ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0098.6—2012

中国金融移动支付 检测规范 第6部分：业务系统

China financial mobile payment—Test specifications—
Part 6: Business system

2012-12-12 发布 2012-12-12 实施

中国人民银行 发布

目　　次

前　言

《中国金融移动支付 检测规范》标准由以下8部分构成：

——第1部分：移动终端非接触式接口；

——第2部分：安全芯片；

——第3部分：客户端软件；

——第4部分：安全单元（SE）应用管理终端；

——第5部分：安全单元（SE）嵌入式软件安全；

——第6部分：业务系统；

——第7部分：可信服务管理系统；

——第8部分：个人信息保护。

本部分为该标准的第6部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分负责起草单位：中国人民银行科技司、中国人民银行金融信息中心、中国金融电子化公司。

本部分参加起草单位：北京银联金卡科技有限公司（银行卡检测中心）、中金国盛认证中心、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）、上海市信息安全测评认证中心、信息产业信息安全测评中心、北京软件产品质量检测检验中心、中钞信用卡产业发展有限公司、上海华虹集成电路有限责任公司、上海复旦微电子股份有限公司、东信和平智能卡股份有限公司、大唐微电子技术有限公司、武汉天喻信息产业股份有限公司、恩智浦半导体有限公司。

本部分主要起草人：李晓枫、陆书春、潘润红、杜宁、李兴锋、张雯华、刘力慷、刘志刚、聂丽琴、李晓、尚可、郭栋、熊文韬、宋铮、李宏达、王冠华、胡一鸣、张晓、平庆瑞、张志茂、陈君、彭美玲、李微、陈吉、程恒。

引　言

随着移动支付新业务、新产品、新管理模式的不断涌现，以客户需求为主导的移动支付业务出现了不断交融和细化的趋势，不同机构、不同部门、不同业务之间的信息交换和信息共享变得越来越频繁。移动支付业务系统检测规范的制定可以有效加强银行、非金融支付服务组织、商户之间的互联、互通及信息共享，降低交易成本，提高市场效率。

本部分对移动支付业务系统的功能、性能、安全性、风险监控、文档审核、外包和机构入网七个检测类进行了检测规定。对于新增需求，将在标准后续的修订过程中逐步纳入。

中国金融移动支付　检测规范　第6部分：业务系统

1　范围

本部分规定了移动支付业务系统的检测内容和判定准则，包括业务系统的功能、性能、安全性、风险监控、文档审核、外包管理和机构入网七个检测类的检测要求、操作规程及判定准则。

本部分适用于指导检测机构制定移动支付业务系统和机构入网的技术标准符合性、安全性检测方案、执行检测以及检测结果符合性判定。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239　信息安全技术 信息系统安全等级保护基本要求

JR/T 0025.7　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

3　术语和定义

下列术语和定义适用于本文件。

3.1

用户　user

通过移动终端发起移动支付的使用者。

3.2

商户　merchant

为用户提供商品或服务内容的主体。

3.3

系统用户数　user counts

系统中所有能够参与远程支付业务的有效用户总数。（单位：个）

3.4

在线用户数　online user counts

系统中的会话用户数。

3.5

并发用户数　concurrent user counts

系统中在正常业务情况下，同一时间发起业务请求的用户数。（单位：个）

3.6

极限检测　limit test

系统的最大处理能力的测试过程或者验证过程。

3.7

系统最大并发用户数 maximum concurrent user counts

系统中在不出现业务处理失败的情况下，能够支持的最大并发用户数。（单位：个）

3.8

业务吞吐量 transaction throughput

系统单位时间内处理的请求数量。（单位：transaction/s）

4 总则

4.1 检测目标

检测目标是在系统版本确定的基础上，对移动支付业务系统功能、性能、安全性、风险监控、文档、外包和联网联合七项检测类进行检测，客观、公正评估系统是否符合中国人民银行对移动支付业务系统的技术标准符合性和安全性要求，保障我国移动支付业务设施的安全稳定运行。

4.2 启动准则

a) 机构提交的业务系统被测版本与生产版本一致；
b) 机构业务系统内部测试进行完毕；
c) 系统需求说明书、系统设计说明书、用户手册、安装手册等相关文档准备完毕；
d) 检测环境准备完毕，具体包括：
   1) 检测环境与生产环境一致或者基本一致，其中网络安全性、主机安全性、数据安全性和运维安全性检测尽量在生产环境下进行；
   2) 业务系统被测版本及其他相关外围系统和设备已完成部署并配置正确；
   3) 用于功能和性能检测的基础数据准备完毕；
   4) 检测用机到位，系统及软件安装完毕；
   5) 检测环境网络配置正确，连接通畅，可以满足检测需求。

4.3 检测相关规定

a) 检测相关操作规定见附录 A。
b) 检测相关判定准则见附录 B。

5 检测项列表

5.1 功能检测项

验证移动支付业务系统的业务功能的正确性，测试系统业务处理的准确性。功能性检测项如表1所示。

表1　功能性检测项列表

编号	检测项			检测项说明
1.1	用户管理		用户信息登记及管理	必测项
			终端设备关联	
			用户审核	必测项
1.2	商户管理		商户信息登记及管理	必测项
			终端设备关联	
			商户信息审核	必测项
			商户证书管理	
1.3	用户账户管理		用户支付账户管理	必测项
			用户支付账户管理审核	
			用户支付账户资金审核	必测项
			用户支付账户充值	必测项
			用户支付账户查询	
			记账、调账	
1.4	商户账户管理		商户账户管理	必测项
			商户账户信息审核	
			商户账户资金审核	必测项
			商户账户查询	必测项
1.5	远程交易处理(适用于远程支付交易，近场支付不适用)	一般支付交易处理	账户查询交易	一般支付必测项
			消费交易	一般支付必测项
			转账交易	一般支付必测项
			空中圈存	一般支付必测项
			脚本处理结果通知	
		短信支付交易处理	建立委托关系	短信支付必测项
			撤销委托关系	短信支付必测项
			消费交易	短信支付必测项
			查询交易	短信支付必测项
1.6	近场交易处理(适用于近场支付交易，远程支付不适用)	联机交易	余额查询	联机交易必测项
			取现	
			存款	
			转账	联机交易必测项
			消费	联机交易必测项
			消费撤销	
			预授权	
			预授权撤销	
			预授权完成	
			预授权完成撤销	
			退货	联机交易必测项
		线下交易	指定账户圈存	

编号	检测项				检测项说明
				非指定账户圈存	
				现金圈存	
				圈提	
			线上交易	指定账户圈存	
				非指定账户圈存	
				SE 参数设置	
		脱机交易		脱机消费	脱机交易必测项
				余额查询	脱机交易必测项
		移动终端交易		账号选择	必测项
				账户列表信息查询	必测项
				账户信息查询	必测项
				余额查询	
		异常处理		冲正交易	必测项
				异常交易确认	必测项
				异常处理存储转发机制	必测项

5.2 性能检测项

验证系统是否满足未来三年业务运行的性能需求。检测内容包括时间特性和资源利用性两方面。性能检测项如表2所示。

表2 性能检测项列表

编号	检测项		检测项说明
2.1	时间特性	支付类业务	必测项
		查询类业务	必测项
2.2	资源利用性	检测过程中服务器资源占用情况	必测项
		压力解除后服务器资源释放情况	必测项

5.3 安全性检测项

5.3.1 物理安全

物理安全检测项如表3所示。

表3 物理安全检测项列表

编号	检测项		检测项说明
3.1.1	物理位置选择	机房和办公场地所在建筑物选择	必测项
		建筑物内机房位置选择	必测项
3.1.2	物理访问控制	机房设置电子门禁系统	必测项
		来访人员申请和审批	必测项
		对机房划分区域进行管理	必测项
		重要区域设置第二道电子门禁系统	必测项
3.1.3	防盗窃和防破坏	设备放置	必测项

编号	检测项		检测项说明
		设备固定	必测项
		通信线缆铺设	必测项
		介质保管	必测项
		机房防盗报警系统	必测项
		机房监控报警系统	必测项
3.1.4	防雷击	安装避雷装置	必测项
		安装防雷保安器	必测项
		交流电源地线	必测项
3.1.5	防火	设置火灾自动消防系统	必测项
		机房应采用耐火的建筑材料	必测项
		采用区域隔离防火措施	必测项
3.1.6	防水和防潮	水管安装要求	必测项
		防雨水措施	必测项
		防水检测和报警	必测项
3.1.7	防静电	接地防静电措施	必测项
		采用防静电地板	必测项
		安装静电消除器等装置（增强要求）	
3.1.8	温湿度控制	机房温湿度自动调节设施	必测项
3.1.9	电力供应	供电线路防护设备配置	必测项
		备用电力供应	必测项
		冗余或并行的电力电缆线路设置	必测项
		备用供电系统	必测项
3.1.10	电磁防护	防止电磁干扰	必测项
		电源线和通信线缆隔离铺设	必测项
		关键区域实施电磁屏蔽（增强要求）	

5.3.2 网络安全

网络安全检测项如表4所示。

表4 网络安全检测项列表

编号	检测项		检测项说明
3.2.1	结构安全	主要设备网络冗余	必测项
		设备网络冗余（增强要求）	
		网络安全路由器	必测项
		网络安全防火墙	必测项
		网络拓扑结构	必测项
		IP 子网划分	必测项
		QoS 保证	必测项
3.2.2	访问控制	网络域安全隔离和限制	必测项
		地址转换和绑定	必测项

编号	检测项		检测项说明
		内容过滤（增强要求）	
		访问控制	必测项
		流量控制	必测项
		会话控制	必测项
		远程拨号访问控制	必测项
3.2.3	安全审计	日志信息	必测项
		网络对象操作审计	必测项
		日志权限和保护	必测项
		审计跟踪极限（增强要求）	
		集中审计（增强要求）	
3.2.4	边界完整性检查	内外网非法连接阻断和定位	必测项
3.2.5	入侵防范	网络 ARP 欺骗攻击	必测项
		信息窃取	必测项
		DOS/DDOS 攻击	必测项
		网络入侵防范机制	必测项
3.2.6	恶意代码防范	恶意代码防范措施	必测项
		定时更新	必测项
3.2.7	网络设备防护	设备用户身份鉴别	必测项
		主要设备用户身份鉴别（增强要求）	
		身份鉴别信息（增强要求）	
		设备登录口令安全性	必测项
		登录地址限制	必测项
		登录失败处理	必测项
		远程管理安全	必测项
		权限分离	必测项
3.2.8	网络安全管理	网络日常维护	必测项
		网络安全管理制度	必测项
		定期补丁安装	必测项
		漏洞扫描	必测项
		设备最小服务配置	必测项
		外部连接的授权和批准	必测项
		控制移动设备的网络接入	必测项
		定期检查违规行为	必测项

5.3.3 主机安全

主机安全检测项如表5所示。

表5 主机安全检测项列表

编号	检测项		检测项说明
3.3.1	身份鉴别	用户身份标识和鉴别	必测项

编号	检测项		检测项说明
		密码口令复杂度设置及定期更换	必测项
		登录失败处理	必测项
		远程管理的传输模式	必测项
		用户名的唯一性	必测项
		用户身份组合鉴别技术	必测项
		鉴别警示信息设置（增强要求）	
		不可伪造的用户身份组合鉴别技术（增强要求）	
3.3.2	访问控制	访问控制功能	必测项
		管理用户的角色分配权限	必测项
		操作系统和数据库系统特权用户的权限分离	必测项
		严格限制默认账户的访问权限	必测项
		多余、过期账户删除	必测项
		重要信息资源敏感标记设置	必测项
		对有敏感标记信息资源的访问控制	必测项
3.3.3	安全审计	审计范围	必测项
		审计的事件	必测项
		审计记录格式	必测项
		审计报表生成	必测项
		审计进程保护	必测项
		审计记录保护	必测项
		集中审计（增强要求）	
3.3.4	剩余信息保护	鉴别信息清除（增强要求）	
		文件、目录、数据库记录等的清空（增强要求）	
3.3.5	入侵防范	入侵行为的记录和报警	必测项
		重要程序的完整性保护	必测项
		最小安装原则	必测项
3.3.6	恶意代码防范	防恶意代码软件	必测项
		恶意代码库	必测项
		防恶意代码软件的统一管理	必测项
3.3.7	资源控制	接入控制	必测项
		超时锁定	必测项
		主机资源监控	必测项
		单个用户资源使用限度控制	必测项
		系统服务水平监控和报警	必测项
		无用的过期信息、文档完整清除	必测项
3.3.8	可信路径	身份鉴别时安全的信息传输路径（增强要求）	
		系统访问时安全的信息传输路径（增强要求）	
3.3.9	系统安全管理	访问控制策略	必测项
		系统漏洞扫描	必测项
		系统补丁	必测项

