非金融机构支付业务设施
技术认证规范

中国人民银行科技司

2011 年 6 月

目　　录

说　明

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认证规范。本规范的评估对象为申请或已获得《支付业务许可证》的非金融机构。

本规范的主要起草单位：中国人民银行科技司，北京中金国盛认证有限公司。

本规范的参与起草单位：中国信息安全认证中心、中国金融电子化公司、银行卡检测中心、中国信息安全测评中心、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）、中金金融认证中心有限公司、上海市信息安全测评认证中心、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）、信息产业部计算机安全技术检测中心、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、北京商服通网络科技有限公司、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、杉德巍康企业服务有限公司等。

非金融机构支付业务设施技术认证规范

1　范围

本规范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的要求。

本规范为认证机构、检测机构对非金融机构支付业务设施进行认证、检测的依据，也可作为非金融机构支付业务设施提供者改进自身技术能力的指导依据。

2　规范性引用文件

下列文件中的条款通过本技术规范的引用而成为本规范的条款。凡是注日期的引用文件，其随后所有的修订单（不包括勘误的内容）或修订版均不适用于本规范；凡是不注日期的引用文件，其最新版本适用于本规范；凡是注明报批的引用文件，正式发布后，正式发布版本适用于本规范。

（1）　JR/T ××××电子支付术语（报批）

（2）　JR/T ××××电子支付文件数据格式（报批）

（3）　JR/T ××××基于 INTERNET 的网上支付安全规范（报批）

（4）　JR/T ××××基于 INTERNET 的网上支付交易模型及流程（报批）

（5）　JR/T ××××基于 INTERNET 的网上支付报文结构及要素（报批）

（6）　GB/T-22239-2008 信息安全技术 信息系统安全等级保护基本要求 第七章第三级基本要求、第八章第四级基本要求

（7）　GB/T-22081-2008 信息技术 安全技术 信息安全管理实用规则 第十四章业务连续性管理

（8）　GB/T- 22080-2008 信息技术安全技术 信息安全管理体系要求

3　术语和定义

3.1　术语

3.1.1　非金融机构支付服务

是指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：

（1）　货币汇兑

（2）　互联网支付

（3） 移动电话支付

（4） 固定电话支付

（5） 数字电视支付

（6） 预付卡的发行与受理

（7） 银行卡收单

（8） 中国人民银行确定的其他支付服务

3.1.2 货币汇兑

是指经汇款方委托，依托公共网络或专用网络，将其货币资金转移给收款方的行为。

3.1.3 互联网支付

是指依托互联网实现收付款方之间货币资金转移的行为。

3.1.4 移动电话支付（近场支付）

是指移动终端上内嵌的智能卡通过非接触方式和支付受理终端进行通讯，实现货币支付与资金转移的行为。

3.1.5 移动电话支付（远程支付）

是指移动终端（通常指手机）以短信、WAP、客户端软件以及客户端软件加智能卡等方式，通过无线通信网络发出支付指令，实现货币支付与资金转移的行为。

3.1.6 固定电话支付

是指电话通过语音 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。

3.1.7 数字电视支付

是指依托交互机顶盒等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。

3.1.8 预付卡的发行与受理

是指以营利为目的发行的、在发行机构之外购买商品或服务的预付价值，包括采取磁条、芯片等技术以卡片、密码等形式发行的预付卡。预付卡不包括：

（1） 仅限于发放社会保障金的预付卡

（2） 仅限于乘坐公共交通工具的预付卡

（3） 仅限于缴纳电话费等通信费用的预付卡

（4） 发行机构与特约商户为同一法人的预付卡

3.1.9　银行卡收单

是指通过销售点（POS）终端等为银行卡特约商户代收货币资金的行为。

3.1.10　一般支付

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。

3.1.11　担保支付

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

3.1.12　协议支付

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，而无需客户在支付服务方授权即可完成付款的支付行为。

3.2　定义

3.2.1　基本要求

是对非金融机构支付业务设施的基础性技术要求。

3.2.2　增强要求

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。

4　评判原则

非金融机构支付业务设施技术认证的评判遵循以下原则：

（1）　客观性原则

必须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。

（2）　公正性原则

必须依据国家法律法规和认可规范，认可准则 CNAS-CC21、CNAS-CC22 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。

（3）　科学性原则

要以科学思想为指导，以事实为依据。

5 技术要求

5.1 货币汇兑系统要求

5.1.1 基本要求

货币汇兑系统应在系统功能、风险监控、系统性能、安全性、系统文档建设方面符合技术标准要求和管理要求，基本要求参见《非金融机构支付服务业务系统检测基本要求_货币汇兑部分》。

检测项参见附录 A.1。

5.1.2 增强要求

5.1.2.1 功能要求

（1） 客户账户管理

— 应实现客户账户的开户、修改、冻结/解冻、销户等功能。

5.1.2.2 风险监控要求

（1） 实名认证

— 应对客户身份进行实名认证。

5.1.2.3 安全性要求

（1） 网络安全

1) 网络结构安全

— 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；

— 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。

2) 网络安全审计

— 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，时钟保持与时钟服务器同步。

3) 网络入侵防范

— 当审查到攻击行为时，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。

4) 网络设备防护

— 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。

（2） 主机安全

1) 身份鉴别

— 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。

2) 可信路径

— 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。

3) 安全审计

— 应能够根据信息系统的统一安全策略，实现集中审计；

— 应保护审计进程，避免受到未预期的中断。

4) 入侵防范

— 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。

（3） 应用安全

1) 身份鉴别

— 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。

2) 安全审计

— 应根据系统统一安全策略，提供集中审计接口。

3) 剩余信息保护

— 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。

4) 应用容错

— 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。

5) 源码安全

— 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) 可信时间戳服务

— 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。

（4） 运维安全

1) 环境管理

— 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。

2) 监控管理

— 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。

5.2 互联网支付系统要求

5.2.1 基本要求

互联网支付系统应在系统功能、风险监控、系统性能、安全性、系统文档建设方面符合技术标准要求和管理要求，基本要求参见《非金融机构支付服务业务系统检测基本要求_互联网支付部分》。

检测项参见附录 A.2。

5.2.2 增强要求

5.2.2.1 功能要求

（1） 客户支付账户管理

— 应实现客户账户的开户、修改、冻结/解冻、销户等功能。

（2） 交易处理

— 报文设计符合《基于 INTERNET 的网上支付报文结构及要素》6.2.1、6.2.2、6.2.3、6.2.9、6.2.12、6.2.13 中的报文结构设计要求；

— 交易模型及流程设计符合《基于 INTERNET 的网上支付交易模型及流程》6.1.1、6.1.2、6.1.3、6.2.1、6.3.1 中的要求。

（3） 资金结算

— 报文设计符合《基于 INTERNET 的网上支付报文结构及要素》6.2.7、6.2.8 中的报文结构设计要求；

— 交易模型及流程设计符合《基于 INTERNET 的网上支付交易模型及流程》6.1.5 中的要求。

（4） 差错处理

— 报文设计符合《基于 INTERNET 的网上支付报文结构及要素》6.2.10、6.2.11 中的报文结构设计要求；

— 交易模型及流程设计符合《基于 INTERNET 的网上支付交易模型及流程》6.2.2 中的要求。

5.2.2.2 风险监控要求

（1） 实名认证

— 应对客户身份进行实名认证。

5.2.2.3 安全性要求

（1） 网络安全

1) 网络结构安全

— 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；

— 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。

2) 网络安全审计

— 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，时钟保持与时钟服务器

同步。

3) 网络入侵防范

— 当审查到攻击行为时，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。

4) 网络设备防护

— 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。

（2） 主机安全

1) 身份鉴别

— 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。

2) 可信路径

— 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。

3) 安全审计

— 应能够根据信息系统的统一安全策略，实现集中审计；

— 应保护审计进程，避免受到未预期的中断。

4) 入侵防范

— 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。

（3） 应用安全

1) 身份鉴别

— 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。

2) 安全审计

— 应根据系统统一安全策略，提供集中审计接口。

3) 剩余信息保护

— 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。

4) 应用容错

— 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。

5) 源码安全

— 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) 可信时间戳服务

— 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。

（4） 运维安全

1) 环境管理

— 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。

2) 监控管理

— 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。

5.3 移动电话支付（近场支付）系统要求

5.3.1 基本要求

移动电话支付（近场支付）系统应在系统功能、风险监控、系统性能、安全性、系统文档建设方面符合技术标准要求和管理要求，基本要求参见《非金融机构支付服务业务系统检测基本要求_移动电话支付（近场支付）部分》。

检测项参见附录 A.3。

5.3.2 增强要求

5.3.2.1 功能要求

（1） 客户支付账户管理

— 应实现客户账户的开户、修改、冻结/解冻、销户等功能。

5.3.2.2 风险监控要求

（1） 实名认证

— 应对客户身份进行实名认证。

5.3.2.3 安全性要求

（1） 网络安全

1) 网络结构安全

— 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；

— 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。

2) 网络安全审计

— 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，时钟保持与时钟服务器同步。

3) 网络入侵防范

— 当审查到攻击行为时，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。

4) 网络设备防护

— 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。

（2） 主机安全

1) 身份鉴别

— 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。

2) 可信路径

— 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。

3) 安全审计

— 应能够根据信息系统的统一安全策略，实现集中审计；

— 应保护审计进程，避免受到未预期的中断。

4) 入侵防范

— 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。

（3） 应用安全

1) 身份鉴别

— 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。

2) 安全审计

— 应根据系统统一安全策略，提供集中审计接口。

3) 剩余信息保护

— 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。

4) 应用容错

— 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。

5) 源码安全

— 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) 可信时间戳服务

— 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。

（4） 运维安全

1) 环境管理

— 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。

2) 监控管理

— 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。

5.4 移动电话支付（远程支付）系统要求

5.4.1 基本要求

移动电话支付（远程支付）系统应在系统功能、风险监控、系统性能、安全性、系统文档建设方面符合技术标准要求和管理要求，基本要求参见《非金融机构支付服务业务系统检测基本要求_移动电话支付（远程支付）部分》。

检测项参见附录 A.4。

5.4.2 增强要求

5.4.2.1 功能要求

（1） 客户支付账户管理

— 应实现客户账户的开户、修改、冻结/解冻、销户等功能。

5.4.2.2 风险监控要求

（1） 实名认证

— 应对客户身份进行实名认证。

5.4.2.3 安全性要求

（1） 网络安全

1) 网络结构安全

— 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；

— 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。

2) 网络安全审计

— 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，时钟保持与时钟服务器同步。

3) 网络入侵防范

— 当审查到攻击行为时，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。

4) 网络设备防护

— 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。

（2） 主机安全

1) 身份鉴别

— 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。

2) 可信路径

— 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。

3) 安全审计

— 应能够根据信息系统的统一安全策略，实现集中审计；

— 应保护审计进程，避免受到未预期的中断。

4) 入侵防范

— 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。

（3） 应用安全

1) 身份鉴别

— 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。

2) 安全审计

— 应根据系统统一安全策略，提供集中审计接口。

3) 剩余信息保护

— 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。

4) 应用容错

— 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。

5) 源码安全

— 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) 可信时间戳服务

— 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。

（4） 运维安全

1) 环境管理

— 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。

2) 监控管理

— 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。

5.5 固定电话支付系统要求

5.5.1 基本要求

固定电话支付系统应在系统功能、风险监控、系统性能、安全性、系统文档建设方面符合技术标准要求和管理要求，基本要求参见《非金融机构支付服务业务系统检测基本要求_固定电话支付部分》。

检测项参见附录 A.5。

5.5.2 增强要求

5.5.2.1 功能要求

（1） 客户支付账户管理

— 应实现客户支付账户的开户、修改、冻结/解冻、销户等功能。

5.5.2.2 风险监控要求

（1） 实名认证

— 应对客户身份进行实名认证。

5.5.2.3 安全性要求

（1） 网络安全

1) 网络结构安全

— 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；

— 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。

2) 网络安全审计

— 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，时钟保持与时钟服务器同步。

3) 网络入侵防范

— 当审查到攻击行为时，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。

4) 网络设备防护

— 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。

（2） 主机安全

1) 身份鉴别

— 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。

2) 可信路径

— 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。

3) 安全审计

— 应能够根据信息系统的统一安全策略，实现集中审计；

— 应保护审计进程，避免受到未预期的中断。

4) 入侵防范

— 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。

（3） 应用安全

1) 身份鉴别

— 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。

2) 安全审计

— 应根据系统统一安全策略，提供集中审计接口。

3) 剩余信息保护

— 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。

4) 应用容错

— 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。

5) 源码安全

— 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) 可信时间戳服务

— 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。

（4） 运维安全

1) 环境管理

— 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。

2) 监控管理

— 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。

5.6 数字电视支付系统要求

5.6.1 基本要求

数字电视支付系统应在系统功能、风险监控、系统性能、安全性、系统文档建设方面符合技术标准要求和管理要求，基本要求参见《非金融机构支付服务业务系统检测基本要求_数字电视支付部分》。

检测项参见附录 A.6。

5.6.2 增强要求

5.6.2.1 功能要求

（1） 客户支付账户管理

— 应实现客户账户的开户、修改、冻结/解冻、销户等功能。

5.6.2.2 风险监控要求

（1） 实名认证

— 应对客户身份进行实名认证。

5.6.2.3 安全性要求

（1） 网络安全

1) 网络结构安全

— 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；

— 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。

2) 网络安全审计

— 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，时钟保持与时钟服务器同步。

3) 网络入侵防范

— 当审查到攻击行为时，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。

4) 网络设备防护

— 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。

（2） 主机安全

1) 身份鉴别

— 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。

2) 可信路径

— 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。

3) 安全审计

— 应能够根据信息系统的统一安全策略，实现集中审计；

— 应保护审计进程，避免受到未预期的中断。

4) 入侵防范

— 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。

（3） 应用安全

1) 身份鉴别

— 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。

2) 安全审计

— 应根据系统统一安全策略，提供集中审计接口。

3) 剩余信息保护

— 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。

4) 应用容错

— 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。

5) 源码安全

— 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) 可信时间戳服务

— 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。

（4） 运维安全

1) 环境管理

— 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。

2) 监控管理

— 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。

5.7 预付卡的发行与受理系统要求

5.7.1 基本要求

预付卡的发行与受理系统应在系统功能、风险监控、系统性能、安全性、系统文档建设方面符合技术标准要求和管理要求，基本要求参见《非金融机构支付服务业务系统检测基本要求_预付卡部分》。

检测项参见附录 A.7。

5.7.2 增强要求

5.7.2.1 功能要求

（1） 客户支付账户管理

— 应实现客户账户的开户、修改、冻结/解冻、销户等功能。

5.7.2.2 风险监控要求

（1） 实名认证

— 应对客户身份进行实名认证。

5.7.2.3 安全性要求

（1） 网络安全

1) 网络结构安全

— 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；

— 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。

2) 网络安全审计

— 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，时钟保持与时钟服务器同步。

3) 网络入侵防范

— 当审查到攻击行为时，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。

4) 网络设备防护

— 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。

（2） 主机安全

1) 身份鉴别

— 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。

2) 可信路径

— 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。

3) 安全审计

— 应能够根据信息系统的统一安全策略，实现集中审计；

— 应保护审计进程，避免受到未预期的中断。

4) 入侵防范

— 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。

（3） 应用安全

1) 身份鉴别

— 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。

2) 安全审计

— 应根据系统统一安全策略，提供集中审计接口。

3) 剩余信息保护

— 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。

4) 应用容错

— 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。

5) 源码安全

— 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) 可信时间戳服务

— 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。

（4） 运维安全

1) 环境管理

— 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。

2) 监控管理

— 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。

5.8 银行卡收单系统要求

5.8.1 基本要求

银行卡收单系统应在系统功能、风险监控、系统性能、安全性、系统文档建设方面符合技术标准要求和管理要求，基本要求参见《非金融机构支付服务业务系统检测基本要求_银行卡收单部分》。

检测项参见附录 A.8。

5.8.2 增强要求

5.8.2.1 功能要求

（1） 对账处理

— 报文设计符合《电子支付文件数据格式》6 中的报文结构设计要求。

（2） 差错处理

— 报文设计符合《电子支付文件数据格式》5.1 中的报文结构设计要求。

5.8.2.2 风险监控要求

（1） 实名认证

— 应对客户身份进行实名认证。

5.8.2.3 安全性要求

（1） 网络安全

1) 网络结构安全

— 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；

— 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。

2) 网络安全审计

— 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，时钟保持与时钟服务器同步。

3) 网络入侵防范

— 当审查到攻击行为时，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。

4) 网络设备防护

— 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。

（2） 主机安全

1) 身份鉴别

— 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。

2) 可信路径

— 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。

3) 安全审计

— 应能够根据信息系统的统一安全策略，实现集中审计；

— 应保护审计进程，避免受到未预期的中断。

4) 入侵防范

— 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。

（3） 应用安全

1) 身份鉴别

— 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

2) 安全审计

— 应根据系统统一安全策略，提供集中审计接口。

3) 剩余信息保护

— 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。

4) 应用容错

— 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。

5) 源码安全

— 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) 可信时间戳服务

— 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。

（4） 运维安全

1) 环境管理

— 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。

2) 监控管理

— 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。

5.9 外包附加要求

对于非金融机构将支付服务业务系统相关运维外包给第三方服务机构的附加要求。外包提供的服务包括：基础设施运维服务、应用系统运维服务和安全管理服务等。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，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。

5.9.1 基本要求

（1） 外包服务的外包内容

— 应明确外包程度及具体内容。

（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。

（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。

（4） 外包商资质

— 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；

— 确定外包行为前应对外包商的运维管理制度评估；

— 确定外包行为前外包模式调查及风险进行评估。

（5） 外包合同

— 明确规定有关各方的权利和义务；

— 明确外包商最低的服务水平；

— 规定保守信息资源机密；

— 规定争议解决办法。

（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。

（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。

检测项见附录 A.9。

5.9.2 增强要求

— 外包商应建立质量管理体系和安全管理体系。

6 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。

附　录　A

（规范性附录）

检测项列表

A.1 货币汇兑系统检测项

A.1.1 功能检测项

编号	检测项		检测说明
1.1	客户管理	1.1.1 客户信息登记及管理	必测项
		1.1.2 商业银行管理	
		1.1.3 客户证书管理	
		1.1.4 客户审核	必测项
1.2	账户管理	1.2.1 客户账户管理	必测项
		1.2.2 客户账户管理审核	
		1.2.3 客户账户查询	必测项
		1.2.4 客户账户资金审核	
1.3	交易处理	1.3.1 内部转账	
		1.3.2 汇款	
		1.3.3 代付	
		1.3.4 代收	
		1.3.5 资金调拨	
		1.3.6 资金归集	
		1.3.7 信用卡还款	
		1.3.8 预存	
		1.3.9 提现	
		1.3.10 交易明细查询	必测项
		1.3.11 交易明细下载	
		1.3.12 清分清算服务	
1.4	资金结算	1.4.1 客户结算	必测项
1.5	对账处理	1.5.1 客户发送对账请求	
		1.5.2 客户下载对账文件	
1.6	差错处理	1.6.1 长款/短款处理	必测项
		1.6.2 订单撤销	必测项
		1.6.3 退回	
1.7	统计报表	1.7.1 业务类报表	必测项
		1.7.2 运行管理类报表	必测项
1.8	运营管理	1.8.1 运营人员权限管理	必测项
		1.8.2 提现管理	
		1.8.3 汇款管理	

A.1.2 风险监控检测项

编号	检测项		检测说明
2.1	账户风险管理	2.1.1 实名认证	
2.2	交易监控	2.2.1 监控规则管理	必测项
		2.2.2 当日交易查询	必测项
		2.2.3 历史交易查询	必测项
		2.2.4 实时交易监控	必测项
		2.2.5 可疑交易处理	必测项
		2.2.6 交易事件报警	必测项
2.3	交易审核	2.3.1 系统自动审核	必测项
		2.3.2 人工审核	必测项
2.4	风控规则	2.4.1 风控规则管理	必测项
		2.4.2 黑名单	必测项
		2.4.3 风险识别	必测项
		2.4.4 事件管理	必测项
		2.4.5 风险报表	必测项

