ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0025.18—2018

中国金融集成电路（IC）卡规范 第18部分：基于安全芯片的线上支付技术规范

China financial integrated circuit card specifications—Part 18: The technical specification of online payment based on secure chip

2018-11-28 发布　　2018-11-28 实施

中国人民银行　发布

目　次

前　言

JR/T 0025—2018《中国金融集成电路（IC）卡规范》分为14部分：

——第1部分：总则；

——第3部分：与应用无关的IC卡与终端接口规范；

——第4部分：借记/贷记应用规范；

——第5部分：借记/贷记应用卡片规范；

——第6部分：借记/贷记应用终端规范；

——第7部分：借记/贷记应用安全规范；

——第8部分：与应用无关的非接触式规范；

——第10部分：借记/贷记应用个人化指南；

——第12部分：非接触式IC卡支付规范；

——第13部分：基于借记/贷记应用的小额支付规范；

——第14部分：非接触式IC卡小额支付扩展应用规范；

——第15部分：电子现金双币支付应用规范；

——第16部分：IC卡互联网终端规范；

——第18部分：基于安全芯片的线上支付技术规范。

本部分为JR/T 0025—2018的第18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/TC 180）归口。

本部分起草单位：中国人民银行、中国金融电子化公司、中国农业银行、中国银行、中国建设银行、交通银行、中国邮政储蓄银行、中国民生银行、上海浦东发展银行、中信银行、中国银联股份有限公司、中金金融认证中心有限公司、银行卡检测中心、北京中金国盛认证有限公司、中国电子科技集团公司第十五研究所、北京握奇数据系统有限公司。

本部分主要起草人：李伟、王永红、陆书春、潘润红、李兴锋、宋汉石、渠韶光、邵阔义、邬向阳、杨倩、聂丽琴、杜宁、周玥、张宏基、程胜、黄本涛、汤沁莹、王禄禄、赵哲、王欢、刘运、魏猛、廖志江、史大鹏、谢元呈、延冰、宋捷、庞杰、李晓、姜鹏、张栋、付小康、黄江、张永峰、高志民、高强裔、尚可、马哲、侯晓晨、吴永强、宋铮、李国俊、金铭彦、杨明庆、魏娜、王冠华、王晓东、刘文其、高峰、郭晶莹。

引　言

随着移动支付的飞速发展，基于安全芯片的借记/贷记支付应用在移动互联网等线上场景中被广泛使用。为促进基于安全芯片的线上支付业务的健康发展，将金融IC卡应用在线上与线下支付场景中进行统一整合。

本部分基于JR/T 0025—2018对于金融IC卡应用的支付应用流程与报文结构要求，结合《中国金融移动支付》系列标准对于移动支付安全单元等账户介质及客户端、支付系统后台服务器等线上支付环节的控制要求，对基于安全芯片的借记/贷记等金融IC卡应用线上支付，从实现基本原理、交易流程、个人化要求、安全要求等方面提出框架性规范要求，为包括金融集成电路（IC）卡及终端制造商、支付系统、应用开发商及检测认证机构提供应用指导。

中国金融集成电路（IC）卡规范
第18部分：基于安全芯片的线上支付技术规范

1 范围

本部分规定了个人移动智能终端如何基于借记/贷记应用和安全芯片，通过移动互联网采取后台账户限额控制和线上支付密码等持卡人身份认证保护措施，实现安全的个人线上支付（以下简称基于安全芯片的线上支付），仅适用于个人支付。

本部分适用于基于安全芯片的线上支付相关系统及产品的设计、开发、制造、运营等单位，也适用于以安全芯片为借记/贷记等金融IC卡应用载体，通过个人移动终端和移动互联网，进行个人线上支付的情况，不适用于商户收单。

