ICS 03.060
CCS A 11

团 体 标 准

T/NIFA 9-2021

移动金融客户端应用软件安全检测规范

Testing specification on financial mobile application software security

2021-4-22 发布　　2021-4-22 实施

中国互联网金融协会
中国支付清算协会　发布

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》和GB/T 20004.1—2016《团体标准化 第1部分：良好行为指南》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国互联网金融协会、中国支付清算协会共同提出。

本文件由中国互联网金融协会归口。

本文件主要起草单位：中国互联网金融协会、中国支付清算协会、中国工商银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、中国建设银行股份有限公司、交通银行股份有限公司、中国邮政储蓄银行股份有限公司、招商银行股份有限公司、中国民生银行股份有限公司、中信银行股份有限公司、中国银联股份有限公司、农信银资金清算中心有限责任公司、中移电子商务有限公司、天翼电子商务有限公司、联通支付有限公司、支付宝（中国）网络技术有限公司、浙江网商银行股份有限公司、财付通支付科技有限公司、鼎铉商用密码测评技术（深圳）有限公司、京东数字科技控股股份有限公司、京东智联云、拉卡拉支付股份有限公司、北京中金国盛认证有限公司、中国网络安全审查技术与认证中心、银行卡检测中心（国家金融 IC 卡安全检测中心）、中国金融电子化公司、中金金融认证中心有限公司、信息产业信息安全测评中心、工业和信息化部计算机与微电子发展研究中心（中国软件测评中心）、国家应用软件产品质量监督检测中心（北京软件产品质量检测检验中心）、航天中认软件测评科技（北京）有限责任公司、中互金认证有限公司、奇安信科技集团股份有限公司、科大讯飞股份有限公司、平安保险等单位。

本文件主要起草人：朱勇、李健、单剑锋、于圆、张赫、田然、任家琪、唐静、王立飞、辛路、王新华、苏莉、刘燕青、陈波、马国光、刑桂伟、于沛、侯晓晨、何一江、薛宇、陈旭东、相海飞、牛康欣、张宇、白帆、黄潇拉、马咪、朱翔宇、刘占明、廖渊、赵鹏、付南、黎马亮、袁丽欧、费会、汪毅、李志蓉、廖勤思、周晶、焦伟、任震、宋铮、姜志辉、吴永强、蒋增增、李振、邹超、李玲、魏晓征、曾辉、王晴晴、张健、陈伟、王峰、申永波、王玲、渠韶光、李博文、张文博、李宇、郭大圣、高峰、曹中全、董晶晶、冀乃杰、赵亮、徐鹏、于泉、张鹏、王焱、孙明慧、史汝辉、李增局、林宝晶、蒯天祥、刘浩、王盈语、向阳等。

移动金融客户端应用软件安全检测规范

1 范围

本文件规定了移动金融客户端应用软件的安全要求，以及客户端应用软件设计、开发、维护和发布的管理要求。

本文件适用于检测机构开展移动金融客户端应用软件安全检测使用，并为相关单位开展客户端应用软件设计、开发、集成和维护等工作提供参考。本文件也适用于检测认证机构对相关产品、应用系统进行安全性和标准符合性测试和认证。

客户端应用软件分为资金交易类、信息采集类和资讯查询类。本文件对每类软件的适用范围参考附录A：应用软件测试范围。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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—2019 移动金融客户端应用软件安全管理规范

JR/T 0171—2020 个人金融信息保护技术规范

3 术语与定义

本文件没有需要界定的术语和定义。

4 缩略语

下列缩略语适用于本文件。

APP：客户端应用软件（Application software）

URI：统一资源标识符（Uniform Resource Identifier）

TEE：可信执行环境（Trusted Execution Environment）

SDK：软件开发工具包（Software Development Kit）

SE：安全单元（Secure Element）

5 客户端应用软件安全要求

5.1 身份认证安全

5.5.1 认证方式

检测目的：

检测客户端身份认证方式及所采用认证要素的安全性。

基本要求：

检测方法：

1) 检查开发文档中客户端应用软件包含的用户身份认证方式、辅助认证方式，对需要用户身份认证的过程进行操作，例如进行客户端登录、支付等。使用客户端应用软件进行登录，检查其登录时所采用的认证要素，确定其是否采用合适的认证要素；
2) 使用客户端应用软件进行身份认证操作时，如：登录和交易操作，检查其在执行这些操作时所需身份认证的认证要素或认证要素组合，确认身份认证要素是否相互独立；
3) 使用客户端应用软件进行如大额交易等操作时，检查客户端应用软件所采用的用户身份认证方式，是否符合相关业务管理要求；
4) 若手势密码、短信验证码、生物特征信息作为认证要素或认证要素组合中的一种时，检查这些类型认证要素的安全性措施是否符合JR/T 0092-2019中5.1.1 d)条款的要求；
5) 若采用图形验证码作为认证的辅助要素，检查图形验证码相关限制性措施和生成方式，检查客户端源文件中是否包含图形验证码文本内容；
6) 检查客户端应用软件进行用户身份认证时，图形验证码是否可单独成为身份验证通过要素；
7) 在新设备首次登录时，查看客户端是否采用了两种或两种以上的要素对用户身份进行认证。

通过标准：

1) 客户端应用软件登录时采用了适宜的认证要素，包括但不限于口令、短信验证码、手势密码、生物特征识别、手机号与 SIM 卡标识信息匹配等方式；
2) 采用的身份认证要素相互独立，即部分要素的损坏或者泄露不应导致其他要素损坏或者泄露；
3) 客户端应用软件交易时满足相关业务管理要求对用户身份进行认证，如对于大额资金交易，客户端采用了两种或两种以上要素对用户身份进行认证等；
4) 手势密码为至少连续不间断的 4 个点；短信验证码应仅可成功使用一次，且仅在规定时间内使用，短信验证码具备长度和随机性的要求，短信验证码所在的短信内容中，告知了用户短信验证码的发送方、用途以及有效时间；声纹要素符合 JR/T 0164—2018 要求；其他生物特征认证要素，符合国家、金融行业标准和相关信息安全管理要求，能够防止非法存储、复制和重放；
5) 图形验证码具有使用时间限制并仅能使用一次，图形验证码由服务器生成，客户端源文件中不包含图形验证码文本内容；
6) 图形验证码未作为独立的身份认证要素；
7) 在新设备首次登录时，采用了两种或两种以上的要素对用户身份进行认证。

增强要求：

检测方法：

1) 使用客户端应用软件执行登录操作，检查是否采用两种或两种以上的要素对用户身份进行认证；
2) 客户端软件在完成身份认证后，客户端置于系统（终端）后台，超过一定时间未操作，再次被唤醒切换到前台，检查其是否采取措施要求对用户身份再次认证。

通过标准：

1) 客户端应用软件登录采用了两种或两种以上的要素对用户身份进行认证；
2) 在用户身份认证后，客户端应用软件进入系统（终端）后台时，超过设定时限后被唤醒切换到前台，需要对用户身份进行重新认证。

5.5.2 认证信息安全

5.1.2.1 安全输入

检测目的：

检查使用客户端应用软件输入认证信息时是否具有安全性措施。

基本要求：

检测方法：

1） 检查开发文档中客户端应用软件对于输入账户登录密码、银行卡支付密码和网络支付交易密码等认证信息时提供的安全性措施；

2） 使用客户端应用软件输入账户登录密码、银行卡支付密码和网络支付交易密码等认证信息时，检查客户端应用软件在输入时是否采用了替换输入框原文、逐字符加密、字符加密、防范键盘窃听、自定义软键盘等措施防止攻击者获取输入信息的明文，并使用内存扫描工具等检查是否可以获取输入的密码明文。