A.1.3 性能检测项

编号	检测项	检测说明
3.1	3.1.1 汇出	
3.2	3.2.1 预存	
3.3	3.3.1 转账	
3.4	3.4.1 交易明细查询	必测项
3.5	3.5.1 日终批处理	

A.1.4 安全性检测项

（1） 网络安全性测试

编号	检测项		检测说明
4.1.1	结构安全	4.1.1.1 网络冗余和备份	必测项
		4.1.1.2 网络安全路由器	必测项
		4.1.1.3 网络安全防火墙	必测项
		4.1.1.4 网络拓扑结构	必测项
		4.1.1.5 IP 子网划分	必测项
		4.1.1.6 QoS 保证	必测项

编号	检测项		检测说明
4.1.2	网络访问控制	4.1.2.1 网络域安全隔离和限制	必测项
		4.1.2.2 地址转换和绑定	必测项
		4.1.2.3 内容过滤	必测项
		4.1.2.4 访问控制	必测项
		4.1.2.5 流量控制	必测项
		4.1.2.6 会话控制	必测项
		4.1.2.7 远程拨号访问控制和记录	必测项
4.1.3	网络安全审计	4.1.3.1 日志信息	必测项
		4.1.3.2 网络系统故障分析	必测项
		4.1.3.3 网络对象操作审计	必测项
		4.1.3.4 日志权限和保护	必测项
		4.1.3.5 审计工具	必测项
4.1.4	边界完整性检查	4.1.4.1 内外网非法连接阻断和定位	必测项
4.1.5	网络入侵防范	4.1.5.1 网络 ARP 欺骗攻击	必测项
		4.1.5.2 信息窃取	必测项
		4.1.5.3 DOS/DDOS 攻击	必测项
		4.1.5.4 网络入侵防范机制	必测项
4.1.6	恶意代码防范	4.1.6.1 恶意代码防范措施	必测项
		4.1.6.2 定时更新	必测项
4.1.7	网络设备防护	4.1.7.1 设备登录设置	必测项
		4.1.7.2 设备登录口令安全性	必测项
		4.1.7.3 登录地址限制	必测项
		4.1.7.4 远程管理安全	必测项
		4.1.7.5 设备用户设置策略	必测项
		4.1.7.6 权限分离	必测项
		4.1.7.7 最小化服务	必测项
4.1.8	网络安全管理	4.1.8.1 网络设备运维手册	必测项
		4.1.8.2 定期补丁安装	必测项
		4.1.8.3 漏洞扫描	必测项
		4.1.8.4 网络数据传输加密	必测项
4.1.9	网络相关人员安全管理	4.1.9.1 网络安全管理人员配备	必测项
		4.1.9.2 网络安全管理人员责任划分规则	必测项
		4.1.9.3 网络安全关键岗位人员管理	必测项

（2） 主机安全性测试

编号	检测项		检测说明
4.2.1	身份鉴别	4.2.1.1 系统与应用管理员用户设置	必测项
		4.2.1.2 系统与应用管理员口令安全性	必测项
		4.2.1.3 登录策略	必测项
4.2.2	访问控制	4.2.2.1 访问控制范围	必测项
		4.2.2.2 主机信任关系	必测项
		4.2.2.3 默认过期用户	必测项
4.2.3	安全审计	4.2.3.1 日志信息	必测项
		4.2.3.2 日志权限和保护	必测项
		4.2.3.3 系统信息分析	必测项
4.2.4	系统保护	4.2.4.1 系统备份	必测项
		4.2.4.2 故障恢复策略	必测项
		4.2.4.3 磁盘空间安全	必测项
		4.2.4.4 主机安全加固	必测项
4.2.5	剩余信息保护	4.2.5.1 剩余信息保护	必测项
4.2.6	入侵防范	4.2.6.1 入侵防范记录	必测项
		4.2.6.2 关闭服务和端口	必测项
		4.2.6.3 最小安装原则	必测项
4.2.7	恶意代码防范	4.2.7.1 防范软件安装部署	必测项
		4.2.7.2 病毒库定时更新	必测项
		4.2.7.3 防范软件统一管理	必测项
4.2.8	资源控制	4.2.8.1 连接控制	必测项
		4.2.8.2 资源监控和预警	必测项
4.2.9	主机安全管理	4.2.9.1 主机运维手册	必测项
		4.2.9.2 漏洞扫描	必测项
		4.2.9.3 系统补丁	必测项
		4.2.9.4 操作日志管理	必测项
4.2.10	主机相关人员安全管理	4.2.10.1 主机安全管理人员配备	必测项
		4.2.10.2 主机安全管理人员责任划分规则	必测项
		4.2.10.3 主机安全关键岗位人员管理	必测项

（3） 应用安全性测试

编号	检测项		检测说明
4.3.1	身份鉴别	4.3.1.1 系统与普通用户设置	必测项
		4.3.1.2 系统与普通用户口令安全性	必测项
		4.3.1.3 登录访问安全策略	必测项
		4.3.1.4 非法访问警示和记录	必测项
		4.3.1.5 客户端鉴别信息安全	必测项
		4.3.1.6 口令有效期限制	必测项
		4.3.1.7 限制认证会话时间	必测项
		4.3.1.8 身份标识唯一性	必测项
		4.3.1.9 及时清除鉴别信息	必测项
4.3.2	WEB 页面安全	4.3.2.1 登录防穷举	必测项
		4.3.2.2 安全控件	必测项
		4.3.2.3 使用数字证书	必测项
		4.3.2.4 独立的支付密码	必测项
		4.3.2.5 网站页面 SQL 注入防范	必测项
		4.3.2.6 网站页面跨站脚本攻击防范	必测项
		4.3.2.7 网站页面源代码暴露防范	必测项
		4.3.2.8 网站页面黑客挂马防范	必测项
		4.3.2.9 网站页面防篡改措施	必测项
		4.3.2.10 网站页面防钓鱼	必测项
4.3.3	访问控制	4.3.3.1 访问权限设置	必测项
		4.3.3.2 自主访问控制范围	必测项
		4.3.3.3 业务操作日志	必测项
		4.3.3.4 关键数据存放	必测项
		4.3.3.5 异常中断防护	必测项
		4.3.3.6 数据库安全配置	必测项
4.3.4	安全审计	4.3.4.1 日志信息	必测项
		4.3.4.2 日志权限和保护	必测项
		4.3.4.3 系统信息查询与分析	必测项
		4.3.4.4 对象操作审计	必测项
		4.3.4.5 审计工具	必测项
		4.3.4.6 事件报警	必测项
4.3.5	剩余信息保护	4.3.5.1 过期信息、文档处理	必测项

编号	检测项		检测说明
4.3.6	资源控制	4.3.6.1 连接控制	必测项
		4.3.6.2 会话控制	必测项
		4.3.6.3 进程资源分配	必测项
		4.3.6.4 资源检测预警	必测项
4.3.7	应用容错	4.3.7.1 数据有效性校验	必测项
		4.3.7.2 容错机制	必测项
		4.3.7.3 故障机制	必测项
		4.3.7.4 回退机制	必测项
4.3.8	报文完整性	4.3.8.1 通信报文有效性	必测项
4.3.9	报文保密性	4.3.9.1 报文或会话加密	必测项
4.3.10	抗抵赖	4.3.10.1 原发和接收证据	必测项
4.3.11	编码安全	4.3.11.1 源代码审查	必测项
		4.3.11.2 插件安全性审查	必测项
		4.3.11.3 编码规范约束	必测项
		4.3.11.4 源代码管理	必测项
		4.3.11.5 版本管理	必测项
4.3.12	电子认证应用	4.3.12.1第三方电子认证机构	必测项
		4.3.12.2关键业务电子认证技术应用	必测项
		4.3.12.3电子签名有效性	必测项
		4.3.12.4服务器证书私钥保护	必测项

（4） 数据安全性测试

编号	检测项		检测说明
4.4.1	数据保护	4.4.1.1 客户身份信息保护	必测项
		4.4.1.2 支付业务信息保护	必测项
		4.4.1.3 会计档案信息保护	必测项
4.4.2	数据完整性	4.4.2.1 重要数据更改机制	必测项
		4.4.2.2 数据备份记录	必测项
		4.4.2.3 保障传输过程中的数据完整性	必测项
		4.4.2.4 备份数据定期恢复	必测项
4.4.3	交易数据以及客户数据的安全性	4.4.3.1 数据物理存储安全	必测项
		4.4.3.2 客户身份认证信息存储安全	必测项

编号	检测项		检测说明
		4.4.3.3 终端信息采集设备硬加密措施或其它防伪手段	必测项
		4.4.3.4 同一安全级别和可信赖的系统之间信息传输	必测项
		4.4.3.5 加密传输	必测项
		4.4.3.6 加密存储	必测项
		4.4.3.7 数据访问控制	必测项
		4.4.3.8 在线的存储备份	必测项
		4.4.3.9 数据备份机制	必测项
		4.4.3.10 本地备份	必测项
		4.4.3.11 异地备份	必测项
		4.4.3.12 备份数据的恢复	必测项
		4.4.3.13 数据销毁制度和记录	必测项
		4.4.3.14 关键链路冗余设计	必测项

（5） 运维安全性测试

编号	检测项		检测说明
4.5.1	环境管理	4.5.1.1 机房基础设施定期维护	必测项
		4.5.1.2 机房的出入管理制度化和文档化	必测项
		4.5.1.3 办公环境的保密性措施	必测项
		4.5.1.4 机房安全管理制度	必测项
		4.5.1.5 机房进出登记表	必测项
4.5.2	介质管理	4.5.2.1 介质的存放环境保护措施	必测项
		4.5.2.2 介质的使用管理文档化	必测项
		4.5.2.3 维修或销毁介质之前清除敏感数据	必测项
		4.5.2.4 介质管理记录	必测项
		4.5.2.5 介质的分类与标识	必测项
4.5.3	设备管理	4.5.3.1 设备管理的责任人员或部门	必测项
		4.5.3.2 设施、设备定期维护	必测项
		4.5.3.3 设备选型、采购、发放等的审批控制	必测项
		4.5.3.4 设备配置标准化	必测项
		4.5.3.5 设备的操作规程	必测项
		4.5.3.6 设备的操作日志	必测项
		4.5.3.7 设备使用管理文档	必测项

编号	检测项		检测说明
		4.5.3.8 设备标识	必测项
4.5.4	人员管理	4.5.4.1 人员录用	必测项
		4.5.4.2 人员转岗、离岗	必测项
		4.5.4.3 人员考核	必测项
		4.5.4.4 安全意识教育和培训	必测项
		4.5.4.5 外部人员访问管理	必测项
		4.5.4.6 职责分离	必测项
4.5.5	监控管理	4.5.5.1 主要网络设备的各项指标监控情况	必测项
		4.5.5.2 主要服务器的各项指标监控情况	必测项
		4.5.5.3 应用运行各项指标监控情况	必测项
		4.5.5.4 异常处理机制	必测项
4.5.6	变更管理	4.5.6.1 变更方案	必测项
		4.5.6.2 变更制度化管理	必测项
		4.5.6.3 重要系统变更的批准	必测项
		4.5.6.4 重要系统变更的通知	必测项
4.5.7	安全事件处置	4.5.7.1 安全事件报告和处置	必测项
		4.5.7.2 安全事件的分类和分级	必测项
		4.5.7.3 安全事件记录和采取的措施	必测项
4.5.8	应急预案管理	4.5.8.1 制定不同事件的应急预案	必测项
		4.5.8.2 相关人员应急预案培训	必测项
		4.5.8.3 定期演练	必测项

（6） 业务连续性测试

编号	检测项		检测说明
4.6.1	业务连续性需求分析	4.6.1.1 业务中断影响分析	必测项
		4.6.1.2 灾难恢复时间目标和恢复点目标	必测项
4.6.2	业务连续性技术环境	4.6.2.1 备份机房	必测项
		4.6.2.2 网络双链路	必测项
		4.6.2.3 网络设备和服务器备份	必测项
		4.6.2.4 高可靠的磁盘阵列	必测项
		4.6.2.5 远程数据库备份	必测项
4.6.3	业务连续性管理	4.6.3.1 业务连续性管理制度	必测项

编号	检测项		检测说明
		4.6.3.2 应急响应流程	必测项
		4.6.3.3 恢复预案	必测项
		4.6.3.4 数据备份和恢复制度	必测项
4.6.4	备份与恢复管理	4.6.4.1 备份数据范围和备份频率	必测项
		4.6.4.2 备份和恢复手册	必测项
		4.6.4.3 备份记录和定期恢复测试记录	必测项
		4.6.4.4 定期数据备份恢复性测试	必测项
4.6.5	日常维护	4.6.5.1 每年业务连续性演练	必测项
		4.6.5.2 定期业务连续性培训	必测项

A.1.5 文档检测项

编号	检测项		检测说明
5.1	用户文档	5.1.1 用户手册	必测项
		5.1.2 操作手册	必测项
5.2	开发文档	5.2.1 需求说明书	必测项
		5.2.2 需求分析文档	必测项
		5.2.3 总体设计方案	必测项
		5.2.4 数据库设计文档	必测项
		5.2.5 概要设计文档	必测项
		5.2.6 详细设计文档	必测项
		5.2.7 工程实施方案	必测项
5.3	管理文档	5.3.1 测试报告	必测项
		5.3.2 系统运维手册	必测项
		5.3.3 系统应急手册	必测项
		5.3.4 运维管理制度	必测项
		5.3.5 安全管理制度	必测项
		5.3.6 安全审计报告	必测项

A.2 互联网支付系统检测项

A.2.1 功能检测项

编号	检测项		检测说明
1.1	客户管理	1.1.1 客户信息登记及管理	必测项
		1.1.2 商业银行管理	
		1.1.3 客户证书管理	

编号	检测项		检测说明
		1.1.4 客户审核	必测项
1.2	账户管理	1.2.1 客户支付账户管理	必测项
		1.2.2 客户支付账户管理审核	
		1.2.3 客户支付账户查询	必测项
		1.2.4 客户支付账户资金审核	
1.3	交易处理	1.3.1 一般支付	一般支付类必测项
		1.3.2 担保支付	担保支付类必测项
		1.3.3 协议支付	协议支付类必测项
		1.3.4 订单撤销	必测项
		1.3.5 转账	
		1.3.6 预存	
		1.3.7 提现	
		1.3.8 积分查询	
		1.3.9 积分兑换	
		1.3.10 积分兑换撤销	
		1.3.11 交易纠纷处理	
		1.3.12 交易明细查询	必测项
		1.3.13 交易明细下载	
		1.3.14 邀请其他人代付	
1.4	资金结算	1.4.1 客户结算	必测项
1.5	对账处理	1.5.1 商户发送对账请求	
		1.5.2 商户下载对账文件	
1.6	差错处理	1.6.1 长款/短款处理	必测项
		1.6.2 单笔退款	必测项
		1.6.3 批量退款	
1.7	统计报表	1.7.1 业务类报表	必测项
		1.7.2 运行管理类报表	必测项
1.8	运营管理	1.8.1 运营人员权限管理	必测项
		1.8.2 提现管理	
		1.8.3 提现财务处理	
		1.8.4 退款风控处理	
		1.8.5 退款财务处理	

A.2.2 风险监控检测项

编号	检测项		检测说明
2.1	账户风险管理	2.1.1 实名认证	
2.2	交易监控	2.2.1 监控规则管理	必测项
		2.2.2 当日交易查询	必测项
		2.2.3 历史交易查询	必测项
		2.2.4 实时交易监控	必测项
		2.2.5 可疑交易处理	必测项
		2.2.6 交易事件报警	必测项
2.3	交易审核	2.3.1 系统自动审核	必测项
		2.3.2 人工审核	必测项
2.4	风控规则	2.4.1 风控规则管理	必测项
		2.4.2 黑名单	必测项
		2.4.3 风险识别	必测项
		2.4.4 事件管理	必测项
		2.4.5 风险报表	必测项

A.2.3 性能检测项

编号	检测项	检测说明
3.1	3.1.1 支付	必测项
3.2	3.2.1 预存	
3.3	3.3.1 转账	
3.4	3.4.1 交易明细查询	必测项
3.5	3.5.1 日终批处理	

A.2.4 安全性检测项

（1） 网络安全性

编号	检测项		检测说明
4.1.1	结构安全	4.1.1.1 网络冗余和备份	必测项
		4.1.1.2 网络安全路由器	必测项
		4.1.1.3 网络安全防火墙	必测项

编号	检测项		检测说明
		4.1.1.4 网络拓扑结构	必测项
		4.1.1.5 IP 子网划分	必测项
		4.1.1.6 QoS 保证	必测项
4.1.2	网络访问控制	4.1.2.1 网络域安全隔离和限制	必测项
		4.1.2.2 地址转换和绑定	必测项
		4.1.2.3 内容过滤	必测项
		4.1.2.4 访问控制	必测项
		4.1.2.5 流量控制	必测项
		4.1.2.6 会话控制	必测项
		4.1.2.7 远程拨号访问控制和记录	必测项
4.1.3	网络安全审计	4.1.3.1 日志信息	必测项
		4.1.3.2 网络系统故障分析	必测项
		4.1.3.3 网络对象操作审计	必测项
		4.1.3.4 日志权限和保护	必测项
		4.1.3.5 审计工具	必测项
4.1.4	边界完整性检查	4.1.4.1 内外网非法连接阻断和定位	必测项
4.1.5	网络入侵防范	4.1.5.1 网络 ARP 欺骗攻击	必测项
		4.1.5.2 信息窃取	必测项
		4.1.5.3 DOS/DDOS 攻击	必测项
		4.1.5.4 网络入侵防范机制	必测项
4.1.6	恶意代码防范	4.1.6.1 恶意代码防范措施	必测项
		4.1.6.2 定时更新	必测项
4.1.7	网络设备防护	4.1.7.1 设备登录设置	必测项
		4.1.7.2 设备登录口令安全性	必测项
		4.1.7.3 登录地址限制	必测项
		4.1.7.4 远程管理安全	必测项
		4.1.7.5 设备用户设置策略	必测项
		4.1.7.6 权限分离	必测项
		4.1.7.7 最小化服务	必测项
4.1.8	网络安全管理	4.1.8.1 网络设备运维手册	必测项
		4.1.8.2 定期补丁安装	必测项
		4.1.8.3 漏洞扫描	必测项
		4.1.8.4 网络数据传输加密	必测项

编号	检测项		检测说明
4.1.9	网络相关人员安全管理	4.1.9.1 网络安全管理人员配备	必测项
		4.1.9.2 网络安全管理人员责任划分规则	必测项
		4.1.9.3 网络安全关键岗位人员管理	必测项

（2） 主机安全性

编号	检测项		检测说明
4.2.1	身份鉴别	4.2.1.1 系统与应用管理员用户设置	必测项
		4.2.1.2 系统与应用管理员口令安全性	必测项
		4.2.1.3 登录策略	必测项
4.2.2	访问控制	4.2.2.1 访问控制范围	必测项
		4.2.2.2 主机信任关系	必测项
		4.2.2.3 默认过期用户	必测项
4.2.3	安全审计	4.2.3.1 日志信息	必测项
		4.2.3.2 日志权限和保护	必测项
		4.2.3.3 系统信息分析	必测项
4.2.4	系统保护	4.2.4.1 系统备份	必测项
		4.2.4.2 故障恢复策略	必测项
		4.2.4.3 磁盘空间安全	必测项
		4.2.4.4 主机安全加固	必测项
4.2.5	剩余信息保护	4.2.5.1 剩余信息保护	必测项
4.2.6	入侵防范	4.2.6.1 入侵防范记录	必测项
		4.2.6.2 关闭服务和端口	必测项
		4.2.6.3 最小安装原则	必测项
4.2.7	恶意代码防范	4.2.7.1 防范软件安装部署	必测项
		4.2.7.2 病毒库定时更新	必测项
		4.2.7.3 防范软件统一管理	必测项
4.2.8	资源控制	4.2.8.1 连接控制	必测项
		4.2.8.2 资源监控和预警	必测项
4.2.9	主机安全管理	4.2.9.1 主机运维手册	必测项
		4.2.9.2 漏洞扫描	必测项
		4.2.9.3 系统补丁	必测项
		4.2.9.4 操作日志管理	必测项