2 规范性引用文件

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

JR/T 0025—2018（所有部分） 中国金融集成电路（IC）卡规范

JR/T 0068 网上银行系统信息安全通用规范

JR/T 0092 中国金融移动支付 客户端技术规范

JR/T 0096.3—2012 中国金融移动支付 联网联合 第3部分：报文交换规范

JR/T 0098.2—2012 中国金融移动支付 检测规范 第2部分：安全芯片

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全芯片 secure chip

在支付中负责交易关键数据的安全存储和运算功能的集成电路芯片。

3.2

基于安全芯片的线上支付 online payment based on secure chip

以安全芯片（或安全单元）为载体，使用借记/贷记应用，采取在后台账户中设置相应的控制限额，并设置线上支付密码等持卡人身份认证保护措施，通过个人移动终端和移动互联网，直接与后台服务器进行交互完成交易处理的支付方式。

3.3

客户端软件 client software

用于完成基于安全芯片的线上支付交易的应用软件以及提供相关功能的组件。

3.4

单笔线上支付限额 single online transaction limit

为控制线上支付交易风险，针对后台账户设置的线上支付交易的单笔授权金额上限。

3.5

累计线上支付限额 cumulative total online transaction limit

为控制线上支付交易风险，针对后台账户设置的线上支付累计可以用于交易的金额上限值，可以周期性清零循环使用。

3.6

线上支付密码 online payment password

用于控制线上支付交易对后台账户进行扣减余额等操作的代码或口令。

3.7

账户介质 account medium

用于存储用户账户信息的安全载体，包括普通金融IC卡、个人移动终端安全单元等。

4 缩略语

下列缩略语适用于本文件。

AC——应用密文（Application Cryptogram）
AAC——应用认证密文（Application Authentication Cryptogram）
AFL——应用文件定位器（Application File Locator）
AIP——应用交互特征（Application Interchange Profile）
ARPC——授权响应密文（Authorization Response Cryptogram）
ARQC——授权请求密文（Authorization Request Cryptogram）
ATC——应用交易计数器（Application Transaction Counter）
CID——密文信息数据（Cryptogram Information Data）
FCI——文件控制信息（File Control Information）
GPO——获取处理选项（Get Processing Options）
PDOL——处理选项数据对象列表（Processing Options Data Object List）
TC——交易证书（Transaction Certificate）
TEE——可信执行环境（Trusted Execution Environment）

5 基于安全芯片的线上支付实现

5.1 基于安全芯片的线上支付基本原理

基于安全芯片的线上支付基本原理是基于现有JR/T 0025—2018安全交易流程，操作后台账户中的金额，完成各类线上支付交易。交易按照现有JR/T 0025—2018的安全要求，应保证交易的完整性、保

