ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0098.7—2012

中国金融移动支付 检测规范 第7部分：可信服务管理系统

China financial mobile payment—Test specifications—
Part 7: Trusted service manager

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7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。可信服务管理系统是移动支付的可信基础设施，提供了移动支付的安全可信、开放共享、多账户应用共存与互联互通的平台。

为确保可信服务管理系统的安全、可靠，在收集、分析和评估可信管理系统风险的基础上，本部分对可信服务管理系统的功能、性能、安全性和文档审核四个方面的检测要求进行了规定。

中国金融移动支付　检测规范　第7部分：可信服务管理系统

1　范围

本部分规定了移动支付可信服务管理系统（简称TSM系统）的检测内容、判定准则，包括可信服务管理系统的功能、性能、安全性和文档审核四个检测类的检测要求、检测项及判定准则。

本部分适用于指导检测机构制定移动支付可信服务管理系统技术标准符合性和安全性检测方案、执行检测以及判定检测结果的符合性。

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　总则

3.1　检测目标

检测目标是在系统版本确定的基础上，对可信服务管理系统功能、性能、安全性和文档四项检测类进行检测，客观、公正评估系统是否符合中国人民银行对可信服务管理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。

3.2　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。

3.3　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。

4 检测项列表

4.1 功能性检测项

验证移动支付TSM系统的业务功能的正确性，检测系统业务处理的准确性，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	安全单元的生命周期管理	安全单元的个人化与注册	必测项
		安全单元的合法性检查	必测项
		安全单元的终止	必测项
		安全单元的挂失与解挂	必测项
		安全单元的锁定与解锁	必测项
		安全单元状态查询	必测项
		安全单元应用信息查询	必测项
		安全单元状态同步	必测项
1.2	辅助安全域生命周期管理	辅助安全域的创建	必测项
		辅助安全域的删除	必测项
		辅助安全域的锁定/解锁	必测项
		辅助安全域密钥更新	必测项
1.3	应用生命周期管理	应用查询	必测项
		应用下载与授权	必测项
		应用个人化	必测项
		应用锁定/解锁	必测项
		应用删除	必测项
		远程管理指令同步	必测项
		SE 应用同步	必测项
1.4	合作 TSM 管理	合作 TSM 管理	必测项
1.5	应用提供方管理	注册	必测项
		审核	必测项
		更新	必测项
		状态变更	必测项
1.6	应用管理	PAID 申请	必测项
		上传	必测项
		测试、审核	必测项
		发布	必测项
		下架	必测项
1.7	移动支付 TSM 系统间接口 / 公共服务平台与 TSM 的接口	PAID 申请	必测项
		应用列表同步	必测项
		应用下载许可	必测项
		应用下载许可（公共服务平台）	必测项
		验证结果通知	必测项

编号	检测项			检测项说明
			安全域密钥交换	必测项
			Token 申请	必测项
			发卡方创建安全域申请	必测项
			发卡方安全域删除/锁定/解锁申请	必测项
			公共服务平台创建安全域申请	
			公共服务平台应用操作许可	
			公共服务平台安全域删除/锁定/解锁申请	
			操作结果通知	必测项
			SE 信息查询	必测项
			SE 应用列表查询	必测项
			SE 身份验证	必测项
			SE 激活	必测项
		TSM 与客户端接口	SE 激活	必测项
			应用查询	必测项
			应用同步	必测项
			应用下载/删除/锁定/解锁	必测项
			应用个人化	必测项
			应用远程管理同步	必测项
			SE 的锁定/解锁/终止	必测项
			安全域的锁定/解锁/终止	必测项

4.2 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，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	安全单元的生命周期管理	安全单元的个人化与注册	必测项
			安全单元的合法性检查	必测项
		辅助安全域生命周期管理	辅助安全域的创建	必测项
		应用生命周期管理	应用查询	必测项
			应用下载与授权	必测项
			应用个人化	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

4.3 安全性检测项

4.3.1 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	必测项
		建筑物内机房位置	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
		机房划分区域管理	必测项
		重要区域第二道电子门禁系统	必测项
3.1.3	防盗窃和防破坏	主要设备放置	必测项
		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	避雷装置	必测项
		防雷保安器	必测项
		交流电源地线	必测项
3.1.5	防火	火灾自动消防系统	必测项
		耐火建筑材料	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	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
		防静电地板	必测项
		静电消除器（增强要求）	
3.1.8	温湿度控制	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	必测项
		备用电力供应	必测项
		冗余电力电缆线路	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
		线缆隔离铺设	必测项
		关键区域电磁屏蔽（增强要求）	

