ICS 35.240.40
A 11

JR

# 中华人民共和国金融行业标准

JR/T 0092—2012

# 中国金融移动支付　客户端技术规范

China financial mobile payment—Technical specification for client software

2012－12－12 发布　　2012－12－12 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/TC180）归口。

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

本标准参加起草单位：中移电子商务有限公司、中国银联股份有限公司、中国邮政储蓄银行、天翼电子商务有限公司、北京银联金卡科技有限公司（银行卡检测中心）、上海华虹集成电路有限责任公司、中钞信用卡产业发展有限公司、惠尔丰电子（北京）有限公司、宏达国际电子股份有限公司、握奇数据系统有限公司、北京同方微电子有限公司、大唐微电子技术有限公司、上海复旦微电子股份有限公司、恩智浦半导体有限公司、金雅拓智能卡公司、上海柯斯软件有限公司、福建联迪商用设备有限公司、武汉天喻信息产业股份有限公司。

本标准主要起草人：李晓枫、陆书春、潘润红、杜宁、李兴锋、韩建国、刘力慷、王妍娟、龚睿、乐祖晖、李一凡、江磊、田小雨、尚可、张柳成、张志茂、罗玲、吴星宇、陈敬宏、覃晖、邹重人、田燕军、范金钰、王晓华、任强、应根军、王文志、于海涛、胡瑞璟、姜达、赵亚平。

# 引　言

随着智能移动终端的普及和移动互联网相关产业的快速发展，移动互联网应用对支付能力的需求变得越来越迫切。客户端作为应用与支付结合的新兴产品，以其便捷的操作、良好的用户体验，成为移动支付一个新的发展趋势。

考虑到客户端应用涉及面广，以及各银行和非金融机构的业务系统现状，为了便于标准的推广，本标准仅对客户端的基本功能、流程及安全技术要求进行了规范。

# 中国金融移动支付 客户端技术规范

## 1 范围

本标准包括移动支付客户端的应用、安全和管理三部分。应用部分定义了系统架构、基本功能、界面要求和交互流程；安全部分定义了客户端相关安全技术要求；管理部分定义了客户端设计、开发、维护、版本发布及安装卸载要求。

本标准适用于移动支付领域客户端软件设计、开发、维护及测试等相关单位。

## 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 0093.2-2012 中国金融移动支付 远程支付应用 第2部分：交易模型及流程规范

JR/T 0094.2-2012 中国金融移动支付 近场支付应用 第2部分：交易模型及流程规范

JR/T 0097-2012 中国金融移动支付 可信服务管理技术规范

## 3 应用场景

客户端可向用户提供支付和TSM应用管理等功能。支付可以分为远程支付和近场支付两大类。在远程支付应用中，用户可以通过客户端进行在线购物、缴纳公用事业费、转账汇款等。在近场支付应用中，用户可以通过客户端对SE账户余额查询、卡片参数设置等操作。

对于TSM应用管理，客户端仅作为SE与TSM的中转通道，详见JR/T 0097-2012。

## 4 客户端软件系统架构

### 4.1 概述

客户端软件可分为基于SE的客户端软件、无SE的客户端软件和SE内嵌的支付软件三种类型。三种客户端软件的系统架构各不相同，详见本标准4.2、4.3和4.4。

### 4.2 基于 SE 的客户端软件

基于SE的客户端软件运行在移动终端操作系统中，通过SE对交易敏感信息等加密，并与远程支付系统建立通信连接，完成支付相关功能，软件架构如图1所示：


图1　基于 SE 的客户端软件架构

——支付应用软件层

客户端软件直接面向用户，通过各种形式的图形化操作界面，为用户提供方便快捷的支付服务。

——网络协议层

为客户端提供基础的网络协议服务，包括各种安全通信协议SSL、TLS、WTLS等，也可根据客户端需求提供定制化的专用网络协议。

——操作系统层

操作系统层是客户端软件运行的基础平台。目前主流的智能移动终端操作系统包括Android、IOS、Windows Phone、Symbian等。

——物理设备层

SE内部安全域存储密钥、数字证书等机密信息，并为客户端提供交易敏感信息加密处理等安全功能。

### 4.3　无 SE 的客户端软件

客户端软件运行在移动终端操作系统中，与远程支付系统建立通信连接，完成支付相关功能,其中交易敏感信息加密由客户端软件完成，软件架构如图2所示:

