ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0098.3—2012

中国金融移动支付 检测规范 第3部分：客户端软件

China financial mobile payment—Test specifications—
Part 3: Client software

2012-12-12 发布 2012-12-12 实施

中国人民银行 发布

目　　次

前　言

《中国金融移动支付 检测规范》标准由以下8部分构成：

——第1部分：移动终端非接触式接口；

——第2部分：安全芯片；

——第3部分：客户端软件；

——第4部分：安全单元（SE）应用管理终端；

——第5部分：安全单元（SE）嵌入式软件安全；

——第6部分：业务系统；

——第7部分：可信服务管理系统；

——第8部分：个人信息保护。

本部分为该标准的第3部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

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

本部分参加起草单位：北京银联金卡科技有限公司（银行卡检测中心）、中金国盛认证中心、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、上海市信息安全测评认证中心、信息产业信息安全测评中心、北京软件产品质量检测检验中心、中钞信用卡产业发展有限公司、上海华虹集成电路有限责任公司、上海复旦微电子股份有限公司、东信和平智能卡股份有限公司、大唐微电子技术有限公司、武汉天喻信息产业股份有限公司、恩智浦半导体有限公司。

本部分主要起草人：李晓枫、陆书春、潘润红、杜宁、李兴锋、张雯华、刘力慷、刘志刚、聂丽琴、李晓、尚可、郭栋、熊文韬、宋铮、李宏达、王冠华、胡一鸣、张晓、平庆瑞、张志茂、陈君、彭美玲、李微、陈吉、程恒。

引　言

随着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。客户端软件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。

考虑到客户端软件运行平台的多样化，软件作为用户支付服务的窗口，选用安全可靠的客户端软件是极其重要的。为确保移动支付业务的安全，在收集、分析和评估移动支付客户端软件风险的基础上，标准的本部分从客户端软件的基本要求、功能、性能和安全四个方面提出对客户端软件的检测要求。

中国金融移动支付　检测规范　第3部分：客户端软件

1　范围

本部分规定了于支持支付业务（包括处理订单）的移动终端客户端软件的检测要求，包括：移动终端客户端程序、支付控件等。对于仅支持内容浏览等关联业务、不直接集成支付功能的应用软件的安全、移动支付终端操作系统安全、SE的安全均不属于本部分的规定范围。

本部分适用于移动支付客户端软件检测机构以及设计、开发、集成、维护、运营单位。

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 0092-2012　中国金融移动支付 客户端技术规范

3　客户端软件系统架构

见JR/T 0092-2012中第4章。

4　基本检测项

4.1　开发与维护

4.1.1　开发环境

检测目的：检查开发环境是否具有配套的维护机制，发现开发环境中可能存在的漏洞。

检测流程：检查开发环境工具清单、维护机制指引，并访谈、分析实际情况是否属实。

通过标准：具有明确的开发环境工具清单和维护机制，未发现开发环境存在明显漏洞。

4.1.2　编码漏洞

检测目的：检查编码是否遵守标准的开发流程和编码安全规范，是否配套单元测试，发现请求、响应、存储、配置等功能中可能存在的漏洞。

检测流程：检查编码规范、关键源代码是否存在安全漏洞。

通过标准：编码符合安全规范，未发现漏洞。

4.1.3　安全补丁

检测目的：检查客户端软件安全补丁的管理程序是否合理。

检测流程：检查客户端软件安全补丁的管理程序、更新记录。

通过标准：应具备完整的安全补丁管理程序，安全补丁应通过充分的评估和测试，确保安装的补丁不与现有的安全配置相冲突。

4.1.4 配置管理

检测目的：检查客户端软件配置的变更是否遵守变更控制规范。
检测流程：检查变更控制规范（包括软件版本管理），抽样检查变更记录。
通过标准：具有变更控制规范，执行记录符合规范要求。

4.1.5 质量检测

检测目的：检查客户端软件质量检测是否具有规范的测试流程和完整的测试记录和报告。
检测流程：检查测试流程规范、测试记录、测试报告。
通过标准：测试流程规范，测试记录、测试报告完整。

4.1.6 发布管理

检测目的：检查是否具有规范的发布流程，在获取到许可后，根据许可来投产发布。
检测流程：检查发布流程、发布记录，并访谈、分析情况是否属实。
通过标准：符合发布流程，发布前实施签名并获得许可。