4.3.2　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
		内容过滤	必测项
		访问控制	必测项
		网络流量及连接数控制	必测项
		会话网络连接控制	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	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	网络设备用户身份鉴别	必测项
		主要网络设备用户身份鉴别（增强要求）	
		身份鉴别信息不可伪造（增强要求）	
		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
		网络设备软件更新	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	必测项

编号	检测项		检测项说明
		控移动设备的网络接入控制	必测项
		定期检查违规行为	必测项

4.3.3 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
		口令复杂度	必测项
		登录失败处理	必测项
		远程管理的传输模式	必测项
		用户名唯一	必测项
		用户身份信息组合鉴别技术	必测项
		鉴别警示信息设置（增强要求）	
		用户身份鉴别信息不可伪造（增强要求）	
3.3.2	访问控制	访问控制策略	必测项
		管理用户角色分配权限	必测项
		特权用户权限分离	必测项
		默认账户访问权限控制	必测项
		非正常帐户处理	必测项
		重要信息敏感标记	必测项
		敏感标记信息访问控制	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）	
		记录清空（增强要求）	
3.3.5	入侵防范	入侵行为记录和报警	必测项
		重要程序完整性保护	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
		不同恶意代码库	必测项
		防恶意代码软件统一管理	必测项
3.3.7	资源控制	接入控制	必测项
		超时锁定	必测项

编号	检测项		检测项说明
		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
		信息文档完整清除	必测项
3.3.8	可信路径	身份鉴别信息传输（增强要求）	
		系统访问信息传输（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
		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

4.3.4 数据安全

安全检测项如表6所示。

表6 数据安全检测项列表

编号	检测项		检测项说明
3.4.1	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
		数据备份记录	必测项
		备份数据定期检查	必测项
3.4.2	数据保密性	数据加密传输	必测项
		数据加密存储	必测项
3.4.3	备份和恢复	本地备份和恢复	必测项
		异地备份	必测项
		关键链路冗余设计	必测项
3.4.4	报文安全	报文格式	必测项
		报文完整性验证	必测项
		报文私密性	必测项
3.4.5	密钥安全	对称加密算法	必测项
		非对称加密算法	必测项
		杂凑算法	必测项
3.4.6	密钥管理	密钥生成	必测项
		密钥传输	必测项
		密钥存储	必测项
		密钥备份	必测项
		密钥恢复	必测项
		密钥归档	必测项
		密钥销毁	必测项

编号	检测项		检测项说明
		密钥更新	必测项

4.3.5 TSM 应用安全

安全检测项如表7所示。

表7 TSM 应用安全检测项列表

编号	检测项		检测项说明
3.5.1	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
		用户身份组合鉴别技术不可伪造（增强要求）	
3.5.2	访问控制	访问控制策略	必测项
		访问控制覆盖范围	必测项
		访问控制策略	必测项
		用户角色权限	必测项
		敏感标记设置（增强要求）	
		敏感标记信息资源访问控制（增强要求）	
		禁止默认帐户访问（增强要求）	
3.5.3	可信路径	身份鉴别信息安全传输路径	必测项
		资源访问信息安全传输路径	必测项
3.5.4	安全审计	审计范围	必测项
		审计保护	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）	
3.5.5	剩余信息保护	鉴别信息清除（增强要求）	
		记录清空（增强要求）	
3.5.6	通信完整性	通信完整性（增强要求）	
3.5.7	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
		加解密运算和密钥管理（增强要求）	
3.5.8	抗抵赖	数据原发证据	必测项
		数据接收证据	必测项
3.5.9	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）	
3.5.10	资源控制	自动结束会话	必测项
		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

编号	检测项		检测项说明
		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）	
3.5.11	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
3.5.12	应用服务器安全	防止网站身份被仿冒	必测项
		未授权存取动作防范	必测项
		防范应用内容被篡改	必测项
		最大并发连接数设置	必测项
		请求超时限制	必测项
		应用服务器负载均衡	必测项
3.5.13	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
		Cookies 标识会话	必测项
		会话标识防泄露	必测项
		Cookies 安全标记	必测项
		防止敏感信息泄露	必测项
		应用审计日志（增强要求）	
3.5.14	异常与容错	敏感信息回退清除	必测项
		页面异常信息处理后显示	必测项
		异常详细信息日志	必测项
3.5.15	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
		服务器端拒绝服务攻击防范	必测项
		文件上传下载访问控制	必测项
		数据库存储过程或参数化（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）	
3.5.16	初始化安全要求	基本要求	必测项
		密钥安全要求	必测项
		证书安全要求	必测项
		证书申请	必测项
3.5.17	SE 应用下载安全	SE 应用下载安全	必测项
3.5.18	SE 开通终端安全要求	传输报文加密	必测项
		POS 终端相关安全要求	必测项
3.5.19	终端与 TSM	传输安全	必测项