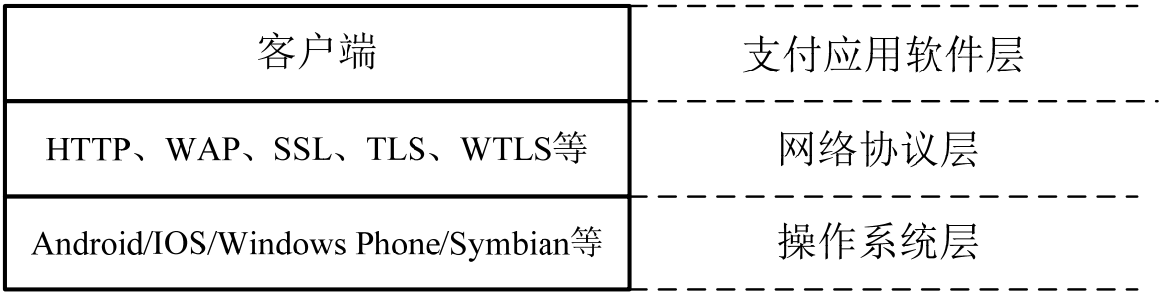


图2　无 SE 的客户端软件架构

——支付应用软件层

客户端软件直接面向用户，通过各种形式的图形化操作界面，为用户提供方便快捷的支付服务。

——网络协议层

为客户端提供基础的网络协议服务，包括但不限于安全通信协议SSL、TLS、WTLS等，也可根据客户端需求提供定制化的专用网络协议。

——操作系统层

操作系统层是客户端软件运行的基础平台。目前智能移动终端操作系统包括Android、IOS、Windows Phone、Symbian等。

### 4.4 SE 内嵌的支付软件

SE内嵌支付软件运行在SE操作系统中，SE操作系统通过标准APDU指令实现SE内嵌支付软件和SE之间的交互。软件架构如图3所示：


图3 SE 内嵌支付软件的软件架构

——应用界面层

应用界面层是与用户直接交互的功能层，基于客户端软件以菜单的模式为用户提供移动支付应用。根据用户需求，应用层可以支持OTA技术实现应用软件空中下载及升级服务。

——传输协议层

传输协议层作为应用界面层和操作系统层间的桥梁，通过标准APDU指令实现两者之间的交互。

——操作系统层

SE操作系统层是SE内嵌支付软件运行的基础平台，负责解析所有应用指令并进行处理，提供基础的安全服务。

——物理设备层

SE是基于客户端软件安全服务的硬件基础，为上层应用提供基础的认证及加解密硬件资源。

## 5 客户端基本功能及流程

### 5.1 概述

客户端与SE、远程支付系统、TSM平台等系统交互完成实现相关功能，系统架构如图4所示：

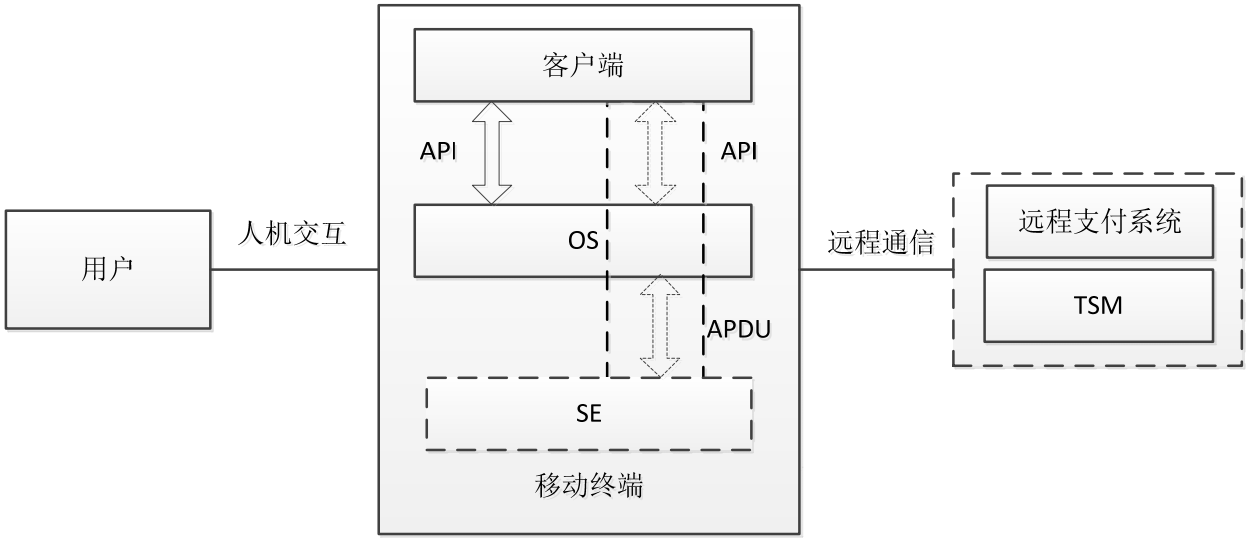


**图4　客户端与相关系统架构**

客户端功能界面应布局合理、风格统一、简洁易用、用户体验良好。考虑到移动终端差异、不同客户端群体偏好不一致等多方面因素，为留出充分的创意空间，本标准中功能界面要求仅从提升支付交易安全性、提升用户体验两方面进行规范。