通过标准：

客户端应用软件在输入账户登录密码、银行卡支付密码和网络支付交易密码等认证信息时采用了替换输入框原文、逐字符加密、字符加密、防范键盘窃听、自定义软键盘，或者通过其他方式保证攻击测试无法获取输入信息的明文。

增强要求：

检测方法：

通过客户端应用软件输入卡片验证码、卡片有效期、银行卡账号、身份证号、手机号等信息，检查其是否对信息提供了安全防护功能。

通过标准：

客户端应用软件提供了客户输入如卡片验证码、卡片有效期、银行卡账号、身份证号、手机号等信息的安全防护功能。

5.1.2.2 个人金融信息展示

检测目的：

检查客户端应用软件在个人金融信息与支付敏感数据显示时是否具有安全性措施。

基本要求：

检测方法：

1） 通过客户端应用软件输入口令，检查客户端是否使用同一特殊字符方式脱敏或屏蔽显示；

2） 通过客户端应用软件输入银行卡密码和网络支付交易密码，检查客户端是否明文显示输入银行卡密码和网络支付交易密码；

3） 查看未登录状态下，客户端软件是否显示用户鉴别信息；

4） 查看已登录状态下，客户端软件是否显示用户鉴别信息；查看银行卡号、手机号码、证件类识别标识或其他识别标识信息的关键信息是否脱敏或屏蔽显示，用户是否可以选择脱敏或屏蔽显示，若上述信息需明文显示，查看客户端软件是否对用户身份进行验证；

5） 涉及其他信息主体的信息时，查看是否进行屏蔽展示，当满足如下条件之一时可不脱敏：

- 其他方主动发起的活动包含的信息，如其他方发起交易、收付款；
- 与其他方已建立信任关系（间接授权），如向其他方收款，其他方已付款；向其他方申请代付，其他方同意付款或者其他方在自己业务应用范围内的联系人；
- 其他法律法规要求的情况。

通过标准：

1） 客户端应用软件的口令框应默认脱敏或屏蔽显示，且脱敏或屏蔽显示时使用同一特殊字符代替；

2） 客户端应用软件未明文显示银行卡密码和网络支付交易密码；

3） 处于未登录状态时，不应展示与个人金融信息主体相关的用户鉴别类别信息；

4) 除银行卡有效期外，用户鉴别类别信息不应明文展示；对于银行卡号、手机号码、证件类识别标识或其他识别标识信息的关键信息等可以直接或组合后确定个人金融信息主体的信息应进行屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应进行用户身份验证；
5) 涉及其他信息主体的信息时，客户端应用软件对显示的信息进行了屏蔽展示。

5.5.3 认证失败处理

检测目的：
客户端应用软件是否提供了有效的认证失败处理机制。
基本要求：
检测方法：
1) 检查开发文档中，客户端应用软件是否提供认证失败处理机制；
2) 检查客户端应用软件在认证用户身份时是否具有认证失败处理机制，如是否采取结束会话、限制非法登录次数和自动退出等措施；
3) 检查客户端应用软件在认证失败后，提供的认证失败信息是否模糊，是否包含用户的账号、交易金额等敏感数据。

通过标准：
1) 客户端应用软件具有合理的认证失败处理功能，如采取结束会话、限制非法登录次数和自动退出等措施；
2) 客户端在提示客户认证失败时，模糊错误提示信息，错误提示信息未泄露用户账号、交易金额等敏感数据。

5.5.4 密码的设定与重置

检测目的：
检查客户端应用软件对于密码设置与重置时是否满足安全要求。
基本要求：
检测方法：
1) 检查开发文档中客户端应用软件包含的用户密码生成方式和密码复杂度校验功能，以及密码重置的身份校验方式；
2) 使用客户端软件进行密码设置时，验证密码复杂度校验功能是否有效，查看是否可以设置简单密码；
3) 使用客户端应用软件进行注册，查看注册过程中，客户端应用软件登录密码和交易密码设置方式，若具有初始登录密码与初始交易密码，则在注册完成后，首次登录时检查是否强制修改初始密码；
4) 使用客户端应用软件进行修改密码，检查在修改密码前是否需要对用户身份进行重新验证；
5) 使用客户端应用软件进行修改密码，检查是否需要输入原密码且是否具有原密码输入错误次数限制；
6) 使用客户端应用软件进行修改密码，检查新密码是否可设置与原密码相同；
7) 使用客户端应用软件进行密码重置，检查是否采取有效措施对身份进行验证。

通过标准：
1) 客户端应用软件提供了密码复杂度校验功能，保证用户设置的密码达到一定的强度，不可设置简单交易密码（如“111111”、“123456”）；
2) 登录密码应满足以下两种复杂度要求之一：

- 长度至少 8 位且要求至少包含数字、大写字母、小写字母以及特殊字符中的两种或两种以上组合；
- 登录密码至少 6 位，具有一定的复杂度要求，不可设置简单密码，后台系统应具有相应的风控措施对登录操作进行风险控制；

3) 限制了用户使用初始登录密码与初始交易密码，若设置初始密码，需强制用户在首次登录后修改初始密码；
4) 在修改密码前，对用户身份进行了重新验证；
5) 修改密码时对原密码输入错误次数进行了限制；
6) 修改密码时新密码不可与原密码相同；
7) 在密码重置时，使用了例如短信验证码、用户注册信息校核等方式，对用户身份进行校验。

增强要求：

检测方法：

1) 检查客户端软件是否配合服务器提供了密码复杂度校验的功能，查看是否可以设置与客户个人信息相似度过高的交易密码；
2) 使用客户端应用软件修改密码或重置密码，检查是否采用两种或两种以上要素进行身份认证；
3) 检查客户端应用软件中是否采取有效措施提醒客户避免设置与常用软件（如社交软件）、网站（如社交平台、论坛）相同或相似的用户名和密码组合；采取有效措施引导客户设置独立的支付密码。

通过标准：

1) 客户端应用软件应配合服务提供了密码复杂度校验功能，保证用户设置的密码达到一定的强度，不可设置简单交易密码（如“111111”、“123456”）或与客户个人信息（如出生日期、证件号码、手机号码等）相似度过高的交易密码；登录密码应满足长度至少 6 位且要求至少包含数字、大写字母、小写字母以及特殊字符中的两种或两种以上组合；
2) 在进行修改密码或密码重置时，采用了如数字证书、生物特征信息等两种或两种以上要素进行身份认证；
3) 客户端采取了有效措施提醒客户避免设置与常用软件（如社交软件）、网站（如社交平台、论坛）相同或相似的用户名和密码组合，并采取有效措施引导客户设置独立的支付密码。

5.2 逻辑安全

5.5.1 逻辑安全设计

检测目的：

检查客户端应用软件安全保障功能的流程设计、业务功能是否存在逻辑漏洞；检查客户端应用软件调试或测试结束后是否及时删除敏感数据。

基本要求：

检测方法：

1) 查看开发文档中与认证、校验等安全保障功能的流程以及资金有关业务功能的逻辑安全设计；
2) 综合多种逻辑攻击手段，尝试绕过客户端软件认证、校验等安全保障功能；
3) 综合多种逻辑攻击手段，尝试对资金有关业务功能进行劫持或篡改。

通过标准：

1) 对于认证、校验等安全保证功能的流程设计合理，未发现逻辑漏洞的出现，认证流程无法被绕过；
2) 对于交易处理功能逻辑设计合理，未发现逻辑漏洞；
3) 客户端代码不存在调用具有已知安全漏洞的函数，不存在敏感数据硬编码。