密性和防抵赖性。根据不同风险防范能力或应用场景设置相应的单笔线上支付限额和累计线上支付限额。

对于后台系统，应能够通过上送联机交易报文的交易发起渠道，区分是否为线上支付交易，交易报文相关要求见JR/T 0096.3—2012。

5.2 基于安全芯片的线上支付应用基本要求

基于安全芯片的线上支付应用应设置单笔线上支付限额和累计线上支付限额，可用金额应以借记/贷记账户可用余额为准，账户介质上不应存储相应的金额数值。

5.3 基于安全芯片的线上支付交易流程

5.3.1 基于安全芯片的线上支付消费交易流程

5.3.1.1 基于标准借记/贷记应用的线上支付消费交易流程

基于标准借记/贷记应用的线上支付消费交易流程如图1所示。

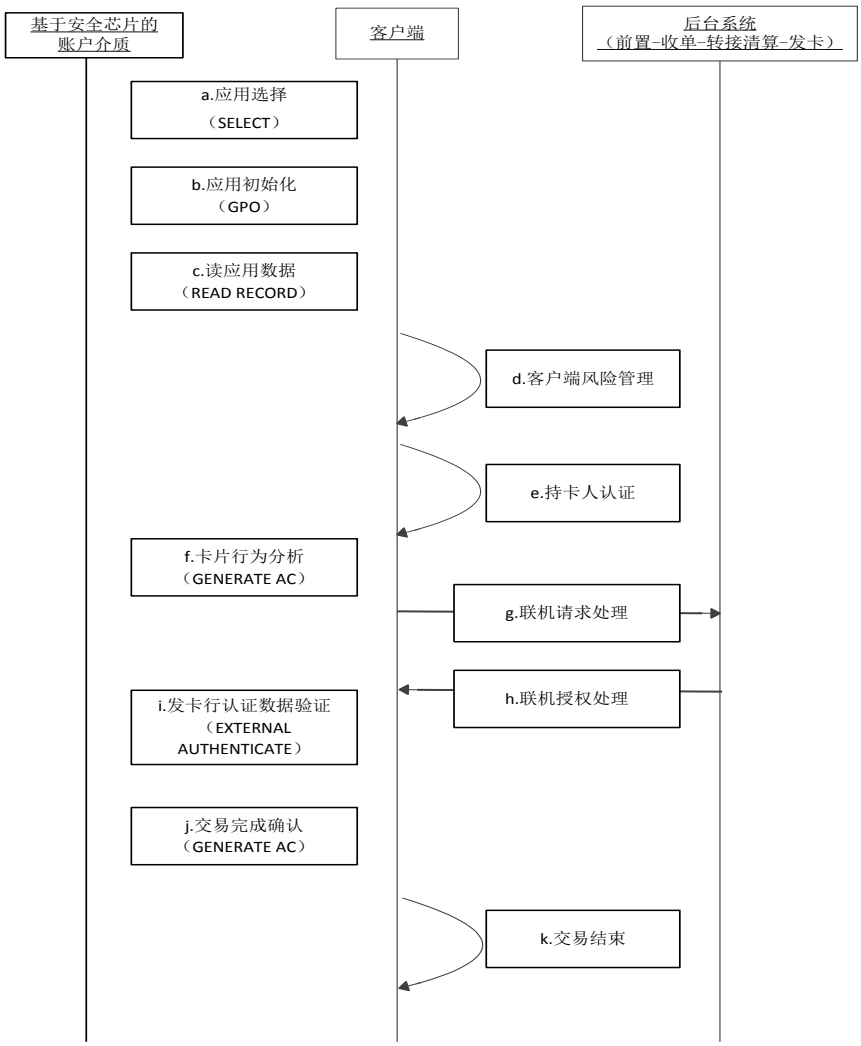

图1 基于标准借记/贷记应用的线上支付消费交易流程图

基于标准借记/贷记应用的线上支付消费交易步骤分述如下：

a） 应用选择（SELECT）

客户端发送SELECT命令选择标准借记/贷记应用，账户介质返回文件控制信息（FCI）。文件控制信息中应包含PDOL，PDOL中至少应包括请求授权金额（标签“9F02”）和交易货币代码（标签“5F2A”）。

b） 应用初始化（GPO）

客户端向账户介质发送GPO命令，表示交易处理开始。当发送此命令时，客户端向账户介质提供处理PDOL请求的数据元。账户介质响应数据内容为AIP和AFL。AIP列出了交易在处理过程中执行的功能；AFL列出交易需要的数据存放文件的短文件标识符、记录号和记录个数。

如果客户端没有收到AIP和AFL，则交易被终止。

c） 读应用数据（READ RECORD）

账户介质收到客户端发送的READ RECORD命令，返回客户端请求的记录内容给客户端。AFL中指定的每一条记录都用一个READ RECORD命令读出。

客户端连续发READ RECORD命令，直到AFL中指定的所有记录都读出。

d） 客户端风险管理

客户端可不进行最低限额、频度等检查。

客户端应发起联机交易，若客户端当前不具备联机能力，则交易请求拒绝，交易终止。

e） 持卡人认证

持卡人认证用于确保持卡人身份合法以及账户介质没有丢失。

若客户端具备联机能力，则要求持卡人输入线上支付密码等持卡人身份认证凭据，并采取必要的安全措施确保用户输入的身份认证凭据的安全。在后续交易处理环节，线上支付密码等持卡人身份认证凭据密文与联机请求报文一起上送至后台系统进行验证。

f） 卡片行为分析

客户端向账户介质发出第1次生成应用密文（GENERATE AC）命令来要求账户介质返回一个标明账户介质授权响应结果的密文，请求联机处理。

账户介质生成应用密文，返回的应用密文类型包括AAC（拒绝交易）、ARQC（请求联机授权）、TC（交易接受）以及向客户端反馈CID、AC、ATC、发卡行应用数据等。