编号	检测项		检测说明
4.2.10	主机相关人员安全管理	4.2.10.1主机安全管理人员配备	必测项
		4.2.10.2主机安全管理人员责任划分规则	必测项
		4.2.10.3主机安全关键岗位人员管理	必测项

（3） 应用安全性

编号	检测项		检测说明
4.3.1	身份鉴别	4.3.1.1 系统与普通用户设置	必测项
		4.3.1.2 系统与普通用户口令安全性	必测项
		4.3.1.3 登录访问安全策略	必测项
		4.3.1.4 非法访问警示和记录	必测项
		4.3.1.5 客户端鉴别信息安全	必测项
		4.3.1.6 口令有效期限制	必测项
		4.3.1.7 限制认证会话时间	必测项
		4.3.1.8 身份标识唯一性	必测项
		4.3.1.9 及时清除鉴别信息	必测项
4.3.2	WEB 页面安全	4.3.2.1 登录防穷举	必测项
		4.3.2.2 安全控件	必测项
		4.3.2.3 使用数字证书	必测项
		4.3.2.4 独立的支付密码	必测项
		4.3.2.5 网站页面 SQL 注入防范	必测项
		4.3.2.6 网站页面跨站脚本攻击防范	必测项
		4.3.2.7 网站页面源代码暴露防范	必测项
		4.3.2.8 网站页面黑客挂马防范	必测项
		4.3.2.9 网站页面防篡改措施	必测项
		4.3.2.10 网站页面防钓鱼	必测项
4.3.3	访问控制	4.3.3.1 访问权限设置	必测项
		4.3.3.2 自主访问控制范围	必测项
		4.3.3.3 业务操作日志	必测项
		4.3.3.4 关键数据存放	必测项
		4.3.3.5 异常中断防护	必测项
		4.3.3.6 数据库安全配置	必测项
4.3.4	安全审计	4.3.4.1 日志信息	必测项

编号	检测项		检测说明
		4.3.4.2 日志权限和保护	必测项
		4.3.4.3 系统信息查询与分析	必测项
		4.3.4.4 对象操作审计	必测项
		4.3.4.5 审计工具	必测项
		4.3.4.6 事件报警	必测项
4.3.5	剩余信息保护	4.3.5.1 过期信息、文档处理	必测项
4.3.6	资源控制	4.3.6.1 连接控制	必测项
		4.3.6.2 会话控制	必测项
		4.3.6.3 进程资源分配	必测项
		4.3.6.4 资源检测预警	必测项
4.3.7	应用容错	4.3.7.1 数据有效性校验	必测项
		4.3.7.2 容错机制	必测项
		4.3.7.3 故障机制	必测项
		4.3.7.4 回退机制	必测项
4.3.8	报文完整性	4.3.8.1 通信报文有效性	必测项
4.3.9	报文保密性	4.3.9.1 报文或会话加密	必测项
4.3.10	抗抵赖	4.3.10.1原发和接收证据	必测项
4.3.11	编码安全	4.3.11.1源代码审查	必测项
		4.3.11.2插件安全性审查	必测项
		4.3.11.3编码规范约束	必测项
		4.3.11.4源代码管理	必测项
		4.3.11.5版本管理	必测项
4.3.12	电子认证应用	4.3.12.1第三方电子认证机构	必测项
		4.3.12.2关键业务电子认证技术应用	必测项
		4.3.12.3电子签名有效性	必测项
		4.3.12.4服务器证书私钥保护	必测项

（4） 数据安全性

编号	检测项		检测说明
4.4.1	数据保护	4.4.1.1 客户身份信息保护	必测项
		4.4.1.2 支付业务信息保护	必测项
		4.4.1.3 会计档案信息保护	必测项

编号	检测项		检测说明
4.4.2	数据完整性	4.4.2.1 重要数据更改机制	必测项
		4.4.2.2 数据备份记录	必测项
		4.4.2.3 保障传输过程中的数据完整性	必测项
		4.4.2.4 备份数据定期恢复	必测项
4.4.3	交易数据以及客户数据的安全性	4.4.3.1 数据物理存储安全	必测项
		4.4.3.2 客户身份认证信息存储安全	必测项
		4.4.3.3 终端信息采集设备硬加密措施或其它防伪手段	必测项
		4.4.3.4 同一安全级别和可信赖的系统之间信息传输	必测项
		4.4.3.5 加密传输	必测项
		4.4.3.6 加密存储	必测项
		4.4.3.7 数据访问控制	必测项
		4.4.3.8 在线的存储备份	必测项
		4.4.3.9 数据备份机制	必测项
		4.4.3.10 本地备份	必测项
		4.4.3.11 异地备份	必测项
		4.4.3.12 备份数据的恢复	必测项
		4.4.3.13 数据销毁制度和记录	必测项
		4.4.3.14 关键链路冗余设计	必测项

（5） 运维安全性

编号	检测项		检测说明
4.5.1	环境管理	4.5.1.1 机房基础设施定期维护	必测项
		4.5.1.2 机房的出入管理制度化和文档化	必测项
		4.5.1.3 办公环境的保密性措施	必测项
		4.5.1.4 机房安全管理制度	必测项
		4.5.1.5 机房进出登记表	必测项
4.5.2	介质管理	4.5.2.1 介质的存放环境保护措施	必测项
		4.5.2.2 介质的使用管理文档化	必测项
		4.5.2.3 维修或销毁介质之前清除敏感数据	必测项
		4.5.2.4 介质管理记录	必测项
		4.5.2.5 介质的分类与标识	必测项

编号	检测项		检测说明
4.5.3	设备管理	4.5.3.1 设备管理的责任人员或部门	必测项
		4.5.3.2 设施、设备定期维护	必测项
		4.5.3.3 设备选型、采购、发放等的审批控制	必测项
		4.5.3.4 设备配置标准化	必测项
		4.5.3.5 设备的操作规程	必测项
		4.5.3.6 设备的操作日志	必测项
		4.5.3.7 设备使用管理文档	必测项
		4.5.3.8 设备标识	必测项
4.5.4	人员管理	4.5.4.1 人员录用	必测项
		4.5.4.2 人员转岗、离岗	必测项
		4.5.4.3 人员考核	必测项
		4.5.4.4 安全意识教育和培训	必测项
		4.5.4.5 外部人员访问管理	必测项
		4.5.4.6 职责分离	必测项
4.5.5	监控管理	4.5.5.1 主要网络设备的各项指标监控情况	必测项
		4.5.5.2 主要服务器的各项指标监控情况	必测项
		4.5.5.3 应用运行各项指标监控情况	必测项
		4.5.5.4 异常处理机制	必测项
4.5.6	变更管理	4.5.6.1 变更方案	必测项
		4.5.6.2 变更制度化管理	必测项
		4.5.6.3 重要系统变更的批准	必测项
		4.5.6.4 重要系统变更的通知	必测项
4.5.7	安全事件处置	4.5.7.1 安全事件报告和处置	必测项
		4.5.7.2 安全事件的分类和分级	必测项
		4.5.7.3 安全事件记录和采取的措施	必测项
4.5.8	应急预案管理	4.5.8.1 制定不同事件的应急预案	必测项
		4.5.8.2 相关人员应急预案培训	必测项
		4.5.8.3 定期演练	必测项

（6） 业务连续性

编号	检测项		检测说明
4.6.1	业务连续性需求分析	4.6.1.1 业务中断影响分析	必测项
		4.6.1.2 灾难恢复时间目标和恢复点目标	必测项

编号	检测项		检测说明
4.6.2	业务连续性技术环境	4.6.2.1 备份机房	必测项
		4.6.2.2 网络双链路	必测项
		4.6.2.3 网络设备和服务器备份	必测项
		4.6.2.4 高可靠的磁盘阵列	必测项
		4.6.2.5 远程数据库备份	必测项
4.6.3	业务连续性管理	4.6.3.1 业务连续性管理制度	必测项
		4.6.3.2 应急响应流程	必测项
		4.6.3.3 恢复预案	必测项
		4.6.3.4 数据备份和恢复制度	必测项
4.6.4	备份与恢复管理	4.6.4.1 备份数据范围和备份频率	必测项
		4.6.4.2 备份和恢复手册	必测项
		4.6.4.3 备份记录和定期恢复测试记录	必测项
		4.6.4.4 定期数据备份恢复性测试	必测项
4.6.5	日常维护	4.6.5.1 每年业务连续性演练	必测项
		4.6.5.2 定期业务连续性培训	必测项

A.2.5 文档检测项

编号	检测项		检测说明
5.1	用户文档	5.1.1 用户手册	必测项
		5.1.2 操作手册	必测项
5.2	开发文档	5.2.1 需求说明书	必测项
		5.2.2 需求分析文档	必测项
		5.2.3 总体设计方案	必测项
		5.2.4 数据库设计文档	必测项
		5.2.5 概要设计文档	必测项
		5.2.6 详细设计文档	必测项
		5.2.7 工程实施方案	必测项
5.3	管理文档	5.3.1 测试报告	必测项
		5.3.2 系统运维手册	必测项
		5.3.3 系统应急手册	必测项
		5.3.4 运维管理制度	必测项
		5.3.5 安全管理制度	必测项
		5.3.6 安全审计报告	必测项

A.3 移动电话支付（近场支付）系统检测项

A.3.1 功能检测项

编号	检测项		检测说明
1.1	账户管理	1.1.1 客户支付账户管理	联机交易类必测项
1.2	卡片管理	1.2.1 制卡	必测项（无卡片发行情况不适用）
		1.2.2 卡片发行	必测项（无卡片发行情况不适用）
		1.2.3 卡片激活	必测项（无卡片发行情况不适用）
		1.2.4 更换	必测项（无卡片发行情况不适用）
		1.2.5 卡片个人化	必测项（无卡片发行情况不适用）
		1.2.6 密码修改	
		1.2.7 挂失/解挂	
		1.2.8 锁定/解锁	
		1.2.9 注销	
1.3	密钥和证书管理	1.3.1 认证中心公钥管理	
		1.3.2 支付机构密钥管理	
		1.3.3 卡片密钥管理	必测项
		1.3.4 支付机构证书管理	
		1.3.5 卡片证书管理	
1.4	交易处理	1.4.1 联机消费	联机交易类必测项
		1.4.2 联机消费撤销	
		1.4.3 联机余额查询	联机交易类必测项
		1.4.4 退货	必测项
		1.4.5 冲正交易	联机交易类必测

编号	检测项		检测说明
			项
		1.4.6 异常卡交易	必测项
		1.4.7 现金充值	
		1.4.8 指定账户圈存	
		1.4.9 非指定账户圈存	
		1.4.10 IC 卡脚本通知	
		1.4.11 圈提	
		1.4.12 脱机消费	脱机交易类必测项
		1.4.13 脱机消费文件处理	脱机交易类必测项
		1.4.14 脱机余额查询	脱机交易类必测项
		1.4.15 交易查询	必测项
1.5	资金结算	1.5.1 客户结算	
1.6	对账处理	1.6.1 发送对账请求	
		1.6.2 生成对账文件	
1.7	差错处理	1.7.1 长款/短款处理	必测项
1.8	统计报表	1.8.1 业务类报表	必测项
		1.8.2 运行管理类报表	必测项

A.3.2 风险监控检测项

编号	检测项		检测说明
2.1	交易监控	2.1.1 监控规则管理	必测项
		2.1.2 当日交易查询	必测项
		2.1.3 历史交易查询	必测项
		2.1.4 实时交易监控	必测项
		2.1.5 可疑交易处理	必测项
		2.1.6 交易事件报警	必测项
2.2	联机交易风险管理	2.2.1 联机交易 ARQC/ARPC 验证	
		2.2.2 联机报文 MAC 验证	
		2.2.3 卡片状态控制	
		2.2.4 单笔消费限额	
		2.2.5 当日累计消费限额	

编号	检测项		检测说明
		2.2.6 当日累计消费次数限制	
		2.2.7 单笔充值金额最大值	
		2.2.8 账户余额限额	必测项
		2.2.9 大额消费商户交易监控	
		2.2.10 密码错误情况下的交易请求	
		2.2.11 非法卡号交易	必测项
2.3	脱机交易风险管理	2.3.1 TAC 验证	脱机交易类必测项
		2.3.2 MAC 验证	脱机交易类必测项
		2.3.3 单笔脱机消费限额	脱机交易类必测项
		2.3.4 单日、单月圈存/充值上限	
		2.3.5 脱机账户余额限额	脱机交易类必测项
2.4	商户风险管理	2.4.1 商户资质审核	必测项
		2.4.2 商户签约	必测项
		2.4.3 特约商户日常风险管理	必测项
		2.4.4 合作的第三方机构的风险管理	
		2.4.5 特约商户强制冻结、解冻、解约	必测项
		2.4.6 可疑商户信息共享	
		2.4.7 风险事件报送	必测项
2.5	受理终端风险管理	2.5.1 受理终端申请、参数设置、程序灌装、使用、更换、维护、撤消的管理	
		2.5.2 受理终端密钥和参数的安全管理	
		2.5.3 控制移动受理终端的安装	
		2.5.4 终端安全检测报告	
		2.5.5 密码键盘安全检测报告	
		2.5.6 终端监控	
2.6	风控规则	2.6.1 风控规则管理	必测项
		2.6.2 黑名单	必测项
		2.6.3 风险识别	必测项
		2.6.4 事件管理	必测项
		2.6.5 风险报表	必测项

A.3.3 性能检测项

编号	检测项	检测说明
3.1	3.1.1 联机消费	联机交易类必测项
3.2	3.2.1 联机余额查询	联机交易类必测项
3.3	3.3.1 联机交易明细查询	
3.4	3.4.1 脱机消费文件处理	脱机交易类必测项
3.5	3.5.1 日终批处理	

A.3.4 安全性检测项

（1） 网络安全性

编号	检测项		检测说明
4.1.1	结构安全	4.1.1.1 网络冗余和备份	必测项
		4.1.1.2 网络安全路由器	必测项
		4.1.1.3 网络安全防火墙	必测项
		4.1.1.4 网络拓扑结构	必测项
		4.1.1.5 IP 子网划分	必测项
		4.1.1.6 QoS 保证	必测项
4.1.2	网络访问控制	4.1.2.1 网络域安全隔离和限制	必测项
		4.1.2.2 地址转换和绑定	必测项
		4.1.2.3 内容过滤	必测项
		4.1.2.4 访问控制	必测项
		4.1.2.5 流量控制	必测项
		4.1.2.6 会话控制	必测项
		4.1.2.7 远程拨号访问控制和记录	必测项
4.1.3	网络安全审计	4.1.3.1 日志信息	必测项
		4.1.3.2 网络系统故障分析	必测项
		4.1.3.3 网络对象操作审计	必测项
		4.1.3.4 日志权限和保护	必测项
		4.1.3.5 审计工具	必测项
4.1.4	边界完整性检查	4.1.4.1 内外网非法连接阻断和定位	必测项
4.1.5	网络入侵防范	4.1.5.1 网络 ARP 欺骗攻击	必测项

编号	检测项		检测说明
		4.1.5.2 信息窃取	必测项
		4.1.5.3 DOS/DDOS 攻击	必测项
		4.1.5.4 网络入侵防范机制	必测项
4.1.6	恶意代码防范	4.1.6.1 恶意代码防范措施	必测项
		4.1.6.2 定时更新	必测项
4.1.7	网络设备防护	4.1.7.1 设备登录设置	必测项
		4.1.7.2 设备登录口令安全性	必测项
		4.1.7.3 登录地址限制	必测项
		4.1.7.4 远程管理安全	必测项
		4.1.7.5 设备用户设置策略	必测项
		4.1.7.6 权限分离	必测项
		4.1.7.7 最小化服务	必测项
4.1.8	网络安全管理	4.1.8.1 网络设备运维手册	必测项
		4.1.8.2 定期补丁安装	必测项
		4.1.8.3 漏洞扫描	必测项
		4.1.8.4 网络数据传输加密	必测项
4.1.9	网络相关人员安全管理	4.1.9.1 网络安全管理人员配备	必测项
		4.1.9.2 网络安全管理人员责任划分规则	必测项
		4.1.9.3 网络安全关键岗位人员管理	必测项

（2） 主机安全性

编号	检测项		检测说明
4.2.1	身份鉴别	4.2.1.1 系统与应用管理员用户设置	必测项
		4.2.1.2 系统与应用管理员口令安全性	必测项
		4.2.1.3 登录策略	必测项
4.2.2	访问控制	4.2.2.1 访问控制范围	必测项
		4.2.2.2 主机信任关系	必测项
		4.2.2.3 默认过期用户	必测项
4.2.3	安全审计	4.2.3.1 日志信息	必测项
		4.2.3.2 日志权限和保护	必测项
		4.2.3.3 系统信息分析	必测项
4.2.4	系统保护	4.2.4.1 系统备份	必测项

编号	检测项		检测说明
		4.2.4.2 故障恢复策略	必测项
		4.2.4.3 磁盘空间安全	必测项
		4.2.4.4 主机安全加固	必测项
4.2.5	剩余信息保护	4.2.5.1 剩余信息保护	必测项
4.2.6	入侵防范	4.2.6.1 入侵防范记录	必测项
		4.2.6.2 关闭服务和端口	必测项
		4.2.6.3 最小安装原则	必测项
4.2.7	恶意代码防范	4.2.7.1 防范软件安装部署	必测项
		4.2.7.2 病毒库定时更新	必测项
		4.2.7.3 防范软件统一管理	必测项
4.2.8	资源控制	4.2.8.1 连接控制	必测项
		4.2.8.2 资源监控和预警	必测项
4.2.9	主机安全管理	4.2.9.1 主机运维手册	必测项
		4.2.9.2 漏洞扫描	必测项
		4.2.9.3 系统补丁	必测项
		4.2.9.4 操作日志管理	必测项
4.2.10	主机相关人员安全管理	4.2.10.1 主机安全管理人员配备	必测项
		4.2.10.2 主机安全管理人员责任划分规则	必测项
		4.2.10.3 主机安全关键岗位人员管理	必测项

（3） 应用安全性

编号	检测项		检测说明
4.3.1	身份鉴别	4.3.1.1 系统与普通用户设置	必测项
		4.3.1.2 系统与普通用户口令安全性	必测项
		4.3.1.3 登录访问安全策略	必测项
		4.3.1.4 非法访问警示和记录	必测项
		4.3.1.5 客户端鉴别信息安全	必测项
		4.3.1.6 口令有效期限制	必测项
		4.3.1.7 限制认证会话时间	必测项
		4.3.1.8 身份标识唯一性	必测项
		4.3.1.9 及时清除鉴别信息	必测项
4.3.2	WEB 页面安全	4.3.2.1 登录防穷举	必测项