### 5.2　版本升级

#### 5.2.1　功能定义

客户端宜具备在线版本检测、升级功能。版本升级分为可选升级与强制升级两种。升级时宜保留原有应用数据，避免影响用户正常使用。

#### 5.2.2　界面要求

客户端升级前，宜向用户显示新版本特性说明。对于强制升级，应向用户说明强制升级原因。

#### 5.2.3　交互流程

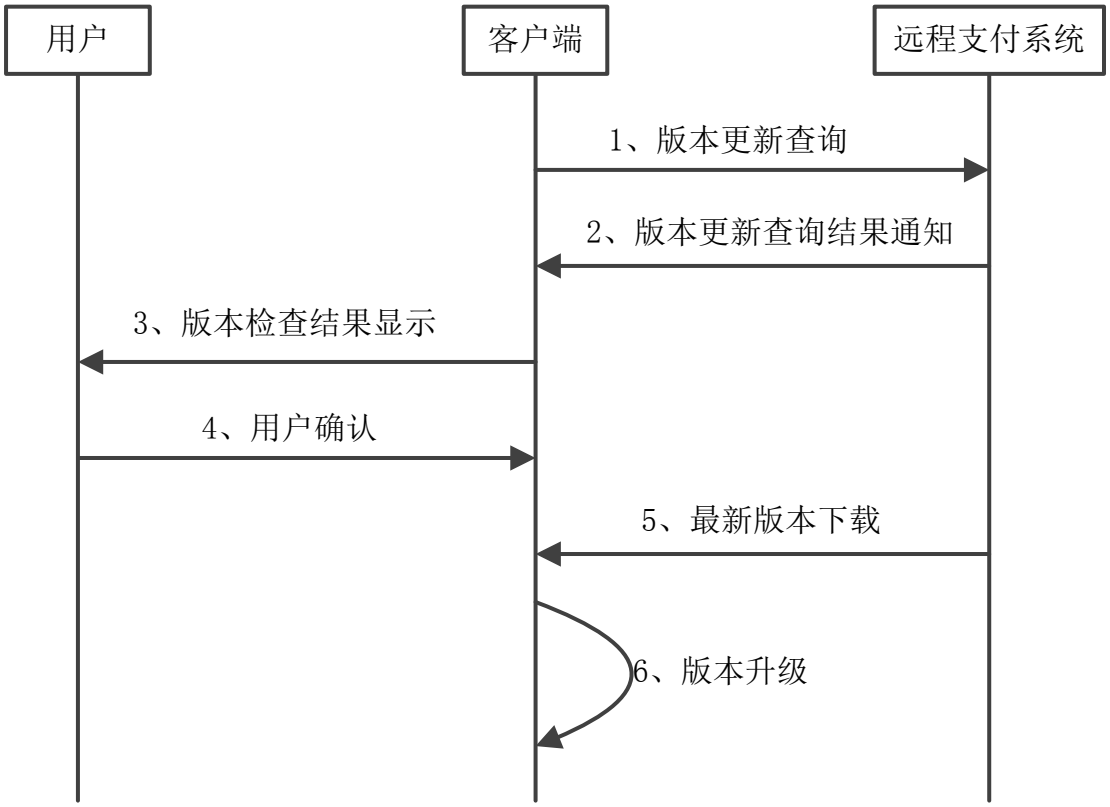


**图5　客户端升级流程**

客户端升级流程如图5所示，说明如下：

步骤1：客户端向远程支付系统发起版本更新查询请求，请求中包含客户端当前版本号；

步骤2：远程支付系统进行客户端版本查询，并将查询结果通知客户端；

步骤3：客户端向用户显示版本查询结果，如有最新版本则提示用户升级，否则本流程结束；

步骤4：用户确认是否升级，如放弃升级，则本流程结束；

步骤5：用户确认升级，则客户端从远程支付系统下载最新版本；

步骤6：客户端新版本下载完成后，进行覆盖安装升级。

### 5.3　SE 注册

#### 5.3.1　功能定义

SE注册是指用户通过客户端向TSM发起并实现SE注册。

#### 5.3.2　界面要求

应向用户显示注册结果。

#### 5.3.3　交互流程

见JR/T 0097-2012的6.4.2。

### 5.4　TSM 应用查询

#### 5.4.1 功能定义

用户通过客户端向 TSM 发起查询,获得可下载的应用列表。

#### 5.4.2 界面要求

应向用户显示TSM上可下载的应用列表。

#### 5.4.3 交互流程

见JR/T 0097-2012的7.4.1。