4.2 安装与卸载

4.2.1 下载获取

检测目的：检查是否提供安全可靠的客户端下载发布渠道。
检测流程：根据指定渠道和路径下载获取客户端软件，分析下载过程。
通过标准：提供官方的下载获取渠道，下载渠道安全可靠。宜支持自动检查、更新版本功能，以便用户及时下载更新。

4.2.2 安装注册

检测目的：检查客户端软件安装注册过程是否具有风险提示和回退机制。
检测流程：根据客户端软件安装指引，安装注册，通过检测工具分析安装前后的环境变化。
通过标准：客户端在安装前，应有明确的风险提示。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应用软件。安装完成后，应明确告知用户成功或失败。如果失败，应有完备的回退机制，确保还原到安装前的系统环境。

4.2.3 卸载清除

检测目的：检查客户端卸载清除是否完全。
检测流程：自行卸载清除，分析卸载前后的系统环境。
通过标准：客户端在卸载时，应满足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，应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、删除系统文件和其它应用软件，确保卸载后的系统环境运行正常。

4.3 文档支持

4.3.1 用户类文档

检测目的：确保面向用户提供了正确的、完整的、友好的指导文档。

检测流程：检查用户类文档，并访谈、分析情况是否属实。用户类文档一般包括：产品简介、用户手册、操作手册、常见问题等。

通过标准：用户类文档正确完整且通俗易懂。

4.3.2 工程类文档

检测目的：确保工程实践中有完整的、可追溯的描述文档。

检测流程：检查工程类文档，并访谈、分析情况是否属实。工程类文档一般包括：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。

通过标准：文档完整且符合实际情况。

4.3.3 管理类文档

检测目的：确保日常运维具备完整的、可执行的管理类文档。

检测流程：检查管理类文档，并访谈、分析情况是否属实。管理类文档一般包括：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。

通过标准：文档完整且符合实际情况。

5 功能检测项

5.1 兼容性检测

5.1.1 硬件兼容性

检测目的：检查客户端软件与不同型号移动终端硬件的兼容支持性情况。

检测流程：根据设计要求，抽样不同型号的移动终端，安装客户端软件，检测相关运行情况。

通过标准：客户端软件应能够调用移动终端硬件资源，以实现其所需功能；客户端软件的安装和运行不应影响移动终端正常运行，不会导致移动终端其它功能不可用。

5.1.2 操作系统兼容性

检测目的：检查客户端软件运行在不同版本的移动终端操作系统时，与操作系统的兼容性情况。

检测流程：根据设计要求，将客户端软件安装到指定平台的不同版本的移动终端操作系统上，检测相关运行情况。

通过标准：客户端软件应能在所支持的不同版本的移动终端操作系统上安装、运行、卸载；客户端软件的安装和运行不应影响移动终端正常运行，不会导致移动终端其它功能不可用。

5.1.3 与其它应用程序的兼容性

检测目的：客户端软件安装后，不得影响现有其它应用程序的正常使用。

检测流程：根据设计要求，客户端软件安装成功后，检测其它应用软件运行情况。

通过标准：已安装的其它应用软件可以正常运行。

5.1.4 浏览器兼容性

检测目的：检查基于浏览器实现的客户端软件与移动终端浏览器的兼容性情况。

检测流程：根据设计要求，安装基于浏览器的客户端软件后，检测相关运行情况。

通过标准：客户端软件应能在所支持的浏览器上正常完成其设计的功能，浏览器的其它功能正常运行。客户端软件浏览器升级后，客户端软件应能及时更新。

5.2 版本升级

检测目的：客户端宜具备在线版本检测、升级功。
检测流程：验证通过客户端软件的升级流程。
通过标准：客户端具备在线版本检测、升级功能。升级时保留原有应用数据，避免影响用户正常使用。。

5.3 SE 管理

5.3.1 SE 注册

检测目的：客户端软件应提供SE注册功能。
检测流程：验证通过客户端软件对SE进行注册操作。
通过标准：若客户端软件基于SE模式，应实现SE注册功能。

5.3.2 SE 应用下载安装

检测目的：客户端软件可提供SE应用下载安装功能。
检测流程：验证通过客户端软件对SE应用进行下载安装操作。
通过标准：若客户端软件基于SE模式，可实现SE应用下载安装功能。