g） 联机请求处理

收到卡片行为分析指令返回结果和数据后，如果账户介质返回交易拒绝，则提示客户支付失败。否则客户端采用加密保护方式，将发卡行应用数据、ARQC、线上支付密码等持卡人身份认证凭据密文等相关交易数据，通过交易请求报文发送给后台系统请求联机处理。后台系统接收到请求后，首先通过请求报文中的交易发起渠道，识别出交易是否为线上支付交易。后台系统验证线上支付密码等持卡人身份认证凭据和ARQC，如后台系统验证失败，则后台系统终止交易并向客户端发送错误信息。

h） 联机授权处理

后台系统进行额度检查，如果授权金额大于单笔线上支付限额，或者授权金额与累计线上支付金额之和大于累计线上支付限额，则后台系统终止交易并向客户端发送错误信息；否则从持卡人账户中扣减相应的交易金额。

当后台系统完成相关交易数据的验证后，将交易结果反馈至客户端，交易结果中至少包含此次线上支付交易是否成功的信息。后台系统使用第1次GENERATE AC命令响应的ARQC和授权响应码生成一个ARPC，把ARPC和授权响应码通过安全方式传送给客户端。

i） 发卡行认证数据验证（EXTERNAL AUTHENTICATE）

客户端应执行发卡行认证，向账户介质发送EXTERNAL AUTHENTICATE命令（含发卡行认证数据）验证ARPC的正确性。外部认证命令的响应码说明发卡行认证数据验证是否通过。如果验证通过，返回响应码“9000”，如果失败，返回响应码“6300”。

如果客户端未收到后台系统签发的ARPC和授权响应码或者账户介质返回失败，客户端提示客户联机处理异常，执行“k）交易结束”相关内容。

j） 交易完成确认（GENERATE AC）

如果发卡行认证数据验证通过，客户端发送第2个GENERATE AC命令给账户介质请求第2个应用密文，请求接受交易，应用密文类型包括AAC（拒绝交易）、TC（交易接受）。