### 5.5 消费交易

#### 5.5.1 功能定义

消费交易是指用户在支付内容平台上选购商品或服务后，通过客户端确认付款的支付流程。

#### 5.5.2 界面要求

支付前宜向用户显示核心订单信息，如商户名称、商品名称、交易金额等，供用户二次确认。

#### 5.5.3 交互流程

见JR/T 0093.2-2012的5.2.4。

### 5.6 远程圈存

#### 5.6.1 功能定义

用户使用客户端，通过远程支付系统，将账户中的资金划入电子现金账户。远程圈存包括指定账户圈存和非指定账户圈存两种。

#### 5.6.2 界面要求

圈存前，宜向用户显示核心交易信息，如账户号、交易金额等，供用户确认。圈存完成后，宜向用户显示圈存结果。

#### 5.6.3 交互流程

见JR/T 0094.2-2012的7.1。

### 5.7 脚本处理结果通知

#### 5.7.1 功能定义

交易中如果包含了账户管理系统的脚本，客户端应将SE的脚本处理结果通知到账户管理系统。

#### 5.7.2 界面要求

属于客户端后台自动运行流程，无界面要求。

#### 5.7.3 交互流程

见JR/T 0093.2-2012的5.6.4。

## 5.8 账户列表信息查询

### 5.8.1 功能定义

在用户进行远程消费、远程圈存等交易之前，客户端应读取SE中相应应用的账号列表信息，并显示给用户，供其选择。

### 5.8.2 界面要求

客户端宜根据用户以往使用情况，优先显示SE默认账户。

### 5.8.3 交互流程

见JR/T 0094.2-2012的7.3.1。