5.3.3 SE 应用查询

检测目的：客户端软件可提供SE应用查询功能。
检测流程：验证通过客户端软件对SE应用进行查询操作。
通过标准：若客户端软件基于SE模式，可实现SE应用查询功能。

5.3.4 SE 应用卸载

检测目的：客户端软件可提供SE应用卸载功能。
检测流程：验证通过客户端软件对SE应用进行卸载操作。
通过标准：若客户端软件基于SE模式，可实现SE应用卸载功能。

5.4 消费交易

检测目的：客户端软件应能与远程支付系统交互，实现联机消费。
检测流程：对联机消费进行不同场景的测试。
通过标准：联机消费的测试结果符合功能设计要求。

5.5 远程圈存

检测目的：客户端软件应能通过与远程支付系统的交互，实现圈存功能。
检测流程：对圈存进行测试，记录输入输出。
通过标准：圈存的测试结果符合功能设计要求。

5.6 联机查询

检测目的：客户端软件应能通过与远程支付系统的交互，实现联机查询功能，如交易限额查询、交易明细查询等。
检测流程：对联机查询进行不同场景的测试。
通过标准：联机查询的测试结果符合功能设计要求。

5.7 脚本处理结果通知

检测目的：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。
检测流程：设计场景进行测试。
通过标准：客户端将SE的脚本处理结果通知到账户管理系统。

5.8 账户列表信息查询

检测目的：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。
检测流程：进行查询账户信息列表测试。
通过标准：客户端可以读取并显示账户信息列表。

5.9 账户选择

检测目的：在用户进行远程消费、远程圈存等交易之前，客户端应选择SE中相应应用的账号。
检测流程：进行查询账户信息列表测试。
通过标准：可以实现选择账户的功能。

5.10 默认账户设置

检测目的：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。
检测流程：使用客户端进行默认账户选择，并验证设置的结果。
通过标准：客户端可以选择、设置默认账户。

5.11 账户信息查询

检测目的：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。
检测流程：进行账户信息查询测试。
通过标准：客户端可以查询SE中制定账户的信息。

5.12 脱机余额查询

检测目的：客户端可以电子现金账户余额进行查询。
检测流程：进行脱机余额查询测试。
通过标准：客户端可以查询电子现金账户余额进行查询。

5.13 SE 参数设置

检测目的：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。
检测流程：进行SE参数设置测试。
通过标准：客户端可以查询和设置SE参数。

6 性能检测项

6.1 登录

检测目的：检查客户端软件登录后，移动终端的资源消耗是否影响移动终端应用正常运行。
检测流程：登录客户端软件后，监测客户端软件对CPU和内存等系统资源的占用情况，查看客户端软件和移动终端其它应用是否正常运行。
通过标准：满足正常使用。

6.2 支付

检测目的：检查执行支付应用时，移动终端的资源消耗是否影响移动终端应用正常运行。
检测流程：登录客户端软件后，执行支付业务，查看客户端软件和移动终端其它应用是否正常运行。
通过标准：满足正常使用。

6.3 交易查询

检测目的：检查执行交易查询时，移动终端的资源消耗是否影响移动终端应用正常运行。
检测流程：登录客户端软件后，执行交易查询业务，查看客户端软件和移动终端其它应用是否正常运行。
通过标准：满足正常使用。

7 安全检测项

7.1 人机交互安全

7.1.1 登录控制

检测目的：检查客户端软件登录时是否需要输入登录密码。
检测流程：验证客户端软件登录时是否需要输入登录密码。
通过标准：应输入登录密码，若用户选择记住登录密码时应进行风险提示。

7.1.2 支付控制

检测目的：检查客户端软件支付时是否需要输入支付密码。
检测流程：验证客户端软件支付时是否需要输入支付密码。
通过标准：应输入支付密码。

7.1.3 密码管理

检测目的：检查客户端软件中登录密码、支付密码等不同用途的密码是否采取不同安全级别的管理。
检测流程：检查开发文档中系统存在的密码种类，以及每种密码的存储方式及安全保护机制。
检查客户端软件中是否区分登录密码和支付密码。
查看用户设置登录密码和支付密码时是否提示不能设为相同。
查看客户端软件是否限制用户不能将登录密码和支付密码设为相同。
通过标准：应有独立的支付密码，并保证支付密码和登录密码不同。

