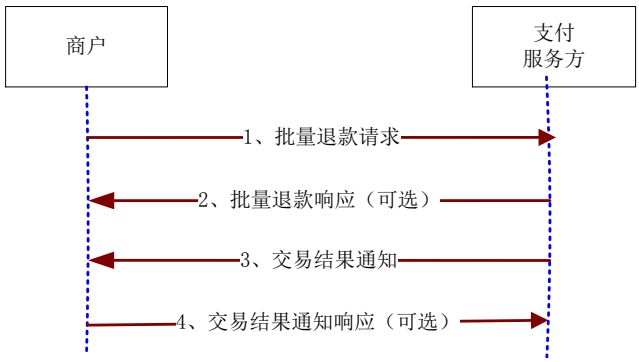
B.2.7.2.2　交易流程

批量退款交易流程如下：

a)　商户生成批量退款请求送给支付服务方；
b)　支付服务方向商户发送批量退款响应；
c)　支付服务方返回商户退款成功信息；
d)　商户向支付服务方发送批量退款结果通知响应，同时通过电子邮件、电话等方式通知客户款项已退回客户账户。

B.2.7.2.3　信息交互过程

批量退款的信息交互过程见图B.21。



图B.21　批量退款信息交互过程

1)　商户汇集一笔或多笔客户退款申请，向支付服务方发起批量退款请求；
2)　支付服务方返回批量退款响应（可选）；
3)　支付服务方向商户发送交易结果通知报文；
4)　商户返回交易结果响应报文（可选）。

B.2.7.2.4　报文

商户与支付服务方之间涉及报文：

a)　批量退款请求报文；
b)　批量退款响应报文；
c)　批量退款结果通知报文；
d)　批量退款结果通知响应报文。

附 录 C
（规范性附录）
基于 Internet 网上支付的文件数据格式

C.1 对账文件

成功的交易参加当日的对账，商户根据自己的业务从支付服务方获取文件，该文件如实反映了纳入当日清算的支付类、委托结算类、退款类与签约/解约类交易的关键信息，供商户核对。

交易对账文件包括如下几个业务信息：

——支付类交易明细：包括一般支付、担保支付、协议支付、预授权支付。成功的支付类交易参加当日的清算，该部分数据反映了纳入当日清算的支付类交易的关键信息，供商户核对；

——委托结算类交易明细：包括单笔委托结算、批量委托结算。成功的委托结算类交易参加当日的清算，该部分数据反映了纳入当日清算的支付类交易的关键信息，供商户核对；

——退款类交易明细：包括单笔退款、批量退款。成功的委托结算类交易参加当日的清算，该部分数据反映了纳入当日清算的支付类交易的关键信息，供商户核对；

——签约/解约明细：包括当日协议签约/解约的明细。

C.1.1 文件名称

文件名称由如下几部分组成：

——类型：trxdata；

——分隔符：_；

——商户编号；

——分隔符：_；

——日期：格式“CCYYMMDD”；

——分隔符：_；

——顺序号；

——后缀：.dat。

C.1.2 记录格式

本部分中仅给出交易对账至少应包括的交易信息见表C.1所示。参与交易的各方可根据实际需要增加其它辅助信息。

表 C.1 交易记录格式

中文名称	标识符	数据格式	值域	说明	备注
接口版本号	Version	anMAX(15)	无	文件格式版本号。	
商户编号	MerchantID	ansMAX(35)	无	商户在支付服务方注册时，支付服务方分配给商户的编号。	
签名方式	SignType	ansMax(8)	无	文件的签名方式。	