编号	检测项		检测项说明
		系统安全管理制度	必测项
		系统管理员权限	必测项
		操作日志管理	必测项

5.3.4 应用安全

应用安全检测项如表6所示。

表6 应用安全检测项列表

编号	检测项		检测项说明
3.4.1	身份鉴别	用户身份标识和鉴别	必测项
		用户身份组合鉴别技术	必测项
		身份标识唯一性和复杂度检查	必测项
		登录失败处理	必测项
		不可伪造的用户身份组合鉴别技术（增强要求）	
3.4.2	访问控制	访问控制策略	必测项
		访问控制覆盖范围	必测项
		授权主体配置访问控制策略	必测项
		管理用户角色权限分配	必测项
		敏感标记设置（增强要求）	
		对有敏感标记信息资源的访问控制（增强要求）	
		禁止默认帐户访问（增强要求）	
3.4.3	可信路径	身份鉴别的安全信息传输路径	必测项
		资源访问的安全信息传输路径	必测项
3.4.4	安全审计	审计范围	必测项
		审计的事件	必测项
		审计记录格式	必测项
		审计报表生成	必测项
		集中审计接口（增强要求）	
3.4.5	剩余信息保护	鉴别信息清除（增强要求）	
		文件、目录、数据库记录等的清空（增强要求）	
3.4.6	通信完整性	采用密码技术保证完整性（增强要求）	
3.4.7	通信保密性	会话初始化验证	必测项
		通信过程中加密	必测项
		进行加解密运算和密钥管理（增强要求）	必测项
3.4.8	抗抵赖	数据原发证据	必测项
		数据接收证据	必测项
3.4.9	软件容错	数据有效性验证	必测项
		自动保护	必测项
		自动恢复（增强要求）	
3.4.10	资源控制	自动结束会话	必测项

编号	检测项		检测项说明
		最大并发会话连接数限制	必测项
		多重并发会话限制	必测项
		时间段内并发会话控制	必测项
		限额分配（增强要求）	
		系统服务水平最小值检测报警	必测项
		服务优先级设定（增强要求）	
3.4.11	交易数据签名	交易关键要素数据签名	必测项
		交易数据签名验证	必测项
3.4.12	会话安全	会话标识唯一性	必测项
		防未经授权访问	必测项
		会话超时时间设置	必测项
		及时清除会话信息	必测项
		防止会话令牌窃取	必测项
		应用审计日志（增强要求）	
3.4.13	常见攻击防范	服务器端数据有效性检查	必测项
		防暴力破解静态密码	必测项
		代码审查	必测项
		开发安全接口	必测项
		防范服务器端拒绝服务攻击	必测项
		文件上传下载访问控制	必测项
		数据库使用存储过程或参数化查询（增强要求）	
		应用程序检查（增强要求）	
		客户端安全控件（增强要求）	
3.4.14	交易处理	支付风险提示	必测项
		终端反馈支付结果到用户	必测项
		账户管理机构通知支付结果	必测项
		支付机构通知支付结果	必测项
3.4.15	报文安全	防重放攻击	必测项
		交易唯一性	必测项
		交易报文完整性检查	必测项
		防重复支付	必测项
		高风险业务数据签名	必测项
		敏感信息保护	必测项
		近场支付报文安全	
3.4.16	短信处理	短信数据存储区域访问控制	必测项
		短信通信安全通道	必测项
		短信报文传输保护	必测项
		委托类交易身份鉴别	必测项
		短信安全提示	必测项

5.3.5 数据安全

数据安全检测项如表7所示。

表7　数据安全检测项列表

编号	检测项		检测项说明
3.5.1	数据完整性	传输过程数据完整性	必测项
		存储过程数据完整性	必测项
3.5.2	数据保密性	数据加密传输	必测项
		数据加密存储	必测项
3.5.3	备份和恢复	本地备份和恢复	必测项
		异地备份	必测项
		交易数据保存时间	必测项
		关键链路冗余设计	必测项
		业务应用无缝切换（增强要求）	
3.5.4	密码算法	对称加密算法	必测项
		非对称加密算法	必测项
		摘要算法	必测项
		近场支付密码算法	近场支付必测项
	数据认证	远程支付服务器认证	必测项
		远程支付用户认证	必测项
		近场支付脱机数据认证	近场支付脱机交易必测项
		近场支付应用密文和发卡行认证	
3.5.7	密钥管理	密钥管理要求	必测项

5.3.6　管理安全

管理安全检测项如表8所示。

表8　管理安全检测项列表

编号	检测项		检测项说明
3.6.1	组织机构	安全管理架构	必测项
		部门和人员职责	必测项
		信息安全相关部门人员职责	必测项
		部门设置	必测项
		支付服务相关部门职责	必测项
		风险管理架构	必测项
3.6.2	管理制度	建立管理制度体系	必测项
		建立贯穿业务系统的过程	必测项
		安全管理制度审计	必测项
3.6.3	安全策略	制订安全保障目标	必测项
		制订安全策略	必测项
		维护资产清单	必测项

编号	检测项		检测项说明
		风险定义与规避	必测项
		安全级别定义与保护措施制订（增强要求）	
3.6.4	人员和文档管理	信息安全管理岗位	必测项
		涉密岗位安全	必测项
		关键岗位人员后备措施	必测项
		员工岗位调动或离职	必测项
		外来人员管理制度	必测项
		文档管理制度	必测项

5.3.7 运行维护安全

运行维护检测项如表9所示。

表9 运行维护安全检测项列表

编号	检测项		检测项说明
3.7.1	环境管理	机房基本设施定期维护	必测项
		机房的出入管理制度化和文档化	必测项
		办公环境的保密性措施	必测项
		机房安全管理制度	必测项
		机房进出登记表	必测项
3.7.2	资产管理	资产清单	必测项
		资产安全管理制度	必测项
		资产标识	必测项
		资产信息规范化管理	必测项
3.7.3	介质管理	介质的使用管理文档化	必测项
		介质的存放环境保护措施	必测项
		介质管理记录	必测项
		介质的维修与销毁	必测项
		介质异地存储	必测项
		介质的分类与标识	必测项
3.7.4	设备管理	设施、设备定期维护	必测项
		设备选型、采购、发放等的审批控制	必测项
		设备维护管理制度	必测项
		设备的操作规程	必测项
		设备外带管理	必测项
3.7.5	监控管理	主要设备指标监控	必测项
		异常处理机制	必测项
		安全管理中心	必测项
3.7.6	密码管理	密码使用管理制度	必测项
3.7.7	变更管理	变更方案	必测项
		变更制度化管理	必测项

编号	检测项		检测项说明
		重要系统变更的批准	必测项
		变更中止与变更恢复	必测项
3.7.8	备份与恢复管理	定期备份	必测项
		备份与恢复管理制度	必测项
		数据的备份策略和恢复策略	必测项
		备份恢复过程记录	必测项
		定期检查备份介质有效性	必测项
3.7.9	安全事件处置	安全事件报告和处置	必测项
		安全事件的分类和分级	必测项
		安全事件记录和采取的措施	必测项
3.7.10	应急预案管理	制定不同事件的应急预案	必测项
		应急预案资源保障	必测项
		相关人员应急预案培训	必测项
		定期演练	必测项
		应急预案定期审查	必测项

5.3.8 业务连续性

业务连续性检测项如表10所示。

表10 业务连续性检测项列表

编号	检测项		检测项说明
3.8.1	业务连续性需求分析	业务中断影响分析	必测项
		灾难恢复时间目标和恢复点目标	必测项
3.8.2	业务连续性技术环境	备份机房	必测项
		网络双链路	必测项
		网络设备和服务器备份	必测项
		远程数据库备份	必测项
3.8.3	业务连续性管理	业务连续性管理制度	必测项
		应急响应流程	必测项
		恢复预案	必测项
		数据备份和恢复制度	必测项
3.8.4	日常维护	业务连续性演练	必测项
		定期业务连续性培训	必测项

5.4 风险监控检测项

验证支付服务业务系统的账户及交易风险，检测项如表11所示。

表11 风险监控检测项列表

编号	检测项		检测项说明
4.1	账户风险管理	账户信息管理	必测项

编号	检测项		检测项说明
		通过信息系统管理账户	必测项
		账户变更	必测项
		账户交易限额设置	必测项
		商户风险评估	必测项
		商户风险评级（增强要求）	
		大额消费商户交易监控	近场支付必测项
		账户余额上限	必测项
		单笔充值上限	
		单笔消费上限	必测项
		单日单月累计消费上限	必测项
		单日累计消费次数限制	必测项
		单日单月圈存/充值上限	近场支付脱机交易必测项
4.2	身份认证	双因素身份认证	必测项
		企业账户认证	必测项
4.3	交易过程监控	支付请求信息记录	必测项
		支付结果信息记录	必测项
		交易信息一致性检查	必测项
		退款处理	必测项
4.4	交易查询	交易查询权限	必测项
		查询结果屏蔽	必测项
		当日交易查询	必测项
		历史交易查询	必测项
4.5	交易监控	交易监控系统	必测项
		风险交易模型	必测项
		风险分析与处理	必测项
		黑名单	必测项
4.6	客户教育	安全风险提示	必测项
		操作风险提示	必测项
		功能演示与风险业务操作手册（增强要求）	
4.7	近场支付受理终端风险管理	终端安全检测报告	近场支付必测项
		密码键盘安全检测报告	近场支付必测项
		受理终端管理流程	近场支付必测项
		受理终端的安装与登记	近场支付必测项
		受理终端监控	近场支付必测项
4.8	近场支付交易风险管理	联机交易 ARQC/ARPC 验证	近场支付联机交易必测项
		联机报文 MAC 验证	近场支付联机交易必测项
		脱机交易 TAC 验证	近场支付脱机交易

编号	检测项		检测项说明
			必测项
		脱机交易 MAC 验证	近场支付脱机交易必测项
		SE 账户状态控制	近场支付必测项
		密码错误情况下的交易请求	近场支付必测项
		非法主账号交易	近场支付必测项

5.5 文档检测项

对支付服务业务系统的用户文档、开发文档、管理文档的完备性、一致性、正确性、规范性，以及是否符合行业标准，是否遵从更新控制和配置管理的要求等方面进行检测，检测项如表12所示。

表12 文档检测项列表

编号	检测项		检测项说明
5.1	用户文档	用户手册	必测项
		操作手册	必测项
5.2	开发文档	需求说明书	必测项
		需求分析文档	必测项
		总体设计方案	必测项
		数据库设计方案	必测项
		概要设计文档	必测项
		详细设计文档	必测项
		工程实施方案	必测项
5.3	管理文档	测试报告	必测项
		系统运维手册	必测项
		系统应急手册	必测项
		运维管理制度	必测项
		安全管理制度	必测项
		安全审计报告	必测项

5.6 外包管理检测项

外包检测项如表13所示。

表13 外包管理检测项

编号	检测项		检测项说明
6.1	外包管理	外包合法化	外包必测项
		风险评估	外包必测项
		资质评估	外包必测项
		外包合同签订	外包必测项
		制定保密协议	外包必测项
		服务提供符合规范要求	外包必测项
		制定控制制度、事件报告程序和应急计划	外包必测项

编号	检测项		检测项说明
		制定外包交付清单	外包必测项
		制定专人管理和监督外包服务	外包必测项

5.7 机构入网检测项

机构入网检测项如表14所示。

表14 机构入网检测项列表

编号	检测项			检测项说明
7.1	通讯接口	通讯协议	入网机构与转接清算系统之间的一个连接应由本地 IP 地址、端口号和远程 IP 地址、端口号唯一确定	必测项
			IP 地址和端口号配置	必测项
			联机交易的连接数目和方式	必测项
			文件传输的连接数目和方式	必测项
			通信接口传输数据不应包含特殊字符和控制字符	必测项
			通信接口不应影响业务流程	必测项
			联机交易建立连接、数据传输、关闭连接的方式	必测项
			应提供超时控制	必测项
			报文数据的最大长度	必测项
			空闲连接处理方式	必测项
			文件传输建立连接、关闭连接的方式	必测项
		网络接口	采用几条主干链路接入银行卡网络	必测项
			有几条备份线路	必测项
7.2	交易处理	近场支付联机交易	余额查询	必测项
			取现	必测项
			存款	必测项
			存款撤销	必测项
			转账	必测项
			消费	必测项
			消费撤销	必测项
			预授权	必测项
			预授权撤销	必测项
			预授权追加	必测项
			预授权完成（请求）	必测项
			预授权完成（通知）	必测项
			预授权完成撤销	必测项
			退款（退货）	必测项
			指定账户圈存	必测项
			非指定账户圈存	必测项
			现金圈存	必测项
			圈提	必测项

编号	检测项			检测项说明
			脚本处理结果通知	必测项
			建立委托	必测项
			解除委托	必测项
			账户验证	必测项
			账户基本能信息查询	必测项
		远程支付联机交易	余额查询	必测项
			转账	必测项
			消费	必测项
			指定账户圈存	必测项
			非指定账户圈存	必测项
			脚本处理结果通知	必测项
			建立委托	必测项
			解除委托	必测项
			账户验证	必测项
			账户基本信息查询	必测项
			充值	必测项
		异常处理	冲正处理	必测项
			确认处理	必测项
		脱机交易	脱机消费	必测项
			电子现金脱机余额查询	必测项
		手工调整交易	受理方发起请求	必测项
			账户管理系统发起请求	必测项
			转接清算系统发起请求	必测项
		超时限定	联机类交易超时限定	必测项
			脱机类交易超时限定	必测项
			手工类交易超时限定	必测项
			批量交易超时限定	必测项
7.3	报文接口		报文结构	必测项
			报文头	必测项
			报文类型	必测项
			报文位图	必测项
			报文域	必测项
			关键信息域和报文的关联	必测项
			报文格式	必测项
7.4	文件接口		普通金融交易明细文件	必测项
			转账交易明细文件	必测项
			差错交易明细文件	必测项
			脱机交易明细文件	必测项
			汇总文件	必测项
			信息文件	必测项