编号	检测项		检测说明
		4.3.2.2 安全控件	必测项
		4.3.2.3 使用数字证书	必测项
		4.3.2.4 独立的支付密码	必测项
		4.3.2.5 网站页面 SQL 注入防范	必测项
		4.3.2.6 网站页面跨站脚本攻击防范	必测项
		4.3.2.7 网站页面源代码暴露防范	必测项
		4.3.2.8 网站页面黑客挂马防范	必测项
		4.3.2.9 网站页面防篡改措施	必测项
		3.3.2.10 网站页面防钓鱼	必测项
4.3.3	访问控制	4.3.3.1 访问权限设置	必测项
		4.3.3.2 自主访问控制范围	必测项
		4.3.3.3 业务操作日志	必测项
		4.3.3.4 关键数据存放	必测项
		4.3.3.5 异常中断防护	必测项
		4.3.3.6 数据库安全配置	必测项
4.3.4	安全审计	4.3.4.1 日志信息	必测项
		4.3.4.2 日志权限和保护	必测项
		4.3.4.3 系统信息查询与分析	必测项
		4.3.4.4 对象操作审计	必测项
		4.3.4.5 审计工具	必测项
		4.3.4.6 事件报警	必测项
4.3.5	剩余信息保护	4.3.5.1 过期信息、文档处理	必测项
4.3.6	资源控制	4.3.6.1 连接控制	必测项
		4.3.6.2 会话控制	必测项
		4.3.6.3 进程资源分配	必测项
		4.3.6.4 资源检测预警	必测项
4.3.7	应用容错	4.3.7.1 数据有效性校验	必测项
		4.3.7.2 容错机制	必测项
		4.3.7.3 故障机制	必测项
		4.3.7.4 回退机制	必测项
4.3.8	报文完整性	4.3.8.1 通信报文有效性	必测项
4.3.9	报文保密性	4.3.9.1 报文或会话加密	必测项
4.3.10	抗抵赖	4.3.10.1 原发和接收证据	必测项

编号	检测项		检测说明
4.3.11	编码安全	4.3.11.1 源代码审查	必测项
		4.3.11.2 插件安全性审查	必测项
		4.3.11.3 编码规范约束	必测项
		4.3.11.4 源代码管理	必测项
		4.3.11.5 版本管理	必测项
4.3.12	电子认证应用	4.3.12.1 第三方电子认证机构	必测项
		4.3.12.2 关键业务电子认证技术应用	必测项
		4.3.12.3 电子签名有效性	必测项
		4.3.12.4 服务器证书私钥保护	必测项
4.3.13	脱机数据认证	4.3.13.1 密钥和证书	脱机交易类必测项（基于电子钱包/电子存折规范的应用不适用）
		4.3.13.2 静态数据认证	
		4.3.13.3 动态数据认证	
4.3.14	应用密文和发卡机构认证	4.3.14.1 应用密文产生	脱机交易类必测项（基于电子钱包/电子存折规范的应用不适用）
		4.3.14.2 发卡机构认证	
		4.3.14.3 密钥管理	
4.3.15	安全报文	4.3.15.1 报文格式	脱机交易类必测项
		4.3.15.2 报文完整性验证	脱机交易类必测项
		4.3.15.3 报文私密性	脱机交易类必测项
		4.3.15.4 密钥管理	脱机交易类必测项
4.3.16	卡片安全	4.3.16.1 共存应用	脱机交易类必测项
		4.3.16.2 密钥的独立性	脱机交易类必测项
		4.3.16.3 卡片内部安全体系	脱机交易类必测项
		4.3.16.4 卡片中密钥的种类	脱机交易类必测项
		4.3.16.5 密钥和个人识别码的存放	脱机交易类必测项
4.3.17	终端安全	4.3.17.1 终端数据安全性要求	脱机交易类必测项
		4.3.17.2 终端设备安全性要求	脱机交易类必测项
		4.3.17.3 终端密钥管理要求	脱机交易类必测项
4.3.18	密钥管理体系	4.3.18.1 认证中心公钥管理	脱机交易类必测项（基于电子钱包/电子存折规范的应用不适用）
		4.3.18.2 发卡机构公钥管理	
		4.3.18.3 发卡机构对称密钥管理	
4.3.19	安全机制	4.3.19.1 对称加密机制	脱机交易类必测项
		4.3.19.2 非对称加密机制	脱机交易类必测项

编号	检测项		检测说明
4.3.20	认可的算法	4.3.20.1 对称加密算法	脱机交易类必测项
		4.3.20.2 非对称加密算法	脱机交易类必测项
		4.3.20.3 哈希算法	脱机交易类必测项

（4） 数据安全性

编号	检测项		检测说明
4.4.1	数据保护	4.4.1.1 客户身份信息保护	必测项
		4.4.1.2 支付业务信息保护	必测项
		4.4.1.3 会计档案信息保护	必测项
4.4.2	数据完整性	4.4.2.1 重要数据更改机制	必测项
		4.4.2.2 银行卡和移动终端设备关联保护	必测项
		4.4.2.3 数据备份记录	必测项
		4.4.2.4 保障传输过程中的数据完整性	必测项
		4.4.2.5 备份数据定期恢复	必测项
4.4.3	交易数据以及客户数据的安全性	4.4.3.1 数据物理存储安全	必测项
		4.4.3.2 客户身份认证信息存储安全	必测项
		4.4.3.3 卡内数据安全	必测项
		4.4.3.4 终端信息采集设备硬加密措施或其它防伪手段	必测项
		4.4.3.5 同一安全级别和可信赖的系统之间信息传输	必测项
		4.4.3.6 加密传输	必测项
		4.4.3.7 加密存储	必测项
		4.4.3.8 数据访问控制	必测项
		4.4.3.9 在线的存储备份	必测项
		4.4.3.10 数据备份机制	必测项
		4.4.3.11 本地备份	必测项
		4.4.3.12 异地备份	必测项
		4.4.3.13 备份数据的恢复	必测项
		4.4.3.14 数据销毁制度和记录	必测项
		4.4.3.15 关键链路冗余设计	必测项

（5） 运维安全性

编号	检测项		检测说明
4.5.1	环境管理	4.5.1.1 机房基础设施定期维护	必测项
		4.5.1.2 机房的出入管理制度化和文档化	必测项
		4.5.1.3 办公环境的保密性措施	必测项
		4.5.1.4 机房安全管理制度	必测项
		4.5.1.5 机房进出登记表	必测项
4.5.2	介质管理	4.5.2.1 介质的存放环境保护措施	必测项
		4.5.2.2 介质的使用管理文档化	必测项
		4.5.2.3 维修或销毁介质之前清除敏感数据	必测项
		4.5.2.4 介质管理记录	必测项
		4.5.2.5 介质的分类与标识	必测项
4.5.3	设备管理	4.5.3.1 设备管理的责任人员或部门	必测项
		4.5.3.2 设施、设备定期维护	必测项
		4.5.3.3 设备选型、采购、发放等的审批控制	必测项
		4.5.3.4 设备配置标准化	必测项
		4.5.3.5 设备的操作规程	必测项
		4.5.3.6 设备的操作日志	必测项
		4.5.3.7 设备使用管理文档	必测项
		4.5.3.8 设备标识	必测项
4.5.4	人员管理	4.5.4.1 人员录用	必测项
		4.5.4.2 人员转岗、离岗	必测项
		4.5.4.3 人员考核	必测项
		4.5.4.4 安全意识教育和培训	必测项
		4.5.4.5 外部人员访问管理	必测项
		4.5.4.6 职责分离	必测项
4.5.5	监控管理	4.5.5.1 主要网络设备的各项指标监控情况	必测项
		4.5.5.2 主要服务器的各项指标监控情况	必测项
		4.5.5.3 应用运行各项指标监控情况	必测项
		4.5.5.4 异常处理机制	必测项
4.5.6	变更管理	4.5.6.1 变更方案	必测项
		4.5.6.2 变更制度化管理	必测项
		4.5.6.3 重要系统变更的批准	必测项
		4.5.6.4 重要系统变更的通知	必测项
4.5.7	安全事件处置	4.5.7.1 安全事件报告和处置	必测项

编号	检测项		检测说明
		4.5.7.2 安全事件的分类和分级	必测项
		4.5.7.3 安全事件记录和采取的措施	必测项
4.5.8	应急预案管理	4.5.8.1 制定不同事件的应急预案	必测项
		4.5.8.2 相关人员应急预案培训	必测项
		4.5.8.3 定期演练	必测项

（6） 业务连续性

编号	检测项		检测说明
4.6.1	业务连续性需求分析	4.6.1.1 业务中断影响分析	必测项
		4.6.1.2 灾难恢复时间目标和恢复点目标	必测项
4.6.2	业务连续性技术环境	4.6.2.1 备份机房	必测项
		4.6.2.2 网络双链路	必测项
		4.6.2.3 网络设备和服务器备份	必测项
		4.6.2.4 高可靠的磁盘阵列	必测项
		4.6.2.5 远程数据库备份	必测项
4.6.3	业务连续性管理	4.6.3.1 业务连续性管理制度	必测项
		4.6.3.2 应急响应流程	必测项
		4.6.3.3 恢复预案	必测项
		4.6.3.4 数据备份和恢复制度	必测项
4.6.4	备份与恢复管理	4.6.4.1 备份数据范围和备份频率	必测项
		4.6.4.2 备份和恢复手册	必测项
		4.6.4.3 备份记录和定期恢复测试记录	必测项
		4.6.4.4 定期数据备份恢复性测试	必测项
4.6.5	日常维护	4.6.5.1 每年业务连续性演练	必测项
		4.6.5.2 定期业务连续性培训	必测项

A.3.5 文档检测项

编号	检测项		检测说明
5.1	用户文档	5.1.1 用户手册	必测项
		5.1.2 操作手册	必测项
5.2	开发文档	5.2.1 需求说明书	必测项
		5.2.2 需求分析文档	必测项

编号	检测项		检测说明
		5.2.3 总体设计方案	必测项
		5.2.4 数据库设计文档	必测项
		5.2.5 概要设计文档	必测项
		5.2.6 详细设计文档	必测项
		5.2.7 工程实施方案	必测项
5.3	管理文档	5.3.1 测试报告	必测项
		5.3.2 系统运维手册	必测项
		5.3.3 系统应急手册	必测项
		5.3.4 运维管理制度	必测项
		5.3.5 安全管理制度	必测项
		5.3.6 安全审计报告	必测项

A.4 移动电话支付（远程支付）系统检测项

A.4.1 功能检测项

编号	检测项		检测说明
1.1	客户管理	1.1.1 客户信息登记及管理	必测项
		1.1.2 终端设备关联	
		1.1.3 商业银行管理	
		1.1.4 客户证书管理	
		1.1.5 客户审核	必测项
1.2	账户管理	1.2.1 客户支付账户管理	必测项
		1.2.2 客户支付账户管理审核	
		1.2.3 银行卡关联	
		1.2.4 客户支付账户查询	必测项
		1.2.5 客户支付账户资金审核	
1.3	卡片管理	1.3.1 制卡	必测项（无卡片发行情况不适用）
		1.3.2 卡片发行	必测项（无卡片发行情况不适用）
		1.3.3 卡片激活	必测项（无卡片发行情况不适

编号	检测项		检测说明
			用）
		1.3.4 卡片个人化	必测项（无卡片发行情况不适用）
		1.3.5 更换	必测项（无卡片发行情况不适用）
		1.3.6 密码修改	
		1.3.7 挂失/解挂	
		1.3.8 锁定/解锁	
		1.3.9 注销	
1.4	密钥和证书管理	1.4.1 认证中心公钥管理	
		1.4.2 支付机构密钥管理	
		1.4.3 卡片密钥管理	必测项（无卡片发行情况不适用）
		1.4.4 支付机构证书管理	
		1.4.5 卡片证书管理	
1.5	交易处理	1.5.1 一般支付	一般支付类必测项
		1.5.2 担保支付	担保支付类必测项
		1.5.3 协议支付	协议支付类必测项
		1.5.4 订单撤销	必测项
		1.5.5 转账	
		1.5.6 预存	
		1.5.7 提现	
		1.5.8 积分查询	
		1.5.9 积分兑换	
		1.5.10 积分兑换撤销	
		1.5.11 交易纠纷处理	
		1.5.12 交易明细查询	必测项
		1.5.13 交易明细下载	
		1.5.14 邀请其他人代付	
1.6	资金结算	1.6.1 客户结算	必测项

编号	检测项		检测说明
1.7	对账处理	1.7.1 发送对账请求	
		1.7.2 生成对账文件	
1.8	差错处理	1.8.1 长款/短款处理	必测项
		1.8.2 单笔退款	必测项
		1.8.3 批量退款	
1.9	统计报表	1.9.1 业务类报表	必测项
		1.9.2 运行管理类报表	必测项
1.10	运营管理	1.10.1 运营人员权限管理	必测项
		1.10.2 提现风控处理	
		1.10.3 提现财务处理	
		1.10.4 退款风控处理	
		1.10.5 退款财务处理	

A.4.2 风险监控检测项

编号	检测项		检测说明
2.1	账户风险管理	2.1.1 实名认证	
		2.1.2 业务范围	短信支付、WAP 支付必测项
		2.1.3 手机号码与账户绑定	短信支付必测项
		2.1.4 账户变更	必测项
2.2	交易监控	2.2.1 监控规则管理	必测项
		2.2.2 当日交易查询	必测项
		2.2.3 历史交易查询	必测项
		2.2.4 实时交易监控	必测项
		2.2.5 可疑交易处理	必测项
		2.2.6 交易事件报警	必测项
2.3	交易风险管理	2.3.1 单笔充值上限	必测项
		2.3.2 单笔消费上限	必测项
		2.3.3 单日、单月累计消费上限	必测项
		2.3.4 当日累计消费次数限制	必测项
		2.3.5 账户资金余额上限	必测项
2.4	交易审核	2.4.1 系统自动审核	必测项
		2.4.2 人工审核	必测项

编号	检测项		检测说明
2.5	风控规则	2.5.1 风控规则管理	必测项
		2.5.2 黑名单	必测项
		2.5.3 风险识别	必测项
		2.5.4 事件管理	必测项
		2.5.5 风险报表	必测项
2.6	商户风险管理	2.6.1 商户资质审核	必测项
		2.6.2 商户签约	必测项
		2.6.3 特约商户日常风险管理	必测项
		2.6.4 合作的第三方机构的风险管理	
		2.6.5 特约商户强制冻结、解冻、解约	必测项
		2.6.6 可疑商户信息共享	
		2.6.7 风险事件报送	必测项

A.4.3 性能检测项

编号	检测项	检测说明
3.1	3.1.1 支付	必测项
3.2	3.2.1 预存	
3.3	3.3.1 转账	
3.4	3.4.1 交易明细查询	必测项
3.5	3.5.1 日终批处理	

A.4.4 安全性检测项

（1） 网络安全性

编号	检测项		检测说明
4.1.1	结构安全	4.1.1.1 网络冗余和备份	必测项
		4.1.1.2 网络安全路由器	必测项
		4.1.1.3 网络安全防火墙	必测项
		4.1.1.4 网络拓扑结构	必测项
		4.1.1.5 IP 子网划分	必测项
		4.1.1.6 QoS 保证	必测项
4.1.2	网络访问控制	4.1.2.1 网络域安全隔离和限制	必测项

编号	检测项		检测说明
		4.1.2.2 地址转换和绑定	必测项
		4.1.2.3 内容过滤	必测项
		4.1.2.4 访问控制	必测项
		4.1.2.5 流量控制	必测项
		4.1.2.6 会话控制	必测项
		4.1.2.7 远程拨号访问控制和记录	必测项
4.1.3	网络安全审计	4.1.3.1 日志信息	必测项
		4.1.3.2 网络系统故障分析	必测项
		4.1.3.3 网络对象操作审计	必测项
		4.1.3.4 日志权限和保护	必测项
		4.1.3.5 审计工具	必测项
4.1.4	边界完整性检查	4.1.4.1 内外网非法连接阻断和定位	必测项
4.1.5	网络入侵防范	4.1.5.1 网络 ARP 欺骗攻击	必测项
		4.1.5.2 信息窃取	必测项
		4.1.5.3 DOS/DDOS 攻击	必测项
		4.1.5.4 网络入侵防范机制	必测项
4.1.6	恶意代码防范	4.1.6.1 恶意代码防范措施	必测项
		4.1.6.2 定时更新	必测项
4.1.7	网络设备防护	4.1.7.1 设备登录设置	必测项
		4.1.7.2 设备登录口令安全性	必测项
		4.1.7.3 登录地址限制	必测项
		4.1.7.4 远程管理安全	必测项
		4.1.7.5 设备用户设置策略	必测项
		4.1.7.6 权限分离	必测项
		4.1.7.7 最小化服务	必测项
4.1.8	网络安全管理	4.1.8.1 网络设备运维手册	必测项
		4.1.8.2 定期补丁安装	必测项
		4.1.8.3 漏洞扫描	必测项
		4.1.8.4 网络数据传输加密	必测项
4.1.9	网络相关人员安全管理	4.1.9.1 网络安全管理人员配备	必测项
		4.1.9.2 网络安全管理人员责任划分规则	必测项
		4.1.9.3 网络安全关键岗位人员管理	必测项

（2） 主机安全性

编号	检测项		检测说明
4.2.1	身份鉴别	4.2.1.1 系统与应用管理员用户设置	必测项
		4.2.1.2 系统与应用管理员口令安全性	必测项
		4.2.1.3 登录策略	必测项
4.2.2	访问控制	4.2.2.1 访问控制范围	必测项
		4.2.2.2 主机信任关系	必测项
		4.2.2.3 默认过期用户	必测项
4.2.3	安全审计	4.2.3.1 日志信息	必测项
		4.2.3.2 日志权限和保护	必测项
		4.2.3.3 系统信息分析	必测项
4.2.4	系统保护	4.2.4.1 系统备份	必测项
		4.2.4.2 故障恢复策略	必测项
		4.2.4.3 磁盘空间安全	必测项
		4.2.4.4 主机安全加固	必测项
4.2.5	剩余信息保护	4.2.5.1 剩余信息保护	必测项
4.2.6	入侵防范	4.2.6.1 入侵防范记录	必测项
		4.2.6.2 关闭服务和端口	必测项
		4.2.6.3 最小安装原则	必测项
4.2.7	恶意代码防范	4.2.7.1 防范软件安装部署	必测项
		4.2.7.2 病毒库定时更新	必测项
		4.2.7.3 防范软件统一管理	必测项
4.2.8	资源控制	4.2.8.1 连接控制	必测项
		4.2.8.2 资源监控和预警	必测项
4.2.9	主机安全管理	4.2.9.1 主机运维手册	必测项
		4.2.9.2 漏洞扫描	必测项
		4.2.9.3 系统补丁	必测项
		4.2.9.4 操作日志管理	必测项
4.2.10	主机相关人员安全管理	4.2.10.1 主机安全管理人员配备	必测项
		4.2.10.2 主机安全管理人员责任划分规则	必测项
		4.2.10.3 主机安全关键岗位人员管理	必测项

（3） 应用安全性

编号	检测项		检测说明
4.3.1	身份鉴别	4.3.1.1 系统与普通用户设置	必测项
		4.3.1.2 系统与普通用户口令安全性	必测项
		4.3.1.3 登录访问安全策略	必测项
		4.3.1.4 非法访问警示和记录	必测项
		4.3.1.5 客户端鉴别信息安全	必测项
		4.3.1.6 口令有效期限制	必测项
		4.3.1.7 限制认证会话时间	必测项
		4.3.1.8 身份标识唯一性	必测项
		4.3.1.9 及时清除鉴别信息	必测项
4.3.2	WEB 页面安全	4.3.2.1 登录防穷举	必测项
		4.3.2.2 安全控件	必测项
		4.3.2.3 使用数字证书	必测项
		4.3.2.4 独立的支付密码	必测项
		4.3.2.5 网站页面 SQL 注入防范	必测项
		4.3.2.6 网站页面跨站脚本攻击防范	必测项
		4.3.2.7 网站页面源代码暴露防范	必测项
		4.3.2.8 网站页面黑客挂马防范	必测项
		4.3.2.9 网站页面防篡改措施	必测项
		4.3.2.10 网站页面防钓鱼	必测项
4.3.3	WAP 页面安全	4.3.3.1 登录防穷举	必测项
		4.3.3.2 使用数字证书	必测项
		4.3.3.3 独立的支付密码	必测项
		4.3.3.4 网站页面 SQL 注入防范	必测项
		4.3.3.5 网站页面跨站脚本攻击防范	必测项
		4.3.3.6 网站页面源代码暴露防范	必测项
		4.3.3.7 网站页面防篡改措施	必测项
		4.3.3.8 网站页面防钓鱼	必测项
4.3.4	客户端程序安全	4.3.4.1 客户端程序保护	必测项(适用于采用客户端进行移动支付方式)
		4.3.4.2 客户端配置文件保护	必测项(适用于采用客户端进行移动支付方式)

