ICS 35.240.40
A11

JR

中华人民共和国金融行业标准

JR/T 0142—2016

银行卡清算业务设施技术要求

Technical requirements of bank card clearing service facilities

2016-07-13 发布　　2016-07-13 实施

中国人民银行　　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准负责起草单位：中国人民银行科技司、中国金融电子化公司。

本标准参加起草单位：中国工商银行、中国农业银行、中国银行、中国建设银行、中国银联股份有限公司、银行卡检测中心、北京中金国盛认证有限公司、中国金融认证中心、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）。

本标准主要起草人：王永红、陆书春、邬向阳、李兴锋、杨倩、汤沁莹、黄本涛、王欢、王禄禄、赵哲、田小雨、刘运、董沙莎、仲海港、王海雷、张霄、刘敏、陈光波、王明爽、郜书鹏、勾传龙、高志民、高强裔、李超、孙茂增、马哲、贾铮、宋铮、赵亮、石竹君、赵春华、高天游。

银行卡清算业务设施技术要求

1 范围

本标准规定了银行卡清算业务设施的功能、风险监控、性能、安全性、业务连续性、个人信息保护、文档等要求。

本标准适用于银行卡清算业务设施的设计、开发、部署和运营等方面。

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。

JR/T 0025（所有部分） 中国金融集成电路（IC）卡规范

JR/T 0071—2012 金融行业信息系统信息安全等级保护实施指引

3 术语与定义

下列术语和定义适用于本文件。

3.1

银行卡清算业务 bank card clearing and settlement

通过制定银行卡清算标准和规则，运营银行卡清算业务系统，授权发行和受理本银行卡清算机构品牌的银行卡，并为发卡机构和收单机构提供其品牌银行卡的机构间交易处理服务，协助完成资金结算的活动。

3.2

银行卡清算业务设施 bank card clearing service facilities

开展银行卡清算业务的设施，包括银行卡清算核心业务系统、CA系统、网络通信系统以及容纳上述系统的专用机房。

3.3

银行卡清算业务处理系统 bank card clearing and settlement processing system

实现银行卡清算业务交易及支付敏感数据处理的信息系统。

3.4

清分 clearing

清算的数据准备阶段，对规定时间内的银行卡交易数据进行分类汇总并依据机构和交易类型计算结算金额的过程。

3.5

结算 settlement

根据清分结果，对交易数据进行净额轧差和提交并完成资金划拨的过程。

3.6

商户类别代码 merchant category code（MCC）

根据商户业务、贸易和服务类型对商户进行分类，识别每一类别的代码。

3.7

发卡行标识代码 bank identification number (BIN)