编号	检测项			检测项说明
7.5	入网机构管理（入网要求）	制度要求	信息安全制度及支付管理制度	必测项
			相关制度专人负责	必测项
			安全制度修订	必测项
			定期对员工进行培训	必测项
			录用员工技术能力审查	必测项
			安全事件报告流程及应急处理预案	必测项
			安全弱点或威胁响应	必测项
			信息验证失败处理	必测项
			支付账户异常情况处理	必测项
			交易安全事件通知	必测项
		机房管理	监视敏感区域	必测项
			机房值班制度	必测项
			来访人员管理	必测项
			设备或存储介质登记	必测项
		网络安全要求	入网机构系统与联网通用系统连接要求	必测项
			入网机构系统与受理终端连接要求	必测项
			入网机构生产网络与其它系统网络逻辑隔离	必测项
			互联网接入审批	必测项
			路由器配置和防火墙策略相关流程	必测项
			路由器配置和防火墙策略检查	必测项
			登录用户身份鉴别	必测项
			拨号用户访问控制	
			网络定期检查	必测项
			阻止非授权用户访问敏感数据	必测项
			网络定期审计	必测项
			恶意代码检测	必测项
		主机系统安全要求	软件和系统访问控制	必测项
			关键数据传输加密	必测项
			系统安全加固	必测项
			软件补丁测试	必测项
			软件补丁管理制度和流程	必测项
			厂商定期维护活动记录	必测项
			主机运行监控	必测项
			硬件状态	必测项
			组合技术用户身份鉴别	必测项
		应用系统安全要求	口令管理规则	必测项
			审计日志	必测项
			数据恢复撤销	必测项
			记录日志	必测项
			生产系统软硬件信息记录	必测项

编号	检测项			检测项说明
			生产系统变更操作审批实施流程	必测项
			系统运维手册	必测项
		账户信息安全和密钥管理	账户基本信息存储	必测项
			硬件加密设备	
			应用系统专用账号	必测项
			交易监控敏感数据屏蔽	必测项
		恶意代码防护	恶意代码防护管理	必测项
		运营管理要求	应用系统数据备份	必测项
			重要系统服务器双击备份	必测项
			网络设备热备份	必测项
7.6	入网商户管理	线下商户管理	线下商户管理要求	必测项
		线上商户管理	交易传输安全	必测项
			业务数据安全	必测项
			交易过程安全	必测项
7.7	入网安全	入网接入线路	入网机构专线接入	必测项
		安全管理制度	安全管理制度要求	必测项
		数据传输安全	数据传输安全控制	必测项
		密钥管理	对称加密算法	必测项
			密钥层次	必测项
			密钥产生	必测项
			密钥分发	必测项
			密钥存储	必测项
			密钥更新	必测项
			密钥销毁	必测项
		报文加密	PIN 传输	必测项
			联机报文 MAC 计算	必测项
			新旧密钥切换	必测项
		关键信息保护	系统传输关键信息保护	必测项

6 功能检测内容

6.1 用户管理

6.1.1 用户信息登记及管理

应实现用户注册、用户信息的编辑等功能。

6.1.2 终端设备关联

应实现将用户账户与移动终端设备相关联的功能，应实现远场移动支付开通确认的功能。

6.1.3 用户审核

应实现用户注册信息的审核、确认开通等功能。

6.2 商户管理

6.2.1 商户信息登记及管理

应实现商户注册、商户信息的编辑等功能。

6.2.2 终端设备关联

应实现将商户账户与移动终端设备相关联的功能，应实现远程移动支付开通确认的功能。

6.2.3 商户信息审核

应实现商户注册信息的审核、确认开通等功能。

6.2.4 商户证书管理

应实现电子证书的申请、发放、更新、作废等服务。

6.3 用户账户管理

6.3.1 用户支付账户管理

应实现用户支付账户开户、销户、修改、状态设置等功能。

6.3.2 用户支付账户管理审核

应实现用户支付账户信息的审核、确认等服务。

6.3.3 用户支付账户资金审核

应实现当用户支付账户资金交易、结算时，进行资金的审核和确认等。

6.3.4 用户支付账户充值

应实现用户支付账户充值、确认等功能。

6.3.5 用户支付账户查询

应实现用户支付账户设置、交易信息、账户余额等信息的查询。

6.3.6 记账、调账

应实现用户支付账户的记账、调账等功能。

6.4 商户账户管理

6.4.1 商户账户管理

应实现商户账户开户、销户、修改、状态设置等功能。

6.4.2 商户账户信息审核

应实现商户账户信息的审核、确认等功能。

6.4.3 商户账户资金审核

应实现当商户账户资金交易、结算时，进行资金的审核和确认等功能。

6.4.4 商户账户查询

应实现商户账户设置、交易信息、账户余额等信息的查询功能。

6.5 远程交易处理

6.5.1 一般支付交易处理

6.5.1.1 账户查询交易

应实现对账户信息、余额、交易明细等的查询功能。

6.5.1.2 消费交易

应实现用户的支付交易的功能。

消费是指用户在支付内容平台上选购商品或服务，并确认付款的支付交易流程，具体业务可以包括：商品订购、公共事业缴费等。

6.5.1.3 转账交易

应实现不同客户支付账户之间相互转账的功能。

6.5.1.4 空中圈存

应实现用户的空中圈存的功能。

用户在移动终端上发起指令，通过无线通信网络将其在账户管理系统上的资金划转到安全芯片上的脱机账户中。

在移动支付中，通过移动互联网或移动智能卡的方式进行远程圈存交易。包括指定账户圈存和非指定账户圈存。

6.5.1.5 脚本处理结果通知

应实现交易的脚本处理结果通知的功能。

在一笔交易（账户查询交易、消费交易、圈存交易）中如果包含了账户管理系统的脚本，交易发起方需要将SE执行的脚本结果立即通知到账户管理系统。

6.5.2 短信支付交易处理

6.5.2.1 建立委托关系

应实现建立委托关系的操作。

建立委托关系交易是由用户通过特定的委托方式主动发起的，用于将本人名下的支付工具号与特定的支付终端号及用户号码之间建立绑定关系；在约定的条件范围内，受托方可以凭此绑定关系，按照约定的委托内容，协助或代替委托方完成消费或其它支付结算服务。

6.5.2.2 撤销委托关系

应实现撤销委托关系的操作。

撤销委托关系是对建立委托关系的反向操作，用于撤销或解除用户名下的支付工具号与特定的支付终端、用户号码之间的绑定关系。

6.5.2.3 消费交易

应实现用户消费交易的操作。

消费交易是指用户从移动终端通过短信发起消费请求指令来完成交易。

6.5.2.4 查询交易

应实现用户查询交易的操作。

查询交易是指用户从移动终端通过短信发起查询请求指令来完成交易。

6.6 近场交易处理

6.6.1 联机交易

6.6.1.1 线下交易

6.6.1.1.1 余额查询

应实现移动终端联机余额查询功能。

余额查询是指用户使用移动终端，通过受理终端查询指定账户余额的过程。

6.6.1.1.2 取现

应实现移动终端联机取现功能。

取现是指客户使用移动终端通过ATM和银行柜面等受理终端渠道提取或预借现金的过程。

6.6.1.1.3 存款

应实现用户的存款功能。

存款指客户通过移动终端在受理终端上发起的将货币存储到指定账户中的过程。

6.6.1.1.4 转账

应实现用户通过移动终端在同一账户管理系统和跨账户管理系统两种模式下的转账。

转账指用户通过移动终端在受理终端上发起的从付款账户划转到收款账户完成货币收付的一种货币结算方式。

6.6.1.1.5 消费

应实现移动终端联机消费功能。

存款指客户通过移动终端在受理终端上发起的将货币存储到指定账户中的过程。

6.6.1.1.6 消费撤销

应实现移动终端联机消费撤销功能。

对已成功的消费进行撤销，在结算前使用撤销交易，退还原始交易金额。撤销交易必须是对原始交易的全额撤销。

6.6.1.1.7 预授权

应实现预授权功能。

预授权交易是指用户使用移动终端通过收单系统就用户预计支付金额向发卡机构索取付款承诺的过程。

6.6.1.1.8 预授权撤销

应实现预授权撤销功能。

预授权撤销是指用户使用移动终端通过收单系统就受卡方由于各种原因对已经联机完成的成功预授权交易主动发起取消的过程。

6.6.1.1.9 预授权完成

应实现预授权完成功能。

预授权完成是指用户使用移动终端通过收单系统就预授权金额或者预授权金额一定比例内金额完成付款的流程。

6.6.1.1.10 预授权完成撤销

应实现预授权完成撤销功能。

预授权完成撤销是指用户使用移动终端，通过收单系统受理，受卡方由于各种原因对已经联机完成的成功预授权完成交易，在该笔交易清算前主动发起取消的过程。

6.6.1.1.11 退款（退货）

应实现退货功能。

退货是指用户使用移动终端通过收单系统在受卡方因商品退回或服务取消时将全额或部分已扣款项退还到用户原扣款账户的过程。

6.6.1.1.12 指定账户圈存

应实现指定账户圈存功能。

指定账户圈存是指用户使用移动终端通过圈存受理终端，将预先与电子现金绑定的借记卡或信用卡中资金（或额度）划入默认电子现金账户的过程。

6.6.1.1.13 非指定账户圈存

应实现非指定账户圈存功能。

非指定账户圈存是指用户使用移动终端通过收单系统受理将转出方账户中资金（或额度）划入电子现金的过程。

6.6.1.1.14 现金圈存

应实现现金圈存功能。

现金圈存是指用户使用移动终端通过收单系统受理将现金存入电子现金账户的过程。

6.6.1.1.15 圈提

应实现圈提的功能。

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

6.6.1.2 线上交易

6.6.1.2.1 指定账户圈存

应实现线上交易指定账户圈存功能。

本交易是指用户使用客户端，通过移动支付业务系统，将预先与电子现金绑定的指定账户中资金（或额度）划入电子现金的过程。

6.6.1.2.2 非指定账户圈存

应实现线上交易非指定账户圈存功能。

本交易是指用户使用客户端，通过移动支付接入平台，选择或输入转出方账号，用户将其在转出方账户上的资金划入电子现金的过程。

6.6.1.2.3 SE 参数设置

应实现SE参数设置功能。

本交易是指用户使用客户端，通过移动支付接入平台，输入相关参数数值，通过发卡行脚本更新的方式修改相关交易参数的过程。

6.6.2 脱机交易

6.6.2.1 脱机消费

应实现移动终端的脱机消费功能。

脱机消费是指用户使用移动终端在电子现金特约受理商户，购物或获取服务后使用电子现金进行支付的过程。

6.6.2.2 余额查询

应实现脱机余额查询功能。

余额查询是指用户使用移动终端在受理终端进行电子现金余额查询的过程。

6.6.3 移动终端交易

6.6.3.1 账号选择

应实现移动终端客户端的账号选择功能。

账号选择是指用户使用移动终端客户端选择SE中已有应用并将选择的应用账号设置为SE默认交易应用账号的过程。

6.6.3.2 账户列表信息查询

应实现移动终端客户端的账户列表信息查询功能。

账户列表信息查询是指用户使用移动终端客户端查询SE中的账户列表信息的过程。

6.6.3.3 账户信息查询

应实现移动终端客户端的账户信息查询功能。

账户信息查询是指用户使用移动终端客户端对SE中所有应用中某一个账户的账户信息进行查询，如：有效期、电子现金账户余额、电子现金余额上限、电子现金单笔交易限额、电子现金重置阈值等信息。

6.6.3.4 余额查询

应实现移动终端客户端的余额查询功能。

余额查询是指用户使用移动终端客户端对SE中某一个账户的电子现金账户余额进行查询。在查询余额前需要选择电子现金账户。

6.6.4 异常处理

6.6.4.1 冲正交易

应实现冲正交易功能。

对于授权类请求或金融类请求，除存款、转账（转入）、查询、圈提（转入）、圈存撤消（转入）等交易请求外，在出现异常时以冲正通知报文取消原交易。

6.6.4.2 异常交易确认通知

应实现异常交易情况的确认通知功能。

对于存款、转账（转入）、圈提（转入）、圈存撤消（转入）交易请求，在出现异常时以确认通知报文确认原交易。

6.6.4.3 异常处理存储转发机制

应实现异常处理存储转发机制功能。

当冲正发送方不能发送冲正通知或未能收到接收方对冲正的应答时，将冲正通知报文存放在存储转发队列中存储转发。当确认发送方不能发送确认通知时，将确认通知报文存放在存储转发队列中存储转发。冲正通知和确认通知不允许跨越清算日。