编号	检测项		检测项说明
		业务数据安全	必测项
		会话密钥	必测项
3.5.20	TSM 与应用提供方	传输安全	必测项
		业务数据安全	必测项
3.5.21	公共服务平台与 TSM 安全技术要求	公共服务平台与 TSM 安全技术要求	必测项

4.3.6 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
		建立贯穿支付系统的过程	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
		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

4.3.7 运行维护安全

运行维护安全检测项如表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

编号	检测项		检测项说明
		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
		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

4.3.8 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
		高可靠的磁盘阵列	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

4.4　文档检测项

对TSM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11所示。

表11　文档检测项列表

编号	检测项		检测项说明
4.1	用户文档	用户手册	必测项
		操作手册	必测项
4.2	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
4.3	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　检测内容

5.1 功能检测内容

5.1.1 安全单元的生命周期管理

5.1.1.1 安全单元的个人化与注册

TSM系统应实现安全单元的个人化与注册的功能。

5.1.1.2 安全单元的合法性检查

TSM系统应具有向公共服务平台发起安全单元合法性验证的功能。

5.1.1.3 安全单元的终止

TSM系统应实现安全单元终止功能，安全单元的终止包括整卡终止和金融SE的终止。

5.1.1.4 安全单元的挂失与解挂

TSM系统应实现安全单元的挂失、解挂功能，包括整卡挂失/解挂和金融SE的挂失/解挂。

5.1.1.5 安全单元的锁定与解锁

TSM系统应实现安全单元的锁定、解锁功能，包括整卡锁定/解锁和金融SE的锁定/解锁。

5.1.1.6 安全单元状态查询

TSM应具有获取系统中注册的安全单元的相关信息的功能。

5.1.1.7 安全单元应用信息查询

TSM应具有安全单元应用信息查询的功能。

5.1.1.8 安全单元状态同步

TSM系统应具有安全单元同步的功能。

5.1.2 辅助安全域生命周期管理

5.1.2.1 辅助安全域的创建

TSM系统应具备在本机构发行的SE中创建辅助安全域的功能。业务系统不能为非本机构发行的SE创建辅助安全域。

5.1.2.2 辅助安全域的删除

TSM系统应具有删除辅助安全域的功能。

5.1.2.3 辅助安全域的锁定/解锁

TSM系统应具有辅助安全域的锁定和解锁的功能。

5.1.2.4 辅助安全域密钥更新

TSM系统应具有更新辅助安全域密钥的功能。

5.1.3 应用生命周期管理

5.1.3.1 应用查询

TSM系统应具有查询应用列表及状态的功能。

5.1.3.2 应用下载与授权

TSM系统应提供应用下载与授权的功能。

5.1.3.3 应用个人化

TSM系统应具有应用个人化的功能。

5.1.3.4 应用锁定/解锁

TSM应具有锁定/解锁应用的功能。

5.1.3.5 应用删除

TSM应具有删除应用的功能。

5.1.3.6 远程管理指令同步

TSM系统应具有与安全单元同步远程管理指令的功能。

5.1.3.7 SE 应用同步

TSM系统应实现SE应用同步功能。

5.1.4 合作 TSM 管理

应实现每个TSM系统与其它合作应用提供方的TSM系统的关系列表功能。

5.1.5 应用提供方管理

5.1.5.1 注册

TSM系统应具有接受应用提供方申请接入的功能。

5.1.5.2 审核

TSM系统应具有审核应用提供方信息的功能。

5.1.5.3 更新

TSM系统应具有更新应用提供方信息的功能。

5.1.5.4 状态变更

TSM系统应具有变更应用提供方信息的功能。

5.1.6 应用管理

5.1.6.1 PAID 申请

TSM系统应实现应用提供方的应用PAID申请功能。

5.1.6.2 上传

TSM系统应具有上传应用的功能。

5.1.6.3 测试、审核

TSM系统应具有审核应用的功能。

5.1.6.4 发布

TSM系统应具有发布应用的功能。

5.1.6.5 下架

TSM系统应实现应用下架功能。

5.1.7 移动支付 TSM 系统间接口

5.1.7.1 公共服务平台与 TSM 的接口

应实现如下系统接口功能：

——PAID 申请；
——应用列表同步；
——应用下载许可；
——应用下载许可（公共服务平台）；
——验证结果通知；
——安全域密钥交换；
——Token 申请；
——发卡方创建安全域申请；
——发卡方安全域删除/锁定/解锁申请；
——公共服务平台创建安全域申请；
——公共服务平台应用操作许可；
——公共服务平台安全域删除/锁定/解锁申请；
——操作结果通知；
——SE 信息查询；
——SE 应用列表查询；
——SE 身份验证；
——SE 激活。

5.1.7.2 TSM 与客户端接口

应实现如下系统接口功能：

——SE 激活；
——应用查询；
——应用同步；
——应用下载/删除/锁定/解锁；
——应用个人化；
——应用远程管理同步；
——SE 的锁定/解锁/终止；
——安全域的锁定/解锁/终止。