7.1.4 认证方式

检测目的：检查客户端软件在大额支付、重要信息修改等关键业务操作时是否采用除密码以外的安全认证机制。
检测流程：检查开发文档中客户端软件包含的用户身份认证方式。

检查客户端软件在大额支付或重要信息修改时，是否采用除密码以外的其它身份认证方式（短信验证码、动态口令卡、移动口令牌、移动数字证书等）。

通过标准：大额支付及重要信息修改等操作应采用双因素认证机制。

7.1.5 鉴别失败处理

检测目的：检查客户端软件是否提供连续鉴别失败处理功能。

检测流程：检查开发文档中客户端软件是否提供连续鉴别失败处理功能。

验证其是否有连续鉴别失败锁定功能。

通过标准：连续鉴别失败次数超过阈值应进行锁定。

7.1.6 重鉴别

检测目的：检查客户端软件是否具备会话超时处理机制，会话超时后应重鉴别。

检测流程：检查开发文档中客户端软件是否提供会话超时重鉴别功能，确认其超时阈值。

尝试空闲操作达到设置阈值，验证是否提供重鉴别功能。

通过标准：闲置时间超过阈值后应重鉴别。

7.1.7 移动终端交易异常处理

检测目的：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。

检测流程：查看交易异常时移动终端的处理情况。

通过标准：交易处理异常后向用户提示出错信息。

7.2 软件安全

7.2.1 程序异常检测

检测目的：检查客户端软件程序配置文件被篡改后，是否具备相应的安全检测和预警措施。

检测流程：检查开发文档中关于客户端软件程序异常检测的要求，确认启动程序异常检测功能的条件。

尝试对客户端软件的配置文件进行篡改。

通过标准：客户端程序应能对程序异常进行检测并预警提示。

7.2.2 数据有效性校验

检测目的：检查客户端软件是否提供数据有效性校验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

检测流程：检查开发文档中关于客户端软件数据有效性校验的要求。

尝试输入异常字符，验证数据有效性校验功能。

通过标准：客户端软件对输入的异常数据应进行校验。

7.2.3 程序调用

检测目的：检查客户端软件接口和数据的封装性，确保客户端软件不被其它程序非授权调用。

检测流程：检查开发文档中关于客户端软件接口的封装性要求。

通过其它程序尝试调用客户端软件的接口。

通过标准：对客户端软件接口进行合理的封装，使其接口无法被其它程序非授权调用。

7.2.4 反编译

检测目的：检查客户端软件是否采取反逆向工程保护措施。
检测流程：检查开发文档中关于客户端软件的反编译要求和实现机制。
尝试进行反编译操作，验证是否成功。
通过标准：应具有抗逆向分析防护措施。

7.3 数据安全

7.3.1 数据录入

7.3.1.1 敏感数据显示

检测目的：检查输入用户口令等敏感信息时，客户端软件界面是否为非明文显示。
检测流程：检查开发文档中关于敏感信息显示的规定。
查看用户通过客户端软件登录时输入的登录密码是否以明文的方式显示。
查看用户通过客户端软件进行支付操作时，输入的支付密码是否以明文方式显示。
若客户端软件中存在其它需要用户输入的敏感数据，则查看是否以明文的方式显示。
通过标准：非明文显示或逐字非明文显示。

7.3.1.2 敏感数据截获

检测目的：检查在用户输入过程中，用户输入的数据应不被移动终端的其它设备或程序非授权获取。
检测流程：检查开发文档中有关敏感信息防截获的安全机制，评估其安全机制是否可行。
对客户端软件进行测试，尝试截获用户输入的敏感数据。
通过标准：采用客户端程序自行设计的专用软键盘等安全措施，防止敏感数据被截获。

7.3.1.3 数据篡改

检测目的：检查用户输入的数据在发送前应不被移动终端的其它设备或程序篡改。
检测流程：检查开发文档中有关重要数据防篡改的安全机制，评估其安全机制是否可行。
对客户端软件进行测试，判断用户输入的重要数据能否被其它程序篡改。
通过标准：采用数据防篡改机制或其它辅助机制防止重要数据被篡改所造成的风险。

7.3.2 数据访问

检测目的：检查敏感数据是否仅供授权用户或应用组件访问。
检测流程：查看客户端软件访问移动终端操作系统的访问方式和权限设置。
通过标准：限制访问存储于移动终端操作系统重要数据。