标识发卡机构的代码。

4 缩略语

下列缩略语适用于本文件。

BIN:发卡行标识代码（Bank Identification Number）

CA:认证中心（Certification Authority）

MCC:商户类别代码（Merchant Category Code）

5 功能要求

5.1 入网机构管理

5.1.1 入网机构资质审核

应具有入网机构资质等信息的录入、审核、分类评级等功能。

5.1.2 黑名单检查及管理

应具有入网机构黑名单检查、管理的功能。

5.1.3 入网机构信息查询

应具有入网机构信息的查询功能。

应能对接入发卡机构的发卡情况进行查询。

应能对接入的收单机构的商户、终端、交易等信息进行查询。

5.1.4 入网机构业务管理

应具有对入网机构受理业务的增加、修改和取消功能。

应能对接入的发卡机构的发卡业务类型，卡片状态等进行管理。

应能对接入的收单机构的受理卡片类型、特约商户类型、受理终端等信息进行管理。

5.1.5 入网机构交易费率管理

应具有入网机构交易费率设置、修改功能。

5.1.6 入网机构信息维护

应具有入网机构信息的增加、修改和删除功能。

5.1.7 入网机构冻结、解冻

应具有暂停入网机构交易和重新恢复入网机构全部或部分交易的功能。

5.1.8 入网机构退出

应具有永久停止入网机构交易的功能。

5.2 BIN 号管理

应具有卡片BIN号管理功能。

5.3 商户 MCC 管理

应具有商户MCC管理功能。

5.4 密钥管理

5.4.1 密钥生成

应具有密钥生成流程及控制。

5.4.2 密钥分发

应具有密钥分发流程及控制。

5.4.3 密钥使用

应具有密钥使用规定及控制。

5.4.4 密钥存储

应具有密钥存储规定及控制。

5.4.5 密钥更新

应具有密钥更新流程及控制。

5.4.6 密钥销毁

应具有密钥销毁流程及控制。

5.5 交易类型

5.5.1 联机类交易

应支持的联机类交易如表1所示。

表1 应支持的联机类交易

编号	交易类型
a)	预授权
b)	预授权撤销

编号	交易类型
c)	预授权完成
d)	预授权完成撤销
e)	消费
f)	消费撤销
g)	取现
h)	转账
i)	存款
j)	存款撤销
k)	现金充值
l)	现金充值撤销
m)	账户验证
n)	汇款
o)	余额查询
p)	IC 卡指定账户圈存
q)	冲正
r)	退货（联机）
s)	汇率查询