5.2 性能检测内容

5.2.1 时间特性

选取系统核心的业务功能进行基准检测、并发检测、极限检测和吞吐量检测，考察其时间特性。

——安全单元的生命周期管理：

- 安全单元的个人化与注册；
- 安全单元的合法性检查。

——辅助安全域生命周期管理：

- 辅助安全域的创建。

——应用生命周期管理：

- 应用查询；
- 应用下载与授权；
- 应用个人化。

5.2.2 资源利用率

5.2.2.1 检测过程中服务器资源占用情况

在对系统核心业务功能的检测过程中，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。

5.2.2.2 压力解除后服务器资源占用情况

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。

5.3 安全检测内容

5.3.1 物理安全

5.3.1.1 物理位置选择

5.3.1.1.1 机房和办公场地所在建筑物

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。

5.3.1.1.2 建筑物内机房位置

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。

5.3.1.2 物理访问控制

5.3.1.2.1 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。

5.3.1.2.2 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。

5.3.1.2.3 机房划分区域管理

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。

5.3.1.2.4 重要区域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。

5.3.1.3 防盗窃和防破坏

5.3.1.3.1 主要设备放置

应将主要设备放置在机房内。

5.3.1.3.2 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。

5.3.1.3.3 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。

5.3.1.3.4 介质保管

应对介质分类标识，存储在介质库或档案室中。

5.3.1.3.5 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。

5.3.1.3.6 机房监控报警系统

应对机房设置监控报警系统。

5.3.1.4 防雷击

5.3.1.4.1 避雷装置

机房建筑应设置避雷装置。

5.3.1.4.2 防雷保安器

应设置防雷保安器，防止感应雷。

5.3.1.4.3 交流电源地线

机房应设置交流电源地线。

5.3.1.5 防火

5.3.1.5.1 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。

5.3.1.5.2 耐火建筑材料

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。

5.3.1.5.3 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。

5.3.1.6 防水和防潮

5.3.1.6.1 水管安装

水管安装，不得穿过机房屋顶和活动地板下。

5.3.1.6.2 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。

5.3.1.6.3 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。

5.3.1.7 防静电

5.3.1.7.1 接地防静电措施

设备应采用必要的接地防静电措施。

5.3.1.7.2 防静电地板

机房应采用防静电地板。

5.3.1.7.3 静电消除器

应采用静电消除器等装置，减少静电的产生（增强要求）。

5.3.1.8 温湿度控制

5.3.1.8.1 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。

5.3.1.9 电力供应

5.3.1.9.1 供电线路防护设备

应在机房供电线路上配置稳压器和过电压防护设备。

5.3.1.9.2 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。

5.3.1.9.3 冗余电力电缆线路

应设置冗余或并行的电力电缆线路为计算机系统供电。

5.3.1.9.4 备用供电系统

应建立备用供电系统。

5.3.1.10 电磁防护

5.3.1.10.1 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。

5.3.1.10.2 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。

5.3.1.10.3 关键区域电磁屏蔽

应对关键区域实施电磁屏蔽。（增强要求）

5.3.2 网络安全

5.3.2.1 结构安全

5.3.2.1.1 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。

5.3.2.1.2 设备网络冗余（增强）

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。（增强要求）

5.3.2.1.3 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。

5.3.2.1.4 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。

5.3.2.1.5 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。

5.3.2.1.6 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。

5.3.2.1.7 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。

5.3.2.2 访问控制

5.3.2.2.1 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。

5.3.2.2.2 地址转换和绑定

重要网段应采取技术手段防止地址欺骗。

5.3.2.2.3 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、POP3等协议命令级的控制。

5.3.2.2.4 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，控制粒度为单个用户。

5.3.2.2.5 网络流量及连接数控制

应限制网络最大流量数及网络连接数。

5.3.2.2.6 会话网络连接控制

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。

5.3.2.2.7 远程拨号访问控制

应限制具有拨号访问权限的用户数量。

5.3.2.3 安全审计