7 性能检测内容

7.1 时间特性

7.1.1 支付类业务

选取系统核心的支付类业务进行基准检测、并发检测、极限检测和吞吐量检测，考察其时间特性。

7.1.2 查询类业务

选取系统核心的查询类业务进行基准检测、并发检测、极限检测和吞吐量检测，考察其时间特性。

7.2 资源利用性

7.2.1 检测过程中服务器资源占用情况

在对系统核心业务的检测过程中，监控服务器包括处理器、内存、磁盘IO、网络带宽等硬件资源的占用情况，考察系统的资源利用性。

7.2.2 压力解除后服务器资源释放情况

解除对系统的压力后，监控服务器处理器和内存资源，检查系统自恢复能力。

8 安全性检测内容

8.1 物理安全

8.1.1 物理位置选择

8.1.1.1 机房和办公场地所在建筑物选择

机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内。

8.1.1.2 建筑物内机房位置选择

生产机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

8.1.2 物理访问控制

8.1.2.1 机房设置电子门禁系统

机房出入口应安排专人值守并配置电子门禁系统，控制、鉴别和记录进入的人员。

8.1.2.2 来访人员申请和审批

需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。

8.1.2.3 对机房划分区域进行管理

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

8.1.2.4 重要区域设置第二道电子门禁系统

重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员。

8.1.3 防盗窃和防破坏

8.1.3.1 设备放置

应将主要设备放置在机房内。

8.1.3.2 设备固定

应将设备或主要部件进行固定，并设置明显的不易除去的标记。

8.1.3.3 通信线缆铺设

应将通信线缆铺设在隐蔽处，可铺设在地下或管道中。

8.1.3.4 介质保管

应对介质分类标识，存储在介质库或档案室中。

8.1.3.5 机房防盗报警系统

应利用光、电等技术设置机房防盗报警系统。

8.1.3.6 机房监控报警系统

应对机房设置监控报警系统。

8.1.4 防雷击

8.1.4.1 安装避雷装置

机房建筑应设置避雷装置。

8.1.4.2 安装防雷保安器

应设置防雷保安器，防止感应雷。

8.1.4.3 交流电源地线

机房应设置交流电源地线。

8.1.5 防火

8.1.5.1 设置火灾自动消防系统

机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。

8.1.5.2 采用耐火的建筑材料

机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

8.1.5.3 采用区域隔离防火措施

机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

8.1.6 防水和防潮

8.1.6.1 水管安装要求

水管安装，不得穿过机房屋顶和活动地板下。

8.1.6.2 防雨水措施

——应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
——应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

8.1.6.3 防水检测和报警

应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

8.1.7 防静电

8.1.7.1 接地防静电措施

设备应采用必要的接地防静电措施。

8.1.7.2 采用防静电地板

机房应采用防静电地板。

8.1.7.3 安装静电消除器等装置（增强要求）

应采用静电消除器等装置，减少静电的产生。

8.1.8 温湿度控制

8.1.8.1 机房温湿度自动调节设施

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

8.1.9 电力供应

8.1.9.1 供电线路防护设备配置

应在机房供电线路上配置稳压器和过电压防护设备。

8.1.9.2 备用电力供应

应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。

8.1.9.3 冗余或并行的电力电缆线路设置

应设置冗余或并行的电力电缆线路为计算机系统供电。

8.1.9.4 备用供电系统

应建立备用供电系统。

8.1.10 电磁防护

8.1.10.1 防止电磁干扰

应采用接地方式防止外界电磁干扰和设备寄生耦合干扰。

8.1.10.2 电源线和通信线缆隔离铺设

电源线和通信线缆应隔离铺设，避免互相干扰。

8.1.10.3 关键区域实施电磁屏蔽（增强要求）

应对关键区域实施电磁屏蔽。

8.2 网络安全

8.2.1 结构安全

8.2.1.1 主要设备网络冗余

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。

8.2.1.2 设备网络冗余（增强要求）

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。

8.2.1.3 网络安全路由器

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。

8.2.1.4 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。

8.2.1.5 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。

8.2.1.6 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。

8.2.1.7 QoS 保证

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。

8.2.2 访问控制

8.2.2.1 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。

8.2.2.2 地址转换和绑定

重要网段应采取技术手段防止地址欺骗。

8.2.2.3 内容过滤（增强要求）

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、POP3等协议命令级的控制。

8.2.2.4 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允许访问规则，决定允许或拒绝用户对受控系统进行资源访问。

8.2.2.5 流量控制

应限制网络最大流量数及网络连接数。

8.2.2.6 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。

8.2.2.7 远程拨号访问控制

应限制具有拨号访问权限的用户数量。

8.2.3 安全审计

8.2.3.1 日志信息

应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。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。

8.2.3.2 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。

8.2.3.3 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。

8.2.3.4 审计跟踪极限（增强要求）

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。

8.2.3.5 集中审计（增强要求）

应根据信息系统的统一安全策略，实现集中审计，时钟保持与时钟服务器同步。

8.2.4 边界完整性检查

8.2.4.1 内外网非法连接阻断和定位

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。

8.2.5 入侵防范

8.2.5.1 网络 ARP 欺骗攻击

应能够有效的防范网络ARP欺骗攻击。

8.2.5.2 信息窃取

应采用防范信息窃取的措施。

8.2.5.3 DOS/DDOS 攻击

应具有防DOS/DDOS攻击设备或技术手段。

8.2.5.4 网络入侵防范机制

a) 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。
b) 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。
c) 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。（增强要求）