5.5.2 软件权限控制

检测目的：

检查客户端应用软件向移动终端操作系统申请权限时是否遵循最小化原则以及申请方式是否合理。

基本要求：

检测方法：

1) 查看开发文档中关于客户端软件的权限申请设计；
2) 检查客户端应用软件申请的操作系统权限是否与具有的功能相关；
3) 客户端应用软件在申请可收集个人信息的权限时，客户端应用软件是否逐一同步向用户告知申请权限的目的，目的是否明确且清晰；
4) 查看用户拒绝某个权限申请后，查看客户端应用软件是否存在频繁征求用户同意、干扰用户正常使用的情况；
5) 查看用户拒绝非必要权限的申请后，客户端应用软件是否拒绝提供业务功能。

通过标准：

1) 客户端应用软件在申请可收集个人信息的权限时，遵循了最小化原则；
2) 客户端应用软件在申请可收集个人信息的权限时，逐一同步告知了用户申请权限的目的，目的表述明确且清晰；
3) 用户拒绝客户端应用软件的某权限申请后，客户端应用软件最多再提示一次，用来解释该权限的申请原因，以及无此权限的后果。若用户坚持拒绝后，则客户端应用软件不应频繁向用户申请该权限，但支持 App 正常运行，或用户主动选择使用的某一具体功能触发征得同意的动作，不属于频繁干扰情形；
4) 用户拒绝非必要权限的申请后，客户端应用软件应正常提供业务功能。

5.5.3 风险控制

检测目的：

1) 检查客户端应用软件是否设计了合理的登录风险控制策略；
2) 检查客户端应用软件是否设计了合理的交易风险控制策略；
3) 检查客户端是否配合业务交易风险控制策略，以安全的方式将相关信息上送至风险控制系统。

基本要求：

检测方法：

1) 检查开发设计文档中是否有明确的账户登录风险控制策略、交易风险策略；
2) 登录客户端应用软件后，闲置一段时间，查看客户端是否自动退出登录状态，查看其退出机制是否与其设计一致；
3) 执行客户端应用软件多点登录，查看是否具有提示登录信息或退出先登录的账户等方式，查看其方式是否与其设计一致；
4) 长时间未登录客户端应用软件，查看在重新登录时，是否增大认证强度，并查看其方式是否与设计文档一致；
5) 执行支付、交易操作，在执行付款前停止操作一段时间，查看交易是否自动终止；
6) 执行不同金额的资金交易，查看客户端应用软件是否对交易进行限额控制，检查其策略是否与设计文档一致；
7) 根据设计策略，执行不同金额的资金交易业务场景，检查交易时执行的不同的身份认证方式，检查其策略是否与管理规定或设计一致；

8） 检查开发文档中是否明确要求客户端需上送交易风险控制所需的相关特征信息。若客户端需上送该类信息，开发文档中应对该类信息进行识别，并就上送策略与安全保护要求进行说明。若客户端需上送信息用于交易风险控制，则对其上送信息的安全防护机制进行安全性检测。

通过标准：

1） 采取了合理的登录风险控制策略，包括但不限于：

- 当用户闲置在线状态超出时限时，采取了合理的账户登录超时控制策略；
- 合理的多点登录策略，如提示登录信息或退出先登录的账户等策略；
- 合理的长期未登录控制策略，当用户长时间未登录时，综合考虑风险情况，增大认证强度；

2） 采取了合理的交易风险控制策略，包括但不限于：

- 针对不同的资金交易金额，采取了合理的身份认证策略；
- 针对不同的资金交易业务场景，采取了合理的策略，比如：限额控制策略、时限控制策略等；

3） 客户端应用软件应配合业务交易风险控制策略，以安全的方式将相关信息上送至风险控制系统。

5.5.4 回退处理

检测目的：

检查客户端应用软件回退处理机制的安全性。

基本要求：

检测方法：

使用客户端应用软件进行交易，检查在交易失败后或交易完成前用户主动撤销交易时，客户端应用软件是否能返回到交易前的有效状态。

通过标准：

交易过程中如遇交易失败或在交易完成前如用户进行撤销操作，能够返回到交易前的有效状态。

5.5.5 异常处理

检测目的：

检查客户端应用软件异常处理机制的安全性。

基本要求：

检测方法：

1） 模拟客户端应用软件发生故障，查看其给出的异常信息中是否包含用户敏感数据；

2） 模拟客户端应用软件出现交易异常，查看向客户提示出错等信息中是否包含用户敏感数据。

通过标准：

1） 客户端应用软件发生故障产生的异常信息，未出现泄露用户敏感数据的情形；

2） 当交易出现异常时，客户端应用软件向客户提示出错等信息，未出现泄露用户敏感数据的情形。

5.3 安全功能设计

5.5.1 组件安全

检测目的：

检查客户端软件使用的系统组件与第三方组件是否存在已知安全问题。

基本要求：

检测方法：

1） 查看开发文档中对系统组件、第三方组件的设计内容，查看其组件版本与来源声明：

- 检查客户端软件代码中调用系统组件与第三方组件的信息，查看其系统组件与第三方组件是否包含已知的漏洞；
- 综合使用动态调试、进程注入等手段验证其系统组件与第三方组件是否可被已知漏洞利用；

2) 查看第三方组件相关文档，验证其组件收集的客户端应用软件信息以及个人信息是否与其文档中允许采集的信息一致；
3) 验证第三方组件在采集客户端应用软件信息和个人信息前，是否获取了用户授权。

通过标准：

1) 客户端应用软件未使用存在已知漏洞的系统组件与第三方组件；
2) 客户端应用软件在使用第三方组件时，不存在第三方组件未经授权收集客户端应用软件信息和个人信息的情况。

5.5.2 接口安全

检测目的：

1) 检查客户端软件是否对软件接口进行保护；
2) 检查客户端软件是否对传入的 URI 进行校验与安全处理；
3) 当客户端软件需要与 TEE、SE 结合使用时，检查是否使用了安全的接口。

基本要求：

检测方法：

1) 查看开发文档中是否包括对接口安全的需求与实现；
2) 检查客户端软件代码中的软件接口代码实现，使用技术手段对客户端软件接口进行授权与非授权的调用；
3) 检查客户端软件代码中对传入 URI 的校验代码实现，使用技术手段检查其是否对 URI 的合理性进行校验，是否具备异常输入容错机制；
4) 若需要与 TEE、SE 结合使用，则查看开发文档，查看接口的调用方式是否安全。

通过标准：

1) 客户端应用软件对软件接口进行保护，其他应用无法对客户端应用软件接口进行非授权调用；
2) 客户端应用软件对传入的 URI 进行校验与安全处理，不存在客户端应用软件因 URI 导致的运行异常或操作异常；
3) 当客户端应用软件需要与 TEE、SE 结合使用时，使用安全的接口。

5.5.3 抗攻击能力

检测目的：

1) 检查客户端软件是否可以抵御静态分析、动态调试；
2) 检查客户端是否使用技术手段对客户端软件进行安全保护；
3) 检查客户端软件是否具有保持自身完整性、真实性，防止篡改及注入的功能；
4) 检查客户端应用软件是否进行签名，签名方案是否安全，签名证书能否有效标识应用软件的来源和发布者；
5) 检查安全输入控件是否具有抵御一定程度攻击的能力；
6) 检查客户端软件是否具有已知漏洞的防范能力。

基本要求：

检测方法：

1) 检查开发文档中是否包含对客户端抗攻击能力的需求分析与设计实现；

2) 综合使用代码脱壳、静态分析、动态调试、代码注入等手段，尝试对客户端软件进行逆向工程；
3) 综合使用代码注入、重编译、界面劫持等手段尝试对客户端软件进行篡改、仿造；
4) 综合使用反编译等手段查看客户端软件的签名证书信息以及签名方式是否为存在风险；
5) 综合使用代码注入、动态调试、进程 HOOK 等手段，尝试获取安全输入控件输入的信息；
6) 综合使用页面篡改、网页源代码暴露、穷举登录尝试、重放攻击、SQL 注入、跨站脚本攻击、钓鱼、木马以及任意文件上传、下载等手段，尝试对客户端软件进行攻击。