GENERATE AC命令的响应信息中包括CID、ATC、AC和发卡行应用数据等。

k） 交易结束

客户端应向持卡人提示相关交易结果信息，如交易发生异常或者失败，建议持卡人进行交易信息查询，实际交易结果以后台结果为准。

5.3.1.2 基于快速借记/贷记非接触式应用（qPBOC）的线上支付消费交易

基于快速借记/贷记非接触式应用（qPBOC）的线上支付消费交易流程如图2所示。

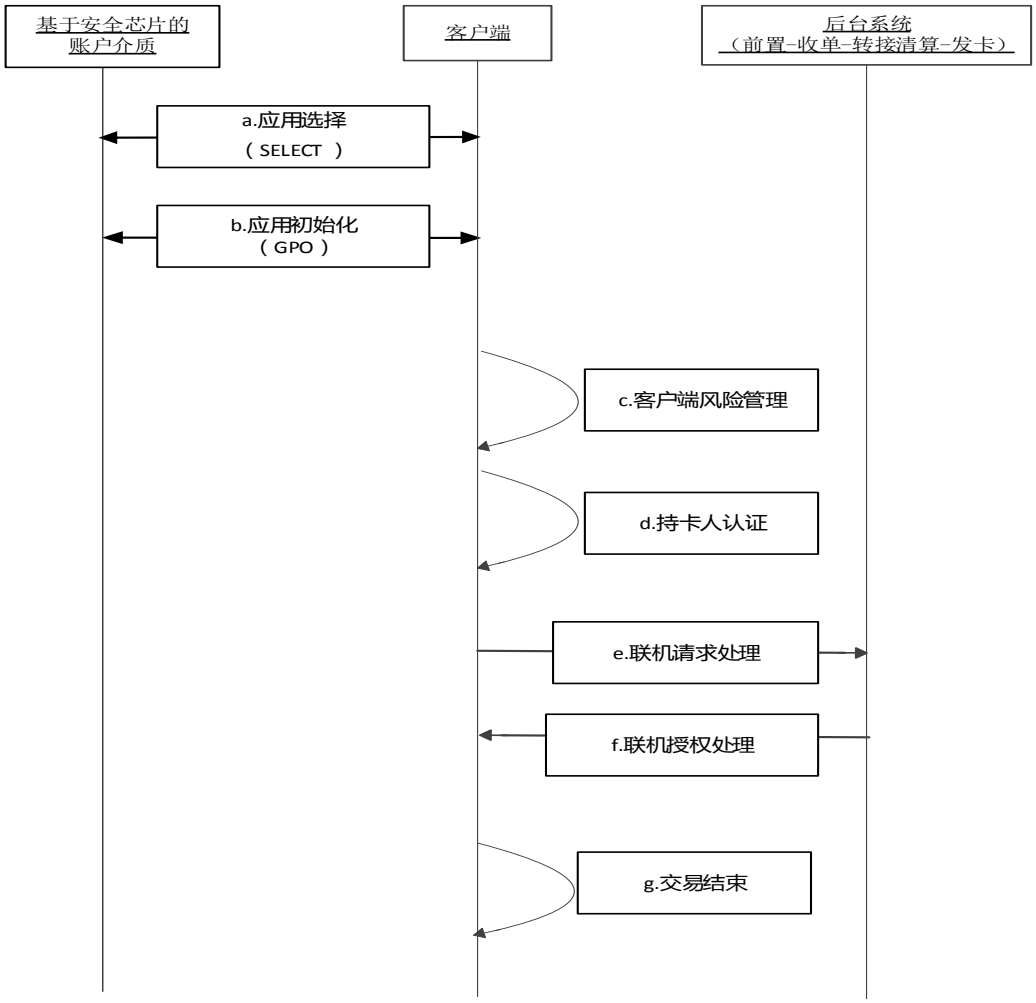

图2 基于 qPBOC 的线上支付消费交易流程图

基于qPBOC的线上支付消费交易步骤分述如下：

a） 应用选择（SELECT）

客户端发送SELECT命令选择qPBOC借记/贷记应用，账户介质返回文件控制信息（FCI）。文件控制信息中应包含PDOL，PDOL中至少应包括请求授权金额（标签“9F02”）和交易货币代码（标签“5F2A”）。

b） 应用初始化（GPO）

客户端向账户介质发送GPO命令，表示交易处理开始。当发送此命令时，客户端向账户介质提供处理PDOL请求的数据元。账户介质响应数据内容为AIP，AIP列出了交易在处理过程中执行的功能。

如果客户端没有收到AIP，则交易被终止。

c） 客户端风险管理

客户端可不进行最低限额、频度等检查。

客户端应发起联机交易，若客户端当前不具备联机能力，则交易请求拒绝，交易终止。

d） 持卡人认证

持卡人认证用于确保持卡人身份合法以及账户介质没有丢失。

若客户端具备联机能力，则要求持卡人输入线上支付密码等持卡人身份认证凭据，并采取必要的安全措施确保用户输入的持卡人身份认证凭据的安全。在后续交易处理环节，线上支付密码密文与联机请求报文一起上送至后台系统进行验证。

e） 联机请求处理

客户端采用加密保护方式，将发卡行应用数据、ARQC、线上支付密码等持卡人身份认证凭据密文等相关交易数据，通过交易请求报文发送给后台系统请求联机处理。后台系统接收到请求后，首先通过请求报文中的交易发起渠道，识别出交易是否为线上支付交易。后台系统验证线上支付密码等持卡人身份认证凭据和ARQC，如后台系统验证失败，则后台系统终止交易并向客户端发送错误信息。

f） 联机授权处理

后台系统进行额度检查，如果授权金额大于单笔线上支付限额，或者授权金额与累计线上支付金额之和大于累计线上支付限额，则后台系统终止交易并向客户端发送错误信息；否则从持卡人账户中扣减相应的交易金额。

当后台系统完成相关交易数据的验证后，将交易结果反馈至客户端。交易结果中至少包含此次线上支付交易是否成功的信息。后台系统校验ARQC，根据校验结果进行交易授权。

g） 交易结束

客户端应向持卡人提示相关交易结果信息，如交易发生异常或者失败，建议持卡人进行交易信息查询，实际交易结果以后台结果为准。

5.3.2 基于安全芯片的线上支付担保支付交易

线上担保支付交易，利用借记/贷记账户的预授权功能，允许持卡人通过客户端向发卡行申请授权，将后台账户的一部分账户余额冻结，作为交易的担保押金。在持卡人获取商品或接受服务后，商户可以向发卡机构进行承兑实际消费金额，完成结算。