## 5.9 账户选择

### 5.9.1 功能定义

在用户进行远程消费、空中圈存等交易之前，客户端应选择SE中相应应用的账号。

### 5.9.2 界面要求

客户端宜根据用户以往使用情况，可以完整展示可供选择的账户列表。

### 5.9.3 交互流程

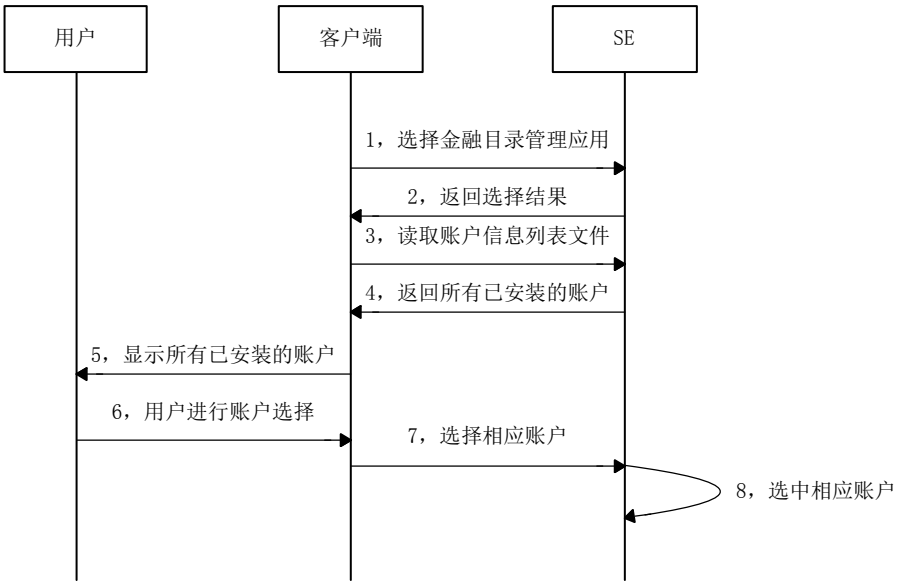


图6 账户选择流程

账户选择流程如图6所示，说明如下：

步骤1：客户端通过PAID选择SE中的金融目录管理应用；

步骤2：返回选择结果，如果失败，流程结束；

步骤3：客户端读所有已安装的账户；
步骤4：返回所有已安装账户信息；
步骤5：向用户显示所有已安装账户；
步骤6：用户选择其中一个账户；
步骤7：客户端向金融目录管理应用发出选择账户的请求；
步骤8：金融目录管理应用受到请求后，选中相应账户。

### 5.10 默认账户设置

#### 5.10.1 功能定义

用户通过客户端对SE中应用的默认交易账户进行修改设置。此默认交易账户指支付交易时的默认账户。

#### 5.10.2 界面要求

由于近场支付时不再对默认账户进行提醒（如乘公交等），因此客户端修改默认账户前，宜请用户进行二次确认。

#### 5.10.3 交互流程

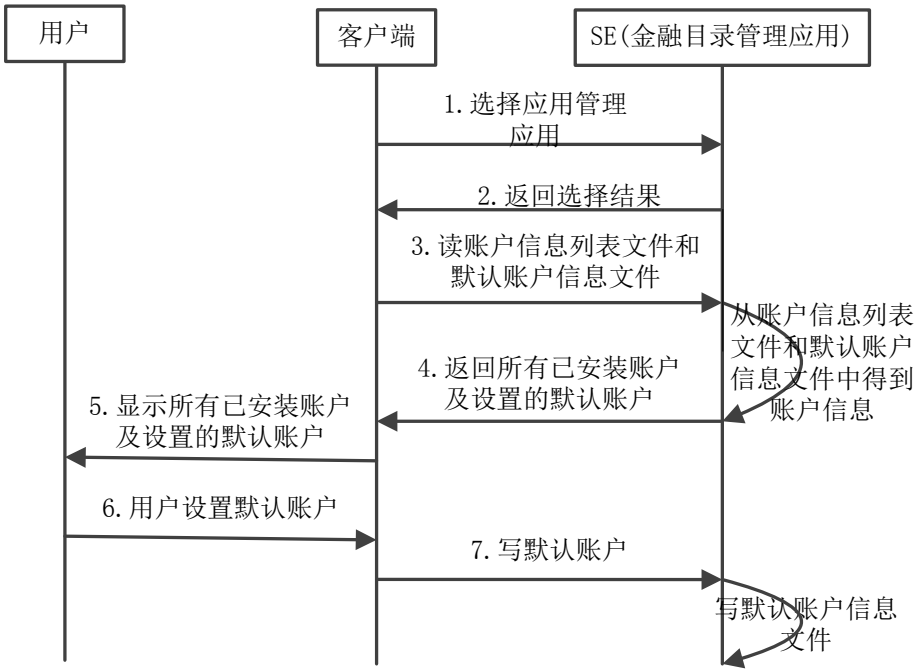


**图7 默认账户设置流程**

默认账户设置流程如图7所示，说明如下：
步骤1：客户端通过PAID选择SE中的金融目录管理应用；
步骤2：返回选择结果，如果失败，流程结束；
步骤3：客户端读所有已安装的账户和默认账户信息；