中文名称	标识符	数据格式	值域	说明	备注
【支付记录 – 开始】	PaymentList			支付类业务记录列表。	
记录数	RecordCount	nMAX(6)	无	支付的笔数。	
汇总金额	TotalAmount	nMAX(16)	无	支付的汇总金额。	
【支付明细 – 记录循环开始】	PaymentDetail			支付类业务一个记录的标识，允许重复。	
交易码	TrxCode	n2	无	标识一笔交易的交易类型的代码。	
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	商户提交交易请求的日期时间。	
交易币种	TrxCurrencyCode	a3	无	交易的币种代码，见 GB/T 12406。	
交易金额	TrxAmount	nMAX(16)	无	交易的金额，最小单位为分。例如 123.45 表示为 12345。	
付款方手续费	PayerFee	nMAX(16)	无	付款方支付的手续费。	
收款方手续费	PayeeFee	nMAX(16)	无	收款方支付的手续费。	
记账日期	AccountingDate	n8	CCYYMMDD	商户与支付服务方之间应转移资金的账务日期。	
实际交易的币种	TrxRealCurrencyCode	a3	无	实际交易的币种代码。	
实际交易金额	TrxRealAmount	nMAX(16)	无	实际发生的交易金额，最小单位为分。例如 123.45 表示为 12345。	
支付服务方流水号	TrxId	ansMAX(50)	无	用于标识商户发起的交易请求编号，在特定时间内不允许重复。	
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方支付成功的日期时间。	
授权码	ApprovalCode	anMAX(6)	无	“预授权成功”填写授权码，其他交易填空。	
商户协议号	MerchantAgreementID	nMAX(50)	无	商户用来唯一标识扣款协议的编号。	
支付服务方协议号	AgreementID	nMAX(50)	无	支付服务方用来唯一标识扣款协议的编号。	

中文名称	标识符	数据格式	值域	说明	备注
【支付明细 - 记录循环结束】					
【支付记录 – 结束】					
【委托结算记录 – 开始】	TransferList			委托结算类业务记录列表。	
记录数	RecordCount	nMAX(6)	无	委托结算的笔数。	
汇总金额	TotalAmount	nMAX(16)	无	委托结算的汇总金额。	
【委托结算明细 – 记录循环开始】	TransferDetail			委托结算业务一个记录的标识，允许重复。	
记录序号	SeqNo	nMAX(6)	无	委托结算交易的记录序号。	
交易码	TrxCode	n2	无	标识一笔交易的交易类型的代码。	
商户交易流水号	RequestID	ansMAX(50)	无	商户委托结算交易的请求号。	
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	商户委托结算交易的请求日期时间。	
交易币种	TrxCurrencyCode	a3	无	委托结算币种。	
交易金额	TrxAmount	nMAX(16)	无	委托结算金额。	
收款方账号	PayeeAccountID	nMAX(34)	无	委托结算收款方的账号。	
收款方名称	PayeeName	mMAX(50)	无	收款方的姓名。	
付款方手续费	PayerFee	nMAX(16)	无	付款方支付的手续费。	
收款方手续费	PayeeFee	nMAX(16)	无	收款方支付的手续费。	
记账日期	AccountingDate	n8	CCYYMMDD	商户与支付服务方之间应转移资金的账务日期。	
支付服务方流水号	TrxId	anMAX(60)	无	支付服务方产生的交易流水号。	
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方支付成功的日期时间。	
【委托结算明细 - 记录循环结束】					
【委托结算记录 – 结束】					
【退款记录 – 开始】	RefundList			退款类业务记录列表。	