线上担保支付交易流程与消费交易流程一致，具体参见5.3.1.1步骤a)—k)或5.3.1.2步骤a)—g)。其中，在联机授权处理过程中，后台系统进行额度检查，如果授权金额大于单笔线上支付限额，或者授权金额与累计线上支付金额之和大于累计线上支付限额，则后台系统终止交易并向客户端发送错误信息；否则从持卡人账户中冻结相应的授权金额。

5.3.3 基于安全芯片的线上支付额度查询

客户端发起线上支付额度查询命令，通过后台系统发送获取线上支付额度报文，允许客户端获取单笔线上支付限额、累计线上支付限额和实际可用线上支付金额。后台系统应在验证持卡人身份合法后，才向客户端反馈相关的查询结果。

客户端接收到来自后台系统线上支付额度，做相应格式化后向持卡人显示。

实际可用线上支付金额为可供持卡人客户端线上支付的最大金额。

欲向持卡人提供此服务的发卡行应在其认证发布的客户端上实现线上支付额度查询功能。

若发卡行仅在部分客户端上提供该服务，则应采取某种方式让持卡人识别出哪些客户端提供该服务（如采用某特定标记）。

5.3.4 基于安全芯片的线上支付日志查询

要获取交易日志，客户端仅需向发卡行系统发送获取线上支付日志报文。系统保存了持卡人最近进行交易的相关日志。发卡行系统应在验证持卡人身份合法后，才向客户端反馈相关的查询结果。具体日志数量由发卡行根据自身需求和条件自行决定。

对于每次交易，发卡行系统在其交易日志中至少应保存以下信息：

——商户名称；

——订单编号；

——交易日期；

——交易时间；

——授权金额；

——交易货币代码；

——交易类型；

——ATC。

客户端通过交易日志查询功能，向持卡人提供最近的交易信息。

欲向持卡人提供交易日志服务的发卡行，宜在其控制下的客户端上实现交易日志查询功能。

5.4 个人化要求

对于支持标准借记/贷记应用的基于安全芯片的线上支付的账户介质宜要求强制执行发卡行认证并成功，即在借记/贷记应用数据中，设置发卡行认证指示位（标签“9F56”）中“发卡行认证必备”为“1”，同时设置应用缺省行为（标签“9F52”） 中“如果发卡行认证必备但没有ARPC收到，交易拒绝位”为“1”。

6 安全要求

6.1 账户介质

账户介质包括普通金融 IC 卡、个人移动终端安全单元等，应满足如下要求：

——采用的安全芯片应符合 JR/T 0098.2—2012 的要求；

——应通过外部安全评估。

6.2 客户端执行环境

客户端执行环境包括但不限于操作系统等，应满足如下要求：

——在安装和更新客户端前，应首先验证客户端安装包的数字签名，保证客户端安装包来源于可信实体；

——应保证客户端拥有独立的程序运行空间和私有的文件系统，保证客户端私有数据不被其他软件非法访问；
——宜实现主动的安全防御机制，例如内置恶意软件检测模块、安全检查工具等；
——客户端执行环境宜采用基于 TEE 技术的安全操作系统；
——当发现重大安全缺陷或安全威胁时，应在门户站点发布警示通知，并通过消息推送、短信、邮件等方式主动通知用户。

6.3 客户端

6.3.1 生命周期管理

6.3.1.1 客户端开发和上线

客户端开发和上线应满足如下要求：
——客户端开发和发布流程应符合 JR/T 0092 中客户端软件管理部分的要求；
——测试环境不应直接使用生产环境真实的账户信息、个人身份信息等；
——客户端发布时应清除未使用的程序代码、编译调试信息和所有的测试环境数据，并永久禁用调试级别和详细级别的日志打印功能；
——应定期对客户端进行外部安全评估，评估内容包括但不限于代码审计、渗透测试、业务流程审计等。