通过标准：

1) 客户端应用软件具备基本的抗攻击能力，能抵御静态分析、动态调试等操作；
2) 客户端代码使用例如代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护；
3) 客户端应用软件安装、启动、更新、执行时对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力；
4) 客户端软件使用了安全的方式对客户端进行了签名，且签名文件可以有效的标识软件来源和发布者；
5) 客户端应用软件如使用安全输入控件，该控件具备抵御一定程度攻击的能力；
6) 客户端软件具有 H5 页面篡改、网页源代码暴露、穷举登录尝试、重放攻击、SQL 注入、跨站脚本攻击、钓鱼、木马以及任意文件上传、下载等已知漏洞的防范能力。

增强要求：

检测方法：

对安全输入控件进行调试时，检查安全输入控件是否提示自身正在被调试。

通过标准：

客户端应用软件如使用安全输入控件，该控件具备检测自身是否正在被调试的能力，并采取适当的风控措施，如给予用户风险提示。

5.5.4 客户端应用软件环境检测

检测目的：

检查客户端应用软件是否具有检测运行环境的能力，是否在检测到运行环境处于root或者已越狱、非可信环境（如模拟器或虚拟机）等异常环境时向后台系统反馈设备环境信息等。

基本要求：

检测方法：

1) 查看开发文档中是否对运行环境检测进行了说明，在处于异常环境时，客户端应用软件是否会向后台反馈设备环境信息；
2) 在处于root或已越狱、非可信环境（如模拟器或虚拟机）等异常环境时，运行客户端应用软件，检查客户端应用软件上送服务器的数据中是否包含设备环境信息等。

通过标准：

客户端应用软件在运行时具备对运行环境的检查能力，检查的范围可包括：系统是否越狱或root、程序运行环境是否可信（例如是否运行在模拟器或虚拟机中）等，并能向后台系统反馈设备环境信息等。

5.4 密码算法及密钥管理

5.5.1 密码算法

检测目的：

1) 检查客户端应用软件是否使用密码算法对资金有关交易或重要业务操作进行保护；

2) 检查客户端应用软件使用的密码算法、密钥长度及密钥管理方式是否符合国家密码主管部门的要求。

基本要求：

检测方法：

1) 检查开发文档中是否包含对密码算法使用、来源等信息的详细描述；
2) 对密钥管理、支付交易等认证信息、交互信息以及敏感信息进行分析，查看是否对上述内容进行了加密保护；
3) 查看如使用以下密码算法，密钥长度是否满足下列要求：
   - 对称密码算法：SM4、AES、3DES 算法的密钥长度满足 128 位及以上；
   - 非对称密码算法：SM2，使用 256 位及以上的密钥长度；RSA，使用 2048 位及以上的密钥长度；
   - 散列算法：SM3、SHA256 及以上。

通过标准：

1) 客户端应用软件使用密码算法对资金有关交易或重要业务操作进行了保护；
2) 密码算法、密钥长度及密钥管理方式符合国家密码主管部门的要求。

5.5.2 密钥管理

检测目的：

1) 密钥在传输过程中是否使用密码算法对密钥进行保护；
2) 随机生成的密钥是否具有一定的随机性与不可预测性；
3) 密钥是否加密存储，密钥储存位置和形式是否安全。

基本要求：

检测方法：

1) 检查开发文档中是否包含对密钥管理过程、交易过程的密钥生成、传输及使用的详细描述；
2) 查看传输过程中的密钥是否进行了加密；
3) 检查客户端软件代码中有关密钥生成的代码部分，查看密钥生成是否使用了随机算法，且随机算法未存在公开漏洞；
4) 查看开发文档中密钥管理文档，判断密钥存储位置和形式是否安全可靠，并检查密钥是否进行了加密存储。

通过标准：

1) 密钥在传输过程中使用密码算法对密钥进行了保护；
2) 随机生成的密钥具有一定的随机性与不可预测性；
3) 密钥加密存储，并且密钥储存位置和形式安全。

5.5 数据安全

5.5.1 数据获取

5.5.1.1 个人金融信息收集

检测目的：

金融业机构应遵循合法、正当、必要的原则，向个人金融信息主体明示收集与使用个人金融信息的目的、方式、范围和规则等，获得个人金融信息主体的授权同意。

基本要求：

检测方法：

1） 查看客户端软件是否通过欺诈、诱骗，或以默认授权、功能捆绑等方式误导强迫个人金融信息主体提供个人金融信息，或违反与用户的约定收集使用个人金融信息的情况；
2） 查看客户端软件是否隐瞒金融产品或服务所具有的收集个人金融信息的功能；
3） 查看客户端软件是否收集法律法规与行业主管部门有关规定明令禁止收集的个人金融信息；
4） 查看客户端软件是否遵循最小化要求，收集个人金融信息的目的应与实现和优化金融产品或服务、防范金融产品或服务的风险有直接关联；
5） 查看客户端软件收集个人金融信息前，是否向个人金融信息主体明确告知金融产品（包含集成的第三方组件）需收集的个人金融信息类别，以及收集、使用个人金融信息的规则，是否征得个人信息主体的自主选择同意；
6） 查看首次启动时，客户端是否引导用户查阅隐私政策，使用权限监控工具，查看客户端是否在获得用户的明示同意后收集个人金融信息，查看收集个人信息频度是否正常；
7） 查看隐私政策的内容是否容易阅读和理解，是否存在字体过小过密、模糊不清等给用户造成难以阅读和理解的情况；
8） 查看在进入客户端应用软件主页面后，点击几次方可访问到隐私政策等个人金融信息的收集使用规则；
9） 查看隐私政策中是否包含隐私政策更新的原因类型以及用户如何访问更新后的隐私政策的方法和途径；
10） 若客户端具有利用用户个人信息和算法向个人推送信息的功能，则查看客户端是否具有关闭该服务的选项；
11） 查看隐私政策中是否包含机构处理用户投诉、更正、删除个人信息以及注销用户的人工处理时限，时限是否超过 15 个工作日；
12） 个人金融信息控制者是否针对隐私政策内容进行了明确要求，隐私政策内容是否合法合规。

通过标准：

1） 客户端应用软件未欺诈、诱骗，或以默认授权、功能捆绑等方式误导强迫个人金融信息主体提供个人金融信息。客户端软件未违反与用户的约定收集使用个人金融信息；
2） 客户端应用软件未隐瞒金融产品或服务所具有的收集个人金融信息的功能；
3） 客户端应用软件未收集法律法规与行业主管部门有关规定明令禁止收集的个人金融信息；
4） 收集个人金融信息应遵循最小化要求，收集个人金融信息的目的应与实现和优化金融产品或服务、防范金融产品或服务的风险有直接关联。直接关联是指无该个人金融信息参与无法实现前述目的；
5） 收集个人金融信息前，应向个人金融信息主体明确告知金融产品（包含集成的第三方组件）需收集的个人金融信息类别，以及收集、使用个人金融信息的规则（如：收集和使用个人金融信息的目的、收集方式、自身的数据安全能力、对外共享、转让、公开披露的规则、投诉与申诉的渠道及响应时限等），并获得个人金融信息主体的明示同意；
6） 客户端应用软件首次启动时，应采取技术措施（如弹窗、明显位置 URL链接等），引导个人金融信息主体查阅隐私政策，并获得其明示同意后，开展有关个人金融信息的收集活动，且收集个人信息的频度正常；
7） 隐私政策容易阅读，且具有简体中文版，不存在给用户造成阅读或理解麻烦的情况；
8） 用户在进入客户端应用软件主页面后，至多4次点击就可访问到隐私政策或个人金融信息的收集使用规则；
9） 隐私政策中包含隐私政策变更的原因以及用户访问更新后隐私政策的途径；
10） 若客户端具有利用用户个人信息和算法向个人推送信息的功能，则客户端具有关闭该服务的功能，且在用户关闭后不得自动开启或延期自动开启；