5.3.2.3.1 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。

5.3.2.3.2 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。

5.3.2.3.3 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。

5.3.2.3.4 审计跟踪极限（增强）

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。（增强要求）

5.3.2.3.5 集中审计（增强）

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。（增强要求）

5.3.2.4 边界完整性检查

5.3.2.4.1 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。

5.3.2.5 入侵防范

5.3.2.5.1 网络 ARP 欺骗攻击

应能够有效的防范网络ARP欺骗攻击。

5.3.2.5.2 信息窃取

应采用防范信息窃取的措施。

5.3.2.5.3 DOS/DDOS 攻击

应具有防DOS/DDOS攻击设备或技术手段。

5.3.2.5.4 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）

5.3.2.6 恶意代码防范

5.3.2.6.1 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。

5.3.2.6.2 定时更新

应维护恶意代码库的升级和检测系统的更新。

5.3.2.7 网络设备防护

5.3.2.7.1 网络设备用户身份鉴别

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。

5.3.2.7.2 主要网络设备用户组合身份鉴别（增强）

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。

5.3.2.7.3 身份鉴别信息不可伪造（增强）

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。

5.3.2.7.4 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。

5.3.2.7.5 登录地址限制

应对网络设备的管理员登录地址进行限制。

5.3.2.7.6 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。

5.3.2.7.7 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。

5.3.2.7.8 权限分离

应实现设备特权用户的权限分离。

5.3.2.8 网络安全管理

5.3.2.8.1 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。

5.3.2.8.2 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。

5.3.2.8.3 网络设备软件更新

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。

5.3.2.8.4 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。

5.3.2.8.5 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。

5.3.2.8.6 外部连接

应保证所有与外部系统的连接均得到授权和批准。

5.3.2.8.7 移动设备网络接入控制

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。

5.3.2.8.8 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。

5.3.3 主机安全

5.3.3.1 身份鉴别

5.3.3.1.1 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。

5.3.3.1.2 口令复杂度

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。

5.3.3.1.3 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。

5.3.3.1.4 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。

5.3.3.1.5 用户名唯一

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。

5.3.3.1.6 用户身份信息组合鉴别技术

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。

5.3.3.1.7 鉴别警示信息设置（增强）

应设置鉴别警示信息，描述未授权访问可能导致的后果。（增强要求）

5.3.3.1.8 用户身份鉴别信息不可伪造（增强）

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。（增强要求）

5.3.3.2 访问控制

5.3.3.2.1 访问控制策略

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。

5.3.3.2.2 管理用户角色分配权限

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。

5.3.3.2.3 特权用户权限分离

应实现操作系统和数据库系统特权用户的权限分离。

5.3.3.2.4 默认账户访问权限控制

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。

5.3.3.2.5 非正常帐户处理

应及时删除多余的、过期的帐户，避免共享帐户的存在。

5.3.3.2.6 重要信息敏感标记

应对重要信息资源设置敏感标记。

5.3.3.2.7 敏感标记信息访问控制

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。

5.3.3.3 安全审计

5.3.3.3.1 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。

5.3.3.3.2 审计事件

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。

5.3.3.3.3 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。

5.3.3.3.4 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。

5.3.3.3.5 审计进程保护

应保护审计进程，避免受到未预期的中断。

5.3.3.3.6 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。