6.3.1.2 客户端分发

客户端分发应满足如下要求：
——在签约时应对用户进行风险提示，要求用户应从官方认可的渠道下载客户端；
——通过门户网站进行分发时，应提供客户端的哈希值供用户校验，同时在显著位置标注官方授权的其他发布途径；
——客户端在应用分发平台中显示的提供商名称应与企业在工商管理机构注册的名称一致；
——应定期从分发平台上下载客户端进行校验，防止客户端安装包被篡改，若发现异常，应立即对客户端下架处理，并在门户网站上进行公布；
——宜通过网站、微博、互动平台等渠道对客户端安装、使用中的注意事项进行宣传，培养用户的安全使用习惯。

6.3.1.3 客户端更新

客户端更新应满足如下要求：
——应有计划地对客户端进行更新，客户端应具备自动检查更新的功能；
——应禁用版本过低的客户端中的交易功能，并在软件界面中提醒用户进行更新。

6.3.1.4 客户端卸载

客户端卸载完成后，文件系统中不应保留任何与用户相关的个人信息及交易数据等。

6.3.2 防逆向

防逆向要求如下：
——客户端应采取有效的干扰措施增加对代码静态分析的难度，如代码混淆、花指令、程序加壳等；
——客户端应至少对以下代码或数据进行混淆，如非公开的函数名称、变量名称、参数名称、可能泄露实现细节的字符串、硬编码的密钥或公钥等；

——客户端宜对关键的代码段进行加密处理；
——客户端宜实现动态防逆向机制，包括但不限于通过动态组件下载等方式，动态下载的组件应在使用完毕后立即清除。

6.3.3 防篡改

防篡改要求如下：
——客户端应在启动和更新过程中对自身的完整性和真实性进行检查，防范软件代码被篡改或替换；
——客户端宜定期或每次登录或每次交易前对自身完整性和真实性进行检查，定期检查宜每 24 小时至少执行一次；
——客户端检查自身完整性和真实性的算法应符合国家密码主管部门的要求；
——客户端应采取必要的安全措施来保证其获取的交易数据是来自安全芯片，不被篡改，如采用随机数与交易流水号绑定的方式以校验交易的合法性。

6.3.4 防重放

防重放要求如下：
——客户端输出的所有编码后的敏感信息、数字签名等与认证和交易相关的数据应保证仅一次有效；
——随机因素的生成应同时满足随机性和不可预测性，使用后应立即失效；
——客户端进行加密和签名运算时，数据块应采用随机数进行填充；
——交易报文中使用的随机数应由后台服务端产生并校验。

6.3.5 安全输入组件

安全输入组件是客户端的必要组件，其用于保证用户输入数据的秘密性和完整性，例如密码键盘、专用文本框等。在用户输入敏感信息时，禁止使用操作系统内置或第三方输入法键盘。

安全输入组件应满足如下要求：
——所有的敏感信息（如 PIN、CVN、有效期等）和关键的交易信息（如交易金额、收款人账号、交易验证码等）应通过安全输入组件进行输入和显示；
——通过安全输入组件输入的敏感信息在输入完成后应立即加密，在输入的任何阶段，内存中都不应出现完整的明文数据；
——通过安全输入组件输入的关键交易信息应采用密码学技术保证其完整性；
——安全输入组件使用的秘密性和完整性保护密钥应基于非对称密码算法协商，并保证每笔交易唯一；
——应对安全输入组件使用的静态密钥进行保护，如采用拆分、编码等方式，防范该密钥被非法篡改和替换；
——如采用第三方安全输入组件，应保证其通过外部安全评估。

密码键盘应满足如下要求：
——使用密码键盘输入敏感信息时，应使用即时加密等安全措施降低恶意软件窃取用户支付敏感信息的风险，应采取自定义键盘等措施防范密码被窃取；
——宜采取防录屏手段防范恶意软件获得密码键盘当前的按键排列顺序。