宜支持的联机类交易如表2所示。

表2　宜支持的联机类交易

编号	交易类型
a)	追加预授权
b)	IC 卡指定账户圈提
c)	IC 卡非指定账户圈存
d)	代授权
e)	代收代付
f)	代扣代缴
g)	通知类交易

5.5.2　脱机类交易

应支持的脱机类交易如表3所示。

表3　应支持的脱机类交易

编号	交易类型
a)	脱机消费

宜支持的脱机类交易如表4所示。

表4　宜支持的脱机类交易

编号	交易类型
a)	退货（脱机）

5.5.3　手工类交易

应支持的手工类交易如表5所示。

表5　应支持的手工类交易

编号	交易类型
a)	差错处理交易
b)	预授权撤销
c)	手工预授权完成

宜支持的手工类交易如表6所示。

表6　宜支持的手工类交易

编号	交易类型
a)	汇款
b)	退货

5.5.4　管理类交易

应支持的管理类交易如表 7 所示。

表7　应支持的管理类交易

编号	交易类型
a)	日切开始/结束
b)	签到/签退
c)	打开/关闭
d)	重置密钥

宜支持的管理类交易如表 8 所示。

表8　宜支持的管理类交易

编号	交易类型
a)	线路测试

5.6　清分结算

5.6.1　资金清分

应能够正确完成资金清分功能。

5.6.2 资金结算

应能够协助完成资金结算功能。

5.7 差错处理

5.7.1 提交差错交易及争议处理

应具备差错、争议交易的提交及处理功能。

5.7.2 差错交易及争议交易查询

应具备差错、争议交易的查询功能。

5.8 信息服务

5.8.1 交易记录要求

交易记录应包括但不限于每笔交易的时间、金额、交易主体、交易方式等信息。

5.8.2 交易查询

应具有对于当日及历史交易的查询功能。
应实现按照时间、交易类型或者客户等交易明细信息进行查询的功能，且能浏览交易明细。
应实现模糊查询功能。

5.8.3 交易统计分析

应具有对交易进行统计分析并产生报表的功能。

5.8.4 清算文件处理

应具备入网机构清算文件上送与下载功能。

5.8.5 发卡行标识代码下发

应具备发卡行标识代码下发功能。

5.8.6 汇率信息查询与下发

应具备汇率信息查询与下发功能。

5.8.7 交易质量分析

宜为入网机构提供交易质量分析服务，如交易成功率、交易承兑率等。

5.9 统计报表

5.9.1 业务类报表

应具有对一段时间内与清算业务有关的各种业务类型以及相关的业务规模等统计功能。

5.9.2 运行管理类报表

应具有对一段时间内运行管理情况进行查询统计的功能。

5.10 支付标记化

应采用支付标记化技术，对银行卡卡号、卡片验证码等信息进行脱敏处理。
应支持基于支付标记化技术的交易处理。

6 风险监控要求

6.1 交易管理

6.1.1 监控规则管理

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

6.1.2 当日交易查询

应实现当日交易信息的查询功能。

6.1.3 历史交易查询

应实现历史交易信息的查询功能。
应支持基于时间段的历史交易查询。

6.1.4 大额交易监控

应实现大额交易监控规则的设置，对经清算机构转接系统处理的银行卡跨行交易进行分析，查找可疑行为，协助入网机构及时进行调查和核实。

6.1.5 可疑交易处理

应实现可疑交易处理规则的设置，以实现对可疑交易的查询、分析处理等服务。

6.1.6 交易事件报警

应实现对违反规则的交易事件进行报警，并提供事件的查询统计。

6.1.7 单笔交易限额

应设置单笔交易限额，超过单笔交易限额的交易触发风控规则。

6.2 风控规则

6.2.1 风控规则管理

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

6.2.2 黑名单

应实现黑名单的管理功能，黑名单内的入网机构、商户、终端、卡片等的交易应触发风控规则。

6.2.3 白名单

应实现白名单的增加、删除、查询等管理功能。

6.2.4 风险识别

应确保在相关风险管理制度中完整、明确的定义各种风险类别。

6.2.5 事件管理

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

6.2.6 风险报表

应提供一段时间内的风险事件记录报表，或提供查询一段时间内的风险事件记录报表功能。

6.3 风险管理

6.3.1 入网机构的信用及清算风险管理

6.3.1.1 信用风险管理

应建立相应的入网机构风险识别标准和方法，识别和评估不同入网机构的信用风险状况。

6.3.1.2 清算风险管理

应要求入网机构在出现挤兑、巨额亏损或资金损失、系统瘫痪等与清算支付能力有关的指标恶化、严重信誉损失事件等情况时要及时向其通报，并启动相应的应急方案，对入网机构出现的支付指令排队、异常清算垫付等进行识别、报告、头寸不足的预警，启动相关预警工作和应对措施。

6.3.1.3 动态风险管理

应开展持续的动态风险管理，如采取分渠道采集信息、加权测评、综合评价的方式，对入网机构的信用情况及对业务风险的持续管理能力定期开展审查与评估。

6.3.2 业务风险管理

6.3.2.1 业务资格管理

应定期检查入网机构的风险评估报告，根据入网机构不同的风险等级，对其申请所开展业务的种类、资格进行区分和管理。

应对入网机构接入设施的标准符合性进行核验，保证接入设施符合国家相关政策及标准要求。

6.3.2.2 发卡业务安全管理

对发卡机构应有严格的安全管理要求，如发卡机构的人员、岗位设置，卡片的生产、运输、保管、发行及销毁等业务流程的执行，客户资信审查制度、交易风险监控体系的建立。对发卡机构、银行卡生产企业等进行必要的安全调查，对于违规机构将视情节轻重给予相应处罚。

6.3.2.3 收单风险指标监控

应监控开展收单业务入网机构的收单风险状况，观察其收单欺诈率是否异常，并采取相应的管理措施。

6.3.2.4 账户信息安全管理

应根据相关数据安全标准，明确要求入网机构及其代理机构、商户在账户信息安全管理方面的责任，并对违反账户信息安全标准的情形制定相应处罚措施。

6.4 风险服务

6.4.1 面向入网机构的风险服务

6.4.1.1 发卡机构风险服务

应提供发卡端风险信息共享服务。收集、整理各发卡机构报送的风险信息，并在参与共享机制的各发卡机构之间进行信息共享。

应提供欺诈交易侦测服务。运用欺诈风险监控规则，对经清算机构转接系统处理的银行卡跨行交易进行分析，并将侦测结果以风险评分、可疑原因代码等形式提示发卡机构，以协助发卡机构及时对疑似欺诈交易进行识别和防范。

应提供疑似伪卡信息侧录点侦测服务。分析比对各发卡机构报送发生伪卡欺诈交易卡号的历史交易记录，侦测疑似伪卡信息泄漏点，以帮助发卡机构及时对该泄漏点发生交易的其他卡片采取换卡、账户监控等措施，防范进一步的伪卡损失。

6.4.1.2 收单机构风险服务

应提供收单端风险信息共享服务。收集、整理各收单机构报送的高风险商户信息，并在参与共享机制的各收单机构之间进行信息共享，以防范欺诈商户被关闭后向其他收单机构申请受理资质进行二次商户欺诈。