5.3.3.3.7 集中审计（增强）

应能够根据信息系统的统一安全策略，实现集中审计。（增强要求）

5.3.3.4 剩余信息保护

5.3.3.4.1 鉴别信息清除

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。（增强要求）

5.3.3.4.2 记录清空

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。（增强要求）

5.3.3.5 入侵防范

5.3.3.5.1 入侵行为记录和报警

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。

5.3.3.5.2 重要程序完整性保护

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。

5.3.3.5.3 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。

5.3.3.6 恶意代码防范

5.3.3.6.1 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。

5.3.3.6.2 不同恶意代码库

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。

5.3.3.6.3 防恶意代码软件统一管理

应支持防恶意代码统一管理。

5.3.3.7 资源控制

5.3.3.7.1 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。

5.3.3.7.2 超时锁定

应根据安全策略设置登录终端的操作超时锁定。

5.3.3.7.3 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。

5.3.3.7.4 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。

5.3.3.7.5 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。

5.3.3.7.6 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。

5.3.3.8 可信路径

5.3.3.8.1 身份鉴别信息传输（增强）

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。（增强要求）

5.3.3.8.2 系统访问信息传输（增强）

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。（增强要求）

5.3.3.9 系统安全管理

5.3.3.9.1 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。

5.3.3.9.2 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。

5.3.3.9.3 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。

5.3.3.9.4 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。

5.3.3.9.5 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。

5.3.3.9.6 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。

5.3.4 数据安全

5.3.4.1 数据完整性

5.3.4.1.1 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。

5.3.4.1.2 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。

5.3.4.1.3 数据备份记录

应具备数据备份记录。

5.3.4.1.4 备份数据定期检查

定期随机抽取备份数据进行解压、还原，检查其内容有效性。

5.3.4.2 数据保密性

5.3.4.2.1 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。

5.3.4.2.2 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。

5.3.4.3 备份和恢复

5.3.4.3.1 本地备份和恢复

应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放。

5.3.4.3.2 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。

5.3.4.3.3 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。

5.3.4.4 报文安全

5.3.4.4.1 报文格式

应参考JR/T 0025.7的相关要求。

5.3.4.4.2 报文完整性验证

应对报文完整性进行验证。

5.3.4.4.3 报文私密性

应保证报文私密性。

5.3.4.5 密钥安全

5.3.4.5.1 对称加密算法

应正确实现DES、3DES、SM4等对称加密算法。

5.3.4.5.2 非对称加密算法

应正确实现RSA、SM2等非对称加密算法。

5.3.4.5.3 杂凑算法

应正确实现SHA-1、SM3等加密算法。

5.3.4.6 密钥管理

5.3.4.6.1 密钥生成

密钥应在国家密码管理机构许可的硬件加密设备中生成。

5.3.4.6.2 密钥传输

密钥传输时，应加密传输不得明文传输。

5.3.4.6.3 密钥存储

应采取严格的控制机制防止未授权的访问，以确保密钥的完整性并防止泄露。

5.3.4.6.4 密钥备份

应对密钥进行异地备份，并确保其安全性。

5.3.4.6.5 密钥恢复

密钥恢复时，密钥管理员及至少2名密钥分管员应同时到达现场，在硬件加密设备中进行，并应有书面操作记录。

5.3.4.6.6 密钥归档

当密钥到期后，密钥管理机构应将其归档保存，归档期限至少为5年，并应确保归档后的密钥对不会再次被使用。

5.3.4.6.7 密钥销毁

密钥归档期结束后，密钥管理机构应进行销毁，且备份的密钥也应一同销毁。密钥的销毁需要在密钥管理员与所有密钥分管员参与下进行，销毁过程应有详细的操作记录。

5.3.4.6.8 密钥更新

密钥应在国家密码管理机构许可的硬件加密设备中更新。

5.3.5 TSM 安全要求

5.3.5.1 初始化安全要求

5.3.5.1.1 基本要求

SE初始化应在安全的环境下进行，初始化的完成需要进行端到端的加密。

5.3.5.1.2 密钥安全要求

初始密钥应符合三级密钥体系的要求生成。密钥的生成、传输、存储等应符合相关密钥管理要求。

5.3.5.1.3 证书安全要求

用户SE个人化安全证书采用预植方式完成，预植过程需要在安全的方式下完成。

5.3.5.1.4 证书申请

证书应按照以下流程申请：由申请人通过柜面向发卡方提出申请，同时发卡方通过RA系统向公共服务平台CA提交申请信息，获得下载凭证，并将下载凭证放入密码信封交由申请人，申请人凭借下载凭证在注册时下载证书。