中文名称	标识符	数据格式	值域	说明	备注
记录数	RecordCount	nMAX(6)	无	批量退款笔数。	
汇总金额	TotalAmount	nMAX(16)	无	批量退款的总金额，应和退款明细的累计金额一致。	
【退款明细 – 记录循环开始】	RefundDetail			一个记录的标识，允许重复。	
记录序号	SeqNo	nMAX(6)	无	退款记录序号。	
交易码	TrxCode	n2	无	标识一笔交易的交易类型的代码。	
商户交易流水号	RequestID	ansMAX(50)	无	退款的交易请求号。	
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	退款的交易请求日期时间。	
交易币种	TrxCurrencyCode			退款的币种。	
交易金额	TrxAmount	nMAX(16)	无	退款的金额。	
记账日期	AccountingDate	n8	CCYYMMDD	退款交易的记账日期。	
支付服务方流水号	TrxId	anMAX(60)	无	原交易的支付服务方流水号。	
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方支付成功的日期时间(针对退款批次本身的)。	
原记账日期	OrigAccountingDate	n8	CCYYMMDD	原交易的记账日期。	
原交易日期时间	OrigTrxDateTime	n14	CCYYMMDDhhmmss	原交易的交易日期时间。	
原支付服务方流水号	OrigTrxId	anMAX(60)	无	原交易的支付服务方流水号。	
原请求日期时间	OrigRequestDateTime	n14	CCYYMMDDhhmmss	原交易的请求日期时间。	
原商户交易流水号	OrigRequestID	ansMAX(50)	无	商户提交的原始交易的商户交易流水号。	
原交易金额	OrigTrxAmount	nMAX(16)	无	原始交易的金额。	
【退款明细 - 记录循环结束】					
【退款记录 – 结束】					
【签约/解约记录 – 开始】	AgreementList			签约/解约类记录列表。	
记录数	RecordCount	nMAX(6)	无	签约/解约的记录数。	

中文名称	标识符	数据格式	值域	说明	备注
【签约/解约明细 – 记录循环开始】	AgreementDetail			签约/解约业务一个记录的标识，允许重复。	
交易码	TrxCode	n2	无	标识一笔交易的交易类型的代码。	
商户交易流水号	RequestID	ansMAX(50)	无	签约/解约的交易请求号。	
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	签约/解约请求日期时间。	
支付服务方流水号	TrxID	anMAX(60)	无	支付服务方产生的交易流水号。	
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方签约/解约成功的日期时间。	
签约/解约标志	AgreementFlag	n1	0～1	签约/解约的标志： 0 – 解约； 1 – 签约。	
商户协议号	MerchantAgreementID	nMAX(50)	无	商户用来唯一标识扣款协议的编号。	
客户标识	CustomerID	mMAX(20)	无	签约客户编号，如电话号码，手机号码等。	
协议业务类型	AgreementType	mMAX(60)	无	协议的业务种类，由支付平台约定。	
【签约/解约明细 - 记录循环结束】					
【签约/解约记录 – 结束】					
签名信息	Sign	ansMAX(2048)	无	除自身外所有数据的签名。	

C.2 批量退款

C.2.1 请求文件

C.2.1.1 文件名称

文件名称由如下几部分组成：

——类型：batchrefundreq；

——分隔符：_；

——商户编号；

——分隔符：_；

——日期：格式“CCYYMMDD”；

——分隔符：_；

——顺序号；

——后缀：.dat。

C.2.1.2 记录格式

本部分中仅给出记录中至少应包括的交易信息见表C.2。参与交易的各方可根据实际需要增加其它辅助信息。

表 C.2 批量退款请求文件记录格式

中文名称	标识符	数据格式	值域	说明	备注
接口版本号	Version	anMAX(15)	无	文件格式版本号。	
商户编号	MerchantID	ansMAX(35)	无	商户在支付服务方注册时，支付服务方分配给商户的编号。	
商户交易流水号	RequestID	ansMAX(50)	无	用于标识商户发起的交易请求的编号，在特定的时间段内不允许重复。	
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	退款的交易请求日期时间。	
记录数	RecordCount	nMAX(6)	无	批量退款记录数。	
汇总金额	TotalAmount	nMAX(16)	无	批量退款的总金额，应和退款明细的累计金额一致。	
签名方式	SignType	ansMax(8)	无	退款文件的签名方式。	
【记录循环开始】	RecordDetail			一个记录的标识，允许重复。	
记录序号	SeqNo	nMAX(6)	无	信息序列号，每个批次从“1”开始计数。	
原商户交易流水号	OrigRequestID	ansMAX(50)	无	商户的原始交易请求号。	
交易金额	TrxAmount	nMAX(16)	无	退款金额。	
原记账日期	OrigAccountingDate	n8	CCYYMMDD	原订单的记账日期。	
原交易日期时间	OrigTrxDateTime	n14	CCYYMMDDhhmmss	原支付成功的日期时间。	
原支付服务方流水号	OrigTrxId	anMAX(60)	无	原订单的支付服务方流水号。	
原请求日期时间	OrigRequestDateTime	n14	CCYYMMDDhhmmss	客户支付后商户网站产生交易请求号的日期。	
订单备注	OrderMemo	mMAX(500)	无	退款原因。	
【记录循环结束】					
签名信息	Sign	ansMAX(2048)	无	除自身外所有数据的签名。	