专用文本框应满足如下要求：
——显示敏感信息时，应以屏蔽方式显示；
——显示交易信息时，应逐字符显示，避免在内存中出现完整的交易信息明文。

6.3.6 图片验证码

图片验证码应满足如下要求：

——图片验证码应由后台服务端产生和验证，图片验证码文本内容不应在客户端出现；

——每个图片验证码应只验证一次，无论验证结果如何，均应使当前验证码失效；

——图片验证码应具有一定的复杂度，有效的枚举空间不得低于 1 万个；

——图片验证码应能有效防范程序自动识别，如采取字符变形、字符叠加、背景干扰、颜色变换等方式；

——如果图片验证码包含数字，宜采用大写数字显示，如壹、贰等；

——图片验证码应具有时效性，有效期不宜超过 3 分钟。

6.3.7 外部接口

外部接口包括但不限于用户交互接口、进程间通信接口等，应满足如下要求：

——应提供外部接口声明，声明应至少包括接口名称、用途、调用方式等内容，不应提供未声明的外部接口，也不应提供非业务必需的外部接口；

——客户端不应提供接收用户 PIN 等敏感信息的外部接口；

——客户端应对外部接口接收的数据内容进行约束，如对非法字符进行校验、对取值范围进行判断、对数据长度进行限制等；

——客户端应优先采用按值传递的方式从外部接口接收数据，确保数据在接收完毕后无法被调用方等外部实体篡改；

——客户端宜保持运行的独立性，不受调用方安全状况的影响；

——外部接口宜提供数字签名等技术手段保证传递数据的完整性和保密性；

——对于供第三方软件调用的接口，客户端宜对调用方的身份合法性进行验证。

6.3.8 敏感信息保护

敏感信息保护要求如下：

——客户端不应存储任何明文或密文的非业务必需的敏感信息；

——银行卡主账号除交易流程中应由用户确认的情况外，显示时应屏蔽部分字段；

——客户端使用的对称密钥和私钥应加密存储，针对这些密钥的加密密钥不应存储在客户端本地，宜采用用户密码等运行时信息分散产生；

——客户端的认证证书和私钥的使用和存储应符合 JR/T 0068 中文件证书部分的要求。

6.3.9 交易确认

客户端用户身份认证与交易认证方式应符合 JR/T 0092 中身份认证安全部分的要求。

6.4 后台服务端

后台服务端应满足如下要求：

——应保证其物理机房、网络、主机、数据、应用、运行维护的安全；

——应保证系统业务连续性；

——应实现对客户端异常事件的审计功能，应能根据规则进行自动或人工处理，异常事件包括但不限于客户端证书无效、客户端软件版本过旧、报文不合法、密码错误次数超限、数字签名无效、重复报文等，如确定为攻击行为应及时切断与客户端的连接并告警；

——应对接收数据的有效性进行校验，防止客户端提交非法数据，进行 SQL 注入等攻击；

——在后台服务端禁用客户端软件（如手机银行）时，应同时禁用所有通过该客户端软件发起的交易，操作应立即生效；

——后台服务端存储的用户认证要素，应加密或使用安全哈希函数编码，应能防范暴力破解等攻击方式；

——服务端日志中不应留存支付敏感信息，如银行卡磁道信息、CVN、CVN2、支付密码、有效期等；

——因业务要求，若后台服务端需导出日志或审计报表时，应采取屏蔽或混淆等方式对敏感信息的输出进行处理；

——制定统一的安全配置策略，对后台服务端使用的开源中间件和软件进行安全配置。

6.5 安全通信

客户端与账户介质的通信应基于安全协议，采取有效的访问控制措施以防范对账户介质的非法访问、恶意攻击、远程挟持等安全隐患。

客户端与后台服务端的通信应满足如下要求：

——客户端应使用安全协议保证与后台服务端通信的秘密性、完整性和真实性，如使用 TLS 协议等；

——后台服务端应使用经过具有资质的电子认证机构颁发的数字证书以标识其真实性；

——应检查安全协议使用的数字证书有效性；

——安全协议不应包含任何已公开的安全缺陷，无法彻底修复的宜采用其他措施弥补；

——安全协议所使用的加密算法的选择与使用应符合国家密码主管部门的要求；

——客户端应对敏感信息进行加密，并对交易报文计算 MAC，加密和 MAC 密钥应采用会话密钥机制，保证一次一密。