编号	检测项		检测说明
		4.3.4.3 独立的支付密码	必测项(适用于采用客户端进行移动支付方式)
		4.3.4.4 密码保护	必测项(适用于采用客户端进行移动支付方式)
		4.3.4.5 程序安全检测与升级	必测项(适用于采用客户端进行移动支付方式)
4.3.5	访问控制	4.3.5.1 访问权限设置	必测项
		4.3.5.2 自主访问控制范围	必测项
		4.3.5.3 业务操作日志	必测项
		4.3.5.4 关键数据存放	必测项
		4.3.5.5 异常中断防护	必测项
		4.3.5.6 数据库安全配置	必测项
4.3.6	安全审计	4.3.6.1 日志信息	必测项
		4.3.6.2 日志权限和保护	必测项
		4.3.6.3 系统信息查询与分析	必测项
		4.3.6.4 对象操作审计	必测项
		4.3.6.5 审计工具	必测项
		4.3.6.6 事件报警	必测项
4.3.7	剩余信息保护	4.3.7.1 过期信息、文档处理	必测项
4.3.8	资源控制	4.3.8.1 连接控制	必测项
		4.3.8.2 会话控制	必测项
		4.3.8.3 进程资源分配	必测项
		4.3.8.4 资源检测预警	必测项
4.3.9	应用容错	4.3.9.1 数据有效性校验	必测项
		4.3.9.2 容错机制	必测项
		4.3.9.3 故障机制	必测项
		4.3.9.4 回退机制	必测项
4.3.10	报文完整性	4.3.10.1 通信报文有效性	必测项
4.3.11	报文保密性	4.3.11.1 报文或会话加密	必测项
4.3.12	抗抵赖	4.3.12.1 原发和接收证据	必测项
4.3.13	编码安全	4.3.13.1 源代码审查	必测项
		4.3.13.2 插件安全性审查	必测项

编号	检测项		检测说明
		4.3.13.3 编码规范约束	必测项
		4.3.13.4 源代码管理	必测项
		4.3.13.5 版本管理	必测项
4.3.14	电子认证应用	4.3.14.1 第三方电子认证机构	必测项
		4.3.14.2 关键业务电子认证技术应用	必测项
		4.3.14.3 电子签名有效性	必测项
		4.3.14.4 服务器证书私钥保护	必测项

（4） 数据安全性

编号	检测项		检测说明
4.4.1	数据保护	4.4.1.1 客户身份信息保护	必测项
		4.4.1.2 支付业务信息保护	必测项
		4.4.1.3 会计档案信息保护	必测项
4.4.2	数据完整性	4.4.2.1 重要数据更改机制	必测项
		4.4.2.2 银行卡和移动终端设备关联保护	必测项
		4.4.2.3 数据备份记录	必测项
		4.4.2.4 保障传输过程中的数据完整性	必测项
		4.4.2.5 备份数据定期恢复	必测项
4.4.3	交易数据以及客户数据的安全性	4.4.3.1 数据物理存储安全	必测项
		4.4.3.2 客户身份认证信息存储安全	必测项
		4.4.3.3 卡内数据安全	必测项
		4.4.3.4 终端信息采集设备硬加密措施或其它防伪手段	必测项
		4.4.3.5 同一安全级别和可信赖的系统之间信息传输	必测项
		4.4.3.6 加密传输	必测项
		4.4.3.7 加密存储	必测项
		4.4.3.8 数据访问控制	必测项
		4.4.3.9 在线的存储备份	必测项
		4.4.3.10 数据备份机制	必测项
		4.4.3.11 本地备份	必测项
		4.4.3.12 异地备份	必测项
		4.4.3.13 备份数据的恢复	必测项

编号	检测项		检测说明
		4.4.3.14 数据销毁制度和记录	必测项
		4.4.3.15 关键链路冗余设计	必测项

（5） 运维安全性

编号	检测项		检测说明
4.5.1	环境管理	4.5.1.1 机房基础设施定期维护	必测项
		4.5.1.2 机房的出入管理制度化和文档化	必测项
		4.5.1.3 办公环境的保密性措施	必测项
		4.5.1.4 机房安全管理制度	必测项
		4.5.1.5 机房进出登记表	必测项
4.5.2	介质管理	4.5.2.1 介质的存放环境保护措施	必测项
		4.5.2.2 介质的使用管理文档化	必测项
		4.5.2.3 维修或销毁介质之前清除敏感数据	必测项
		4.5.2.4 介质管理记录	必测项
		4.5.2.5 介质的分类与标识	必测项
4.5.3	设备管理	4.5.3.1 设备管理的责任人员或部门	必测项
		4.5.3.2 设施、设备定期维护	必测项
		4.5.3.3 设备选型、采购、发放等的审批控制	必测项
		4.5.3.4 设备配置标准化	必测项
		4.5.3.5 设备的操作规程	必测项
		4.5.3.6 设备的操作日志	必测项
		4.5.3.7 设备使用管理文档	必测项
		4.5.3.8 设备标识	必测项
4.5.4	人员管理	4.5.4.1 人员录用	必测项
		4.5.4.2 人员转岗、离岗	必测项
		4.5.4.3 人员考核	必测项
		4.5.4.4 安全意识教育和培训	必测项
		4.5.4.5 外部人员访问管理	必测项
		4.5.4.6 职责分离	必测项
4.5.5	监控管理	4.5.5.1 主要网络设备的各项指标监控情况	必测项
		4.5.5.2 主要服务器的各项指标监控情况	必测项
		4.5.5.3 应用运行各项指标监控情况	必测项
		4.5.5.4 异常处理机制	必测项

编号	检测项		检测说明
4.5.6	变更管理	4.5.6.1 变更方案	必测项
		4.5.6.2 变更制度化管理	必测项
		4.5.6.3 重要系统变更的批准	必测项
		4.5.6.4 重要系统变更的通知	必测项
4.5.7	安全事件处置	4.5.7.1 安全事件报告和处置	必测项
		4.5.7.2 安全事件的分类和分级	必测项
		4.5.7.3 安全事件记录和采取的措施	必测项
4.5.8	应急预案管理	4.5.8.1 制定不同事件的应急预案	必测项
		4.5.8.2 相关人员应急预案培训	必测项
		4.5.8.3 定期演练	必测项

（6） 业务连续性

编号	检测项		检测说明
4.6.1	业务连续性需求分析	4.6.1.1 业务中断影响分析	必测项
		4.6.1.2 灾难恢复时间目标和恢复点目标	必测项
4.6.2	业务连续性技术环境	4.6.2.1 备份机房	必测项
		4.6.2.2 网络双链路	必测项
		4.6.2.3 网络设备和服务器备份	必测项
		4.6.2.4 高可靠的磁盘阵列	必测项
		4.6.2.5 远程数据库备份	必测项
4.6.3	业务连续性管理	4.6.3.1 业务连续性管理制度	必测项
		4.6.3.2 应急响应流程	必测项
		4.6.3.3 恢复预案	必测项
		4.6.3.4 数据备份和恢复制度	必测项
4.6.4	备份与恢复管理	4.6.4.1 备份数据范围和备份频率	必测项
		4.6.4.2 备份和恢复手册	必测项
		4.6.4.3 备份记录和定期恢复测试记录	必测项
		4.6.4.4 定期数据备份恢复性测试	必测项
4.6.5	日常维护	4.6.5.1 每年业务连续性演练	必测项
		4.6.5.2 定期业务连续性培训	必测项

A.4.5 文档检测项

编号	检测项		检测说明
5.1	用户文档	5.1.1 用户手册	必测项
		5.1.2 操作手册	必测项
5.2	开发文档	5.2.1 需求说明书	必测项
		5.2.2 需求分析文档	必测项
		5.2.3 总体设计方案	必测项
		5.2.4 数据库设计文档	必测项
		5.2.5 概要设计文档	必测项
		5.2.6 详细设计文档	必测项
		5.2.7 工程实施方案	必测项
5.3	管理文档	5.3.1 测试报告	必测项
		5.3.2 系统运维手册	必测项
		5.3.3 系统应急手册	必测项
		5.3.4 运维管理制度	必测项
		5.3.5 安全管理制度	必测项
		5.3.6 安全审计报告	必测项

A.5 固定电话支付系统检测项

A.5.1 功能检测项

编号	检测项		检测说明
1.1	客户管理	1.1.1 客户信息登记及管理	必测项
		1.1.2 终端设备关联	
		1.1.3 电话语音密码	
		1.1.4 商业银行管理	
		1.1.5 客户证书管理	
		1.1.6 客户审核	必测项
1.2	账户管理	1.2.1 客户支付账户管理	必测项
		1.2.2 客户支付账户管理审核	
		1.2.3 银行卡关联	
		1.2.4 客户支付账户查询	必测项
		1.2.5 客户支付账户资金审核	
1.3	语音 IVR 管理	1.3.1 IVR 登录	
		1.3.2 按键输入	必测项
		1.3.3 电话回拨	
		1.3.4 用户信息保护	必测项
1.4	交易处理	1.4.1 一般支付	一般支付类必测项

编号	检测项		检测说明
		1.4.2 担保支付	担保支付类必测项
		1.4.3 协议支付	协议支付类必测项
		1.4.4 消费撤销	必测项
		1.4.5 转账	
		1.4.6 预存	
		1.4.7 提现	
		1.4.8 积分查询	
		1.4.9 积分兑换	
		1.4.10 积分兑换撤销	
		1.4.11 交易纠纷处理	
		1.4.12 交易明细查询	必测项
		1.4.13 交易明细下载	
		1.4.14 邀请其他人代付	
1.5	资金结算	1.5.1 客户结算	必测项
1.6	对账处理	1.6.1 商户发送对账请求	
		1.6.2 商户下载对账文件	
1.7	差错处理	1.7.1 长款/短款处理	必测项
		1.7.2 单笔退款	必测项
		1.7.3 批量退款	
1.8	统计报表	1.8.1 业务类报表	必测项
		1.8.2 运行管理类报表	必测项
1.9	运营管理	1.9.1 运营人员权限管理	必测项
		1.9.2 提现风控处理	
		1.9.3 提现财务处理	
		1.9.4 退款风控处理	
		1.9.5 退款财务处理	

A.5.2 风险监控检测项

编号	检测项		检测说明
2.1	账户风险管理	2.1.1 实名认证	
2.2	交易监控	2.2.1 监控规则管理	必测项
		2.2.2 当日交易查询	必测项
		2.2.3 历史交易查询	必测项
		2.2.4 实时交易监控	必测项
		2.2.5 异常交易监控	必测项
		2.2.6 交易事件报警	必测项
2.3	交易审核	2.3.1 系统自动审核	必测项
		2.3.2 人工审核	必测项
2.4	风控规则	2.4.1 风控规则管理	必测项

编号	检测项		检测说明
		2.4.2 黑名单	必测项
		2.4.3 风险识别	必测项
		2.4.4 事件管理	必测项
		2.4.5 风险报表	必测项

A.5.3 性能检测项

编号	检测项	检测说明
3.1	3.1.1 支付	必测项
3.2	3.2.1 IVR 呼入	
3.3	3.3.1 预存	
3.4	3.4.1 转账	
3.5	3.5.1 交易明细查询	必测项
3.6	3.6.1 日终批处理	

A.5.4 安全性检测项

（1） 网络安全性测试

编号	检测项		检测说明
4.1.1	结构安全	4.1.1.1 网络冗余和备份	必测项
		4.1.1.2 网络安全路由器	必测项
		4.1.1.3 网络安全防火墙	必测项
		4.1.1.4 网络拓扑结构	必测项
		4.1.1.5 IP 子网划分	必测项
		4.1.1.6 QoS 保证	必测项
4.1.2	网络访问控制	4.1.2.1 网络域安全隔离和限制	必测项
		4.1.2.2 地址转换和绑定	必测项
		4.1.2.3 内容过滤	必测项
		4.1.2.4 访问控制	必测项
		4.1.2.5 流量控制	必测项
		4.1.2.6 会话控制	必测项
		4.1.2.7 远程拨号访问控制和记录	必测项

编号	检测项		检测说明
4.1.3	网络安全审计	4.1.3.1 日志信息	必测项
		4.1.3.2 网络系统故障分析	必测项
		4.1.3.3 网络对象操作审计	必测项
		4.1.3.4 日志权限和保护	必测项
		4.1.3.5 审计工具	必测项
4.1.4	边界完整性检查	4.1.4.1 内外网非法连接阻断和定位	必测项
4.1.5	网络入侵防范	4.1.5.1 网络 ARP 欺骗攻击	必测项
		4.1.5.2 信息窃取	必测项
		4.1.5.3 DOS/DDOS 攻击	必测项
		4.1.5.4 网络入侵防范机制	必测项
4.1.6	恶意代码防范	4.1.6.1 恶意代码防范措施	必测项
		4.1.6.2 定时更新	必测项
4.1.7	网络设备防护	4.1.7.1 设备登录设置	必测项
		4.1.7.2 设备登录口令安全性	必测项
		4.1.7.3 登录地址限制	必测项
		4.1.7.4 远程管理安全	必测项
		4.1.7.5 设备用户设置策略	必测项
		4.1.7.6 权限分离	必测项
		4.1.7.7 最小化服务	必测项
4.1.8	网络安全管理	4.1.8.1 网络设备运维手册	必测项
		4.1.8.2 定期补丁安装	必测项
		4.1.8.3 漏洞扫描	必测项
		4.1.8.4 网络数据传输加密	必测项
4.1.9	网络相关人员安全管理	4.1.9.1 网络安全管理人员配备	必测项
		4.1.9.2 网络安全管理人员责任划分规则	必测项
		4.1.9.3 网络安全关键岗位人员管理	必测项

（2） 主机安全性测试

编号	检测项		检测说明
4.2.1	身份鉴别	4.2.1.1 系统与应用管理员用户设置	必测项
		4.2.1.2 系统与应用管理员口令安全性	必测项
		4.2.1.3 登录策略	必测项

编号	检测项		检测说明
4.2.2	访问控制	4.2.2.1 访问控制范围	必测项
		4.2.2.2 主机信任关系	必测项
		4.2.2.3 默认过期用户	必测项
4.2.3	安全审计	4.2.3.1 日志信息	必测项
		4.2.3.2 日志权限和保护	必测项
		4.2.3.3 系统信息分析	必测项
4.2.4	系统保护	4.2.4.1 系统备份	必测项
		4.2.4.2 故障恢复策略	必测项
		4.2.4.3 磁盘空间安全	必测项
		4.2.4.4 主机安全加固	必测项
4.2.5	剩余信息保护	4.2.5.1 剩余信息保护	必测项
4.2.6	入侵防范	4.2.6.1 入侵防范记录	必测项
		4.2.6.2 关闭服务和端口	必测项
		4.2.6.3 最小安装原则	必测项
4.2.7	恶意代码防范	4.2.7.1 防范软件安装部署	必测项
		4.2.7.2 病毒库定时更新	必测项
		4.2.7.3 防范软件统一管理	必测项
4.2.8	资源控制	4.2.8.1 连接控制	必测项
		4.2.8.2 资源监控和预警	必测项
4.2.9	主机安全管理	4.2.9.1 主机运维手册	必测项
		4.2.9.2 漏洞扫描	必测项
		4.2.9.3 系统补丁	必测项
		4.2.9.4 操作日志管理	必测项
4.2.10	主机相关人员安全管理	4.2.10.1 主机安全管理人员配备	必测项
		4.2.10.2 主机安全管理人员责任划分规则	必测项
		4.2.10.3 主机安全关键岗位人员管理	必测项

（3） 应用安全性测试

编号	检测项		检测说明
4.3.1	身份鉴别	4.3.1.1 系统与普通用户设置	必测项
		4.3.1.2 系统与普通用户口令安全性	必测项
		4.3.1.3 登录访问安全策略	必测项

编号	检测项		检测说明
		4.3.1.4 非法访问警示和记录	必测项
		4.3.1.5 客户端鉴别信息安全	必测项
		4.3.1.6 口令有效期限制	必测项
		4.3.1.7 限制认证会话时间	必测项
		4.3.1.8 身份标识唯一性	必测项
		4.3.1.9 及时清除鉴别信息	必测项
4.3.2	WEB 页面安全	4.3.2.1 登录防穷举	必测项
		4.3.2.2 安全控件	必测项
		4.3.2.3 使用数字证书	必测项
		4.3.2.4 独立的支付密码	必测项
		4.3.2.5 网站页面 SQL 注入防范	必测项
		4.3.2.6 网站页面跨站脚本攻击防范	必测项
		4.3.2.7 网站页面源代码暴露防范	必测项
		4.3.2.8 网站页面黑客挂马防范	必测项
		4.3.2.9 网站页面防篡改措施	必测项
		4.3.2.10 网站页面防钓鱼	必测项
4.3.3	访问控制	4.3.3.1 访问权限设置	必测项
		4.3.3.2 自主访问控制范围	必测项
		4.3.3.3 业务操作日志	必测项
		4.3.3.4 关键数据存放	必测项
		4.3.3.5 异常中断防护	必测项
		4.3.3.6 数据库安全配置	必测项
4.3.4	安全审计	4.3.4.1 日志信息	必测项
		4.3.4.2 日志权限和保护	必测项
		4.3.4.3 系统信息查询与分析	必测项
		4.3.4.4 对象操作审计	必测项
		4.3.4.5 审计工具	必测项
		4.3.4.6 事件报警	必测项
4.3.5	剩余信息保护	4.3.5.1 过期信息、文档处理	必测项
4.3.6	资源控制	4.3.6.1 连接控制	必测项
		4.3.6.2 会话控制	必测项
		4.3.6.3 进程资源分配	必测项
		4.3.6.4 资源检测预警	必测项

编号	检测项		检测说明
4.3.7	应用容错	4.3.7.1 数据有效性校验	必测项
		4.3.7.2 容错机制	必测项
		4.3.7.3 故障机制	必测项
		4.3.7.4 回退机制	必测项
4.3.8	报文完整性	4.3.8.1 通信报文有效性	必测项
4.3.9	报文保密性	4.3.9.1 报文或会话加密	必测项
4.3.10	抗抵赖	4.3.10.1 原发和接收证据	必测项
4.3.11	编码安全	4.3.11.1 源代码审查	必测项
		4.3.11.2 插件安全性审查	必测项
		4.3.11.3 编码规范约束	必测项
		4.3.11.4 源代码管理	必测项
		4.3.11.5 版本管理	必测项
4.3.12	电子认证应用	4.3.12.1 第三方电子认证机构	必测项
		4.3.12.2 关键业务电子认证技术应用	必测项
		4.3.12.3 电子签名有效性	必测项
		4.3.12.4 服务器证书私钥保护	必测项

（4） 数据安全性测试

编号	检测项		检测说明
4.4.1	数据保护	4.4.1.1 客户身份信息保护	必测项
		4.4.1.2 支付业务信息保护	必测项
		4.4.1.3 会计档案信息保护	必测项
4.4.2	数据完整性	4.4.2.1 重要数据更改机制	必测项
		4.4.2.2 终端设备关联保护	必测项
		4.4.2.3 数据备份记录	必测项
		4.4.2.4 保障传输过程中的数据完整性	必测项
		4.4.2.5 备份数据定期恢复	必测项
4.4.3	交易数据以及客户数据的安全性	4.4.3.1 数据物理存储安全	必测项
		4.4.3.2 客户身份认证信息存储安全	必测项
		4.4.3.3 同一安全级别和可信赖的系统之间信息传输	必测项
		4.4.3.4 加密传输	必测项
		4.4.3.5 加密存储	必测项