步骤4：金融目录管理应用从账户信息列表文件和默认账户信息文件中提取相应信息并返回给客户端；

步骤5：向用户显示所有已安装账户及设置的默认账户；

步骤6：用户设置其中一个账户为默认账户；

步骤7：客户端向金融目录管理应用发出写默认账户的请求，金融目录管理应用受到请求后，写默认账户信息文件中的记录。

### 5.11 账户信息查询

#### 5.11.1 功能定义

用户通过客户端查询 SE 所有应用中指定账户的信息，包括但不限于电子现金账户余额、电子现金账户余额上限、电子现金单笔交易限额、电子现金重置阈值等。

#### 5.11.2 界面要求

在查询前，客户端宜优先显示SE默认账户。

#### 5.11.3 交互流程

见JR/T 0094.2-2012的7.3.3。

### 5.12 余额查询

#### 5.12.1 功能定义

用户通过客户端对 SE 中默认账户的电子现金账户余额进行查询。

#### 5.12.2 界面要求

在查询余额前，需要选择待查询的电子现金账户。

#### 5.12.3 交互流程

见JR/T 0094.2-2012的7.3.4。

### 5.13 卡片参数设置

#### 5.13.1 功能定义

用户可通过客户端修改SE中应用的交易参数，包括但不限于电子现金账户余额上限、电子现金单笔交易限额、电子现金重置阈值等。

#### 5.13.2 界面要求

用户修改前，宜请用户进行二次确认。

#### 5.13.3 交互流程

见JR/T 0094.2-2012的7.1。

## 6 客户端安全技术要求

## 6.1 人机交互安全

### 6.1.1 密码管理

密码管理要求如下：

——支付密码应满足以下安全管理要求

1) 支付密码不能保存在移动终端本地；
2) 用户输入支付密码时，应提供即时加密功能；
3) 认证操作结束后立即清除缓存，防止信息泄漏。

——登录密码等其它密码应满足以下安全管理要求

1) 登录密码等其它密码不能明文保存在移动终端本地；
2) 用户输入登录密码等其它密码时，应提供即时加密功能；
3) 认证操作结束后立即清除缓存，防止信息泄漏。

### 6.1.2 认证方式

对于大额支付、重要信息修改等关键业务，除密码认证以外，客户端还应采用其它安全认证方式。

### 6.1.3 登录失败处理

客户端对用户登录应采取限定连续登录失败次数等措施。

### 6.1.4 移动终端交易异常处理

当客户端检测到移动终端交易出现异常时应向用户提示出错信息。

## 6.2 软件安全

### 6.2.1 数据有效性校验

客户端宜提供数据有效性校验功能，保证通过人机接口或通信接口输入的数据格式或长度等信息符合系统设定要求，如输入的资金金额、账户等信息应不含特殊字符。

### 6.2.2 页面回退清除敏感信息机制

客户端宜支持页面回退清除敏感信息的机制。

### 6.2.3 反编译

客户端宜采用反逆向工程保护措施，如客户端可采取代码混淆等技术手段，防范攻击者对客户端的反编译分析。

### 6.2.4 防篡改

客户端启动和更新时，宜进行真实性和完整性校验，防范客户端被篡改。

## 6.3 数据安全

### 6.3.1 数据录入

数据录入要求如下：

——敏感数据安全显示

对于密码等敏感数据，客户端不应明文显示。

——敏感数据防截获

用户输入敏感数据时，宜采取安全措施保证敏感数据不被移动终端的其他设备或程序非授权获取。

——敏感数据防篡改

用户输入敏感数据时，宜采取防篡改机制保证数据不被移动终端的其他设备或程序篡改。

### 6.3.2 数据访问

宜根据业务需要保证敏感数据仅供授权用户或授权应用组件访问。