8.2.6 恶意代码防范

8.2.6.1 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。

8.2.6.2 定时更新

应维护恶意代码库的升级和检测系统的更新。

8.2.7 网络设备防护

8.2.7.1 设备用户身份鉴别

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。

8.2.7.2 主要设备用户身份鉴别（增强要求）

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。

8.2.7.3 身份鉴别信息（增强要求）

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。

8.2.7.4 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。

8.2.7.5 登录地址限制

应对网络设备的管理员登录地址进行限制。

8.2.7.6 登录失败处理

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。

8.2.7.7 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。

8.2.7.8 权限分离

应实现设备特权用户的权限分离。

8.2.8 网络安全管理

8.2.8.1 网络日常维护

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。

8.2.8.2 网络安全管理制度

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作出规定。

8.2.8.3 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。

8.2.8.4 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。

8.2.8.5 设备最小服务配置

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。

8.2.8.6 外部连接的授权和批准

应保证所有与外部系统的连接均得到授权和批准。

8.2.8.7 控制移动设备的网络接入

应依据安全策略允许或者拒绝便携式和移动式设备的网络接入。

8.2.8.8 定期检查违规行为

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。

8.3 主机安全

8.3.1 身份鉴别

8.3.1.1 用户身份标识和鉴别

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。

8.3.1.2 密码口令复杂度设置及定期更换

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。

8.3.1.3 登录失败处理

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。

8.3.1.4 远程管理的传输模式

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。

8.3.1.5 用户名的唯一性

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。

8.3.1.6 用户身份组合鉴别技术

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。

8.3.1.7 鉴别警示信息设置（增强要求）

应设置鉴别警示信息，描述未授权访问可能导致的后果。

8.3.1.8 不可伪造的用户身份组合鉴别技术（增强要求）

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。

8.3.2 访问控制

8.3.2.1 访问控制功能

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。

8.3.2.2 管理用户的角色分配权限

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。

8.3.2.3 操作系统和数据库系统特权用户的权限分离

应实现操作系统和数据库系统特权用户的权限分离。

8.3.2.4 严格限制默认账户的访问权限

应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令。

8.3.2.5 多余、过期账户删除

应及时删除多余的、过期的帐户，避免共享帐户的存在。

8.3.2.6 重要信息资源敏感标记设置

应对重要信息资源设置敏感标记。

8.3.2.7 对有敏感标记信息资源的访问控制

应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

8.3.3 安全审计

8.3.3.1 审计范围

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。

8.3.3.2 审计的事件

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。

8.3.3.3 审计记录格式

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。

8.3.3.4 审计报表生成

应能够根据记录数据进行分析，并生成审计报表。

8.3.3.5 审计进程保护

应保护审计进程，避免受到未预期的中断。

8.3.3.6 审计记录保护

应保护审计记录，避免受到未预期的删除、修改或覆盖等。

8.3.3.7 集中审计（增强要求）

应能够根据信息系统的统一安全策略，实现集中审计。

8.3.4 剩余信息保护

8.3.4.1 鉴别信息清除（增强要求）

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。

8.3.4.2 文件、目录、数据库记录等的清空（增强要求）

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。

8.3.5 入侵防范

8.3.5.1 入侵行为的记录和报警

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。

8.3.5.2 重要程序的完整性保护

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。

8.3.5.3 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。

8.3.6 恶意代码防范

8.3.6.1 防恶意代码软件

应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

8.3.6.2 恶意代码库

主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。

8.3.6.3 防恶意代码软件的统一管理

应支持防恶意代码统一管理。

8.3.7 资源控制

8.3.7.1 接入控制

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。

8.3.7.2 超时锁定

应根据安全策略设置登录终端的操作超时锁定。

8.3.7.3 主机资源监控

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。

8.3.7.4 单个用户资源使用限度控制

应限制单个用户对系统资源的最大或最小使用限度。

8.3.7.5 系统服务水平监控和报警

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。

8.3.7.6 无用的过期信息、文档完整清除

应每月对无用的过期信息、文档进行完整清除。

8.3.8 可信路径

8.3.8.1 身份鉴别时安全的信息传输路径（增强要求）

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。

8.3.8.2 系统访问时安全的信息传输路径（增强要求）

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。

8.3.9 系统安全管理

8.3.9.1 访问控制策略

应根据业务需求和系统安全分析确定系统的访问控制策略。

8.3.9.2 系统漏洞扫描

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。

8.3.9.3 系统补丁

应安装系统的最新补丁程序，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。

8.3.9.4 系统安全管理制度

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作出具体规定。

8.3.9.5 系统管理员权限

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。

8.3.9.6 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 应用安全

8.4.1 身份鉴别

8.4.1.1 用户身份标识和鉴别

应提供并启用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。

8.4.1.2 用户身份组合鉴别技术

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。

8.4.1.3 身份标识唯一性和复杂度检查

应提供并启用用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。

8.4.1.4 登录失败处理

应提供并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。

8.4.1.5 不可伪造的用户身份组合鉴别技术（增强要求）

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。

8.4.2 访问控制

8.4.2.1 访问控制策略

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。

8.4.2.2 访问控制覆盖范围

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。

8.4.2.3 授权主体配置访问控制策略

应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限。

8.4.2.4 管理用户角色权限分配

应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

8.4.2.5 敏感标记设置（增强要求）

应具有对重要信息资源设置敏感标记的功能。

8.4.2.6 敏感标记信息资源访问控制（增强要求）

应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

8.4.2.7 禁止默认帐户访问（增强要求）

应由授权主体配置访问控制策略，并禁止默认帐户的访问。

8.4.3 可信路径

8.4.3.1 身份鉴别的安全信息传输路径

在应用系统对用户进行身份鉴别时，应能够建立一条安全的信息传输路径。

8.4.3.2 资源访问的安全信息传输路径

在用户通过应用系统对资源进行访问时，应用系统应保证在被访问的资源与用户之间应能够建立一条安全的信息传输路径。

8.4.4 安全审计

8.4.4.1 审计范围

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。

8.4.4.2 审计保护

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。

8.4.4.3 审计记录格式

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。

8.4.4.4 审计报表生成

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。

8.4.4.5 集中审计接口（增强要求）

应能够根据信息系统的统一安全策略，实现集中审计。

8.4.5 剩余信息保护

8.4.5.1 鉴别信息清除（增强要求）

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。

8.4.5.2 文件、目录、数据库记录等的清空（增强要求）

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。

8.4.6 通信完整性

8.4.6.1 采用密码技术保证完整性（增强要求）

应采用密码技术保证通信过程中数据的完整性。

8.4.7 通信保密性

8.4.7.1 会话初始化验证

在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证。

8.4.7.2 通信过程中加密

应对通信过程中的整个报文或会话过程进行加密。

8.4.7.3 进行加解密运算和密钥管理（增强要求）

应基于硬件化的设备对重要通信过程进行加解密运算和密钥管理。

8.4.8 抗抵赖

8.4.8.1 数据原发证据

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。

8.4.8.2 数据接收证据

应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

8.4.9 软件容错

8.4.9.1 数据有效性验证

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；

8.4.9.2 自动保护

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。

8.4.9.3 自动恢复（增强要求）

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。

8.4.10 资源控制

8.4.10.1 自动结束会话

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。

8.4.10.2 最大并发会话连接数限制

应能够对系统的最大并发会话连接数进行限制。

8.4.10.3 多重并发会话限制

应能够对单个帐户的多重并发会话进行限制。

8.4.10.4 时间段内并发会话控制

应能够对一个时间段内可能的并发会话连接数进行限制。

8.4.10.5 限额分配（增强要求）

应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额。

8.4.10.6 系统服务水平最小值检测报警

应能够对系统服务水平降低到预先规定的最小值时进行检测和报警。

8.4.10.7 服务优先级设定（增强要求）

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帐户或请求进程的优先级，根据优先级分配系统资源。

8.4.11 交易数据签名

8.4.11.1 交易关键要素数据签名

对于高风险业务交易应使用数字证书对交易数据中的关键要素进行签名，关键要素包括但不限于商户编号、订单号、订单日期时间、交易币种、交易金额、账号等。

8.4.11.2 交易数据签名验证

应验证交易数据签名的正确性、签名方证书的有效性、签名方证书与身份的一致性。

8.4.12 会话安全

8.4.12.1 会话标识唯一性

会话标识应唯一、随机、不可猜测。

8.4.12.2 防未经授权访问

会话过程中应维持认证状态，防止信息未经授权访问。

8.4.12.3 会话超时时间设置

会话应设置超时时间，当空闲时间超过设定时间自动终止会话。

8.4.12.4 及时清除会话信息

会话结束后，应及时清除会话信息。

8.4.12.5 防止会话令牌窃取

应采取措施防止会话令牌在传输、存储过程中被窃取。

8.4.12.6 应用审计日志（增强要求）

应用审计日志应记录暴力破解会话令牌的事件。

8.4.13 常见攻击防范

8.4.13.1 服务器端数据有效性检查

应在服务器端对客户及商户提交的数据进行有效性检查（如对提交的表单、参数等进行合法性判断和非法字符过滤等），或对输出进行安全处理。

8.4.13.2 防暴力破解静态密码

应具有防范暴力破解静态密码的保护措施，例如使用图形验证码。

8.4.13.3 代码审查

应进行代码审查，防范应用程序中不可信数据被解析为命令或查询语句等。

8.4.13.4 开发安全接口

应开发安全的接口，如通过避免语句的完全解释或采用参数化接口等方式实现。

8.4.13.5 防范服务器端拒绝服务攻击

应采取有效措施防范服务器端的拒绝服务攻击。

8.4.13.6 文件上传下载访问控制

应对文件的上传和下载进行访问控制，避免执行恶意文件或未授权访问。

8.4.13.7 数据库使用存储过程或参数化查询（增强要求）

数据库应使用存储过程或参数化查询，并严格定义数据库用户的角色和权限。

8.4.13.8 应用程序检查（增强要求）

应通过自动化工具（如弱点扫描工具、静态代码检测工具等）对应用程序进行检查。

8.4.13.9 基于浏览器应用防恶意软件（增强要求）

基于浏览器的应用，应使用安全控件等措施以降低恶意软件窃取用户敏感信息的风险。

8.4.14 交易处理

8.4.14.1 支付风险提示

对远程支付，应在确认支付之前向客户提示订单信息及支付风险。

8.4.14.2 终端反馈支付结果到用户

应将交易的支付结果通过移动终端和/或受理终端及时、完整的反馈到用户。

8.4.14.3 账户管理机构通知支付结果

客户的账户管理机构应将交易的支付结果以约定的方式及时、完整的通知客户与支付机构。

8.4.14.4 支付机构通知支付结果

支付机构应将交易的支付结果以约定的方式及时、完整的通知商户。

8.4.15 报文安全

8.4.15.1 防重放攻击

应可防止对交易的重放攻击。

8.4.15.2 交易唯一性

应用系统应保证在一段时期内同一商户交易、订单的唯一性。

8.4.15.3 交易报文完整性检查

应用系统应检查交易请求报文中记载的交易要素是否完整并符合业务规则，并拒绝不完整或者不符合业务规则的交易请求。

8.4.15.4 防重复支付

应用系统应防止对支付成功的订单重复支付。

8.4.15.5 高风险业务数据签名

对于大额支付等高风险业务（支付机构可根据自身情况对高风险业务交易进行界定）应使用数字证书对交易数据中的关键要素进行签名，关键要素包括但不限于商户编号、订单号、订单日期时间、交易币种、交易金额、账号等。

8.4.15.6 敏感信息保护

应保证交易隐私信息的保密性，如姓名、有效身份证件号码、联系方式、交易内容等。用户账号及证件号码等敏感信息只能按业务要求进行保存和使用，显示时应进行屏蔽处理。

8.4.15.7 近场支付报文安全

对于近场支付，具体报文应符合JR/T 0025.7的相关要求。

8.4.16 短信处理

8.4.16.1 短信数据存储区域访问控制

对数据存储区域的访问要实施控制，保证信息安全。

8.4.16.2 短信通信安全通道

短信处理平台与移动支付业务系统之间，应采用安全通道（如专线、VPN或同级别的安全协议如HTTPS）进行通信，保证机密性。

8.4.16.3 短信报文传输保护

短信处理平台与移动支付业务系统之间的报文宜采用报文鉴别码或数字签名，防止报文被篡改，实现报文的一致性和完整性。

8.4.16.4 委托类交易身份鉴别

在委托类交易中，应在建立、撤销、变更委托关系时进行鉴别，鉴别手段可以包括手机号码有效性验证、银行卡有效性验证、用户身份真实性验证等，根据业务需要还可增加电子邮箱验证等其他辅助验证环节。

8.4.16.5 短信安全提示

在实际交易过程中，应提示用户及时删除交易相关短信，防止向外误发和被他人窥视。

8.5 数据安全

8.5.1 数据完整性

8.5.1.1 传输过程数据完整性

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。

8.5.1.2 存储过程数据完整性

应能够检测到系统管理数据、鉴别信息和重要业务数据在存储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。

8.5.2 数据保密性

8.5.2.1 数据加密传输

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。

8.5.2.2 数据加密存储

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。

8.5.3 备份和恢复

8.5.3.1 本地备份和恢复

应提供本地数据备份与恢复功能。对数据应进行定期备份，备份周期至少满足每天增量备份，每周一次全量备份；备份介质场外存放。

8.5.3.2 异地备份

应提供异地备份功能，将数据备份至灾难备份中心。

8.5.3.3 交易数据保存时间

交易数据保存时间应不少于法律法规及部门规章规定的年限。

8.5.3.4 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。

8.5.3.5 业务应用无缝切换（增强要求）

应建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备，实现业务应用的无缝切换。

8.5.4 密码算法

8.5.4.1 对称加密算法

应符合国家行业主管部门的要求，正确实现DES、3DES、SM4等对称加密算法。

8.5.4.2 非对称加密算法

应符合国家行业主管部门的要求，正确实现RSA、SM2等非对称加密算法。

8.5.4.3 摘要算法

应符合国家行业主管部门的要求，应正确实现SHA-1、SM3等加密算法。

8.5.4.4 近场支付密码算法

近场支付的密码算法应能够实现规定的安全机制。

8.5.5 数据认证

8.5.5.1 远程支付服务器认证

与移动终端直接通讯的移动支付业务系统服务器上，应安装服务器证书，标识服务器真实身份。当客户端进行交易时，应通过安全协议（如包括当不限于SSL/TLS等协议），验证服务器的身份合法性。

8.5.5.2 远程支付用户认证

用户数据认证可采用多种形式（如数字证书、一次性口令等），当客户端采用数字证书认证时，应使用用户证书对关键要素或报文整体进行签名，由应用系统验证签名有效性。

8.5.5.3 近场支付脱机数据认证

脱机数据认证应符合相关标准的要求。

8.5.5.4 近场支付应用密文和发卡行认证

应用密文和发卡行认证应符合相关标准的要求。

8.5.6 密钥管理

8.5.6.1 密钥管理要求

密钥管理应遵循金融业数据安全保密的国家标准和国际标准，采用安全可靠的加密算法。基于SE的应用，其相关密钥的存贮和交易信息的加密/解密在硬件加密设备中进行，并定期更换密钥。

8.6 管理安全

8.6.1 组织机构

8.6.1.1 安全管理架构

应建立信息安全管理架构，设置专门的信息安全工作的职能部门或团队。

8.6.1.2 部门和人员职责

应明确相关部门的信息安全职责，并详细定义部门人员配置及岗位职责。

8.6.1.3 信息安全相关部门人员职责

信息安全相关部门人员应详细了解本单位研发、运行及管理机构职责设置。

8.6.1.4 部门设置

应设置专门的业务系统研发、测试、运行维护、安全、风险控制等部门或团队。

8.6.1.5 支付服务相关部门职责

应制订明确的支付服务相关部门的安全管理职责，并详细定义各部门人员配置。

8.6.1.6 风险管理架构

应建立风险管理架构，相关人员应详细了解本单位研发、运行及管理机构职责设置。

8.6.2 管理制度

8.6.2.1 建立管理制度体系

应建立安全管理制度体系，明确工作职责、规范工作流程、降低安全风险，应制订移动支付安全管理工作的总体方针和策略。应指定或授权专门的部门或人员负责安全管理制度的制订。

8.6.2.2 建立贯穿业务系统的过程

应建立贯穿业务系统设计、编码、测试、运行维护、评估以及应急处置等过程，并涵盖安全制度、安全规范、安全操作规程和操作记录手册等方面的信息安全管理制度体系。

8.6.2.3 安全管理制度审计

应每年组织相关部门和人员对安全管理制度体系的合理性和适用性审计，及时修订安全管理制度的不足。

8.6.3 安全策略

8.6.3.1 制订安全保障目标

应制订明确的业务系统总体安全保障目标。

8.6.3.2 制订安全策略

应制订针对业务系统设计与开发、测试与验收、运行与维护、备份与恢复、应急事件处置以及客户信息保密等的安全策略。应制订业务系统使用的应用系统、网络设备、安全设备的配置和使用的安全策略。

8.6.3.3 维护资产清单

应维护详细的资产清单，资产清单应包括资产的价值、所有人、管理员、使用者和安全等级等条目，并根据安全等级制订相应的安全保护措施。

8.6.3.4 风险定义与规避

应明确系统存在的威胁，并根据威胁分析系统的脆弱性，对已发现的风险应尽快修补或制订规避措施。应针对不同的风险规定相应的可能性等级列表，并根据风险严重等级制订应急恢复方案和演练计划。

8.6.3.5 安全级别定义与保护措施制订（增强要求）

应按照GB/T 22239规定所有数据的安全级别，并制订与其安全级别相应的保护措施。

8.6.4 人员和文档管理

8.6.4.1 信息安全管理岗位

应设置信息安全管理岗位，明确相关岗位在信息安全管理过程中所承担的责任。

8.6.4.2 涉密岗位安全

应与涉密岗位员工签署保密协议，或在劳动合同中设置保密条款，确保员工理解认同公司相关信息安全策略，承诺安全责任与义务。

8.6.4.3 关键岗位人员后备措施

应对关键岗位设定人员后备措施，并加强其安全培训，确保员工了解各自岗位职责以及违反安全规定可能导致的后果。

8.6.4.4 员工岗位调动或离职

应具有员工岗位调动或离职的安全管理制度，避免账号、设备、技术资料及相关信息等泄露。

8.6.4.5 外来人员管理制度

应建立外来人员管理制度，提交操作记录，必要时要求其签订保密协议。

8.6.4.6 文档管理制度

应建立文档管理制度，文档资料按密级或敏感程度进行登记、分类并由专人保管，重要文档资料的使用、外借或销毁应经过审批流程并进行记录。

8.7 运行维护安全

8.7.1 环境管理

8.7.1.1 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。

8.7.1.2 机房的出入管理制度化和文档化

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

8.7.1.3 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。

8.7.1.4 机房安全管理制度

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

8.7.1.5 机房进出登记表

应具有机房进出登记表。

8.7.2 资产管理

8.7.2.1 资产清单

应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。

8.7.2.2 资产安全管理制度

应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。

8.7.2.3 资产标识

应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。

8.7.2.4 资产信息规范化管理

应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

8.7.3 介质管理

8.7.3.1 介质的使用管理文档化

应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定。

8.7.3.2 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。

8.7.3.3 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。

8.7.3.4 介质的维修与销毁

应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，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。

8.7.3.5 介质异地存储

应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同。

8.7.3.6 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。

8.7.4 设备管理

8.7.4.1 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。

8.7.4.2 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。

8.7.4.3 设备维护管理制度

应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等。应确保信息处理设备必须经过审批才能带离机房或办公地点。

8.7.4.4 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。

8.7.4.5 设备外带管理

应确保信息处理设备必须经过审批才能带离机房或办公地点。

8.7.5 监控管理

8.7.5.1 主要设备指标监控

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

8.7.5.2 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。

8.7.5.3 安全管理中心

应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

8.7.6 密码管理

8.7.6.1 密码使用管理制度

应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

8.7.7 变更管理

8.7.7.1 变更方案

应确认系统中要发生的变更，并制定变更方案。

8.7.7.2 变更制度化管理

应建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、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。

8.7.7.3 重要系统变更的批准

应建立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，记录变更实施过程，并妥善保存所有文档和记录。

8.7.7.4 变更中止与变更恢复

应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

8.7.8 备份与恢复管理

8.7.8.1 定期备份

应识别需要定期备份的重要业务信息、系统数据及软件系统等。

8.7.8.2 备份与恢复管理制度

应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范。

8.7.8.3 数据的备份策略和恢复策略

应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。

8.7.8.4 备份恢复过程记录

应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存。

8.7.8.5 定期检查备份介质有效性

应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

8.7.9 安全事件处置

8.7.9.1 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。应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点。