应提供商户风险监控服务。运用欺诈风险监控规则，对经清算机构转接系统处理的银行卡跨行交易进行分析，查找特约商户疑似欺诈行为，协助收单机构及时对疑似欺诈商户进行调查和核实。

应提供止付卡数据库服务。接收发卡机构提供的止付卡信息，整理汇总成立止付卡数据库，并负责对止付卡数据库进行更新和维护，以利于收单机构开展免授权业务。

6.4.1.3 综合类风险服务

应提供风险提示服务。向入网机构通报当前突出风险状况或重大风险事件，及时提醒入网机构注意防范风险隐患，并提出防范建议和措施。

应提供业务培训服务。聘请银行卡产业风险管理、反欺诈技术专家，为入网机构、司法机关提供风险管理业务培训，介绍最新的反欺诈技术和风险管理方法。

6.4.2 面向司法机构的风险服务

应为司法机构提供案件协查与案件管理功能。案件协查功能应实现对涉案卡、商户、终端的交易信息查询以及对于特定卡号发生交易的提醒。案件管理功能应支持司法机构录入、查询、合并不同的案件。

7 性能要求

银行卡清算业务设施应满足业务运行的性能需求，保障业务的交易成功率和系统可用性。

银行卡清算业务设施应具有支撑处理高峰期业务多用户并发压力的能力，如典型交易、复杂业务流程、频繁的用户操作等业务场景。

银行卡清算业务设施应具有大数据量处理能力。

银行卡清算业务设施应具有压力解除后的自恢复能力。

8 安全性要求

8.1 总体要求

应遵守国家安全、国家网络安全相关法律法规，严格落实《银行卡清算机构管理办法》（中国人民银行 中国银行业监督管理委员会令〔2016〕第2号）、《中国人民银行关于进一步加强银行卡风险管理的通知》（银发〔2016〕170号）相关规定，确保银行卡清算业务设施的安全、稳定和高效运行。银行卡清算业务设施应使用经国家密码管理机构认可的商用密码产品，且其核心业务系统不得外包。境内发行的银行卡在境内使用时，其相关交易处理应当通过境内银行卡清算业务设施完成。