5.3.5.2 SE 应用下载安全

在委托管理模式进行应用操作需采用令牌机制进行应用下载审核。

5.3.5.3 SE 开通终端安全要求

5.3.5.3.1 传输报文加密

所有连接TSM系统的开卡终端与TSM系统之间的报文应采用对称密钥进行加密传输。

5.3.5.3.2 POS 终端相关安全要求

POS终端应符合相关安全规范要求。

机构使用的终端应经过金融行业主管部门授权认可的权威检测机构的检测，并最终获取主管部门的认证。

5.3.5.4 终端与 TSM

5.3.5.4.1 传输安全

——终端通过互联网进行连接 TSM 传输数据时，应采用数字证书保证数据的机密性、完整性和不可抵赖性；

——应使用足够强度的加密算法和安全协议保护客户端与服务器之间的连接，例如使用包括但不限于 SSL/TLS 和 IPSEC 等协议；

——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；

——客户端到服务器的 SSL 加密密钥长度应不低于 128 位，用于签名的 SM2 密钥为 256 位，RSA 密钥长度应不低于 1024 位；

——定时重新协商会话密钥；

——对于数据短信传输模式，包括上行短信和下行短信，关键数据域必须经通讯层加密及 MAC 校验码计算；

——数字证书的签发须有公共服务平台端的 CA 进行统一签发。

5.3.5.4.2 业务数据安全

——终端与 TSM 必须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应用数据下载安装指令、响应数据等，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；

——客户手机号、密码、证件号码等敏感信息按要求进行加密传输、保存和使用，显示时应进行屏蔽处理；

——通过互联网传输数据必须采用数字证书保证数据的机密性和完整性；

——数字证书的签发须有公共服务平台端的 CA 进行统一签发。

5.3.5.4.3 会话密钥

——会话包括报文加密会话密钥、报文 MAC 会话密钥；

——在加密 SE 和 TSM 系统之间传送的报文数据时，报文加密会话密钥由报文加密主密钥加上会话特征数据分散生成；

——在计算 SE 和 TSM 系统之间传送的报文数据的 MAC 时，报文 MAC 会话密钥由报文 MAC 主

密钥加上会话的特征数据分散生成；

——其中特征数据中包含的随机数由硬件设备随机数发生器产生。

5.3.5.5 TSM 与应用提供方

5.3.5.5.1 传输安全

——应使用足够强度的加密算法和安全协议保护 TSM 与应用发卡方之间的连接，通过互联网传输必须采用数字证书进行双向证书认证；

——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；

——TSM 到应用发卡方的 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 SM2 密钥长度应为 256 位；

——定时重新协商会话密钥；

——对于应用方下发的个人化数据以及应用下载数据，须通过数字证书等方式确保内容不被篡改；

——数字证书的签发须有公共服务平台端的 CA 进行统一签发。

5.3.5.5.2 业务数据安全

——TSM 与应用发卡方必须对发送的报文关键要素进行签名加密，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应用数据下载安装指令、响应数据等，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；

——通过互联网传输业务数据必须采用数字证书保证数据的机密性和完整性；

——数字证书的签发须有公共服务平台端的 CA 进行统一签发。

5.3.5.6 公共服务平台与 TSM 安全技术要求

——应使用足够强度的加密算法和安全协议保护公共服务平台与 TSM 之间的安全连接，通过互联网传输必须进行双向数字证书认证，例如可使用包括但不限于 SSL/TLS 等协议；

——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；

——公共服务平台与 TSM 的 SSL 加密密钥长度应不低于 128 位，用于签名的 RSA 密钥长度不低于 1024 位，用于签名的 SM2 密钥长度应不低于 256 位；

——定时重新协商会话密钥；

——对于公共服务平台与 TSM 之间的敏感数据传输，须采用数字证书等方式确保内容的机密性和完整性；

——数字证书的签发须有公共服务平台端的 CA 进行统一签发。

5.3.6 管理安全

5.3.6.1 组织机构

5.3.6.1.1 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。

5.3.6.1.2 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。

5.3.6.1.3 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。

5.3.6.1.4 部门设置

应设置专门的支付系统研发、测试、运行维护、安全、风险控制等部门或团队。

5.3.6.1.5 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。

5.3.6.1.6 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。

5.3.6.2 管理制度

5.3.6.2.1 建立管理制度体系

a) 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；
b) 应制订移动支付安全管理工作的总体方针和策略；
c) 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。

5.3.6.2.2 信息安全管理制度体系

应建立贯穿支付系统设计、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。

5.3.6.2.3 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。

5.3.6.3 安全策略

5.3.6.3.1 制订安全保障目标

应制订明确的支付系统总体安全保障目标。

5.3.6.3.2 制订安全策略

a) 应制订针对支付系统设计与开发、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；
b) 应制订支付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。