编号	检测项		检测说明
		4.4.3.6 数据访问控制	必测项
		4.4.3.7 在线的存储备份	必测项
		4.4.3.8 数据备份机制	必测项
		4.4.3.9 本地备份	必测项
		4.4.3.10 异地备份	必测项
		4.4.3.11 备份数据的恢复	必测项
		4.4.3.12 数据销毁制度和记录	必测项
		4.4.3.13 关键链路冗余设计	必测项

（5） 运维安全性测试

编号	检测项		检测说明
4.5.1	环境管理	4.5.1.1 机房基础设施定期维护	必测项
		4.5.1.2 机房的出入管理制度化和文档化	必测项
		4.5.1.3 办公环境的保密性措施	必测项
		4.5.1.4 机房安全管理制度	必测项
		4.5.1.5 机房进出登记表	必测项
4.5.2	介质管理	4.5.2.1 介质的存放环境保护措施	必测项
		4.5.2.2 介质的使用管理文档化	必测项
		4.5.2.3 维修或销毁介质之前清除敏感数据	必测项
		4.5.2.4 介质管理记录	必测项
		4.5.2.5 介质的分类与标识	必测项
4.5.3	设备管理	4.5.3.1 设备管理的责任人员或部门	必测项
		4.5.3.2 设施、设备定期维护	必测项
		4.5.3.3 设备选型、采购、发放等的审批控制	必测项
		4.5.3.4 设备配置标准化	必测项
		4.5.3.5 设备的操作规程	必测项
		4.5.3.6 设备的操作日志	必测项
		4.5.3.7 设备使用管理文档	必测项
		4.5.3.8 设备标识	必测项
4.5.4	人员管理	4.5.4.1 人员录用	必测项
		4.5.4.2 人员转岗、离岗	必测项
		4.5.4.3 人员考核	必测项
		4.5.4.4 安全意识教育和培训	必测项

编号	检测项		检测说明
		4.5.4.5 外部人员访问管理	必测项
		4.5.4.6 职责分离	必测项
4.5.5	监控管理	4.5.5.1 主要网络设备的各项指标监控情况	必测项
		4.5.5.2 主要服务器的各项指标监控情况	必测项
		4.5.5.3 应用运行各项指标监控情况	必测项
		4.5.5.4 异常处理机制	必测项
4.5.6	变更管理	4.5.6.1 变更方案	必测项
		4.5.6.2 变更制度化管理	必测项
		4.5.6.3 重要系统变更的批准	必测项
		4.5.6.4 重要系统变更的通知	必测项
4.5.7	安全事件处置	4.5.7.1 安全事件报告和处置	必测项
		4.5.7.2 安全事件的分类和分级	必测项
		4.5.7.3 安全事件记录和采取的措施	必测项
4.5.8	应急预案管理	4.5.8.1 制定不同事件的应急预案	必测项
		4.5.8.2 相关人员应急预案培训	必测项
		4.5.8.3 定期演练	必测项

（6） 业务连续性测试

编号	检测项		检测说明
4.6.1	业务连续性需求分析	4.6.1.1 业务中断影响分析	必测项
		4.6.1.2 灾难恢复时间目标和恢复点目标	必测项
4.6.2	业务连续性技术环境	4.6.2.1 备份机房	必测项
		4.6.2.2 网络双链路	必测项
		4.6.2.3 网络设备和服务器备份	必测项
		4.6.2.4 高可靠的磁盘阵列	必测项
		4.6.2.5 远程数据库备份	必测项
4.6.3	业务连续性管理	4.6.3.1 业务连续性管理制度	必测项
		4.6.3.2 应急响应流程	必测项
		4.6.3.3 恢复预案	必测项
		4.6.3.4 数据备份和恢复制度	必测项
4.6.4	备份与恢复管理	4.6.4.1 备份数据范围和备份频率	必测项
		4.6.4.2 备份和恢复手册	必测项
		4.6.4.3 备份记录和定期恢复测试记录	必测项

编号	检测项		检测说明
		4.6.4.4 定期数据备份恢复性测试	必测项
4.6.5	日常维护	4.6.5.1 每年业务连续性演练	必测项
		4.6.5.2 定期业务连续性培训	必测项

A.5.5 文档检测项

编号	检测项		检测说明
5.1	用户文档	5.1.1 用户手册	必测项
		5.1.2 操作手册	必测项
5.2	开发文档	5.2.1 需求说明书	必测项
		5.2.2 需求分析文档	必测项
		5.2.3 总体设计方案	必测项
		5.2.4 数据库设计文档	必测项
		5.2.5 概要设计文档	必测项
		5.2.6 详细设计文档	必测项
		5.2.7 工程实施方案	必测项
5.3	管理文档	5.3.1 测试报告	必测项
		5.3.2 系统运维手册	必测项
		5.3.3 系统应急手册	必测项
		5.3.4 运维管理制度	必测项
		5.3.5 安全管理制度	必测项
		5.3.6 安全审计报告	必测项

A.6 数字电视支付系统检测项

A.6.1 功能检测项

编号	检测项		检测说明
1.1	客户管理	1.1.1 客户信息登记及管理	必测项（卡支付不适用）
		1.1.2 商业银行管理	
		1.1.3 客户证书管理	
		1.1.4 客户审核	必测项（卡支付不适用）
1.2	账户管理	1.2.1 客户支付账户管理	必测项
		1.2.2 客户支付账户管理审核	
		1.2.3 客户支付账户查询	必测项
		1.2.4 客户支付账户资金审核	
1.3	交易处理	1.3.1 消费	必测项
		1.3.2 消费撤销	必测项

编号	检测项		检测说明
		1.3.3 转账	
		1.3.4 预存	
		1.3.5 提现	
		1.3.6 交易纠纷处理	
		1.3.7 交易明细查询	必测项
		1.3.8 委托交易	
		1.3.9 冲正交易	
		1.3.10 缴费	
		1.3.11 缴费撤销	
		1.3.12 退货	
		1.3.13 销账	
		1.3.14 预授权	
		1.3.15 预授权撤销	
		1.3.16 预授权完成	
		1.3.17 预授权完成撤销	
		1.3.18IC 卡指定账户圈存	
		1.3.19IC 卡现金充值	
		1.3.20IC 卡脱机交易上传	
		1.3.21 账单费用查询	
1.4	资金结算	1.4.1 客户结算	必测项
1.5	对账处理	1.5.1 客户发送对账请求	
		1.5.2 客户下载对账文件	
1.6	差错处理	1.6.1 长款/短款处理	必测项
		1.6.2 单笔退款	必测项
		1.6.3 批量退款	
1.7	统计报表	1.7.1 业务类报表	必测项
		1.7.2 运行管理类报表	必测项

A.6.2 风险监控检测项

编号	检测项		检测说明
2.1	账户风险管理	2.1.1 实名认证	
2.2	交易监控	2.2.1 监控规则管理	必测项
		2.2.2 当日交易查询	必测项
		2.2.3 历史交易查询	必测项
		2.2.4 实时交易监控	必测项
		2.2.5 可疑交易处理	必测项（卡支付不适用）
		2.2.6 交易事件报警	必测项（卡支付不适用）
2.3	交易审核	2.3.1 系统自动审核	必测项（卡支付不适用）

编号	检测项		检测说明
		2.3.2 人工审核	必测项（卡支付不适用）
2.4	风控规则	2.4.1 风控规则管理	必测项（卡支付不适用）
		2.4.2 黑名单	必测项（卡支付不适用）
		2.4.3 风险识别	必测项（卡支付不适用）
		2.4.4 事件管理	必测项（卡支付不适用）
		2.4.5 风险报表	必测项（卡支付不适用）

A.6.3 性能检测项

编号	检测项	检测说明
3.1	3.1.1 消费	必测项
3.2	3.2.1 交易明细查询	必测项
3.3	3.3.1 充值	
3.4	3.4.1 转账	
3.5	3.5.1 日终批处理	

A.6.4 安全性检测项

（1） 网络安全性测试

编号	检测项		检测说明
4.1.1	结构安全	4.1.1.1 网络冗余和备份	必测项
		4.1.1.2 网络安全路由器	必测项
		4.1.1.3 网络安全防火墙	必测项
		4.1.1.4 网络拓扑结构	必测项
		4.1.1.5 IP 子网划分	必测项
		4.1.1.6 QoS 保证	必测项
4.1.2	网络访问控制	4.1.2.1 网络域安全隔离和限制	必测项
		4.1.2.2 地址转换和绑定	必测项
		4.1.2.3 内容过滤	必测项

编号	检测项		检测说明
		4.1.2.4 访问控制	必测项
		4.1.2.5 流量控制	必测项
		4.1.2.6 会话控制	必测项
		4.1.2.7 远程拨号访问控制和记录	必测项
4.1.3	网络安全审计	4.1.3.1 日志信息	必测项
		4.1.3.2 网络系统故障分析	必测项
		4.1.3.3 网络对象操作审计	必测项
		4.1.3.4 日志权限和保护	必测项
		4.1.3.5 审计工具	必测项
4.1.4	边界完整性检查	4.1.4.1 内外网非法连接阻断和定位	必测项
4.1.5	网络入侵防范	4.1.5.1 网络 ARP 欺骗攻击	必测项
		4.1.5.2 信息窃取	必测项
		4.1.5.3 DOS/DDOS 攻击	必测项
		4.1.5.4 网络入侵防范机制	必测项
4.1.6	恶意代码防范	4.1.6.1 恶意代码防范措施	必测项
		4.1.6.2 定时更新	必测项
4.1.7	网络设备防护	4.1.7.1 设备登录设置	必测项
		4.1.7.2 设备登录口令安全性	必测项
		4.1.7.3 登录地址限制	必测项
		4.1.7.4 远程管理安全	必测项
		4.1.7.5 设备用户设置策略	必测项
		4.1.7.6 权限分离	必测项
		4.1.7.7 最小化服务	必测项
4.1.8	网络安全管理	4.1.8.1 网络设备运维手册	必测项
		4.1.8.2 定期补丁安装	必测项
		4.1.8.3 漏洞扫描	必测项
		4.1.8.4 网络数据传输加密	必测项
4.1.9	网络相关人员安全管理	4.1.9.1 网络安全管理人员配备	必测项
		4.1.9.2 网络安全管理人员责任划分规则	必测项
		4.1.9.3 网络安全关键岗位人员管理	必测项

（2） 主机安全性测试

编号	检测项		检测说明
4.2.1	身份鉴别	4.2.1.1 系统与应用管理员用户设置	必测项

编号	检测项		检测说明
		4.2.1.2 系统与应用管理员口令安全性	必测项
		4.2.1.3 登录策略	必测项
4.2.2	访问控制	4.2.2.1 访问控制范围	必测项
		4.2.2.2 主机信任关系	必测项
		4.2.2.3 默认过期用户	必测项
4.2.3	安全审计	4.2.3.1 日志信息	必测项
		4.2.3.2 日志权限和保护	必测项
		4.2.3.3 系统信息分析	必测项
		4.2.3.4 用户操作审计	必测项
4.2.4	系统保护	4.2.4.1 系统备份	必测项
		4.2.4.2 故障恢复策略	必测项
		4.2.4.3 磁盘空间安全	必测项
		4.2.4.4 主机安全加固	必测项
4.2.5	剩余信息保护	4.2.5.1 过期信息、文档处理	必测项
4.2.6	入侵防范	4.2.6.1 入侵防范记录	必测项
		4.2.6.2 关闭服务和端口	必测项
		4.2.6.3 最小安装原则	必测项
4.2.7	恶意代码防范	4.2.7.1 防范软件安装部署	必测项
		4.2.7.2 病毒库定时更新	必测项
		4.2.7.3 防范软件统一管理	必测项
4.2.8	资源控制	4.2.8.1 连接控制	必测项
		4.2.8.2 资源监控和预警	必测项
4.2.9	主机安全管理	4.2.9.1 主机运维手册	必测项
		4.2.9.2 漏洞扫描	必测项
		4.2.9.3 系统补丁	必测项
		4.2.9.4 操作日志管理	必测项
4.2.10	主机相关人员安全管理	4.2.10.1 主机安全管理人员配备	必测项
		4.2.10.2 主机安全管理人员责任划分规则	必测项
		4.2.10.3 主机安全关键岗位人员管理	必测项

（3） 应用安全性测试

编号	检测项	检测说明

编号	检测项		检测说明
4.3.1	身份鉴别	4.3.1.1 系统与普通用户设置	必测项
		4.3.1.2 系统与普通用户口令安全性	必测项
		4.3.1.3 登录访问安全策略	必测项
		4.3.1.4 非法访问警示和记录	必测项
		4.3.1.5 客户端鉴别信息安全	必测项
		4.3.1.6 口令有效期限制	必测项
		4.3.1.7 限制认证会话时间	必测项
		4.3.1.8 身份标识唯一性	必测项
		4.3.1.9 及时清除鉴别信息	必测项
4.3.2	WEB 页面安全	4.3.2.1 登录防穷举	必测项
		4.3.2.2 安全控件	必测项
		4.3.2.3 使用数字证书	必测项
		4.3.2.4 独立的支付密码	必测项
		4.3.2.5 网站页面 SQL 注入防范	必测项
		4.3.2.6 网站页面跨站脚本攻击防范	必测项
		4.3.2.7 网站页面源代码暴露防范	必测项
		4.3.2.8 网站页面黑客挂马防范	必测项
		4.3.2.9 网站页面防篡改措施	必测项
		4.3.2.10 网站页面防钓鱼	必测项
4.3.3	访问控制	4.3.3.1 访问权限设置	必测项
		4.3.3.2 自主访问控制范围	必测项
		4.3.3.3 业务操作日志	必测项
		4.3.3.4 关键数据存放	必测项
		4.3.3.5 异常中断防护	必测项
		4.3.3.6 数据库安全配置	必测项
4.3.4	安全审计	4.3.4.1 日志信息	必测项
		4.3.4.2 日志权限和保护	必测项
		4.3.4.3 系统信息查询与分析	必测项
		4.3.4.4 对象操作审计	必测项
		4.3.4.5 审计工具	必测项
		4.3.4.6 事件报警	必测项
4.3.5	剩余信息保护	4.3.5.1 过期信息、文档处理	必测项
4.3.6	资源控制	4.3.6.1 连接控制	必测项
		4.3.6.2 会话控制	必测项
		4.3.6.3 进程资源分配	必测项
		4.3.6.4 资源检测预警	必测项
4.3.7	应用容错	4.3.7.1 数据有效性校验	必测项

编号	检测项		检测说明
		4.3.7.2 容错机制	必测项
		4.3.7.3 故障机制	必测项
		4.3.7.4 回退机制	必测项
4.3.8	报文完整性	4.3.8.1 通信报文有效性	必测项
4.3.9	报文保密性	4.3.9.1 报文或会话加密	必测项
4.3.10	抗抵赖	4.3.10.1 原发和接收证据	必测项
4.3.11	编码安全	4.3.11.1 源代码审查	必测项
		4.3.11.2 插件安全性审查	必测项
		4.3.11.3 编码规范约束	必测项
		4.3.11.4 源代码管理	必测项
		4.3.11.5 版本管理	必测项
4.3.12	电子认证应用	4.3.12.1 第三方电子认证机构	必测项
		4.3.12.2 关键业务电子认证技术应用	必测项
		4.3.12.3 电子签名有效性	必测项
		4.3.12.4 服务器证书私钥保护	必测项
4.3.13	终端安全	4.3.13.1 终端设备安全性要求	必测项

（4） 数据安全性测试

编号	检测项		检测说明
4.4.1	数据保护	4.4.1.1 客户身份信息保护	必测项
		4.4.1.2 支付业务信息保护	必测项
		4.4.1.3 会计档案信息保护	必测项
4.4.2	数据完整性	4.4.2.1 重要数据更改机制	必测项
		4.4.2.2 数据备份记录	必测项
		4.4.2.3 保障传输过程中的数据完整性	必测项
		4.4.2.4 备份数据定期恢复	必测项
4.4.3	交易数据以及客户数据的安全性	4.4.3.1 数据物理存储安全	必测项
		4.4.3.2 客户身份认证信息存储安全	必测项
		4.4.3.3 终端信息采集设备硬加密措施或其它防伪手段	必测项
		4.4.3.4 同一安全级别和可信赖的系统之间信息传输	必测项
		4.4.3.5 加密传输	必测项
		4.4.3.6 加密存储	必测项
		4.4.3.7 数据访问控制	必测项

编号	检测项		检测说明
		4.4.3.8 在线的存储备份	必测项
		4.4.3.9 数据备份机制	必测项
		4.4.3.10 本地备份	必测项
		4.4.3.11 异地备份	必测项
		4.4.3.12 备份数据的恢复	必测项
		4.4.3.13 数据销毁制度和记录	必测项
		4.4.3.14 关键链路冗余设计	必测项

（5） 运维安全性测试

编号	检测项		检测说明
4.5.1	环境管理	4.5.1.1 机房基础设施定期维护	必测项
		4.5.1.2 机房的出入管理制度化和文档化	必测项
		4.5.1.3 办公环境的保密性措施	必测项
		4.5.1.4 机房安全管理制度	必测项
		4.5.1.5 机房进出登记表	必测项
4.5.2	介质管理	4.5.2.1 介质的存放环境保护措施	必测项
		4.5.2.2 介质的使用管理文档化	必测项
		4.5.2.3 维修或销毁介质之前清除敏感数据	必测项
		4.5.2.4 介质管理记录	必测项
		4.5.2.5 介质的分类与标识	必测项
4.5.3	设备管理	4.5.3.1 设备管理的责任人员或部门	必测项
		4.5.3.2 设施、设备定期维护	必测项
		4.5.3.3 设备选型、采购、发放等的审批控制	必测项
		4.5.3.4 设备配置标准化	必测项
		4.5.3.5 设备的操作规程	必测项
		4.5.3.6 设备的操作日志	必测项
		4.5.3.7 设备使用管理文档	必测项
		4.5.3.8 设备标识	必测项
4.5.4	人员管理	4.5.4.1 人员录用	必测项
		4.5.4.2 人员转岗、离岗	必测项
		4.5.4.3 人员考核	必测项
		4.5.4.4 安全意识教育和培训	必测项
		4.5.4.5 外部人员访问管理	必测项
		4.5.4.6 职责分离	必测项
4.5.5	监控管理	4.5.5.1 主要网络设备的各项指标监控情况	必测项

编号	检测项		检测说明
		4.5.5.2 主要服务器的各项指标监控情况	必测项
		4.5.5.3 应用运行各项指标监控情况	必测项
		4.5.5.4 异常处理机制	必测项
4.5.6	变更管理	4.5.6.1 变更方案	必测项
		4.5.6.2 变更制度化管理	必测项
		4.5.6.3 重要系统变更的批准	必测项
		4.5.6.4 重要系统变更的通知	必测项
4.5.7	安全事件处置	4.5.7.1 安全事件报告和处置	必测项
		4.5.7.2 安全事件的分类和分级	必测项
		4.5.7.3 安全事件记录和采取的措施	必测项
4.5.8	应急预案管理	4.5.8.1 制定不同事件的应急预案	必测项
		4.5.8.2 相关人员应急预案培训	必测项
		4.5.8.3 定期演练	必测项

（6） 业务连续性测试

编号	检测项		检测说明
4.6.1	业务连续性需求分析	4.6.1.1 业务中断影响分析	必测项
		4.6.1.2 灾难恢复时间目标和恢复点目标	必测项
4.6.2	业务连续性技术环境	4.6.2.1 备份机房	必测项
		4.6.2.2 网络双链路	必测项
		4.6.2.3 网络设备和服务器备份	必测项
		4.6.2.4 高可靠的磁盘阵列	必测项
		4.6.2.5 远程数据库备份	必测项
4.6.3	业务连续性管理	4.6.3.1 业务连续性管理制度	必测项
		4.6.3.2 应急响应流程	必测项
		4.6.3.3 恢复预案	必测项
		4.6.3.4 数据备份和恢复制度	必测项
4.6.4	备份与恢复管理	4.6.4.1 备份数据范围和备份频率	必测项
		4.6.4.2 备份和恢复手册	必测项
		4.6.4.3 备份记录和定期恢复测试记录	必测项
		4.6.4.4 定期数据备份恢复性测试	必测项
4.6.5	日常维护	4.6.5.1 每年业务连续性演练	必测项