11）隐私政策中包含机构处理用户投诉、更正、删除个人信息以及注销用户的人工处理时限，时限未超过15个工作日；

12）个人金融信息控制者在制定隐私政策时，其内容包括以下内容：

a）个人金融信息控制者的基本情况，包括注册名称、注册地址、常用办公地点和相关负责人的联系方式等；

b）收集、使用个人金融信息的目的，以及目的所涵盖的各个业务功能，例如将个人金融信息用于推送商业广告，将个人金融信息用于形成直接用户画像及其用途等；

c）各业务功能分别收集的个人金融信息，以及收集方式和频率、存放地域、存储期限等个人金融信息处理规则和实际收集的个人金融信息范围；

d）对外共享、转让、公开披露个人金融信息的目的、涉及的个人金融信息类型、接收个人金融信息的第三方类型，以及所承担的相应法律责任；

e）遵循的个人金融信息安全基本原则，具备的数据安全能力，以及采取的个人金融信息安全保护措施；

f）个人金融信息主体的权利和实现机制，如访问方法、更正方法、删除方法、注销账户的方法、撤回同意的方法、获取个人金融信息副本的方法、约束信息系统自动决策的方法等；

g）提供个人金融信息后可能存在的安全风险，及不提供个人金融信息可能产生的影响；

h）处理个人金融信息主体询问、投诉的渠道和机制,以及外部纠纷解决机构及联络方式。

5.5.1.2 数据防窃取

检测目的：

1） 检查敏感数据在输入过程中是否有实时加密，内存中是否存在完整的敏感数据明文；

2） 检查客户端软件的临时文件是否出现敏感信息；

3） 检查客户端软件身份认证结束后是否有存储敏感信息；

4） 检查客户端软件内存中是否存在完整的银行卡密码和网络支付交易密码明文；

5） 检查客户端软件是否采取技术手段防止内存中的敏感数据密文被还原为明文；

6） 检查客户端应用软件是否实现身份认证过程的防截屏、录屏。

基本要求：

检测方法：

1） 查看送检文档中有关敏感信息加密的说明,检查代码片段验证敏感信息在输入后是否立即进行加密，并且明文缓存在使用完毕后立即清除；

2） 综合采用现有的按键拦截、屏幕录制、内存扫描、代码注入、动态调试等测试技术，查看是否可窃取到用户输入的敏感数据；

3） 查看客户端软件的临时文件中是否出现敏感信息，临时文件包括但不限于Cookies、本地临时文件和移动数据库文件等；

4） 查看客户端软件在身份认证结束后是否有存储敏感信息；

5） 查看客户端软件运行日志中是否含有支付敏感信息；

6） 查看客户端软件内存中是否存在完整的银行卡密码和网络支付交易密码明文。

通过标准：

1） 客户端应用软件运行时，内存中不存在完整的银行卡密码和网络支付交易密码明文；

2） 客户端应用软件的临时文件中未出现支付敏感信息，临时文件包括但不限于 Cookies、本地临时文件等；

3） 客户端应用软件程序在身份认证结束后未存储支付敏感信息；

4） 客户端应用软件运行日志中不存在支付敏感信息及完整的敏感数据原文。

增强要求：

检测方法：

1） 综合使用代码注入、动态调试等方法，尝试还原内存中加密的敏感数据；

2） 检查客户端应用软件是否实现身份认证过程的防截屏、录屏，如输入手势验证码、登录口令等。

通过标准：

1） 内存中加密的敏感数据不能通过技术手段还原为明文；

2） 客户端应用软件已实现身份认证过程的防截屏、录屏，如输入手势验证码、登录口令等。

5.5.1.3 数据防篡改

检测目的：

检查用户输入关键交易数据时，是否采取防篡改机制保证数据不被移动终端的其他程序篡改。

基本要求：

检测方法：

1） 查看送检文档中对于关键交易数据的相关说明，典型的关键交易数据如收款人账号、交易金额、订单号等；

2） 检查送检文档中有关关键交易数据防篡改的安全机制，评估其安全防护强度。综合采用代码注入、动态调试等手段，尝试篡改用户输入的关键交易数据。

通过标准：

用户输入关键交易数据时，如收款人信息、交易金额、订单号等，已采取防篡改机制保证数据不被移动终端的其他程序篡改。

5.5.1.4 数据有效性

检测目的：

检查客户端是否在数据获取时提供了数据有效性校验功能，确保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。

基本要求：

检测方法：

1） 查看客户端人机接口和通信接口，检查客户端通过这些接口获取了哪些数据，这些数据是否具有固定格式或其它约束，如长度限制、是否包含特殊字符等；

2） 对于具有固定格式的数据，如银行卡号、邮箱、手机号、身份证号等，检查客户端是否根据其格式进行了前置有效性检查；

3） 对于其它格式约束的数据，如长度限制、不能包含特殊字符等，检查客户端是否进行了相应的检查。

通过标准：

客户端应用软件在数据获取时提供有效性校验功能，确保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。

5.5.2 数据访问控制

检测目的：

1） 检查是否能越过授权访问客户端数据；

2） 检查客户端是否访问了终端中非业务必需的文件和数据。

基本要求：

检测方法：

1) 查看送检文档的相关说明，检查客户端在操作系统提供的安全机制之外，采取哪些额外措施保护自身数据不被非法访问；
2) 查看送检文档的相关说明，检查客户端是否仅访问了终端中业务必需的文件和数据，如基于SE的客户端是否仅能访问已获授权的SE应用等；
3) 执行相关测试，如检查接口暴露级别、文件权限等，验证声明的访问控制措施是否正确实现。

通过标准：

1) 已采取措施保护客户端应用软件数据仅能被授权用户或授权应用组件访问；
2) 客户端应用软件在授权范围内，未访问非业务必需的文件和数据。

5.5.3 数据传输

5.5.3.1 通讯安全

检测目的：

1) 检查客户端软件是否使用安全协议进行通信；
2) 检查客户端采用的安全协议是否存在已公开漏洞；
3) 检查安全协议采用的密码算法是否符合国家密码主管部门的要求；
4) 检查客户端软件所使用的互联网协议是否支持IPv6，查看通过IPv6环境下是否可以正常使用；
5) 检查客户端软件域名（若有域名）是否能够解析为IPv6地址；
6) 查看客户端应用软件图标或启动界面是否显性显示IPv6标识；
7) 检查客户端应用软件在IPv6环境下网络连接的稳定性，分时段发起客户端应用软件连接，记录连接失败率；
8) 检查客户端应用软件分别在IPv6和IPv4环境下连接时间有无明显差异，分时段发起应用连接，记录时延。

基本要求：

检测方法：

1) 查看送检文档中关于网络通讯协议的说明，检查是否采用公开的安全协议，查看协议版本和实现，检查是否存在公开的安全漏洞；
2) 如果使用自定义协议，评估其安全级别是否符合要求；
3) 综合使用中间人攻击、进程HOOK等手段，检查客户端与服务器是否进行了安全认证；
4) 检查软件的后台服务器是否具有IPv6域名。在只分配IPv6的网络内使用APP，查看APP是否可以正常运行；
5) 使用dig命令检查客户端软件域名（若有域名）IPv6地址，dig <应用域名> AAAA +noall +answer。