银行卡清算业务处理系统应符合本章要求，非业务处理系统安全性要求应至少达到国家信息安全等级保护三级。银行卡清算业务处理系统应与非业务处理系统进行严格的安全隔离。

8.2 物理安全

应符合JR/T 0071—2012，6.3.1.1中的要求。

8.3 网络安全

应符合JR/T 0071—2012，6.3.1.2中除列项1）a)之外的所有要求。

应保证主要网络设备和通信线路冗余，主要网络设备业务处理能力能满足业务高峰期需要的2倍以上，双线路设计时，应由不同的服务商提供。

8.4 主机安全

应符合JR/T 0071—2012，6.3.1.3中要求。

8.5 应用安全

8.5.1 身份鉴别

应符合JR/T 0071—2012，6.3.1.4中列项1）要求。

8.5.2 安全标记

应符合JR/T 0071—2012，6.3.1.4中列项2）要求。

8.5.3 访问控制

应符合JR/T 0071—2012，6.3.1.4中列项3）要求。

8.5.4 可信路径

应符合JR/T 0071—2012，6.3.1.4中列项4）要求。

8.5.5 安全审计

应符合JR/T 0071—2012，6.3.1.4中列项5）要求。

8.5.6 剩余信息保护

应符合JR/T 0071—2012，6.3.1.4中列项6）要求。

8.5.7 通信完整性

应符合JR/T 0071—2012，6.3.1.4中列项7）要求。

8.5.8 通信保密性

应符合JR/T 0071—2012，6.3.1.4中列项8）要求。

8.5.9 抗抵赖

应符合JR/T 0071—2012，6.3.1.4中列项9）要求。

8.5.10 软件容错

应符合JR/T 0071—2012，6.3.1.4中列项10）要求。

8.5.11 资源控制

应符合JR/T 0071—2012，6.3.1.4中列项11）要求。

8.5.12 安全报文

8.5.12.1 报文格式

应符合JR/T 0025中的规定。

8.5.12.2 报文完整性验证

应对报文完整性进行验证。

8.5.12.3 报文私密性

应保证报文私密性。

8.5.12.4 密钥管理

应对密钥进行安全管理。

8.5.13 WEB 页面安全

8.5.13.1 登录防穷举

应提供登录防穷举的措施，如图片验证码、数字证书等。

8.5.13.2 安全控件

登录应使用安全控件或更高级别的安全措施。

8.5.13.3 使用数字证书

应使用服务器证书，并在整个生命周期保障令牌的安全。

8.5.13.4 网站页面注入防范

网站页面应采取防范SQL注入、Path注入和LDAP注入等风险的措施。

8.5.13.5 网站页面跨站脚本攻击防范

网站页面应采取防范跨站脚本攻击风险的措施。

8.5.13.6 网站页面源代码暴露防范

网站页面应采取防范源代码暴露的措施。

8.5.13.7 网站页面黑客挂马防范

应采取防范网站页面黑客挂马的机制和措施。

8.5.13.8 网站页面防篡改措施

应采取网站页面防篡改措施。

8.5.13.9 网站页面防钓鱼

网站页面应提供防钓鱼网站的防伪信息验证。

8.5.14 编码安全

8.5.14.1 源代码审查

宜对源代码进行安全性审查，提供源代码审查报告。

应通过自动化工具（如弱点扫描工具、静态代码审查工具等）对应用程序进行检查。

8.5.14.2 插件安全性审查

应对插件进行安全性审查，提供插件审查报告。

8.5.14.3 编码规范约束

应按照编码规范进行编码，具有编码规范约束制度。

8.5.14.4 源代码管理

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

8.5.14.5 版本管理

应具有代码版本管理制度。

8.5.14.6 软件开发管理

应制定软件开发管理制度和代码编写安全规范，明确说明开发过程的控制方法和人员行为准则，要求开发人员参照规范编写代码，不得在程序中设置后门或恶意代码程序。

应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

应确保提供软件设计的相关文档和使用指南，并由专人负责保管。

应确保对程序资源库的修改、更新、发布进行授权和批准。

在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性。

8.5.14.7 环境分离

应确保开发环境与实际运行环境物理分开。

应确保开发人员和测试人员分离。

应确保开发人员不能兼任系统管理员或业务操作人员。

应确保测试数据和测试结果受到控制。

8.6 数据安全

8.6.1 数据完整性

应符合JR/T 0071—2012，6.3.1.5中列项1）要求。

8.6.2 数据保密性

应符合JR/T 0071—2012，6.3.1.5中列项2）要求。

8.6.3 备份和恢复

应符合JR/T 0071—2012，6.3.1.5中除列项3）e)、h）之外的所有要求。

对于异地数据备份中心，应与生产中心直线距离至少达到1000公里，可以接管所有核心业务的运行。

8.6.4 数据保护

8.6.4.1 客户身份信息保护

应按规定妥善保管客户身份基本信息，对客户身份信息的保管期限自业务关系结束当年起至少保存15年。

8.6.4.2 清算业务信息保护

应按规定妥善保管清算业务信息，保管期限自业务关系结束当年起至少保存15年。

8.6.4.3 会计档案信息保护

应按规定妥善保管会计档案，保管期限适用财政部、国家档案局的相关规定。

8.6.5 交易数据以及客户数据的安全性

8.6.5.1 数据物理存储安全

应具备并使用高可用的数据物理存储环境。

8.6.5.2 客户身份认证信息存储安全

应不允许保存非本机构的客户身份认证信息（如银行卡磁道信息或芯片信息、卡片验证码、卡片有效期、个人标识码、银行卡交易密码、指纹等敏感信息）。

应对客户的其他敏感信息，如卡号、户名、开户手机、电子邮箱等信息采取保护措施，防止未经授权擅自对个人信息进行查看、篡改、泄露和破坏。对重要信息关键字段应进行散列或加密存储。