8.7.9.2 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。

8.7.9.3 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。

8.7.10 应急预案管理

8.7.10.1 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。

8.7.10.2 应急预案资源保障

应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障。

8.7.10.3 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。

8.7.10.4 定期演练

应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期。

8.7.10.5 应急预案定期审查

应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。

8.8 业务连续性

8.8.1 业务连续性需求分析

8.8.1.1 业务中断影响分析

应进行业务中断影响分析。

8.8.1.2 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。

8.8.2 业务连续性技术环境

8.8.2.1 备份机房

应具备备份机房。

8.8.2.2 网络双链路

应具备双链路。

8.8.2.3 网络设备和服务器备份

应具备同城应用级备份设施。

8.8.2.4 远程数据库备份

应具备远程备份数据库。

8.8.3 业务连续性管理

8.8.3.1 业务连续性管理制度

应具备业务连续性管理制度。

8.8.3.2 应急响应流程

应具备应急响应流程。

8.8.3.3 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。

8.8.3.4 数据备份和恢复制度

应具备数据备份和恢复管理制度。

8.8.4 日常维护

8.8.4.1 业务连续性演练

应每年进行业务连续性演练。

8.8.4.2 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 风险监控检测内容

9.1 账户风险管理

9.1.1 账户信息管理

应按支付业务管理办法及反洗钱规定的要求，获取、保存、管理客户和商户的基本信息，应通过安全有效的方式对客户和商户的有效身份证件或其他有效身份证明文件进行核实。

9.1.2 通过信息系统管理账户

应通过信息系统管理客户和商户基本信息，确保信息的保密性与完整性。

9.1.3 账户变更

应按照接入要求对客户和商户基本信息变更进行核实，对用户行身份认证，并保存变更记录。

9.1.4 账户交易限额设置

应针对客户和商户的交易需求及安全属性分别设置交易限额，包括但不限于文件证书限额。

9.1.5 商户风险评估

应对商户进行分类及风险评估，并提供与风险评估结果匹配的支付服务。

9.1.6 商户风险评级（增强要求）

应通过信息系统建立商户风险评级体系，并提供与风险等级匹配的支付服务。

9.1.7 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。

9.1.8 账户余额上限

应对移动支付账户余额最大值进行限制，并符合国家法律法规要求。

9.1.9 单笔充值上限

应规定移动支付账户单笔充值金额最大值，并进行限制或者触发风控规则。

9.1.10 单笔消费上限

超过单笔消费限额的交易应有记录并触发风控规则，如为脱机消费，则应以现场联机方式实现。

9.1.11 单日单月累计消费上限

应对单日、单月累计消费额度进行限制。

9.1.12 单日累计消费次数限制

单日累计消费次数应进行限制。

9.1.13 单日单月圈存/充值上限

应规定脱机账户单日、单月圈存/充值金额最大值，并进行限制或者触发风控规则。

9.2 身份认证

9.2.1 双因素身份认证

对于高风险业务应使用双因素身份认证。双因素身份认证方式的其中一种方式应至少包括客户持有、特有并用于身份认证的信息，包括但不限于物理介质、电子设备、生物特征等。

9.2.2 企业账户认证

使用企业账户进行支付时，应至少使用硬件承载的数字证书等安全认证方式。

9.3 交易过程监控

9.3.1 支付请求信息记录

应准确完整记录交易的支付请求信息，如商户编号、商户交易流水号、商户订单号、交易金额、交易日期时间等；向客户的发卡/账户机构提交的支付请求应包含支付及风险防范相关的数据要素。

9.3.2 支付结果信息记录

应准确完整记录交易的支付结果信息，如支付时间、支付金额、支付方式、付款方、收款方、发卡/账户机构的反馈应答信息等；应在从客户的发卡/账户机构获取的支付结果中包含支付及风险防范相关的数据要素。

9.3.3 交易信息一致性检查

应根据从商户及客户的发卡/账户机构获取的交易数据，检查交易信息的一致性，识别潜在的非法交易、欺诈交易等。

9.3.4 退款处理

退款时应与原支付交易对应，将款项退回原结算账户。

9.4 交易查询

9.4.1 交易查询权限

应保证仅客户或授权人员能够查询交易账户信息。

9.4.2 查询结果屏蔽

应将查询结果中的敏感信息进行屏蔽。

9.4.3 当日交易查询

应实现当日交易信息的查询。

9.4.4 历史交易查询

应实现历史交易信息的查询。

9.5 交易监控

9.5.1 交易监控系统

应建立交易监控系统，能够甄别并预警潜在风险交易，例如套现、洗钱、欺诈等可疑交易，并生成风险监控报告。

9.5.2 风险交易模型

应根据交易的风险特征建立风险交易模型，有效监测可疑交易，对检测到的可疑交易建立报告、复核、查结机制。

9.5.3 风险分析与处理

应对监控到的风险交易进行及时分析与处置。

9.5.4 黑名单

应依据已识别并确认的风险数据，建立黑名单数据库。在系统中应提供黑名单的定义和管理功能，并可根据情况实时冻结与黑名单监控对象发生的交易行为。

9.6 客户教育

9.6.1 安全风险提示

应在网站建立独立风险提示和安全介绍的页面或栏目，对客户进行安全风险提示，对安全控制措施进行说明。

9.6.2 操作风险提示

应在风险类业务的操作前、操作中进行风险提示；或在客户第一次交易时进行风险提示和安全教育。

9.6.3 功能演示与风险业务操作手册（增强要求）

应建立业务功能的演示版或尝试机制，让客户充分了解业务处理流程和功能实现。应提供风险类业务操作的手册，对客户进行宣传和教育。

9.7 近场支付受理终端风险管理

9.7.1 终端安全检测报告

使用的终端应提供由具有检测资质机构检测通过的安全检测报告，报告内容要能反映终端的安全状况。

9.7.2 密码键盘安全检测报告

使用的密码键盘应提供由具有检测资质机构检测通过的安全检测报告，报告内容要能反映终端的安全状况。

9.7.3 受理终端管理流程

受理终端的申请、参数设置、程序灌装、使用、更换、维护、撤销、回收等管理应有明确的流程。

9.7.4 受理终端的安装与登记

应建立受理终端的信息管理（登记）制度，保证信息完整有效、实时更新；移动受理终端的安装应严格限制，详细登记。

9.7.5 受理终端监控

应建立受理终端的定期巡检制度，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。应建立受理终端的异常情况处理制度，保证出现异常情况可以得到及时有效处理。

9.8 近场支付交易风险管理

9.8.1 联机交易 ARQC/ARPC 验证

应能够进行联机交易的联机认证。

9.8.2 联机报文 MAC 验证

应对联机交易报文进行MAC验证。

9.8.3 脱机交易 TAC 验证

脱机交易中，应进行TAC验证。

9.8.4 脱机交易 MAC 验证

脱机交易中，应进行MAC验证。

9.8.5 SE 账户状态控制

应对SE账户各种状态进行控制，正确识别冻结、过期等状态。

9.8.6 密码错误情况下的交易请求

应能够有效的控制密码错误情况下的交易请求，并进行记录。

9.8.7 非法主账号交易

应能够有效的控制非法主账号交易，并进行记录。

10 文档审核内容

10.1 用户文档

10.1.1 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人或解释输出显示的用户界面。

10.1.2 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。

10.2 开发文档

10.2.1 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。

10.2.2 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。

10.2.3 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。

10.2.4 数据库设计文档

数据库设计文档应描述数据库的设计。所谓数据库指存储在一个或多个计算机文件中的相关数据的集合，它们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。

10.2.5 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。

10.2.6 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。

10.2.7 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，本文档中“软件开发”一词涵盖了新开发、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。

10.3 管理文档

10.3.1 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。

10.3.2 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。

10.3.3 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。

10.3.4 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。

10.3.5 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。

10.3.6 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 外包管理检测内容

11.1 外包合法化

外包内容应符合法律法规的要求。

11.2 风险评估

应对外包行为和外包模式进行风险评估。

11.3 资质评估

确定外包行为前应对外包服务提供方的经验和能力、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。

11.4 外包合同签订

应与外包服务提供方就外包内容签订合同，合同中应明确各方的权利、义务及责任和争议解决办法。

11.5 制定保密协议

应在合同中设定安全保密条款或单独签署安全保密协议。

11.6 服务提供方符合规范要求

应在合同中设定条款要求外包服务提供方提供的外包服务符合规范的本部分要求。

11.7 制定控制制度、事件报告程序和应急计划

应制订对外包的控制制度、事件报告程序和应急计划。

11.8 制定外包交付清单

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。

11.9 指定专人管理和监督外包服务

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。

12 机构入网检测内容

12.1 通讯接口

12.1.1 通讯协议

应实现如下通讯协议功能：

——入网机构与转接清算系统之间的一个连接应由本地 IP 地址、端口号和远程 IP 地址、端口号唯一确定；

——IP 地址和端口号配置；

——联机交易的连接数目和方式；

——文件传输的连接数目和方式；

——通信接口传输数据不应包含特殊字符和控制字符；

——通信接口不应影响业务流程；

——联机交易建立连接、数据传输、关闭连接的方式；

——应提供超时控制；

——报文数据的最大长度；

——空闲连接处理方式；

——文件传输建立连接、关闭连接的方式。

12.1.2 网络接口

应实现如下网络接口功能：

a) 入网机构应至少通过两条主干链路接入转接清算系统网络。
b) 入网机构应保证拥有至少一条备份线路（如拨号线路）与转接清算系统网络相连。

12.2 交易处理

12.2.1 近场支付联机交易

应正确实现如下近场支付联网联合功能：
——余额查询；；
——取现；
——存款；
——存款撤销；
——转账；
——消费；
——消费撤销；
——预授权；
——预授权撤销；
——预授权追加；
——预授权完成（请求）；
——预授权完成（通知）；
——预授权完成撤销；
——退款（退货）；
——指定账户圈存；
——非指定账户圈存；
——现金圈存；
——圈提；
——脚本处理结果通知；
——建立委托；
——解除委托；
——账户验证；
——账户基本信息查询。

12.2.2 远程支付联机交易

应正确实现如下远程支付联网联合功能：
——余额查询；
——转账；
——消费；
——指定账户圈存；
——非指定账户圈存；
——脚本处理结果通知；
——建立委托；
——解除委托；
——账户验证；
——账户基本信息查询；

——充值。

12.2.3 异常处理

应实现如下异常处理联网联合功能：

——冲正处理；

——确认处理。

12.2.4 脱机交易

应实现如下脱机交易联网联合功能：

——脱机消费；

——电子现金脱机余额查询。

12.2.5 手工调整交易

应实现如下手工调整交易联网联合功能：

——受理方发起请求；

——账户管理系统发起请求；

——转接清算系统发起请求。

12.2.6 超时限定

应实现如下超时限定功能：

——联机类交易超时限定；

——脱机类交易超时限定；

——手工类交易超时限定；

——批量交易超时限定。

12.3 报文接口

12.3.1 报文结构

应正确实现如下部分的报文结构：

a) 报文头；

b) 报文类型；

c) 报文位图；

d) 系列报文域。

12.3.2 报文头

应包括域说明，正常报文和拒绝报文的报文头。

12.3.3 报文类型

应包括版本号，报文类型标识符。

12.3.4 报文位图

应包括报文位图格式。

12.3.5 报文域

应包括报文域，具体报文域说明。

12.3.6 关键信息域和报文的关联

应实现如下关联功能：
——应答报文和请求报文；
——冲正交易和原始交易；
——消费撤销和消费；
——预授权撤销和预授权；
——预授权完成和预授权；
——预授权完成撤销和预授权完成；
——转入确认和转账交易；
——退货和消费交易。

12.3.7 报文格式

应具有正确的转接类联机交易报文和管理类联机交易报文格式。

12.4 文件接口

12.4.1 普通金融交易明细文件

应具有正确的正确普通金融交易明细文件的文件名称和记录格式。

12.4.2 转账交易明细文件

应具有正确的转账交易明细文件的文件名称和记录格式。

12.4.3 差错交易明细文件

应具有正确的差错交易明细文件的文件名称和记录格式。

12.4.4 脱机交易明细文件

应具有正确的脱机交易明细文件的文件名称和记录格式。

12.4.5 汇总文件

应具有正确的汇总文件的文件名称和记录格式。

12.4.6 信息文件

应具有正确的信息文件的文件名称和记录格式。

12.5 入网机构管理

12.5.1 制度要求

12.5.1.1 信息安全及支付管理制度

应建立信息安全制度，支付风险管理制度，并通过有效而正式的方式进行发布。

12.5.1.2 相关制度专人负责

应指定专人负责信息安全制度的建立、分发、复查和培训。

12.5.1.3 安全制度修订

应每年复查信息安全制度，重新评估安全控制及过程，对不适用或需改进的地方进行修订。

12.5.1.4 定期对员工进行培训

应定期对员工进行安全培训，培训内容包括各类安全制度、信息系统运维手册和应急预案等。

12.5.1.5 录用员工技术能力审查

应审查录用员工的技术能力和背景资料，并签署保密协议。

12.5.1.6 安全事件报告流程及应急处理预案

应建立安全事件报告流程及应急处理预案，建立不同类别信息安全事件的报告程序，所有相关员工需知道安全事件的报告程序。

12.5.1.7 安全弱点或威胁响应

所有相关员工都需注意及报告系统或服务任何可疑的安全弱点或威胁。

12.5.1.8 信息验证失败处理

客户提供的身份信息和银行账户信息经多次验证仍未通过的，应予以重点关注，并暂停相关业务处理。

12.5.1.9 支付账户异常情况处理

发现支付账户信息被盗取、欺诈、洗钱等风险事件的，应对客户采取暂停交易、限制账户使用等相关措施；对于涉嫌犯罪的，应立即向当地公安机关报案，同时向所在地中国人民银行分支机构报告。