通过标准：

1) 在客户端应用软件与服务器之间建立安全的信息传输通道，协议版本已及时更新至安全稳定版本；
2) 确保采用的安全协议不包含已知的公开漏洞；
3) 软件的后台服务器均具有 IPv6 域名，且软件在只分配 IPv6 的网络环境内可正常运行；
4) 客户端应用软件图标或启动界面显性显示 IPv6 标识；
5) 分时段发起客户端应用软件连接失败率不超过 5%；
6) 访问延迟均值应小于 15%或 75ms（二者中取最大值）。

增强要求：

检测方法：

检查客户端与服务器是否进行了双向认证。

通过标准：

客户端应用软件与服务器进行了双向认证，可通过密钥、证书等密码技术手段实现服务器与客户端应用软件之间的安全认证。

5.5.3.2 数据保密性

检测目的：

检查敏感数据在本地程序组件间或通过公共网络传输时，是否采取措施（如加密等）确保其保密性。

基本要求：

检测方法：

1) 查看送检文档，检查客户端会传输哪些敏感数据（如登录口令、查询口令、支付敏感信息、用于用户鉴别的个人生物识别信息等），数据传输过程中是否进行了加密；
2) 检查敏感数据在客户端应用软件与本地其他应用软件间传输时，若本地其他应用软件不能提供与金融客户端软件相应等级的加密接口，是否评估敏感数据调用的风险，并设计补救措施；
3) 检查数据的加密算法、密钥长度及密钥管理方式是否符合国家密码主管部门与本文件4.4.1中的要求；
4) 尝试截获传输报文，验证敏感数据是否采取加密措施。

通过标准：

1) 敏感数据（如登录口令、支付敏感信息等）在客户端应用软件与本地其他应用软件间传输时，已采取加密等措施确保其保密性，若本地其他应用软件不能提供与金融客户端软件相应等级的加密接口，则已评估敏感数据调用的风险，并设计补救措施；
2) 敏感数据（如登录口令、支付敏感信息等）在通过公共网络传输时，已采取加密等措施确保其保密性。

5.5.3.3 数据完整性

检测目的：

检查关键的交易数据在本地程序组件间或通过公共网络传输时，是否采取措施（如MAC等）确保其完整性。

基本要求：

检测方法：

1) 查看送检文档，检查客户端会传输哪些关键的交易数据，如收款人信息、交易金额、订单号等，数据传输过程中是否添加了完整性校验值；
2) 检查产生完整性校验值的算法是否为HMAC、CBC-MAC或同等安全级别，校验值计算接口是否可被其它程序非法调用；
3) 检查关键的交易数据，在客户端应用软件与本地其他应用软件间传输时，若本地其他应用软件不能提供与金融客户端软件相应等级的数据完整性保护措施，是否评估关键数据传输的风险，并设计补救措施；
4) 尝试截获传输报文，验证关键交易数据是否采取完整性校验手段。

通过标准：

1) 关键的交易数据，如收款人信息、交易金额、订单号等，在客户端应用软件与本地其他应用软件间传输时，已采取措施（如数字签名、MAC 等）确保其完整性，若本地其他应用软件不能提供与金融客户端软件相应等级的数据完整性保护措施，则已评估关键数据传输的风险，并设计补救措施；
2) 关键的交易数据、个人身份信息，如收款人信息、交易金额、订单号等，在通过公共网络传输时，已采取措施（如数字签名、MAC 等）确保其完整性。

5.5.3.4 数据抗抵赖

检测目的：

检查客户端是否可保证资金类交易数据的不可抵赖性。

基本要求：

检测方法：

1) 查看送检文档中有关交易数据抗抵赖的说明，检查客户端采用何种方式确保交易数据的抗抵赖性，包括发送抗抵赖和接收抗抵赖两方面的要求；
2) 评估抗抵赖采用的安全机制是否有效；
3) 如采用数字签名算法，检查签名算法和密钥长度是否符合国家密码主管部门的要求。

通过标准：

通过客户端应用软件发起的资金类交易报文，确保交易报文的不可抵赖性，在有条件的情况下宜采用数字证书技术。

5.5.3.5 数据防重放

检测目的：

检查客户端应用软件发起的身份认证类或资金类交易报文是否能够防止重放攻击。

基本要求：

检测方法：

1) 查看送检文档中有关客户端应用软件发起身份认证类或资金类交易报文防止重放攻击的说明，检查客户端采用何种方式确保防止重放攻击；
2) 评估防止重放攻击采用的安全机制是否有效。

通过标准：

通过客户端应用软件发起的身份认证或资金类交易报文，能够防止重放攻击。

5.5.4 数据存储

5.5.4.1 个人金融信息存储

检测目的：

1) 检查客户端是否未在本地文件系统中以任何形式存储用户的支付敏感信息与金融业务查询口令；
2) 检查客户端是否仅保存业务必需的个人金融信息，并限制数据存储量；
3) 检查客户端软件是否在本地文件系统中存储敏感数据明文。

基本要求：

检测方法：

1) 查看送检文档有关客户端涉及支付敏感信息的说明，检查客户端是否会将支付敏感信息保存在文件系统中；
2) 查看送检文档有关客户端涉及个人金融信息的说明，检查客户端是否会将个人金融信息保存在文件系统中，是否仅保存必须的个人金融信息，是否限制数据存储量；
3) 使用文件系统管理工具查看客户端保存的个人金融信息是否与声明一致；
4) 查看送检文档中有关客户端涉及敏感数据存储的说明，检查客户端软件本地文件系统中是否明文存储敏感数据。

通过标准：

1) 客户端应用软件不应以任何形式存储支付敏感信息与金融业务查询口令；

2) 在满足法律、管理规定的前提下，客户端应用软件应仅保存业务必需的个人金融信息，并限制数据存储量；
3) 客户端软件本地文件系统中没有明文存储敏感数据。

5.5.4.2 加密密钥存储

检测目的：

检查客户端是否确保无法通过逆向工程等手段直接从本地文件系统中恢复完整的密钥明文。

基本要求：

检测方法：

查看送检文档中有关加密算法的说明，检查客户端对敏感数据(如登录口令、支付敏感信息等)的加密使用了哪些加密算法，加密算法的密钥如何进行管理，本地是否明文存储对称密钥和非对称密钥对中的私钥。

通过标准：

客户端应用软件确保无法通过逆向工程等手段直接从本地文件系统中恢复完整的密钥明文。

5.5.5 数据展示

检测目的：

检查客户端应用软件在显示个人信息时应屏蔽关键字段。

基本要求：

检测方法：

检查除交易对账、转账收款方确认等必须由用户确认的情况外，客户端应用软件在显示个人信息如银行账号、身份证号、手机号、姓名等时应屏蔽关键字。

通过标准：

除交易对账、转账收款方确认等必须由用户确认的情况外，对于银行卡号、手机号码、证件类识别标识或其他识别标识信息等可以直接或组合后确定个人金融信息主体的信息应进行屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应进行用户身份验证。

5.5.6 数据销毁

5.5.6.1 残余信息保护

检测目的：

1) 检查敏感数据在使用完毕后，是否立即进行清除；
2) 检查客户端软件账户退出时，是否清除非业务功能运行所必需留存的业务数据；
3) 检查客户端软件卸载完成后，文件系统中是否残留与用户相关的个人信息及敏感数据等；
4) 客户端版本更新时，应考虑对客户端缓存数据的维护，包括Document、Library、Caches等目录；
5) 检查是否可以通过技术手段恢复已清除的个人信息及敏感数据。