8.6.5.3 终端信息采集设备硬加密措施或其他防伪手段

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

8.6.5.4 同一安全级别和可信赖的系统之间信息传输

某一安全级别的系统应只能向同级别或更高级别可信赖的系统传输数据。

8.6.5.5 数据销毁制度和记录

应具有数据销毁制度和相关记录。

8.7 运维安全

8.7.1 岗位设置

应符合JR/T 0071—2012，6.3.2.2中列项1)要求。

8.7.2 人员配备

应符合JR/T 0071—2012，6.3.2.2中列项2)要求。

8.7.3 人员管理

应符合JR/T 0071—2012，6.3.2.3中的要求。

8.7.4 环境管理

应符合JR/T 0071—2012，6.3.2.5中列项1)要求。

8.7.5 资产管理

应符合JR/T 0071—2012，6.3.2.5中列项2)要求。

8.7.6 介质管理

应符合JR/T 0071—2012，6.3.2.5中除列项3)1）之外的所有要求。
应建立重要数据多重备份机制，其中至少1份备份介质应存放于异地安全区域。

8.7.7 设备管理

应符合JR/T 0071—2012，6.3.2.5中列项4)要求。

8.7.8 监控管理和安全管理中心

应符合JR/T 0071—2012，6.3.2.5中列项5)要求。

8.7.9 网络安全管理

应符合JR/T 0071—2012，6.3.2.5中列项6)要求。
应至少每季度对网络系统进行一次漏洞扫描，并保存扫描记录。
应对扫描发现的漏洞进行处理。

8.7.10 系统安全管理

应符合JR/T 0071—2012，6.3.2.5中列项7)要求。

8.7.11 恶意代码防范管理

应符合JR/T 0071—2012，6.3.2.5中列项8)要求。

8.7.12 密码管理

应符合JR/T 0071—2012，6.3.2.5中列项9)要求。

8.7.13 变更管理

应符合JR/T 0071—2012，6.3.2.5中列项10)要求。

9 业务连续性要求

9.1 总体要求

银行卡清算业务处理系统应符合本章要求，非业务处理系统业务连续性要求应至少达到国家信息安全等级保护三级。

9.2 备份与恢复管理

应符合JR/T 0071—2012，6.3.2.5中除列项11）f）、l)之外的所有要求。

灾难恢复的需求应至少每年进行一次再分析，当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略。

异地备份中心应建立与主系统处理能力相同的灾难备份系统，主备系统采用轮换交替使用的双系统模式。主备系统实际切换时间应满足实时切换，通信线路应分别接入主备系统。

9.3 安全事件处置

应符合JR/T 0071—2012，6.3.2.5中除列项12)f）之外的所有要求。

发生系统中断、信息泄漏安全事件的，应立即将有关情况报告中国人民银行，并以书面形式报告事故的原因、影响及补救措施。

9.4 应急预案管理

应符合JR/T 0071—2012，6.3.2.5中列项13)要求。

9.5 业务中断影响分析

应进行业务中断影响分析。

9.6 灾难恢复时间目标和恢复点目标

应具备灾难恢复时间目标和恢复点目标，核心业务系统应实现及时自动切换，确保业务连续稳定运行。

9.7 可用性指标

应具备高可用性，保障业务处理7×24小时不间断运行。

9.8 备份机房

应具有异地应用级备份机房。

9.9 网络双链路

应具备双链路。双链路应来自不同运营商，双链路线缆应通过不同入口管道接入机房建筑物。

9.10 网络设备和服务器备份

主机房应具有应用级备份设施。

9.11 高可靠的存储介质

应使用磁盘阵列等高可靠的存储介质。

9.12 远程数据库备份

应具备远程备份数据库。

10 个人信息保护

10.1 基本要求

应严格落实《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》（银发〔2011〕17号）相关规定和要求。