12.5.1.10 交易安全事件通知

发生与移动支付交易相关的安全事件应及时通知移动支付联网通用管理机构。

12.5.2 机房管理

12.5.2.1 监视敏感区域

应使用人工或闭路电视监控系统监视敏感区域。

12.5.2.2 机房值班制度

应建立值班制度，配备值班人员，对机房内各类设备运行情况进行日常监控，并处置突发事件。

12.5.2.3 来访人员管理

非授权工作人员或来访人员因工作需要需进入机房，应必须经过申请、审批和登记，并由授权人员授权专人全程陪同。

12.5.2.4 设备或存储介质登记

电子设备或存储介质进出机房，须经审批并登记。

12.5.3 网络安全要求

12.5.3.1 入网机构系统与联网通用系统连接要求

a) 接入方式应使用专线、基于专网的 MPLS 等。
b) 使用基于 MPLS(Internet)的 IPSEC/SSL 等安全协议、基于 Internet 的 MPLS，应充分考虑相关风险，并遵循相关安全要求。
c) 禁止接入 Internet。

12.5.3.2 入网机构系统与受理终端连接要求

a) 受理终端与入网机构应用系统之间的通讯，如需先经过商户的网络或系统，入网机构应对敏感信息（主要有磁道信息、验证码、个人标识代码及有效期）加密或督促商户采取安全措施，确保移动支付账户敏感信息不被泄漏，防止支付指令被篡改。
b) 受理终端采用 GPRS/CDMA 方式接入入网机构系统时应对敏感信息加密。

12.5.3.3 入网机构生产网络与其它系统网络逻辑隔离

接入转接清算系统的入网机构生产网络必须与不涉及移动支付交易信息的网络（如办公网络）逻辑隔离。

12.5.3.4 互联网接入审批

入网机构应对互联网接入本单位生产网络严格审批，如因业务需要必须接入，须在互联网接入处布放防火墙和入侵检测（防御）设备等安全设备，监视可能的攻击行为，记录入侵事件的发生，并报警正在发生的入侵事件。

12.5.3.5 路由器配置和防火墙策略相关流程

应建立对所有的路由配置和防火墙策略的批准、测试和变更的正式流程，路由配置和防火墙策略在每次变更后须及时归档。

12.5.3.6 路由配置和防火墙策略检查

应定期对路由配置和防火墙策略进行检查，对路由器和防火墙的事件日志、入侵检测（防御）设备的告警事件进行分析和处理。

12.5.3.7 登录用户身份鉴别

对登录网络及网络安全设备的用户进行身份鉴别，严格控制可以修改网络及网络安全设备配置的账号。

12.5.3.8 拨号用户访问控制

如果有拨号访问网络方式，应对拨号用户严格访问控制，每个用户须分别自行设置口令，口令不得少于8位，并应定期修改，不允许外部拨号或其他方式的远程维护连接。

12.5.3.9 网络定期检查

定期或在网络发生重大变更后，应对安全控制措施、网络连接和限制措施进行渗透性测试或漏洞扫描，应对网络及网络安全设备系统设置、补丁配置和已知的漏洞进行检查，并确认没有生产网络用户私自连接到外部网络，外部访问不能非授权进入生产网络。

12.5.3.10 非授权用户敏感数据访问控制

为阻止非授权用户对内部网络中敏感数据的访问，应采取物理隔离、划分VLAN、主机路由等方式分隔不同的用户和信息系统。

12.5.3.11 网络定期审计

应定期对网络和网络安全设备的内部或外部审计，以验证其配置或策略是否适合入网机构的安全要求。

12.5.3.12 恶意代码检测

应在网络边界及核心业务网段处对恶意代码（主要是病毒和木马）进行检测或清除。

12.5.4 主机系统安全要求

12.5.4.1 软件系统访问控制

根据“知所必需”原则，应严格进行对软件和系统的访问控制，禁用不必要的缺省用户。定期对用户访问文件、目录、数据库等权限进行检查，加强用户管理，剔除不活动用户，防止用户权限过大。

12.5.4.2 关键数据传输加密

应参考国际通行的相关安全规范要求，制订用户口令密码使用、管理和更新制度和措施。加强系统身份认证等关键数据传输加密，防止口令泄露。

12.5.4.3 系统安全加固

应对系统进行安全加固。如禁用所有不必要的、不安全的服务、协议和应用程序；设定系统安全参数以防止误用/滥用，删除默认设置；严禁下载或使用免费软件或共享软件；移除系统或应用程序中不必要、不安全的功能等。

12.5.4.4 软件补丁测试

在软件补丁安装以前，应在测试系统中进行严格测试，确保测试通过后再进行安装。

12.5.4.5 软件补丁管理制度和流程

应制定软件补丁管理制度和流程，对所有生产系统安装必须的操作系统和应用系统补丁。

12.5.4.6 厂商定期维护活动记录

厂商应定期维护活动须进行审批并记录，维护人员进出应专人陪同并记录相关操作。

12.5.4.7 主机运行监控

应进行主机运行监控，监控主机的CPU、硬盘、内存、网络等资源的使用情况，监控特定进程（主要的系统进程）的状态，限制对重要账户的添加和更改。

12.5.4.8 硬件状态

应定义硬件的非正常状态，并在故障持续预设定时间后，作为安全事件进行报告。

12.5.4.9 组合技术用户身份鉴别

主机和应用系统应采用两种以上组合的鉴别技术实现用户身份鉴别。

12.5.5 应用系统安全要求

12.5.5.1 口令管理规则

应建立口令管理规则，设定各类口令长度（不得小于6位）、复杂度（必须包含数字和字符）、修改周期（不得长于3个月）、不可明文传输、应加密存储等要求。

12.5.5.2 审计日志

审计日志应受到保护，仅接受授权用户的访问，审计日志需至少保存三个月。

12.5.5.3 数据恢复销毁

大容量存储介质在实施外包数据恢复时，应确保数据安全；在更换或废弃时，应对其中数据彻底销毁，确保数据不可恢复。在需要废弃、销毁含重要信息的介质时，应严格报批手续，做好登记，由双人负责实施，在保卫人员的监督下，采用物理破坏盘片的形式予以彻底销毁。移动支付联网通用生产相关数据不得直接在入网机构的测试环境中使用。

12.5.5.4 记录日志

软件或系统的配置更改，补丁安装以及升级需受内部变更管理控制，应保留相应的日志。

12.5.5.5 生产系统软硬件信息记录

应记录并定期查阅生产系统设备中的所有软件名称及版本，并对关键软件的参数配置以及安装文件进行备份以防止意外损坏。

12.5.5.6 生产系统变更操作审批实施流程

应建立生产系统变更操作的审批和实施流程。需制定变更计划，按计划实施变更；在变更实施前制定、评审并测试变更方案；在变更实施时，要求双人复核。

12.5.5.7 系统运维手册

应对各类信息系统基础设施和应用系统制定运维手册，并定期补充更新。

12.5.6 账户信息安全和密钥管理

12.5.6.1 账户基本信息存储

入网机构的系统应只能存储用于交易清分、差错处理所必需的最基本的账户信息，不得存储磁道信息、验证码、个人标识代码(PIN)的明文和密文及有效期。

12.5.6.2 硬件加密设备

交易处理如涉及对个人标识代码(PIN)进行加解密操作的，应配备经权威部门安全认证的硬件加密设备，并采用双倍长密钥算法加解密。

12.5.6.3 应用系统专用账号

应用系统专用账号应仅供应用程序访问数据库使用，不将其作为访问账号向用户提供。正常情况下数据库操作应通过交易或应用程序访问的方式进行，应关闭非必须的访问数据库应用工具。

12.5.6.4 交易监控敏感数据屏蔽

入网机构如存在交易监控，监控屏应屏蔽用户敏感数据，如账号（屏蔽账号校验位前的若干位），磁道信息、验证码、个人标识代码及有效期。

12.5.7 恶意代码防护

12.5.7.1 恶意代码防护管理

应配备相应的人员负责恶意代码防护工作的日常管理及维护，监控计算机系统恶意代码防护情况，定期察看恶意代码威胁日志，并对日志中的威胁记录进行处理。用户在装载外部介质上的数据和程序之前必须对外部介质进行扫描以防止病毒。

12.5.8 运营管理要求

12.5.8.1 应用系统数据备份

涉及移动支付交易的应用系统数据需每日进行增量备份，应定期进行完全备份。备份的数据应定期进行同城异处存放。

12.5.8.2 重要系统服务器双机备份

重要的生产系统服务器应采用双机备份的设计，其所连接的磁盘阵列应为冗余阵列。

12.5.8.3 网络设备热备份

防火墙、路由器、交换机等网络设备均应有热备份，接入移动支付联网通用管理机构网络的通信线路应有备份，并且备份线路与主线路应采用不同运营商提供的路由。

12.6 入网商户管理

12.6.1 线下商户管理

12.6.1.1 线下商户管理要求

对于线下商户，使用近场支付服务时，技术上要求按照受理终端及通讯网络提供方规定执行，并由其确保支付过程的安全性。

12.6.2 线上商户管理

12.6.2.1 交易传输安全

a) 应使用足够强度的加密算法和安全协议保护移动终端与远程支付系统之间的连接，且尽可能进行双向认证，例如可使用包括但不限于 SSL/TLS 或 IPSEC 等协议；
b) 如使用 SSL 协议，应使用 3.0 及以上相对高版本的协议，取消对低版本协议的支持；
c) 移动终端到远程支付系统的 SSL 加密密钥长度应不低于 128 位，用于签名的 RSA 密钥长度应不低于 1024 位，用于签名的 ECC 密钥长度应不低于 160 位；
d) 应定时重新协商会话密钥。

12.6.2.2 业务数据安全

a) 支付内容平台与远程支付系统应当对发送的报文关键要素计算 MAC 或进行签名加密，以供接收方校验报文的真实性及保证关键要素数据的机密性。关键要素包括但不限于商户代码、订单

编号、订单日期时间、交易金额等。报文的接收方，用与发送方相同的方法计算 MAC 或进行验签，并验证报文 MAC 或签名的正确性；

b) 交易原始数据包括但不限于交易报文，交易数据保存应将敏感信息进行加密处理，包含但不仅限于姓名、联系方式、交易内容等信息，保存时间应不少于法律法规及国家或行业相关部门规章规定的年限。

12.6.2.3 交易过程安全

a) 支付内容平台应必须支持与远程支付系统之间的相互正常访问，包含但不仅限于负载均衡、限制最大并发连接数等技术手段；
b) 支付内容平台与远程支付系统应可防止对交易的重放攻击；
c) 支付内容平台应对常见的 WEB 攻击（如跨站脚本攻击、注入攻击、拒绝服务攻击等）进行有效防范；
d) 支付内容平台与远程支付系统应实现相互身份鉴别，包含但不仅限于证书签名等技术手段；
e) 应保证交易的抗抵赖性，包含但不仅限于证书签名等技术手段；
f) 支付内容平台与远程支付系统应防止对支付成功的订单重复支付。

12.7 入网安全

12.7.1 入网接入线路

12.7.1.1 入网机构专线接入

入网机构与转接清算系统应以专线方式连接，每一个接入机构都应有主备通讯设备和主备通讯线路，主备线应尽量选择当地不同的运营商，避免通讯设备与线路的单点故障。

12.7.2 安全管理制度

12.7.2.1 安全管理制度要求

入网机构在与转接清算系统联网的接口建设中应提供严格的系统安全管理制度，包括信息存取控制、应用系统操作、物理实体（机房、设备、通信网络、记录媒体等）、加密算法、密钥管理、人员管理等。

12.7.3 数据传输安全

12.7.3.1 数据传输安全控制

应实现以下数据传输安全控制要求：

a) 密钥管理机制：在技术上应实施严格和可靠的密钥分配过程；
b) 个人标识码(PIN)的加密及转换机制：不允许 PIN 明码出现在通信线路上和人工可操作的存储媒体上；
c) 交易报文来源正确性鉴别(MAC)；
d) 系统间敏感数据应加密并计算 MAC。

