CCS 03 060
CCS A11

Q/CZCB

浙江稠州商业银行移动金融客户端应用企业标准

Q/CZCB 11701—2020

浙江稠州商业银行移动金融客户端应用

Mobile financial client application of Zhejiang Chuzhou commercial bank

2020－9－30 发布　　2020－10－1 实施

浙江稠州商业银行　　发布

目　　次

企业标准信息公共服务平台
公开　2020年09月30日 10点33分

前　言

本标准参照 GB/T 1.1——2020 给出的规则起草。

本标准由浙江稠州商业银行提出并归口。

本标准起草单位：浙江稠州商业银行。

本标准主要起草人：杨保林，宋程，张波，毛镔瑶，应会，王品，周倩倩，叶长柯，陈璐，刘振德。

企业标准信息公共服务平台
公开 2020年09月30日 10点33分

浙江稠州商业银行移动金融客户端应用

1 范围

本标准规定了浙江稠州商业银行（以下简称“稠州银行”）移动金融客户端应用标准，明确了安全性，技术先进性，创新及前瞻性的规范要求。同时针对金融客户端在服务创新和技术前瞻方面也给出了具体要求。

本标准适用于稠州银行的移动金融客户端应用。

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。

GB/T 37668-2019信息技术互联网内容无障碍可访问性技术要求与测试方法

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

GB/T 34975-2017信息安全技术移动智能终端应用软件安全技术要求和测试评价方法

JR/T 0156-2017移动终端支付可信环境技术规范

JR/T 0100-2013银行业软件测试文档规范

GB/T 35278-2017信息安全技术移动终端安全保护技术要求

GB/T 17901.1-2020信息技术安全技术密钥管理第1部分：框架

GB/T 37036.1-2018信息技术移动设备生物特征识别第1部分：通用要求

GB/T 33767.1-2017信息技术生物特征样本质量第1部分：框架

IOS/IEC 30107信息技术生物特征识别呈现攻击检测

GB/T 35273-2017信息安全技术个人信息安全规范

3 术语和定义

3.1 移动金融客户端应用软件 financial mobile application software

在移动终端上为用户提供金融交易服务的应用软件

注：包括但不限于可执行文件、组件等。

3.2 个人金融信息 Person financial information

金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。

3.3 响应时间 The response time

指服务处理一个请求或一个任务的耗时。

3.4 收集 collect

获得个人金融信息的控制权的行为。

注1：收集行为包括由个人金融信息主体主动提供、通过与个人金融信息主体交互或记录个人金融信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取个人金融信息等行为。

注2：如金融产品或服务提供者提供工具供个人金融信息主体使用，提供者不对个人金融信息进行访问的，则不属于本标准所称的收集。例如手机银行客户端应用软件在终端获取用户指纹特征信息用于本地鉴权后，指纹特征信息不回传至提供者，则不属于用户指纹特征信息的收集行为。

3.5 短信验证码 SMScode

后台系统以手机短信形式发送到用户绑定手机上的随机数，用户通过回复该随机数进行身份认证。

注：包括但不限于银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等。

3.6 支付标记 paymenttoken(Token)

作为支付账号等原始交易要素的替代值，用于完成特定场景支付交易。

3.7 支付账号 paymentaccount

具有金融交易功能的银行账户、非银行支付机构支付账户及银行卡卡号。

注：包括但不限于银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等。

3.8 共享 sharing

个人金融信息控制者向其他控制者提供个人金融信息，且双方分别对个人金融信息拥有独立控制权的过程。

3.9 转让 transferofcontrol

将个人金融信息控制权由一个控制者向另一个控制者转移的过程。

注：包括但不限于银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等。

3.10 公开披露 publicdisclosure

向社会或不特定群体发布信息的行为。

3.11 去标识化 de-identification

通过对个人金融信息的技术处理，使其在不借助额外信息的情况下，无法识别个人金融信息主体的过程。

注：去标识化仍建立在个体基础之上，保留了个体颗粒度，采用假名、加密、加验的哈希函数等技术手段替代对个人金融信息的标识。

3.12 删除 delete

在金融产品和服务所涉及的系统中去除个人金融信息的行为，使其保持不可被检索、访问的状态。

4 缩略语

下列缩略语适用于本规范。

API：应用编程接口（Application Programming Interface）

SDK：软件开发工具包（SoftwareDevelopmentKit）

5 基本安全要求

移动金融客户端软件应遵照JR/T0092-2019、GB/T17901.1-2020、GB/T35278-2017、JR/T0156-2017的要求。

5.1 移动金融客户端软件设计

a) 移动金融客户端软件设计应遵循安全、可靠、可维护和可扩展等原则，制定用于指导客户端软件设计与开发的总体方案；
b) 移动金融客户端软件应提供功能简单易用、界面风格统一、专业术语一致、交互体验良好的用户界面；
c) 移动金融客户端软件应遵循合法、必要、最小化的原则，不收集与所提供服务无关的个人金融信息；
d) 移动金融客户端软件收集个人金融信息或用户授权等操作前，要以通俗易懂、简单明了的方式展示个人金融信息收集使用规则，并经用户自主选择同意；
e) 移动金融客户端软件不得以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反与用户的约定收集使用个人金融信息；
f) 用户明确表示不同意后，不应继续收集个人信息或者打开收集个人信息的权限，也不应频繁征求用户同意、干扰用户正常使用；
g) 不得因用户不同意收集非必要个人信息或打开非必要权限，而拒绝提供相关的业务服务；
h) 移动金融客户端软件应提供访问、更正个人金融信息，以及授权撤销、账号注销等功能；
i) 移动金融客户端软件应避免使用存在已知漏洞的系统组件与第三方组件；
j) 移动金融客户端软件在使用第三方组件时，应避免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；
k) 移动金融客户端软件应对软件接口进行保护，防止其他应用对客户端应用软件接口进行非授权调用；
l) 移动金融客户端软件应对传入的URI进行校验与安全处理，防止客户端应用软件运行异常或操作异常。