### 6.3.3 数据存储

——关键数据存储

在满足法律、管理规定和业务需求的前提下，客户端宜保留最少的用户敏感数据（如登录密码、软件证书、账户信息等），并限制数据存储量和保留时间。

——用户信息存储安全

客户端不应保存用户支付信息（如银行卡磁道信息、CVN、CVN2、支付密码等）及其密文。

——敏感信息显示

客户端显示敏感信息时，宜屏蔽部分内容，如银行账号、身份证号等。

——残余信息保护

客户端在使用过身份认证、交易等敏感信息后，应及时清除敏感数据。

### 6.3.4 数据传输

——远程数据传输保密性

支付密码等敏感数据通过公共网络传输时应采取加密措施，保证敏感数据传输的保密性。

——本地数据传输保密性

支付密码等敏感数据在本地软件其他进程间传输时应采取加密措施，保证敏感数据传输的保密性。

——数据传输完整性

交易数据在传输时，客户端应采取安全措施（如MAC等）以确保交易数据的完整性。

## 6.4 通信安全

### 6.4.1 网络通讯协议

网络通讯协议：

——应在客户端与服务器之间建立安全的信息传输通道，宜进行双向认证，例如使用 SSL/TLS 或 IPSEC 等协议；

——如使用 SSL 协议，应使用 3.0 及以上相对高版本的协议，取消对低版本协议的支持；

——客户端到远程支付系统的 SSL 加密密钥长度应不低于 128 位，用于签名的 RSA 密钥长度应不低于 1024 位，用于签名的 ECC 密钥长度应不低于 256 位或 SM2 密钥长度应不低于 256 位。

### 6.4.2 安全认证

客户端的网络协议层应对远程支付系统进行身份认证。

### 6.4.3 抗抵赖

通过客户端发送的报文的关键要素宜进行数字签名，以确保支付内容的真实性和不可抵赖性。

# 7 客户端软件管理要求

## 7.1 设计要求

设计要求如下：

——客户端设计应遵循安全、可靠、易用、可维护和可扩展等原则；

——客户端宜提供易用、风格统一、体验良好的用户界面。

## 7.2 开发要求

开发要求如下：

——客户端开发过程中应遵守严格的开发流程和编码安全规范，进行完整的测试，避免在请求、响应、存储、配置等功能中存在漏洞；

——客户端开发过程中应建立并维护开发文档，包括需求说明、需求分析、概要设计、详细设计、数据模型设计、源码归档、测试用例、配置管理等；

——客户端开发完成后，应同步完成产品手册、用户手册等相关文档。

## 7.3 维护要求

维护要求如下：

——应制定科学、合理的管理策略和执行条例，指导各种角色的工作协同、实施步骤、质量管控、安全检测等，规范日常运维流程，消除繁杂凌乱现象，使得小差错提前暴露，避免由此引起大事故的发生；

——建立并维护：工程实施、项目管理、测试报告、变更控制、系统运维管理、监控与应急管理、安全管理、安全审计等文档。

## 7.4 发布要求

发布要求如下：

——客户端应有规范的上线发布流程，并应提供安全可靠的客户端下载、发布、升级渠道；

——客户端在安装前，应有明确的风险提示，对于无法在安装前进行风险提示的操作系统，建议在安装后运行的第一步提示用户。安装过程中，应拥有独立的安装目录，唯一的应用标识符，明确的版本序号，不得篡改、覆盖、删除系统文件和其它软件。安装完成后，应明确告知用户成功或失败；

——客户端在卸载时，应严格依据登记注册的卸载项，逐项删除清理，因涉及到金融领域，须删除运行时产生的所有缓存文件、日志文件等，同时不得篡改、覆盖、删除系统文件和其他软件，确保卸载后系统环境正常运行。

# 参 考 文 献

[1] JR/T 0068-2012 网上银行系统信息安全通用规范