基本要求：

检测方法：

1) 查看送检文档或代码片段，检查敏感数据在使用完毕后立即清除的证据；
2) 使用调试或内存扫描工具，检查内存中是否长期存在敏感信息明文；
3) 客户端软件在账户退出时，检查是否清除了非业务功能运行所必需留存的业务数据；
4) 卸载客户端软件，检查文件系统是否残留客户端数据，如调试日志等；
5) 客户端版本更新后，检查是否对缓存数据进行维护。

通过标准：

1) 客户端应用软件应在敏感数据使用完毕后，对其立即进行清除；
2) 客户端应用软件账户退出时，已清除非业务功能运行所必需留存的业务数据，保证客户信息的安全性；
3) 客户端应用软件卸载完成后，文件系统中不应残留任何个人金融信息；
4) 客户端版本更新后，在必要的情况下，完成了对缓存数据的维护。

增强要求：

检测方法：

尝试通过技术手段恢复已清除的个人信息及敏感数据，查看是否可以成功恢复。

通过标准：

无法通过技术手段恢复客户端应用软件已清除的敏感数据。

5.5.6.2 页面返回保护

检测目的：

检查客户端是否支持页面返回自动清除敏感信息的机制。

基本要求：

检测方法：

1) 查看送检文档中有关敏感信息的说明，检查客户端哪些页面涉及敏感信息的显示和处理；查看客户端应用软件从前台进入后台时，超过设定时限的处理策略；
2) 操作客户端进入上述页面，输入敏感信息跳转至其他页面后，重新进入该页面时，检查敏感信息是否自动清除。

通过标准：

客户端应用软件支持页面返回后自动清除银行卡密码、网络支付交易密码、登录口令等敏感信息的机制。

增强要求：

检测方法：

1) 调出后台列表界面，查看客户端在后台列表中的预览界面是否采取模糊或其他防护措施；
2) 当客户端应用软件从前台进入后台时，超过设定时限后是否清除页面中已输入的敏感数据。

通过标准：

1) 客户端应用软件对后台任务列表中的预览界面采取模糊或其他防护措施；
2) 当客户端应用软件从前台进入后台时，超过设定时限后已清除页面中已输入的敏感数据。

5.5.6.3 会话失效

检测目的：

检查客户端应用软件在安全退出登录时，是否向服务器发送会话结束请求，使当前会话状态失效。

基本要求：

检测方法：

1) 查看送检文档中客户端应用软件在安全退出登录的说明；
2) 检查客户端应用软件在安全退出登录时，是否向服务器发送会话结束请求，使当前会话状态失效。

通过标准：

客户端应用软件在安全退出登录时，向服务器发送会话结束请求，使当前会话状态失效。

6 客户端应用软件管理要求

6.1 设计要求

检测目的：

检查是否具有指导客户端应用软件设计与开发的总体方案，是否提供易用、风格统一、体验良好的用户界面，客户端应用软件对个人金融信息的收集和个人信息修改是否符合要求。客户端应用软件所采用的智能语音交互技术是否满足相关要求。

基本要求：

检测方法：

1） 检查客户端应用软件设计与开发的总体方案文档，是否提供遵循安全、可靠、易用、可维护和可扩展等原则的设计；
2） 检查客户端应用软件用户界面，是否易于使用、风格统一、体验良好；
3） 检查客户端应用软件相关设计文档，查看客户端软件是否只收集与所提供服务相关的个人金融信息；
4） 检查客户端应用软件相关设计文档，查看客户端软件是否明示个人金融信息收集使用规则，并征得个人金融信息主体自主选择同意；
5） 检查客户端应用软件相关设计文档，检查客户端应用软件是否存在默认、捆绑、停止安装使用等手段变相强迫用户授权，或违反与用户的约定收集使用个人金融信息的情况；
6） 检查客户端应用软件所采用的智能语音交互技术是否满足 JR/T 0092—2019 附录 B 中的相关要求；
7） 若客户端软件收集了 C3、C2[1]类别的信息，查看客户端软件所属的机构主体是否具有金融行业相关资质；
8） 检查客户端应用软件相关设计文档，查看客户端应用软件及隐私政策中是否提供访问、更正个人金融信息，以及授权撤销、账户注销等功能或途径，并验证其正确性；
9） 检查客户端应用软件相关设计文档，查看在注销过程中，客户端应用软件是否给用户设置不必要或不合理的条件。

通过标准：

1） 提供遵循安全、可靠、易用、可维护和可扩展等原则客户端应用软件设计方案，总体方案完整且符合实际情况；
2） 客户端应用软件提供易用、风格统一、体验良好的用户界面；
3） 客户端应用软件遵循合法、正当、必要的原则，不收集与所提供服务无关的个人金融信息；
4） 客户端应用软件收集个人金融信息或用户授权等操作前，以通俗易懂、简单明了的方式展示个人金融信息收集使用规则，并经个人金融信息主体自主选择同意；
5） 客户端应用软件未以默认、捆绑、停止安装使用等手段变相强迫用户授权，未违反与用户的约定收集使用个人金融信息；
6） 客户端应用软件所采用的智能语音交互技术满足 JR/T 0092—2019 附录 B 中的相关要求；
7） 不应委托或授权无金融业相关资质的机构收集 C3、C2 类别信息；
8） 客户端应用软件或隐私政策中提供了访问、更正个人金融信息，以及授权撤销、账户注销等功能或途径；
9） 查看在注销过程中，客户端应用软件未给用户设置不必要或不合理的条件；

1）C3、C2 类别的定义参考 JR/T 0171—2020 《个人金融信息保护技术规范》

10）提供的文档中所述内容应与客户端软件的实际功能一致。

增强要求：

检测方法：

检查客户端应用软件设计文档和访谈相关人员，哪些设计是否采用了人工智能技术，并验证相关功能模块的易用性。

通过标准：

客户端应用软件设计在遵循易用性原则的基础上，采用人工智能技术应用，如应用智能语音交互技术。

6.2 开发要求

检测目的：

1) 检查开发过程是否遵守规范的开发流程、项目管理流程和编码安全规范，是否进行测试，发现开发环境中可能存在的漏洞；
2) 确保开发过程中有完整的、可追溯的描述文档；
3) 确保面向用户提供了正确的、完整的、友好的指导文档；
4) 是否具有规范的发布流程。

基本要求：

检测方法：

1) 访谈开发人员是否制定了开发流程，并检查开发过程文档和记录是否严格依据开发流程执行；
2) 访谈开发人员是否制定了项目管理流程，并检查项目管理文档和记录是否严格依据管理流程执行；
3) 检查使用的开发及编译工具是否通过合法途径获取。检查开发工具安装包的校验值是否与原厂提供相等，是否定期对开发和编译工具进行安全性检查；
4) 访谈开发人员是否编制了编码规范，检查相关记录和文档是否按照规范执行；
5) 访谈安全员，是否针对源代码进行安全性审查，查看源代码审计报告，报告中的漏洞是否得到及时修复；
6) 检查测试流程规范、测试记录、测试报告是否完整，对所发现的在请求、响应、存储、配置等功能中的漏洞是否及时得到修复；
7) 检查所提供的开发类文档是否完整，是否提供有效的文档管理机制；
8) 检查用户类文档或检查是否提供在线帮助说明功能，并访谈、分析情况是否属实；
9) 检查变更控制规范（包括软件版本管理），抽样检查变更记录、版本管理记录、源代码扫描记录、发布审核记录等；
10) 查看客户端的开发测试环境与生产环境进行有效的隔离。查看客户端软件中是否存有测试数据。查看测试环境中是否存在真实的个人金融信息。