编号	检测项		检测说明
		4.6.5.2 定期业务连续性培训	必测项

A.6.5 文档检测项

编号	检测项		检测说明
5.1	用户文档	5.1.1 用户手册	必测项
		5.1.2 操作手册	必测项
5.2	开发文档	5.2.1 需求说明书	必测项
		5.2.2 需求分析文档	必测项
		5.2.3 总体设计方案	必测项
		5.2.4 数据库设计文档	必测项
		5.2.5 概要设计文档	必测项
		5.2.6 详细设计文档	必测项
		5.2.7 工程实施方案	必测项
5.3	管理文档	5.3.1 测试报告	必测项
		5.3.2 系统运维手册	必测项
		5.3.3 系统应急手册	必测项
		5.3.4 运维管理制度	必测项
		5.3.5 安全管理制度	必测项
		5.3.6 安全审计报告	必测项

A.7 预付卡的发行与受理系统检测项

A.7.1 功能检测项

编号	检测项		检测说明
1.1	账户管理	1.1.1 客户支付账户管理	联机交易类必测项
1.2	卡片管理	1.2.1 制卡	必测项
		1.2.2 卡片发行	必测项
		1.2.3 卡片激活	必测项
		1.2.4 充值	
		1.2.5 卡片有效期延长	
		1.2.6 换卡	必测项
		1.2.7 补卡	
		1.2.8 密码修改	
		1.2.9 卡片冻结/解冻	
		1.2.10 卡片挂失/解挂	
		1.2.11 锁卡/解锁	

编号	检测项		检测说明
		1.2.12 退卡	
		1.2.13 销卡	
1.3	密钥和证书管理	1.3.1 认证中心公钥管理	
		1.3.2 发卡机构密钥管理	
		1.3.3 IC 卡密钥管理	脱机交易类必测项
		1.3.4 发卡机构证书管理	
		1.3.5 IC 卡证书管理	
1.4	交易处理	1.4.1 联机消费	联机交易类必测项
		1.4.2 联机消费撤销	非必测项
		1.4.3 联机余额查询	联机交易类必测项（密码卡不适用）
		1.4.4 退货	必测项（密码卡不适用）
		1.4.5 冲正交易	联机交易类必测项（密码卡不适用）
		1.4.6 异常卡交易	必测项
		1.4.7 现金充值	
		1.4.8 指定账户圈存	
		1.4.9 非指定账户圈存	
		1.4.10 IC 卡脚本通知	
		1.4.11 圈提	
		1.4.12 脱机消费	脱机交易类必测项
		1.4.13 脱机消费文件处理	脱机交易类必测项
		1.4.14 脱机余额查询	脱机交易类必测项
		1.4.15 交易查询	必测项
1.5	资金结算	1.5.1 客户结算	
1.6	对账处理	1.6.1 发送对账请求	
		1.6.2 生成对账文件	
1.7	差错处理	1.7.1 长款/短款处理	必测项
1.8	统计报表	1.8.1 业务类报表	必测项
		1.8.2 运行管理类报表	必测项

A.7.2 风险监控检测项

编号	检测项	检测说明

编号	检测项		检测说明
2.1	联机交易风险管理	2.1.1 联机交易 ARQC/ARPC 验证	
		2.1.2 联机报文 MAC 验证	
		2.1.3 卡片状态控制	
		2.1.4 单笔消费限额	
		2.1.5 当日累计消费限额	
		2.1.6 当日累计消费次数限制	
		2.1.7 单笔充值金额最大值	
		2.1.8 账户余额限额	必测项
		2.1.9 大额消费商户交易监控	
		2.1.10 密码错误情况下的交易请求	
		2.1.11 非法卡号交易	必测项
		2.1.12 卡片有效期检查	
		2.1.13 无磁无密交易	
2.2	脱机交易风险管理	2.2.1 TAC 验证	脱机交易类必测项
		2.2.2 MAC 验证	脱机交易类必测项
2.3	终端风险管理	2.3.1 POS 机申请、参数设置、程序灌装、使用、更换、维护、撤消的管理	
		2.3.2 POS 机密钥和参数的安全管理	
		2.3.3 控制移动 POS 机的安装	
		2.3.4 终端安全审查报告	
		2.3.5 密码键盘安全审查报告	
		2.3.6 终端监控	

A.7.3 性能检测项

编号	检测项	检测说明
3.1	3.1.1 联机消费	联机交易类必测项
3.2	3.2.1 联机余额查询	必测项（密码卡不适用）
3.3	3.3.1 联机交易明细查询	
3.4	3.4.1 批量发行	
3.5	3.5.1 批量充值	

3.6	3.6.1 批量作废	
3.7	3.7.1 脱机消费文件处理	脱机交易类必测项
3.8	3.8.1 日终批处理	

A.7.4 安全性检测项

（1） 网络安全性

编号	检测项		检测说明
4.1.1	结构安全	4.1.1.1 网络冗余和备份	必测项
		4.1.1.2 网络安全路由器	必测项
		4.1.1.3 网络安全防火墙	必测项
		4.1.1.4 网络拓扑结构	必测项
		4.1.1.5 IP 子网划分	必测项
		4.1.1.6 QoS 保证	必测项
4.1.2	网络访问控制	4.1.2.1 网络域安全隔离和限制	必测项
		4.1.2.2 地址转换和绑定	必测项
		4.1.2.3 内容过滤	必测项
		4.1.2.4 访问控制	必测项
		4.1.2.5 流量控制	必测项
		4.1.2.6 会话控制	必测项
		4.1.2.7 远程拨号访问控制和记录	必测项
4.1.3	网络安全审计	4.1.3.1 日志信息	必测项
		4.1.3.2 网络系统故障分析	必测项
		4.1.3.3 网络对象操作审计	必测项
		4.1.3.4 日志权限和保护	必测项
		4.1.3.5 审计工具	必测项
4.1.4	边界完整性检查	4.1.4.1 内外网非法连接阻断和定位	必测项
4.1.5	网络入侵防范	4.1.5.1 网络 ARP 欺骗攻击	必测项
		4.1.5.2 信息窃取	必测项
		4.1.5.3 DOS/DDOS 攻击	必测项
		4.1.5.4 网络入侵防范机制	必测项
4.1.6	恶意代码防范	4.1.6.1 恶意代码防范措施	必测项
		4.1.6.2 定时更新	必测项

编号	检测项		检测说明
4.1.7	网络设备防护	4.1.7.1 设备登录设置	必测项
		4.1.7.2 设备登录口令安全性	必测项
		4.1.7.3 登录地址限制	必测项
		4.1.7.4 远程管理安全	必测项
		4.1.7.5 设备用户设置策略	必测项
		4.1.7.6 权限分离	必测项
		4.1.7.7 最小化服务	必测项
4.1.8	网络安全管理	4.1.8.1 网络设备运维手册	必测项
		4.1.8.2 定期补丁安装	必测项
		4.1.8.3 漏洞扫描	必测项
		4.1.8.4 网络数据传输加密	必测项
4.1.9	网络相关人员安全管理	4.1.9.1 网络安全管理人员配备	必测项
		4.1.9.2 网络安全管理人员责任划分规则	必测项
		4.1.9.3 网络安全关键岗位人员管理	必测项

（2） 主机安全性

编号	检测项		检测说明
4.2.1	身份鉴别	4.2.1.1 系统与应用管理员用户设置	必测项
		4.2.1.2 系统与应用管理员口令安全性	必测项
		4.2.1.3 登录策略	必测项
4.2.2	访问控制	4.2.2.1 访问控制范围	必测项
		4.2.2.2 主机信任关系	必测项
		4.2.2.3 默认过期用户	必测项
4.2.3	安全审计	4.2.3.1 日志信息	必测项
		4.2.3.2 日志权限和保护	必测项
		4.2.3.3 系统信息分析	必测项
4.2.4	系统保护	4.2.4.1 系统备份	必测项
		4.2.4.2 故障恢复策略	必测项
		4.2.4.3 磁盘空间安全	必测项
		4.2.4.4 主机安全加固	必测项
4.2.5	剩余信息保护	4.2.5.1 剩余信息保护	必测项
4.2.6	入侵防范	4.2.6.1 入侵防范记录	必测项

编号	检测项		检测说明
		4.2.6.2 关闭服务和端口	必测项
		4.2.6.3 最小安装原则	必测项
4.2.7	恶意代码防范	4.2.7.1 防范软件安装部署	必测项
		4.2.7.2 病毒库定时更新	必测项
		4.2.7.3 防范软件统一管理	必测项
4.2.8	资源控制	4.2.8.1 连接控制	必测项
		4.2.8.2 资源监控和预警	必测项
4.2.9	主机安全管理	4.2.9.1 主机运维手册	必测项
		4.2.9.2 漏洞扫描	必测项
		4.2.9.3 系统补丁	必测项
		4.2.9.4 操作日志管理	必测项
4.2.10	主机相关人员安全管理	4.2.10.1 主机安全管理人员配备	必测项
		4.2.10.2 主机安全管理人员责任划分规则	必测项
		4.2.10.3 主机安全关键岗位人员管理	必测项

（3） 应用安全性

编号	检测项		检测说明
4.3.1	身份鉴别	4.3.1.1 系统与普通用户设置	必测项
		4.3.1.2 系统与普通用户口令安全性	必测项
		4.3.1.3 登录访问安全策略	必测项
		4.3.1.4 非法访问警示和记录	必测项
		4.3.1.5 客户端鉴别信息安全	必测项
		4.3.1.6 口令有效期限制	必测项
		4.3.1.7 限制认证会话时间	必测项
		4.3.1.8 身份标识唯一性	必测项
		4.3.1.9 及时清除鉴别信息	必测项
4.3.2	WEB 页面安全	4.3.2.1 登录防穷举	必测项
		4.3.2.2 安全控件	必测项
		4.3.2.3 使用数字证书	必测项
		4.3.2.4 独立的支付密码	必测项
		4.3.2.5 网站页面 SQL 注入防范	必测项
		4.3.2.6 网站页面跨站脚本攻击防范	必测项

编号	检测项		检测说明
		4.3.2.7 网站页面源代码暴露防范	必测项
		4.3.2.8 网站页面黑客挂马防范	必测项
		4.3.2.9 网站页面防篡改措施	必测项
		4.3.2.10 网站页面防钓鱼	必测项
4.3.3	访问控制	4.3.3.1 访问权限设置	必测项
		4.3.3.2 自主访问控制范围	必测项
		4.3.3.3 业务操作日志	必测项
		4.3.3.4 关键数据存放	必测项
		4.3.3.5 异常中断防护	必测项
		4.3.3.6 数据库安全配置	必测项
4.3.4	安全审计	4.3.4.1 日志信息	必测项
		4.3.4.2 日志权限和保护	必测项
		4.3.4.3 系统信息查询与分析	必测项
		4.3.4.4 对象操作审计	必测项
		4.3.4.5 审计工具	必测项
		4.3.4.6 事件报警	必测项
4.3.5	剩余信息保护	4.3.5.1 过期信息、文档处理	必测项
4.3.6	资源控制	4.3.6.1 连接控制	必测项
		4.3.6.2 会话控制	必测项
		4.3.6.3 进程资源分配	必测项
		4.3.6.4 资源检测预警	必测项
4.3.7	应用容错	4.3.7.1 数据有效性校验	必测项
		4.3.7.2 容错机制	必测项
		4.3.7.3 故障机制	必测项
		4.3.7.4 回退机制	必测项
4.3.8	报文完整性	4.3.8.1 通信报文有效性	必测项
4.3.9	报文保密性	4.3.9.1 报文或会话加密	必测项
4.3.10	抗抵赖	4.3.10.1 原发和接收证据	必测项
4.3.11	编码安全	4.3.11.1 源代码审查	必测项
		4.3.11.2 插件安全性审查	必测项
		4.3.11.3 编码规范约束	必测项
		4.3.11.4 源代码管理	必测项
		4.3.11.5 版本管理	必测项

编号	检测项		检测说明
4.3.12	电子认证应用	4.3.12.1 第三方电子认证机构	必测项
		4.3.12.2 关键业务电子认证技术应用	必测项
		4.3.12.3 电子签名有效性	必测项
		4.3.12.4 服务器证书私钥保护	必测项
4.3.13	脱机数据认证	4.3.13.1 密钥和证书	脱机交易类必测项
		4.3.13.2 静态数据认证	脱机交易类必测项
		4.3.13.3 动态数据认证	脱机交易类必测项
4.3.14	应用密文和发卡机构认证	4.3.14.1 应用密文产生	脱机交易类必测项
		4.3.14.2 发卡机构认证	脱机交易类必测项
		4.3.14.3 密钥管理	脱机交易类必测项
4.3.15	安全报文	4.3.15.1 报文格式	脱机交易类必测项
		4.3.15.2 报文完整性验证	脱机交易类必测项
		4.3.15.3 报文私密性	脱机交易类必测项
		4.3.15.4 密钥管理	脱机交易类必测项
4.3.16	卡片安全	4.3.16.1 共存应用	脱机交易类必测项
		4.3.16.2 密钥的独立性	脱机交易类必测项
		4.3.16.3 卡片内部安全体系	脱机交易类必测项
		4.3.16.4 卡片中密钥的种类	脱机交易类必测项
4.3.17	终端安全	4.3.17.1 终端数据安全性要求	脱机交易类必测项
		4.3.17.2 终端设备安全性要求	脱机交易类必测项
		4.3.17.3 终端密钥管理要求	脱机交易类必测项
4.3.18	密钥管理体系	4.3.18.1 认证中心公钥管理	脱机交易类必测项
		4.3.18.2 发卡机构公钥管理	脱机交易类必测项
		4.3.18.3 发卡机构对称密钥管理	脱机交易类必测项
4.3.19	安全机制	4.3.19.1 对称加密机制	脱机交易类必测项
		4.3.19.2 非对称加密机制	脱机交易类必测项
4.3.20	认可的算法	4.3.20.1 对称加密算法	脱机交易类必测项
		4.3.20.2 非对称加密算法	脱机交易类必测项
		4.3.20.3 哈希算法	脱机交易类必测项

（4） 数据安全性

编号	检测项	检测说明

编号	检测项		检测说明
4.4.1	数据保护	4.4.1.1 客户身份信息保护	必测项
		4.4.1.2 支付业务信息保护	必测项
		4.4.1.3 会计档案信息保护	必测项
4.4.2	数据完整性	4.4.2.1 重要数据更改机制	必测项
		4.4.2.2 数据备份记录	必测项
		4.4.2.3 保障传输过程中的数据完整性	必测项
		4.4.2.4 备份数据定期恢复	必测项
4.4.3	交易数据以及客户数据的安全性	4.4.3.1 数据物理存储安全	必测项
		4.4.3.2 客户身份认证信息存储安全	必测项
		4.4.3.3 终端信息采集设备硬加密措施或其它防伪手段	必测项
		4.4.3.4 同一安全级别和可信赖的系统之间信息传输	必测项
		4.4.3.5 加密传输	必测项
		4.4.3.6 加密存储	必测项
		4.4.3.7 数据访问控制	必测项
		4.4.3.8 在线的存储备份	必测项
		4.4.3.9 数据备份机制	必测项
		4.4.3.10 本地备份	必测项
		4.4.3.11 异地备份	必测项
		4.4.3.12 备份数据的恢复	必测项
		4.4.3.13 数据销毁制度和记录	必测项
		4.4.3.14 关键链路冗余设计	必测项

（5） 运维安全性

编号	检测项		检测说明
4.5.1	环境管理	4.5.1.1 机房基础设施定期维护	必测项
		4.5.1.2 机房的出入管理制度化和文档化	必测项
		4.5.1.3 办公环境的保密性措施	必测项
		4.5.1.4 机房安全管理制度	必测项
		4.5.1.5 机房进出登记表	必测项
4.5.2	介质管理	4.5.2.1 介质的存放环境保护措施	必测项
		4.5.2.2 介质的使用管理文档化	必测项

编号	检测项		检测说明
		4.5.2.3 维修或销毁介质之前清除敏感数据	必测项
		4.5.2.4 介质管理记录	必测项
		4.5.2.5 介质的分类与标识	必测项
4.5.3	设备管理	4.5.3.1 设备管理的责任人员或部门	必测项
		4.5.3.2 设施、设备定期维护	必测项
		4.5.3.3 设备选型、采购、发放等的审批控制	必测项
		4.5.3.4 设备配置标准化	必测项
		4.5.3.5 设备的操作规程	必测项
		4.5.3.6 设备的操作日志	必测项
		4.5.3.7 设备使用管理文档	必测项
		4.5.3.8 设备标识	必测项
4.5.4	人员管理	4.5.4.1 人员录用	必测项
		4.5.4.2 人员转岗、离岗	必测项
		4.5.4.3 人员考核	必测项
		4.5.4.4 安全意识教育和培训	必测项
		4.5.4.5 外部人员访问管理	必测项
		4.5.4.6 职责分离	必测项
4.5.5	监控管理	4.5.5.1 主要网络设备的各项指标监控情况	必测项
		4.5.5.2 主要服务器的各项指标监控情况	必测项
		4.5.5.3 应用运行各项指标监控情况	必测项
		4.5.5.4 异常处理机制	必测项
4.5.6	变更管理	4.5.6.1 变更方案	必测项
		4.5.6.2 变更制度化管理	必测项
		4.5.6.3 重要系统变更的批准	必测项
		4.5.6.4 重要系统变更的通知	必测项
4.5.7	安全事件处置	4.5.7.1 安全事件报告和处置	必测项
		4.5.7.2 安全事件的分类和分级	必测项
		4.5.7.3 安全事件记录和采取的措施	必测项
4.5.8	应急预案管理	4.5.8.1 制定不同事件的应急预案	必测项
		4.5.8.2 相关人员应急预案培训	必测项
		4.5.8.3 定期演练	必测项

（6） 业务连续性

编号	检测项		检测说明
4.6.1	业务连续性需求分析	4.6.1.1 业务中断影响分析	必测项
		4.6.1.2 灾难恢复时间目标和恢复点目标	必测项
4.6.2	业务连续性技术环境	4.6.2.1 备份机房	必测项
		4.6.2.2 网络双链路	必测项
		4.6.2.3 网络设备和服务器备份	必测项
		4.6.2.4 高可靠的磁盘阵列	必测项
		4.6.2.5 远程数据库备份	必测项
4.6.3	业务连续性管理	4.6.3.1 业务连续性管理制度	必测项
		4.6.3.2 应急响应流程	必测项
		4.6.3.3 恢复预案	必测项
		4.6.3.4 数据备份和恢复制度	必测项
4.6.4	备份与恢复管理	4.6.4.1 备份数据范围和备份频率	必测项
		4.6.4.2 备份和恢复手册	必测项
		4.6.4.3 备份记录和定期恢复测试记录	必测项
		4.6.4.4 定期数据备份恢复性测试	必测项
4.6.5	日常维护	4.6.5.1 每年业务连续性演练	必测项
		4.6.5.2 定期业务连续性培训	必测项

A.7.5 文档检测项

编号	检测项		检测说明
5.1	用户文档	5.1.1 用户手册	必测项
		5.1.2 操作手册	必测项
5.2	开发文档	5.2.1 需求说明书	必测项
		5.2.2 需求分析文档	必测项
		5.2.3 总体设计方案	必测项
		5.2.4 数据库设计文档	必测项
		5.2.5 概要设计文档	必测项
		5.2.6 详细设计文档	必测项
		5.2.7 工程实施方案	必测项
5.3	管理文档	5.3.1 测试报告	必测项
		5.3.2 系统运维手册	必测项
		5.3.3 系统应急手册	必测项
		5.3.4 运维管理制度	必测项