C.2.2 结果文件

C.2.2.1 文件名称

文件名称由如下几部分组成：

——类型：batchrefundrsp；
——分隔符：_；
——商户编号；
——分隔符：_；
——日期：格式“CCYYMMDD”；
——分隔符：_；
——顺序号；
——后缀：.dat。

C.2.2.2 记录格式

本部分中仅给出记录中至少应包括的交易信息见表C.3。参与交易的各方可根据实际需要增加其它辅助信息。

表 C.3 批量退款结果文件记录格式

中文名称	标识符	数据格式	值域	说明	备注
接口版本号	Version	anMAX(15)	无	文件格式版本号。	
商户编号	MerchantID	ansMAX(35)	无	商户在支付服务方注册时，支付服务方分配给商户的编号。	
商户交易流水号	RequestID	ansMAX(50)	无	退款的交易请求号。	
请求日期时间	RequestDateTime	n14	CCYYMMDDhhmmss	退款交易请求日期时间。	
处理状态	ProcessStatus	n1	0～1	用于表示处理服务器是否接受请求的标志： 0 – 拒绝/失败； 1 – 接受/成功。	如果失败,则没有明细文件。
支付服务方流水号	TrxId	anMAX(60)	无	支付服务方产生的交易流水号（针对退款批次本身的）。	
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	支付服务方支付成功的日期时间。	
交易错误码	TrxErrorCode	n6	无	用于表示交易结果的错误码。	
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	
记录数	RecordCount	nMAX(6)	无	批量退款记录数。	
汇总金额	TotalAmount	nMAX(16)	无	成功退款的汇总金额。	
签名方式	SignType	ansMax(8)	无	退款文件的摘要/签名方式。	
【记录循环开始】	RecordDetail			一个记录的标识，允许重复。	
记录序号	SeqNo	nMAX(6)	无	收款信息序列号，每个批次从“1”开始计数。	

中文名称	标识符	数据格式	值域	说明	备注
原记账日期	OrigAccountingDate	n8	CCYYMMDD	填写原订单的记账日期。	
原支付服务方流水号	OrigTrxId	n14	CCYYMMDDhhmmss	原订单的支付服务方流水号。	
交易状态	TrxStatus	n1	无	交易状态： 0 – 未处理； 1 – 成功； 2 – 失败； 3 – 状态未明； ……。	
交易错误码	TrxErrorCode	n6	无	用于表示交易结果错误类型的代码。	
交易结果信息	TrxResultMsg	mMAX(100)	无	用于描述交易结果的信息，可以中文或英文等。	
记账日期	AccountingDate	n8	CCYYMMDD	本退款交易的记账日期。	
支付服务方流水号	TrxId	anMAX(60)	无	本退款交易的交易流水号。	
交易日期时间	TrxDateTime	n14	CCYYMMDDhhmmss	本退款交易的日期时间。	
已退款次数	RefundCount	n2	无	用于描述一笔交易的累计退款次数。	
已退款金额	RefundAmount	nMAX(16)	无	用于描述一笔交易的累计退款金额。	
【记录循环结束】					
签名信息	Sign	ansMAX(2048)	无	除自身外所有数据的签名。	

参 考 文 献

[1] GB/T 22080-2008 信息技术 安全技术 信息安全管理体系要求
[2] GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则
[3] GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求