12.7.4 密钥管理

12.7.4.1 加密算法

a) 对称加密算法；

b） 非对称加密算法。

12.7.4.2 密钥层次

a） 密钥层次；
b） 密钥间关系。

12.7.4.3 密钥产生

a） 主密钥；
b） 成员主密钥；
c） 工作密钥。

12.7.4.4 密钥分发

a） 成员主密钥分发途径；
b） 工作密钥分发途径。

12.7.4.5 密钥存储

a） 主密钥；
b） 工作密钥和成员主密钥。

12.7.4.6 密钥更新

a） 主密钥的更新；
b） 成员主密钥的更新；
c） 工作密钥的更新。

12.7.4.7 密钥销毁

密钥销毁过程

12.7.5 报文加密

12.7.5.1 PIN 传输

应正确实现如下功能：
a） PIN 的数据类型；
b） PIN 的字符集；
c） PIN 数据块；
d） PIN 的加密方法。

12.7.5.2 联机报文 MAC 计算

应正确实现如下功能：
a） MAC 报文域选择；
b） MAC 报文域构成规则；
c） MAC 计算。

12.7.5.3 新旧密钥切换

应正确实现新旧密钥切换。

12.7.6 关键信息保护

12.7.6.1 系统传输关键信息保护

应对各相关系统和转接清算系统间传输报文的关键数据域进行加密。

附 录 A
（规范性附录）
操作规程

A.1 基本规定

a) 检测启动应满足《检测规范》以及其他相关规定的要求；
b) 检测机构的检测流程包括但不限于：前期准备、现场检测、综合分析、出具报告等部分。其中，现场检测包括但不限于：启动会议、末次会议、中间问题沟通及最终问题确认环节；
c) 在准备阶段，检测机构应向被检测机构提供《移动支付业务系统检测准备清单》，要求被检测机构填写《移动支付业务系统情况调查表》，并且要求其逐页签字确认并反馈，同时检测机构要与被检测机构共同制定《移动支付业务系统检测计划》，并且双方签字确认；
d) 检测机构对现场检测中检测出的问题进行分析汇总，向被检测机构出具《移动支付业务系统检测问题确认单》，并且双方逐页签字确认；被检测机构要声明外包情况，并盖章后反馈给检测机构；
e) 问题确认后，经过检测机构和被检测机构协商，被检测机构可以就某些或者全部问题进行整改，并出具《移动支付业务系统检测整改报告》，整改后检测机构要进行回归测试；
f) 现场检测过程中要保证检测环境、系统版本稳定，一旦进入现场检测阶段，不允许再修改；
g) 被检测机构的涉密文档、核心配置等材料，检测机构要在被检测机构的制度约定下，协商查看方式、地点等。

A.2 功能检测

a) 功能检测的目的是在检测环境下，从适合性和准确性两方面考虑，检测《检测规范》中规定的业务功能处理及相关要求。凡检测基本要求中必测项描述为“……功能”的，必须完全由系统中的功能模块实现；其他情况可以部分由人工实现；
b) 检测人员应在检测报告中声明《检测规范》中规定的业务功能点所对应的系统位置；
c) 被检测机构应声明支持的浏览器及其版本，以及其他必需共存软件的版本情况，检测人员应根据声明采取随机抽样的方式确定检测环境中浏览器的版本或共存软件的版本，被检测机构按照确定的版本搭建客户端的模拟环境，检测人员应在检测报告中声明使用的浏览器或必要共存软件的版本；
d) 检测人员应采用黑盒测试方法。适合性方面建议采用功能分解的方法，将每一个功能加以分解，确保各个功能被全面地检测；准确性方面建议采用如等价类划分、边界值分析、猜错法、因果图等方法，确保功能检测的充分性；
e) 检测人员检测时应获取测试数据，包括获取现有的测试数据或生成新的数据，并按照要求验证所有数据。

A.3 性能检测

a) 性能检测主要目的是在规定的硬件环境条件和给定的业务压力下，考核系统是否满足性能需求。通过对系统时间特性和资源特性两方面的检测，应考察系统以下 3 个方面能力：一是系统的并发能力；二是在规定的硬件环境条件和给定的业务压力下，考核系统是否满足性能需求和压力解除后系统自恢复能力；三是系统性能极限；
b) 检测人员应按照《移动支付业务系统情况调查表》中声明的需求，确定在规定环境下的并发用户数、在线用户数、场景压力分配比例、吞吐量、大数据量、系统自恢复时间等指标，并在检测报告中声明；
c) 检测人员应在检测开始前检查检测环境，主要包括：基础数据是否到位、测试用账户和数据是否准备完毕等，并在检测报告中声明检测环境、检测工具、基础数据量等信息；
d) 在系统的并发能力验证方面，检测人员应采用并发检测策略，记录响应时间、并发用户数、系统资源利用情况；
e) 在压力解除后系统自恢复能力验证方面，检测人员应采用吞吐量测试策略，记录平均响应时间、吞吐量、在线用户数、系统恢复时间及系统资源利用情况（CPU、内存等）。在线用户数的分配比例参照场景压力分配比例，吞吐量的测试典型场景选择按照《检测规范》性能部分要求的业务测试点进行选择，其中必测项必须包含在典型场景内；
f) 在系统性能极限验证方面，检测人员应采用极限测试策略，记录响应时间、并发用户数、系统资源利用情况（CPU、内存等）。在执行极限测试时，当被测并发用户数落入并发用户数的 1.5-3 倍区间内，可以停止测试，当前被测并发用户数可以视作极限并发用户数。

A.4 安全性检测

a) 安全性检测应根据《检测规范》内容逐项检测，并结合对现场人员的抽查记录，进行统计分析，对相应表格的各项评价内容给出评价；
b) 安全性检测的检测方法应包括但不限于：
   1) 对网络设备、主机设备以及相关应用安全配置策略的检测；
   2) 对相关文档的审核；
   3) 用相应工具设备或安全设备对网络、主机等设备进行扫描；
   4) 故障知识库的检查、对日志访问权限和保存的检查；
   5) 检查防恶意代码产品（硬件、软件、或通过其他安全设备实现）的策略配置、漏洞更新情况；
   6) 检查部署何种安全设备或在安全设备上开启何种策略来抵抗 DOS/DDOS 攻击；
   7) 检查设备采用哪两种身份鉴别机制、对配置文件的离线备份的检查；
   8) 对系统备份策略、备份数据如何保存、遇到问题如何恢复等进行检查；
   9) 对审计安全配置、审计日志保存空间的权限分配等策略的检查；
   10) 对管理员是否使用漏洞扫描设备对主机设备进行定期扫描等进行检查；
   11) 对主机操作系统上用户权限划分的检查；
   12) 对相关应用的渗透性检测；
   13) 对登录口令的复杂度要求、登录失败处理参数进行检查；
   14) 对数据存放位置的权限的检查；
   15) 对程序出现问题后的故障恢复措施进行检测；
   16) 对通信报文和会话进行抓包分析，分析报文是否采用校验或密码技术保证保密性；
   17) 对被测系统是否提供原发和抗抵赖功能进行检测，检测系统如何给出原发或接收证据；
   18) 对使用的认证技术和证书进行检查，检查服务器证书保护措施；

19) 对使用的监控手段和设备进行核查；
20) 对备份设备、备份链路、备份数据等的查看。

A.5 风险监控检测

a) 风险监控检测是针对移动支付业务系统风险监控能力的检测，检测机构须遵照《检测规范》中风险监控检测部分包含的检测项进行检测，并给出相应的评价；
b) 风险监控的检测方法应包括但不限于：
   1) 检测移动支付机构在相关风险管理制度中是否完整、明确地描述账户风险事件类型和相应的风险控制措施；
   2) 通过行为记录、日志检查、账户资金变更跟踪等手段进行风险分析；
   3) 检测对账户的人工操作是否保证处理过程中的职责分离；
   4) 检测移动支付　　机构在相关风险管理制度中是否明确定义各类交易监控和交易审核规则；
   5) 通过实际交易或查看交易监控与交易审核规则，以及相关记录验证交易监控与交易审核的实时性；
   6) 通过报表查询检测交易记录的正确性；
   7) 通过检测交易监控系统对风险交易和异常交易的识别，检测其对异常事件的预警能力；
   8) 检测风险管理体系中是否支持人工对规则进行维护。没有功能模块实现，但是线下采用人工补偿方法可以正确实现该功能的，可降低一级问题级别。

A.6 文档审核

a) 文档检测是针对被检测机构文档的完整性、有效性、一致性、是否符合相关标准等方面进行检测，内容应包括：用户文档、开发文档和管理文档，以上内容须遵照《检测规范》中文档检测部分包含的检测项进行检测，并给出相应的评价；
b) 用户文档检测应按《检测规范》文档检测中用户文档部分的检测内容进行检测，检测方法包括但不限于：
   1) 检测操作和文档描述是否一致；
   2) 通过查阅版本历史的方式检测文档的版本控制和管理。
c) 开发文档检测应按《检测规范》文档检测中开发文档部分的检测内容进行检测，检测方法包括但不限于：
   1) 依据待查内容列表对被检测文档进行审核；
   2) 结合功能检测结果检测开发文档和系统实现的一致性；
   3) 检测开发文档之间是否存在冲突。
d) 管理文档检测应按《检测规范》文档检测中管理文档部分的检测内容进行检测，检测方法主要采用抽查的方式，依据待查内容列表对被检测文档进行审核。

A.7 外包管理检测

a) 外包检测是针对支付系统外包给第三方机构的情况下对外包服务相关内容进行的检测，内容应包括：外包服务的外包内容、外包服务在第三方的处理情况、安全保密协议、风险评估、外包

商资质、外包合同、控制和监督以及外包交付流程，以上内容须遵照《检测规范》中外包附加检测部分包含的检测项进行检测，并给出相应的评价；

b) 外包提供的服务应包括：基础设施运维服务、应用系统运维服务和安全管理服务等。其中，基础设施运维服务是指对 IT 基础设施进行监视、日常维护和维修保障；基础设施运维服务包括网络系统、主机系统、存储/备份系统、安全系统等；应用系统运维服务是指对应用系统进行维护及改进。安全管理服务是指对 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；

c) 外包服务的外包内容审查主要通过被检测机构和外包第三方服务机构的合同和安全保密协议进行服务内容的检测；

d) 外包服务在第三方的处理情况检测主要查看被检测机构对外包服务商的监督和管理情况，及相关记录执行情况；

e) 外包风险评估检测应要求被检测机构提供有关外包服务的外包商评估材料等；

f) 外包商资质检测应对外包商资质进行审查，检查是否保留资质证明材料；

g) 控制和监督检测应查看被检测机构对外包服务的控制和监督措施，并评估本措施的有效性；

h) 外包交付流程检测应查看第三方外包机构向被检测机构提交的项目交付材料清单和业务培训证明材料。

附 录 B
（规范性附录）
判定准则

B.1 问题等级分类

B.1.1 严重性问题

与相关法律法规、标准规范有明显冲突；系统不满足业务需求；主要业务流程不正确；存在安全风险，会对客户利益造成严重的损害。

B.1.2 一般性问题

局部功能无法正常使用，但不影响系统整体流程的实现；存在安全风险，会对客户利益造成直接或潜在的损害。

B.1.3 建议性问题

功能能够正常使用，但系统易用性差；存在安全风险，但不会对客户利益造成直接或潜在的损害。

B.2 检测结果判定

B.2.1 检测项结果判定原则

a) 不符合：在检测过程中，发现严重性问题和一般性问题，该检测项的检测结果判定为“不符合”；
b) 符合：在检测过程中，未发现问题或仅发现建议性问题，该检测项的检测结果判定为“符合”；
c) 不适用：在各检测类检测过程中，根据厂商声明，被检测系统未提供的非必测项可判定为“不适用”，必测项不能判定为“不适用”，风险监控类、安全类检测项除外。在风险监控类、安全类检测过程中，检测要求对抗的威胁在被测系统中不存在，该检测项判定为“不适用”。判定为不适用的风险监控类、安全类检测项需说明原因和带来的安全影响。

B.2.2 检测类结果判定原则

a) 不符合：该检测类中存在因严重问题导致的“不符合”检测项，则该检测类的检测结果判定为“不符合”。该检测类中存在因一般问题导致的“不符合”检测项，如果不符合率为以下情况的，则该检测类的检测结果判定为“不符合”：
   1) 属于功能类的检测项，其检测结果中不符合率大于 15%；
   2) 属于风险监控类的检测项，其检测结果中不符合率大于 15%；
   3) 属于性能类的检测项，其检测结果中不符合率大于 15%；
   4) 属于安全类的检测项，其检测结果中不符合率大于 15%；
   5) 属于文档类的检测项，其检测结果中不符合率大于 15%。

b) 符合：该检测类中检测项的检测结果全部为“符合”，则该检测类的检测结果判定为“符合”。该检测类中存在因一般问题导致的“不符合”检测项，如果不符合率为以下情况的，则该检测类的检测结果判定为“符合”：

1) 属于功能类的检测项，其检测结果中不符合率小于或等于 15%；
2) 属于风险监控类的检测项，其检测结果中不符合率小于或等于 15%；
3) 属于性能类的检测项，其检测结果中不符合率小于或等于 15%；
4) 属于安全类的检测项，其检测结果中不符合率小于或等于 15%；
5) 属于文档类的检测项，其检测结果中不符合率小于或等于 15%。

B.2.3 检测报告结果判定原则

a) 不符合：检测类的检测结果存在“不符合”，检测报告结果判定为“不符合”；
b) 符合：其他情况检测报告结果判定为“符合”。