通过标准：

1) 客户端应用软件开发过程中遵守严格的开发流程、项目管理流程和编码安全规范，进行完整的测试，在请求、响应、存储、配置等功能中未存在漏洞；
2) 客户端应用软件开发过程中建立并维护开发文档，开发文档完整且符合实际情况；
3) 客户端应用软件的开发工具均通过合法途径获取，且校验值与合法渠道提供的校验值一致，开发及编译工具定期进行安全性检查；
4) 客户端应用软件开发完成后，同步完成产品手册、用户手册或提供在线帮助说明功能，用户类文档正确完整且通俗易懂；在线帮助说明功能可正确实现，说明内容正确完整且通俗易懂；
5) 客户端应用软件的每次重要更新、升级，都必须经过严格归档、源代码扫描、发布审核等步骤，

变更文档完整且符合实际情况，记录完整；

6) 对开发测试环境与生产环境进行有效隔离；

7) 开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化（不应仅使用加密技术）脱敏处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需信息除外。

6.3 发布要求

检测目的：

检查发布过程是否遵守规范的上线发布流程，检查应用软件的上线、发布、安装、更新过程中的安全保护机制。

基本要求：

检测方法：

1) 访谈相关人员，是否制定上线发布流程，检查发布流程、发布记录；

2) 检查客户端应用软件是否进行签名，检查应用软件的签名证书是否采用权威机构颁发，能否有效标识应用软件的来源和发布者；检查应用软件下载官网是否明确标识应用软件版本号、哈希值；

3) 根据指定渠道和路径下载获取客户端软件，分析下载、更新过程；

4) 检查客户端应用软件发布相关管理制度，是否对发布前删除调试或测试中存留的敏感数据进行规定，是否严格依据制度执行；

5) 根据客户端应用软件安装指引进行安装，查看安装过程中是否具有明确标识，通过检测工具分析安装前后的环境变化；

6) 检查客户端应用软件的更新方式，版本更新前是否取得用户的明示同意；

7) 客户端应用软件若支持动态模块更新，检查动态模块更新方式，更新后是否进行签名校验，分析更新前后的环境及配置变化。

通过标准：

1) 具有规范的客户端应用软件上线发布流程，发布过程符合发布流程，发布记录完整；应用软件进行签名和保护，标识应用软件的来源和发布者；提供官方的下载获取渠道，下载渠道安全可靠；

2) 客户端应用软件在发布前删除了调试或测试中存留的敏感数据；

3) 客户端应用软件安装过程中，拥有独立的安装目录，唯一的应用标识符，明确的版本序号，未篡改、覆盖、删除系统文件和其它软件；

4) 如果客户端应用软件有新版本，未经用户允许不得自动安装新版本；

5) 客户端应用软件若支持动态模块更新，使用加密信道与服务端通信传输更新模块或对更新模块进行签名校验；动态模块更新后未影响用户使用，未修改用户已有的安全配置。

6.4 维护要求

检测目的：

检查客户端应用软件运维是否遵守规范的日常运维流程，检查客户端应用软件版本升级、卸载清除过程中的安全保护机制。

基本要求：

检测方法：

1) 检查运维管理类文档，是否能指导各类角色的工作协同、实施步骤、质量管控、安全检测等，规范日常运维流程。运维管理类文档一般包括：工程实施、项目管理、安全测试报告、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；

2) 检查客户端应用软件界面是否具有明确应用标识符和版本序号，检查客户端应用软件更新接口和更新记录；
3) 检查以 SDK、Html5 等形式对外提供的金融交易类服务，是否记录了 SDK、Html5 信息及引用本 SDK、Html5 的外部应用软件信息；
4) 检查是否明确个人金融信息保护责任人与责任机构，并履行了相应职责。

通过标准：

1) 制定了科学、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，运维管理类文档完整且符合实际情况；
2) 客户端应用软件具有明确的应用标识符和版本序号，设计了合理的更新接口，当某一版本被证明存在安全隐患时，及时进行修复更新；
3) 以 SDK 等形式对外提供金融交易类服务时，记录了 SDK 信息及引用本 SDK 的外部应用软件信息；
4) 应明确个人金融信息保护责任人和个人金融信息保护责任机构，并履行以下工作职责：
   - 负责制定和管理本机构个人金融信息安全管理制度；
   - 制定、实施、定期更新隐私政策和相关规程；
   - 监督本机构内部，以及本机构与外部合作方个人金融信息安全管理；
   - 开展信息安全管理内部审计、分析处理信息安全相关事件；
   - 组织开展个人金融信息安全影响评估，提出个人金融信息保护的对策建议；
   - 组织在金融产品或服务上线发布前进行技术检测，避免未知（与金融产品或服务功能及隐私政策不符）的个人金融信息收集、使用、共享等处理行为；
   - 公布投诉与申诉方式等信息并及时受理个人金融信息有关的投诉、申诉。

附 录 A
（规范性附录）
应用软件测试范围

资金交易类客户端应用软件是指直接面向用户提供资金交易服务的移动金融客户端应用软件；信息采集类客户端应用软件是指不直接向用户提供资金交易服务，但需要采集个人敏感信息的移动金融客户端应用软件；资讯查询类客户端应用软件是指仅提供金融产品推介、信息查询、资讯推送等服务的移动金融客户端应用软件。资金交易类客户端应用软件应符合资金交易、信息保护等所有技术及管理安全要求。信息采集类客户端应用软件应重点符合信息保护相关技术及管理安全要求。资讯查询类客户端应用软件参照执行相关客户端应用软件安全和管理要求。具体测试范围如下表（其中●代表属于该类软件测试范围、○代表不属于该类软件的测试范围）：

检测序号	检测项名称	资金交易类	信息采集类	资讯查询类
4.1.1	认证方式	●	●	●
4.1.2.1	安全输入	●	●	○
4.1.2.2	个人金融信息显示	●	●	●
4.1.3	认证失败处理	●	●	●
4.1.4	密码的设定与重置	●	●	●
4.2.1	逻辑安全设计	●	●	○
4.2.2	软件权限控制	●	●	●
4.2.3	风险控制	●	●	○
4.2.4	回退处理	●	○	○
4.2.5	异常处理	●	●	●
4.3.1	组件安全	●	●	●
4.3.2	接口安全	●	●	●
4.3.3	抗攻击能力	●	●	●
4.3.4	客户端应用软件	●	●	●

	环境检测			
4.4.1	密码算法	●	●	○
4.4.2	密钥管理	●	●	○
4.5.1.1	个人金融信息收集	●	●	○
4.5.1.2	数据防窃取	●	●	○
4.5.1.3	数据防篡改	●	○	○
4.5.1.4	数据有效性	●	●	●
4.5.2	数据访问控制	●	●	●
4.5.3.1	通讯安全	●	●	●
4.5.3.2	数据保密性	●	●	○
4.5.3.3	数据完整性	●	●	○
4.5.3.4	数据抗抵赖	●	○	○
4.5.3.5	数据防重放	●	●	●
4.5.4.1	个人金融信息存储	●	●	○
4.5.4.2	加密密钥存储	●	●	○
4.5.5	数据展示	●	●	●
4.5.6.1	残余信息保护	●	●	○
4.5.6.2	页面返回保护	●	●	○
4.5.6.3	会话失效	●	●	●
5.1	设计要求	●	●	●

5.2	开发要求	●	●	●
5.3	发布要求	●	●	●
5.4	维护要求	●	●	●

参 考 文 献

[1] JR/T 0164-2018 移动金融基于声纹识别的安全应用技术规范

[2] App专项治理工作组.App违法违规收集使用个人信息自评估指南.2019年3月

[3] 国家互联网信息办公室秘书局 工业和信息化部办公厅 公安部办公厅 市场监管总局办公厅.关于印发《App违法违规收集使用个人信息行为认定方法》的通知.2019年11月28日

[4] 全国信息安全标准化技术委员会秘书处.关于发布《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南》的通知.2020年7月22日