个人信息保护应贯穿个人信息的收集、传输、存储、使用、销毁等整个生命周期的各环节。

收集，指在进行移动金融活动的过程中，为实现金融认证授权、风险控制、信用服务等目的，对个人信息主体的个人信息进行获取和记录的过程。

传输，指在进行移动金融活动的过程中，已获取的个人信息在已获授权机构或企业的系统内或系统间转移的过程。

存储，指已获取的个人信息在已获授权机构或企业的系统内保存的过程。

使用，指对已获取的个人信息进行加工、利用，以及对外提供等的过程。

销毁，指对个人信息进行删除，或对个人信息存储介质进行消磁、焚烧、粉碎等，使个人信息不再可获得的过程。

10.2 个人信息收集

个人信息收集应遵循以下技术要求：

——应根据个人信息重要程度（个人信息被泄露或修改后对个人信息主体造成的影响程度）不同，确定采用的收集技术方案。重要的个人信息，应采用有效的技术措施保证个人信息在收集过程中的真实性、保密性和完整性，防止被未授权的第三方获取或篡改；

——应确保收集端已被删除或释放的信息不可被其他应用程序或其自身再次使用；

——对于重要的个人信息，应确保收集信息来源的可追溯性。

10.3 个人信息传输

应确保个人信息在传输过程中的真实性、保密性和完整性，包括但不限于以下技术要求：

a) 应使用有效技术手段对个人信息传输系统中各个节点进行身份验证，针对关键资金交易等场景宜使用双向身份认证，防止中间人攻击；

b) 敏感的个人信息通过公共网络传输时，应使用加密信道传输；

c) 重要的个人信息在传输时应对数据内容进行加密；

d) 应对传输的信息进行完整性验证；

e) 对于生物认证信息的传输，还应遵循以下技术要求：

   1) 性能要求较高的数据，如实时视频等，宜采用加密、加水印等手段保证信息的保密性和不可否认性；

   2) 宜采取数字签名等技术手段保证信息的不可否认性和可追溯性，防范数据被篡改泄露。

10.4 个人信息存储

个人信息存储应遵循以下技术要求：

——应提供个人信息的安全存储环境；

——若个人信息在服务器端存储，则存储个人信息的设备不应部署在网络边界上；

——对于重要的个人信息应使用加密等技术手段实现安全存储；
——对于不需要还原为明文的个人信息，应采用不可逆的加密算法进行存储；
——根据业务需要应上传到服务器存储的生物认证信息，在服务器端应采取单向不可逆脱敏和加密处理；
——个人信息加密存储应采用高强度的密码算法和加密强度。

10.5 个人信息使用

10.5.1 个人信息访问控制与审计

个人信息使用应采用以下访问控制及审计措施，以防止信息泄露和信息滥用：
——应根据职责划分不同等级角色，对不同角色赋予相应权限，以角色的形式分配用户账号；
——系统每项功能均应实现权限控制，也可进行单独授权，如信息资产的读、写、修改、删除、执行等操作权限可分别授予；
——应授予不同账户处理业务所需个人信息的最小权限，并在不同账户之间形成相互制约关系；
——应根据“双人控制”原则，对访问权限进行分配；
——信息访问的授权设置应遵循职责分离原则；
——应采取控制措施防止任何人员单独进行整个业务的交易或操作程序，即由启动至完成的工序不应只由一个人控制；
——访问控制粒度应细化：个人信息管理者在数据使用的过程中应建立技术架构支持数据的访问控制管理，结构化数据的权限申请的数据单元应能细化到表、表中的字段，半结构化数据要求权限申请的数据单元细化到字段，非结构化数据（包括文本文件、音频、视频、图片、短信等）要求权限申请的数据单元细化到文件；
——对所有个人信息使用的权限管理应能够发放、回收、过期处理；
——应保证数据操作日志的完备性和可查性，对数据操作人员的日常使用情况和所有操作行为进行完整记录，支持对个人信息使用行为的可追溯性，具体操作日志包括但不限于业务操作日志、系统日志等；
——应对数据使用过程中的情况进行监控，确保数据的合理使用；
——应坚持数据使用后的审计，定期对员工的数据使用情况进行内外部审计，审计内容包括但不限于内部流程管控是否合理、数据使用情况是否符合机构内部流程要求，以及是否存在违法违规等情况，并应根据审计结果在合理时间内对相关问题进行修复。