编号	检测项		检测说明
		5.3.5 安全管理制度	必测项
		5.3.6 安全审计报告	必测项

A.8 银行卡收单系统检测项

A.8.1 功能检测项

编号	检测项		检测说明
1.1	特约商户管理	1.1.1 商户提交资质材料	必测项
		1.1.2 黑名单检查及管理	必测项
		1.1.3 商户信息查询	必测项
		1.1.4 商户操作员管理	
		1.1.5 商户受理业务管理	必测项
		1.1.6 商户信息维护	必测项
		1.1.7 商户冻结、解冻	必测项
		1.1.8 商户退出	
1.2	终端机具信息管理	1.2.1 机具申领控制	必测项
		1.2.2 机具信息维护	
		1.2.3 机具信息查询	
1.3	密钥管理	1.3.1 密钥生成	必测项
		1.3.2 密钥分发	必测项
		1.3.3 密钥使用	必测项
		1.3.4 密钥存储	必测项
		1.3.5 密钥更新	必测项
		1.3.6 密钥销毁	必测项
1.4	交易处理	1.4.1 消费	必测项
		1.4.2 消费撤销	必测项
		1.4.3 余额查询	必测项
		1.4.4 预授权	
		1.4.5 预授权撤销	
		1.4.6 预授权完成	
		1.4.7 预授权完成撤销	
		1.4.8 追加预授权	

编号	检测项		检测说明
		1.4.9 退货	必测项
		1.4.10 指定账户圈存	
		1.4.11 非指定账户圈存	
		1.4.12 现金充值	
		1.4.13 圈提	
		1.4.14 脱机消费	
		1.4.15 IC 卡参数下载	
		1.4.16 交易明细查询	必测项
		1.4.17 冲正交易	联机交易必测项
1.5	资金结算	1.5.1 银行清算	
		1.5.2 商户结算	
1.6	对账处理	1.6.1 发送对账请求	
		1.6.2 下载对账文件	
1.7	差错处理	1.7.1 拒付管理	
		1.7.2 单笔退款	必测项
		1.7.3 批量退款	
		1.7.4 差错交易查询	必测项
		1.7.5 对账差错处理	必测项
1.8	统计报表	1.8.1 业务类报表	必测项
		1.8.2 运行管理类报表	必测项

A.8.2 风险监控检测项

编号	检测项		检测说明
2.1	联机交易管理	2.1.1 联机交易 ARQC/ARPC 验证	
		2.1.2 联机报文 MAC 验证	必测项
		2.1.3 黑名单管理	必测项
		2.1.4 单笔消费限额	
		2.1.5 大额消费商户交易监控	必测项
		2.1.6 异常交易监控	
		2.1.7 无磁无密交易	
2.2	收单风险管理	2.2.1 商户资质审核	必测项
		2.2.2 商户签约	必测项

编号	检测项		检测说明
		2.2.3 特约商户日常风险管理	必测项
		2.2.4 合作的第三方机构的风险管理	
		2.2.5 特约商户强制冻结、解冻、解约	必测项
		2.2.6 可疑商户信息共享	
		2.2.7 风险事件报送	必测项
2.3	终端风险管理	2.3.1 POS 机申请、参数设置、程序灌装、使用、更换、维护、撤消、回收的管理	必测项
		2.3.2 POS 机密钥和参数的安全管理	必测项
		2.3.3 控制移动 POS 机的安装	
		2.3.4 终端安全审查报告和终端入网审查报告	
		2.3.5 密码键盘安全审查报告	
		2.3.6 终端监控	
2.4	风控规则	2.4.1 风控规则管理	必测项
		2.4.2 风险识别	必测项
		2.4.3 风险事件管理	必测项
		2.4.4 风险报表	

A.8.3 性能检测项

编号	检测项	检测说明
3.1	3.1.1 消费	必测项
3.2	3.2.1 预授权	
3.3	3.3.1 日终批处理	必测项
3.4	3.4.1 圈存	
3.5	3.5.1 圈提	

A.8.4 安全性检测项

（1） 网络安全性

编号	检测项		检测说明
4.1.1	结构安全	4.1.1.1 网络冗余和备份	必测项
		4.1.1.2 网络安全路由器	必测项
		4.1.1.3 网络安全防火墙	必测项
		4.1.1.4 网络拓扑结构	必测项

编号	检测项		检测说明
		4.1.1.5 IP 子网划分	必测项
		4.1.1.6 QoS 保证	必测项
4.1.2	网络访问控制	4.1.2.1 网络域安全隔离和限制	必测项
		4.1.2.2 地址转换和绑定	必测项
		4.1.2.3 内容过滤	必测项
		4.1.2.4 访问控制	必测项
		4.1.2.5 流量控制	必测项
		4.1.2.6 会话控制	必测项
		4.1.2.7 远程拨号访问控制和记录	必测项
4.1.3	网络安全审计	4.1.3.1 日志信息	必测项
		4.1.3.2 网络系统故障分析	必测项
		4.1.3.3 网络对象操作审计	必测项
		4.1.3.4 日志权限和保护	必测项
		4.1.3.5 审计工具	必测项
4.1.4	边界完整性检查	4.1.4.1 内外网非法连接阻断和定位	必测项
4.1.5	网络入侵防范	4.1.5.1 网络 ARP 欺骗攻击	必测项
		4.1.5.2 信息窃取	必测项
		4.1.5.3 DOS/DDOS 攻击	必测项
		4.1.5.4 网络入侵防范机制	必测项
4.1.6	恶意代码防范	4.1.6.1 恶意代码防范措施	必测项
		4.1.6.2 定时更新	必测项
4.1.7	网络设备防护	4.1.7.1 设备登录设置	必测项
		4.1.7.2 设备登录口令安全性	必测项
		4.1.7.3 登录地址限制	必测项
		4.1.7.4 远程管理安全	必测项
		4.1.7.5 设备用户设置策略	必测项
		4.1.7.6 权限分离	必测项
		4.1.7.7 最小化服务	必测项
4.1.8	网络安全管理	4.1.8.1 网络设备运维手册	必测项
		4.1.8.2 定期补丁安装	必测项
		4.1.8.3 漏洞扫描	必测项
		4.1.8.4 网络数据传输加密	必测项
4.1.9	网络相关人员安全	4.1.9.1 网络安全管理人员配备	必测项

编号	检测项		检测说明
	管理	4.1.9.2 网络安全管理人员责任划分规则	必测项
		4.1.9.3 网络安全关键岗位人员管理	必测项

（2） 主机安全性

编号	检测项		检测说明
4.2.1	身份鉴别	4.2.1.1 系统与应用管理员用户设置	必测项
		4.2.1.2 系统与应用管理员口令安全性	必测项
		4.2.1.3 登录策略	必测项
4.2.2	访问控制	4.2.2.1 访问控制范围	必测项
		4.2.2.2 主机信任关系	必测项
		4.2.2.3 默认过期用户	必测项
4.2.3	安全审计	4.2.3.1 日志信息	必测项
		4.2.3.2 日志权限和保护	必测项
		4.2.3.3 系统信息分析	必测项
4.2.4	系统保护	4.2.4.1 系统备份	必测项
		4.2.4.2 故障恢复策略	必测项
		4.2.4.3 磁盘空间安全	必测项
		4.2.4.4 主机安全加固	必测项
4.2.5	剩余信息保护	4.2.5.1 剩余信息保护	必测项
4.2.6	入侵防范	4.2.6.1 入侵防范记录	必测项
		4.2.6.2 关闭服务和端口	必测项
		4.2.6.3 最小安装原则	必测项
4.2.7	恶意代码防范	4.2.7.1 防范软件安装部署	必测项
		4.2.7.2 病毒库定时更新	必测项
		4.2.7.3 防范软件统一管理	必测项
4.2.8	资源控制	4.2.8.1 连接控制	必测项
		4.2.8.2 资源监控和预警	必测项
4.2.9	主机安全管理	4.2.9.1 主机运维手册	必测项
		4.2.9.2 漏洞扫描	必测项
		4.2.9.3 系统补丁	必测项
		4.2.9.4 操作日志管理	必测项
4.2.10	主机相关人员安全	4.2.10.1 主机安全管理人员配备	必测项

编号	检测项		检测说明
	管理	4.2.10.2 主机安全管理人员责任划分规则	必测项
		4.2.10.3 主机安全关键岗位人员管理	必测项

（3） 应用安全性

编号	检测项		检测说明
4.3.1	身份鉴别	4.3.1.1 系统与普通用户设置	必测项
		4.3.1.2 系统与普通用户口令安全性	必测项
		4.3.1.3 登录访问安全策略	必测项
		4.3.1.4 非法访问警示和记录	必测项
		4.3.1.5 客户端鉴别信息安全	必测项
		4.3.1.6 口令有效期限制	必测项
		4.3.1.7 限制认证会话时间	必测项
		4.3.1.8 身份标识唯一性	必测项
		4.3.1.9 及时清除鉴别信息	必测项
4.3.2	WEB 页面安全	4.3.2.1 登录防穷举	必测项
		4.3.2.2 安全控件	必测项
		4.3.2.3 使用数字证书	必测项
		4.3.2.4 独立的支付密码	必测项
		4.3.2.5 网站页面 SQL 注入防范	必测项
		4.3.2.6 网站页面跨站脚本攻击防范	必测项
		4.3.2.7 网站页面源代码暴露防范	必测项
		4.3.2.8 网站页面黑客挂马防范	必测项
		4.3.2.9 网站页面防篡改措施	必测项
		4.3.2.10 网站页面防钓鱼	必测项
4.3.3	访问控制	4.3.3.1 访问权限设置	必测项
		4.3.3.2 自主访问控制范围	必测项
		4.3.3.3 业务操作日志	必测项
		4.3.3.4 关键数据存放	必测项
		4.3.3.5 异常中断防护	必测项
		4.3.3.6 数据库安全配置	必测项
4.3.4	安全审计	4.3.4.1 日志信息	必测项
		4.3.4.2 日志权限和保护	必测项

编号	检测项		检测说明
		4.3.4.3 系统信息查询与分析	必测项
		4.3.4.4 对象操作审计	必测项
		4.3.4.5 审计工具	必测项
		4.3.4.6 事件报警	必测项
4.3.5	剩余信息保护	4.3.5.1 过期信息、文档处理	必测项
4.3.6	资源控制	4.3.6.1 连接控制	必测项
		4.3.6.2 会话控制	必测项
		4.3.6.3 进程资源分配	必测项
		4.3.6.4 资源检测预警	必测项
4.3.7	应用容错	4.3.7.1 数据有效性校验	必测项
		4.3.7.2 容错机制	必测项
		4.3.7.3 故障机制	必测项
		4.3.7.4 回退机制	必测项
4.3.8	报文完整性	4.3.8.1 通信报文有效性	必测项
4.3.9	报文保密性	4.3.9.1 报文或会话加密	必测项
4.3.10	抗抵赖	4.3.10.1 原发和接收证据	必测项
4.3.11	编码安全	4.3.11.1 源代码审查	必测项
		4.3.11.2 插件安全性审查	必测项
		4.3.11.3 编码规范约束	必测项
		4.3.11.4 源代码管理	必测项
		4.3.11.5 版本管理	必测项
4.3.12	电子认证应用	4.3.12.1 第三方电子认证机构	必测项
		4.3.12.2 关键业务电子认证技术应用	必测项
		4.3.12.3 电子签名有效性	必测项
		4.3.12.4 服务器证书私钥保护	必测项
4.3.13	脱机数据认证	4.3.13.1 密钥和证书	IC 卡系统必测项
		4.3.13.2 静态数据认证	IC 卡系统必测项
		4.3.13.3 动态数据认证	IC 卡系统必测项
4.3.14	安全报文	4.3.14.1 报文格式	IC 卡系统必测项
		4.3.14.2 报文完整性验证	IC 卡系统必测项
		4.3.14.3 报文私密性	IC 卡系统必测项
		4.3.14.4 密钥管理	IC 卡系统必测项
4.3.15	终端安全	4.3.15.1 终端数据安全性要求	IC 卡系统必测项

编号	检测项		检测说明
		4.3.15.2 终端设备安全性要求	IC 卡系统必测项
		4.3.15.3 终端密钥管理要求	IC 卡系统必测项
4.3.16	安全机制	4.3.16.1 对称加密机制	IC 卡系统必测项
		4.3.16.2 非对称加密机制	IC 卡系统必测项
4.3.17	认可的算法	4.3.17.1 对称加密算法	IC 卡系统必测项
		4.3.17.2 非对称加密算法	IC 卡系统必测项
		4.3.17.3 哈希算法	IC 卡系统必测项

（4） 数据安全性

编号	检测项		检测说明
4.4.1	数据保护	4.4.1.1 客户身份信息保护	必测项
		4.4.1.2 支付业务信息保护	必测项
		4.4.1.3 会计档案信息保护	必测项
4.4.2	数据完整性	4.4.2.1 重要数据更改机制	必测项
		4.4.2.2 数据备份记录	必测项
		4.4.2.3 保障传输过程中的数据完整性	必测项
		4.4.2.4 备份数据定期恢复	必测项
4.4.3	交易数据以及客户数据的安全性	4.4.3.1 数据物理存储安全	必测项
		4.4.3.2 客户身份认证信息存储安全	必测项
		4.4.3.3 终端信息采集设备硬加密措施或其它防伪手段	必测项
		4.4.3.4 同一安全级别和可信赖的系统之间信息传输	必测项
		4.4.3.5 加密传输	必测项
		4.4.3.6 加密存储	必测项
		4.4.3.7 数据访问控制	必测项
		4.4.3.8 在线的存储备份	必测项
		4.4.3.9 数据备份机制	必测项
		4.4.3.10 本地备份	必测项
		4.4.3.11 异地备份	必测项
		4.4.3.12 备份数据的恢复	必测项
		4.4.3.13 数据销毁制度和记录	必测项
		4.4.3.14 关键链路冗余设计	必测项

（5） 运维安全性

编号	检测项		检测说明
4.5.1	环境管理	4.5.1.1 机房基础设施定期维护	必测项
		4.5.1.2 机房的出入管理制度化和文档化	必测项
		4.5.1.3 办公环境的保密性措施	必测项
		4.5.1.4 机房安全管理制度	必测项
		4.5.1.5 机房进出登记表	必测项
4.5.2	介质管理	4.5.2.1 介质的存放环境保护措施	必测项
		4.5.2.2 介质的使用管理文档化	必测项
		4.5.2.3 维修或销毁介质之前清除敏感数据	必测项
		4.5.2.4 介质管理记录	必测项
		4.5.2.5 介质的分类与标识	必测项
4.5.3	设备管理	4.5.3.1 设备管理的责任人员或部门	必测项
		4.5.3.2 设施、设备定期维护	必测项
		4.5.3.3 设备选型、采购、发放等的审批控制	必测项
		4.5.3.4 设备配置标准化	必测项
		4.5.3.5 设备的操作规程	必测项
		4.5.3.6 设备的操作日志	必测项
		4.5.3.7 设备使用管理文档	必测项
		4.5.3.8 设备标识	必测项
4.5.4	人员管理	4.5.4.1 人员录用	必测项
		4.5.4.2 人员转岗、离岗	必测项
		4.5.4.3 人员考核	必测项
		4.5.4.4 安全意识教育和培训	必测项
		4.5.4.5 外部人员访问管理	必测项
		4.5.4.6 职责分离	必测项
4.5.5	监控管理	4.5.5.1 主要网络设备的各项指标监控情况	必测项
		4.5.5.2 主要服务器的各项指标监控情况	必测项
		4.5.5.3 应用运行各项指标监控情况	必测项
		4.5.5.4 异常处理机制	必测项
4.5.6	变更管理	4.5.6.1 变更方案	必测项
		4.5.6.2 变更制度化管理	必测项
		4.5.6.3 重要系统变更的批准	必测项

编号	检测项		检测说明
		4.5.6.4 重要系统变更的通知	必测项
4.5.7	安全事件处置	4.5.7.1 安全事件报告和处置	必测项
		4.5.7.2 安全事件的分类和分级	必测项
		4.5.7.3 安全事件记录和采取的措施	必测项
4.5.8	应急预案管理	4.5.8.1 制定不同事件的应急预案	必测项
		4.5.8.2 相关人员应急预案培训	必测项
		4.5.8.3 定期演练	必测项

（6） 业务连续性

编号	检测项		检测说明
4.6.1	业务连续性需求分析	4.6.1.1 业务中断影响分析	必测项
		4.6.1.2 灾难恢复时间目标和恢复点目标	必测项
4.6.2	业务连续性技术环境	4.6.2.1 备份机房	必测项
		4.6.2.2 网络双链路	必测项
		4.6.2.3 网络设备和服务器备份	必测项
		4.6.2.4 高可靠的磁盘阵列	必测项
		4.6.2.5 远程数据库备份	必测项
4.6.3	业务连续性管理	4.6.3.1 业务连续性管理制度	必测项
		4.6.3.2 应急响应流程	必测项
		4.6.3.3 恢复预案	必测项
		4.6.3.4 数据备份和恢复制度	必测项
4.6.4	备份与恢复管理	4.6.4.1 备份数据范围和备份频率	必测项
		4.6.4.2 备份和恢复手册	必测项
		4.6.4.3 备份记录和定期恢复测试记录	必测项
		4.6.4.4 定期数据备份恢复性测试	必测项
4.6.5	日常维护	4.6.5.1 每年业务连续性演练	必测项
		4.6.5.2 定期业务连续性培训	必测项

A.8.5 文档检测项

编号	检测项		检测说明
5.1	用户文档	5.1.1 用户手册	必测项

编号	检测项		检测说明
		5.1.2 操作手册	必测项
5.2	开发文档	5.2.1 需求说明书	必测项
		5.2.2 需求分析文档	必测项
		5.2.3 总体设计方案	必测项
		5.2.4 数据库设计文档	必测项
		5.2.5 概要设计文档	必测项
		5.2.6 详细设计文档	必测项
		5.2.7 工程实施方案	必测项
5.3	管理文档	5.3.1 测试报告	必测项
		5.3.2 系统运维手册	必测项
		5.3.3 系统应急手册	必测项
		5.3.4 运维管理制度	必测项
		5.3.5 安全管理制度	必测项
		5.3.6 安全审计报告	必测项

A.9 外包附加检测项

编号	检测项		检测说明
6.1	外包服务的外包内容	6.1.1 外包程度及具体内容	必测项
6.2	安全保密协议	6.2.1 签署外包安全保密协议	必测项
		6.2.2 保障托管数据的安全、可靠	必测项
		6.2.3 明确双方责任	必测项
6.3	风险评估	6.3.1 评估业务外包相关风险	必测项
		6.3.2 外包商的合同义务和要求	必测项
		6.3.3 控制和报告程序	必测项
		6.3.4 外包协议的持续评估	必测项
		6.3.5 符合监管要求和准则	必测项
		6.3.6 外包服务应急计划	必测项
6.4	外包商资质	6.4.1 外包商提供支付服务的经验和能力评估	必测项
		6.4.2 外包商硬件资源评估	必测项
		6.4.3 外包商的财务状况评估	必测项
		6.4.4 外包商的资金构成、人员构成以及主管部门的审批	必测项

编号	检测项		检测说明
		6.4.5 外包商的运维管理制度评估	必测项
		6.4.6 外包模式调查及风险评估	必测项
6.5	外包合同	6.5.1 明确规定有关各方的权利和义务	必测项
		6.5.2 明确外包商最低的服务水平	必测项
		6.5.3 规定保守信息资源机密	必测项
		6.5.4 规定争议解决办法	必测项
6.6	控制和监督	6.6.1 对外包业务的管理和监督	必测项
		6.6.2 定期评估外包商的财务状况	必测项
		6.6.3 定期审查合同条款的履行	必测项
6.7	外包交付	6.7.1 制定详细的系统交付清单	必测项
		6.7.2 技术人员的业务培训	必测项