5.3.6.3.3 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。

5.3.6.3.4 风险定义与规避

a) 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；

b) 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。

5.3.6.3.5 安全级别定义与保护措施制订（增强）

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。

5.3.6.4 人员和文档管理

5.3.6.4.1 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。

5.3.6.4.2 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。

5.3.6.4.3 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。

5.3.6.4.4 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。

5.3.6.4.5 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。

5.3.6.4.6 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。

5.3.7 运行维护安全

5.3.7.1 环境管理

5.3.7.1.1 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。

5.3.7.1.2 机房出入管理

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。

5.3.7.1.3 办公环境保密性措施

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。

5.3.7.1.4 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。

5.3.7.1.5 机房进出登记表

应具有机房进出登记表。

5.3.7.2 资产管理

5.3.7.2.1 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。

5.3.7.2.2 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。

5.3.7.2.3 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。

5.3.7.2.4 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。

5.3.7.3 介质管理

5.3.7.3.1 介质使用管理

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。

5.3.7.3.2 介质存放环境保护措施

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。

5.3.7.3.3 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。

5.3.7.3.4 介质维修与销毁

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。

5.3.7.3.5 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。

5.3.7.3.6 介质分类与标识

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。

5.3.7.4 设备管理

5.3.7.4.1 设施定期维护

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。

5.3.7.4.2 设备采购审批控制

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。

5.3.7.4.3 设备维护管理制度

a) 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；
b) 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。

5.3.7.4.4 设备操作规程

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。

5.3.7.4.5 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。

5.3.7.5 监控管理

a) 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；
b) 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；
c) 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。

5.3.7.5.1 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。

5.3.7.5.2 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。

5.3.7.5.3 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。

5.3.7.6 密码管理

5.3.7.6.1 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。

5.3.7.7 变更管理

5.3.7.7.1 变更方案

应确认系统中要发生的变更，并制定变更方案。

5.3.7.7.2 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。

5.3.7.7.3 重要系统变更批准

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。

5.3.7.7.4 变更中止与恢复

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。

5.3.7.8 备份与恢复管理

5.3.7.8.1 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。

5.3.7.8.2 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。

5.3.7.8.3 数据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。

5.3.7.8.4 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。

5.3.7.8.5 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。

5.3.7.9 安全事件处置

5.3.7.9.1 安全事件报告和处置

a) 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；
b) 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；
c) 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。

5.3.7.9.2 安全事件分类和分级

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。

5.3.7.9.3 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。

5.3.7.10 应急预案管理

5.3.7.10.1 制定不同事件应急预案

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。

5.3.7.10.2 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。

5.3.7.10.3 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。

5.3.7.10.4 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。

5.3.7.10.5 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。

5.3.8 业务连续性

5.3.8.1 业务连续性需求分析

5.3.8.1.1 业务中断影响分析

应进行业务中断影响分析。

5.3.8.1.2 灾难恢复

应具备灾难恢复时间目标和恢复点目标。

5.3.8.2 业务连续性技术环境

5.3.8.2.1 备份机房

应具备备份机房。

5.3.8.2.2 网络双链路

应具备双链路。

5.3.8.2.3 网络设备和服务器备份

应具有同城应用级备份设施。

5.3.8.2.4 磁盘阵列

应使用高可靠的磁盘阵列。

5.3.8.2.5 远程数据库备份

应具备远程备份数据库。

5.3.8.3 业务连续性管理

5.3.8.3.1 业务连续性管理制度

应具备业务连续性管理制度。

5.3.8.3.2 应急响应流程

应具备应急响应流程。

5.3.8.3.3 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。

5.3.8.3.4 数据备份和恢复制度

应具备数据备份和恢复管理制度。

5.3.8.4 日常维护

5.3.8.4.1 业务连续性演练

应每年进行业务连续性演练。

5.3.8.4.2 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。

5.4 文档检测内容

5.4.1 用户文档

5.4.1.1 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。

5.4.1.2 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。

5.4.2 开发文档

5.4.2.1 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。

5.4.2.2 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。

5.4.2.3 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。

5.4.2.4 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。

5.4.2.5 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。

5.4.2.6 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。

5.4.2.7 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。

5.4.3 管理文档

5.4.3.1 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。

5.4.3.2 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。

5.4.3.3 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。

5.4.3.4 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。

5.4.3.5 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。

5.4.3.6 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。

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《TSM 系统检测准备清单》，要求被检测机构填写《TSM 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《TSM 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《TSM 系统检测问题确认单》，并且双方逐页签字确认或盖骑缝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《TSM 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，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；

b) 检测人员应按照《TSM 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 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。

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”。