10.5.2 个人信息展示

个人信息展示应遵循以下技术要求：

a) 未登录状态不应展示与具体个人信息主体相关的重要信息。
b) 已登录状态个人信息展示的技术要求如下：
   1) 可查看个人信息主体自身所有的信息（口令等信息在任何渠道和区域均不可展示）；
   2) 对于身份证号、银行卡号等可以直接确定个人信息主体的信息应进行屏蔽展示；
   3) 涉及其他重要个人信息主体的信息时，宜进行屏蔽展示。

后台系统个人信息展示应遵循以下技术要求：

——后台系统个人信息展示默认需要屏蔽处理；
——后台系统应禁止开放式查询，严格限制批量查询；
——后台系统应对查询操作进行授权、身份验证和审计。

10.5.3 个人信息的测试

重要的个人信息不应用于测试。如果测试使用了真实个人信息，那么在使用之前应去除或修改所有会导致个人信息泄露的细节和内容，达到有效脱敏的效果，并遵循以下技术要求：

——应对测试数据进行访问控制；

——每次数据的使用前应获得单独的授权；

——应对测试数据的复制、使用和删除等操作进行记录，以便于审查追踪。

10.5.4 个人信息对外提供

个人信息对外提供应遵循以下技术要求：

——个人信息的对外提供，应保护个人数据的保密性，不被其他未获得个人信息管理者授权的个人、组织和机构截获和利用；

——个人信息对外提供的，提供方应通过技术手段监控数据获取的方式和过程是否符合通过协议条款方式所约定的对方责任和要求；

——应保证对外提供的个人信息数据的完整性；

——应保证个人信息接收方具备对接收的数据所属等级要求的相应保护能力和资质；

——对外提供个人信息应进行审核和记录，应保证对外提供个人信息内容和过程的可追溯性；

——应对提供的个人信息范围、数量进行控制，必要时对提供的个人信息进行脱敏处理。

10.6 个人信息销毁

存储个人信息的各实体不应只采用删除索引或删除文件系统的方式进行个人信息销毁，应采用不可恢复的方式，如焚烧、粉碎、消磁等。

11 文档要求

11.1 基本要求

本章中涉及的文档均要求为中文文档，如有非中文内容，应当同时提供相应中文译本，并以中文译本为准。

文档内容要结构完整、描述一致、格式统一，并进行有效的版本控制和密级管理。

所有技术文档和管理制度的起草、修订、更新均应根据其适用范围经相应管理层审批后，通过正式、有效的方式发布。

11.2 用户文档

11.2.1 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。用户手册还包括软件操作的一些特别的方面，诸如，关于特定岗位或任务的指令等。用户手册是为由用户操作的软件而开发的，具有要求联机用户输入或解释输出显示的用户界面。

11.2.2 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。

11.3 开发文档

11.3.1 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：说明能满足用户什么需要，与现有系统或过程的关系，以及使用方式等。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。

11.3.2 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。

11.3.3 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。

11.3.4 数据库设计文档

数据库设计文档应描述数据库的设计。数据库可由用户或计算机程序通过数据库管理系统加以访问。数据库设计文档还描述了存取或操纵数据所使用的软件配置项。数据库设计文档是实现数据库及相关软件配置项的基础。数据库设计文档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。

11.3.5 安全设计文档

安全设计文档应描述系统总体安全策略、安全技术框架、安全管理策略和详细的安全设计方案，并在系统中正确实现。

11.3.6 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。概要设计文档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。

11.3.7 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。详细设计文档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。

11.3.8 工程实施方案

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

11.4 管理文档

11.4.1 测试验收文档

测试验收文档应包括测试验收方案和测试验收报告。

测试验收方案应包含但不限于验收内容、测试对象和方法、测试预期结果以及验收测试工作计划等。

测试验收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。通过测试验收报告，需方能够评估所执行的合格性测试及其测试结果。

11.4.2 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。

11.4.3 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。

11.4.4 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。

11.4.5 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。

11.4.6 安全审计报告

应由专业审计人员根据有关的法律法规和系统所有者的委托，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。

参 考 文 献

[1] GB/T 12406—2008 表示货币和资金的代码
[2] GB/T 22080—2008 信息技术 安全技术 信息安全管理体系要求
[3] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则
[4] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求