7.3.3 数据存储

7.3.3.1 敏感数据存储

检测目的：检查客户端软件是否保留最少的敏感数据，限制数据存储量和保留时间，达到恰好能满足法律、管理规定和业务需要的程度。
检测流程：检查开发文档中关于移动终端操作系统敏感数据的保留情况，保留的空间和时间是否进行限制，并明确保留的位置。
检查确认客户端软件关于敏感数据的存储情况。
通过标准：仅存储最少的敏感数据，口令等敏感数据应加密存储。

7.3.3.2 用户身份认证信息存储安全

检测目的：检查客户端软件应不保存非必须的用户身份认证信息，如银行卡磁道信息、CVN、CVN2、交易密码等。

检测流程：检查开发文档中关于移动终端操作系统中用户的身份认证信息保留情况。
检查确认客户端软件关于用户身份认证信息的存储情况。

通过标准：不保存非必须的用户身份认证信息。

7.3.3.3 敏感信息显示

检测目的：检查显示敏感信息（如账户号码、身份证号等）时是否对敏感信息全部或部分字段予以屏蔽。

检测流程：查看开发文档，客户端软件关于账户号码、身份证号码等显示是否采取安全措施。
案例验证确认账户号码、身份证号码等显示时的安全措施的有效性。

通过标准：对账户号码、身份证号码等敏感信息进行全部或部分屏蔽。

7.3.3.4 残留敏感信息保护

检测目的：检查客户端软件在使用过敏感信息后，内存中是否仍然有残留敏感信息。

检测流程：检查开发文档中客户端软件防止内存中残留敏感信息的措施。
在移动终端上输入敏感信息并完成相应功能的操作后，测试验证敏感信息的残留情况。

通过标准：内存无敏感信息残留。

7.3.4 数据传输

7.3.4.1 远程数据传输保密性

检测目的：检查敏感数据远程传输时是否采取加密措施。

检测流程：查看是否采取了有效措施以确保敏感数据的保密性。
确认数据的加解密方式、加密密钥长度及密钥管理方式。
尝试截获远程敏感数据的传输，验证其是否采取安全加密措施。

通过标准：应对敏感数据进行远程加密传输。

7.3.4.2 本地数据传输保密性

检测目的：检查敏感数据和本地其它实体间传输时是否采取加密措施。

检测流程：查看开发文档中关于敏感数据在客户端软件和本地其它实体间传输时采取的保密措施。
确认数据的加解密方式、加密密钥长度及密钥管理方式。
尝试截获本地敏感数据的传输，验证其是否采取安全加密措施。

通过标准：应对敏感数据进行本地加密传输。

7.3.4.3 数据传输完整性

检测目的：检查是否采取有效措施以确保支付数据的完整性。

检测流程：检查开发文档中关于客户端软件对支付数据完整性保护措施的要求。
验证客户端软件采取的完整性保护措施。

通过标准：应采取MAC等完整性保护措施。

7.4 通信安全

7.4.1 网络通讯协议

检测目的：检查客户端软件和远程服务器间是否使用SSL/TLS或IPSec等安全协议进行通信。若采取WAP模式，则检查客户端软件是否支持WTLS协议。

检测流程：检查开发文档中关于网络通讯协议的加密要求。

查看SSL/TLS等协议版本。

验证加密协议的使用情况。

通过标准：采取的安全协议应包括但不限于SSL/TLS或IPSec；应采用SSL3.0/TLS1.0以上；WAP支持WTLS。

7.4.2 安全认证

检测目的：检查客户端软件的安全协议层是否对客户端和远程服务器双方的身份进行认证。

检测流程：检查开发文档中关于安全协议层的安全认证要求。

查看服务端对客户端的身份认证方式，包括提供对手机号码绑定或移动终端标识符绑定等认证方式，并验证其有效性。

查看客户端对服务器端的身份认证方式，包括提供服务器证书，并验证其有效性。

通过标准：应实行双向认证。

7.4.3 抗抵赖

检测目的：检查客户端软件是否可保证支付内容的不可抵赖性。

检测流程：检查开发文档中关于客户端软件的通信抗抵赖要求。

确认并验证客户端软件对支付内容的抗抵赖机制。

通过标准：可采取签名机制等抗抵赖措施。

参 考 文 献

[1] JR/T 0068-2012　网上银行系统信息安全通用规范