5.2 移动金融客户端软件开发

a) 移动金融客户端软件开发过程中应遵守严格的开发流程、项目管理流程和安全编码规范，并进行完整充分的测试，避免应用存在漏洞；
b) 移动金融客户端软件开发过程中应建立并维护开发文档；
c) 采用合理的版本控制策略，新功能需建新分支开发，自测后合入主分支，提交记录描述清楚。
d) 发布节点打上Tag，描述清楚此次发布的主要功能点；
e) 开发中Log日志统一管理，Release版本关闭日志；
f) 申请系统权限最小化原则，及时删除多余权限；
g) 移动金融客户端软件在开发完成后，应同步完成产品手册、用户手册或提供在线帮助说明功能；
h) 移动金融客户端软件在每次重要更新、升级，都必须经过严格归档、源代码审计、功能测试、性能测试、安全测试、安全加固、发布审核等步骤。

5.3 移动金融客户端软件测试

5.3.1 功能测试

开发者应测试客户端应用软件的安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a) 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对其他测试结果的任何顺序依赖性；
b) 预期的测试结果，表明测试成功后的预期输出；
c) 实际测试结果和预期测试结果一致。

5.3.2 性能测试

规定测试项目的所有应有的输出和特征（如：相应时间），提供各个输出或特征性的正确值（必要时允许适当的误差）。根据测试的结果，提出可立即投产、修复一定异常后投产或不宜投产等建议，建议中应包括识别性能异常合集和分析异常根本原因的过程。

5.3.3 安全测试

安全测试包括安全检测、渗透测试和代码评审。

移动金融客户端软件在每次重要更新、升级前应执行代码评审及至少安全检测、人工渗透测试中的一项，并修复相关漏洞。具体要求如下：

a) 应修复安全检测报告中的高危漏洞；
b) 应修复渗透测试报告中所有已发现漏洞；
c) 应修复代码评审报告中所有已发现漏洞。

5.4 移动金融客户端软件发布

5.4.1 移动金融客户端发布要求

a) 移动金融客户端软件应有规范的上线发布流程，由应用软件的所有方对应用软件进行签名和保护，标识应用软件的来源发发布者，提供安全可靠的应用软件下载、发布、升级渠道；
b) 移动金融客户端软件应当删除调试或测试中存留的敏感数据；
c) 移动金融客户端软件安装过程中，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、删除系统文件和其他软件；
d) 移动金融客户端软件有新版本时，不能未经用户允许自动安装新版本。

5.4.2 移动金融客户端安全加固

根据JR/T 0092-2019的要求，客户端应用软件应具备基本的抗攻击能力。客户端在发布前应采用加固工具进行加壳、加固，加固选择项须开启防逆向，防篡改，防调试，数据防泄漏，页面数据防护等功能，使客户端能够抵御反编译、篡改、劫持、静态分析、动态调试等攻击行为。

5.4.3 移动金融客户端发布

功能、性能、安全测试均符合预期，并进行加固后，向客户端应用软件发布单位申请发布审核申请通过后，发布单位将客户端应用软件发布到各大应用市场。

IOS程序须发布在AppStore，Android程序的发布平台须包含华为市场、腾讯应用宝、360市场、OPPO市场、小米市场、百度市场、阿里应用分发平台等。

5.5 移动金融客户端软件运维

a） 应制定科学、合理的管理策略和运维制度，指导相关部门和人员，进行工作协同、安全检测、版本发布，规范日常管理工作和流程；
b） 建立客户端应用软件的应急预案和故障通报流程，便于应急和信息通报；
c） 客户端应用软件应具有明确的应用标识符和版本序号，当在实际应用过程中，某一版本被证明存在安全隐患时，应及时进行修复更新；
d） 当客户端应用软件以 SDK 等形式对外提供金融交易服务时，应记录 SDK 信息，以及引用本 SDK 的外部应用系统信息。

5.6 移动金融客户端软件下线

5.6.1 下线受理

业务部门经过充分评估后，根据业务标准提出下线申请，申请获批后，应向中国互联网金融协会提交注销备案申请，并在中国互联网金融协会注销备案并公告后，通知运维部门进行下线准备，运维部门进行下线受理。

5.6.2 下线处理

运维部门根据业务部门申请，进行移动金融客户端下线，同时应回收所涉及的软硬件资源，并根据个人金融信息保护要求作好信息销毁工作。

5.7 金融客户端身份认证

5.7.1 认证安全

a） 提供鉴别失败处理措施，用户可通过找回密码、联系客服等方式重置密码；
b） 具备身份认证失败次数限制，对于连续认证失败超过 3 次的账号应采取锁定、冻结等处理措施禁止继续认证，防止暴力破解；
c） 身份认证的错误提示不应泄露具体的账号错误信息，应采用模糊的信息提示，如“账号或密码错误”等；
d） 具备登录超时后锁定或注销功能。

5.7.2 认证方式

a） 客户端应用软件登录时应采用适宜的验证要素，包括但不限于口令、短信验证码、手势密码、生物特征识别等方式，且确保使用的身份验证方式相互独立；
b） 登录密码应具备长度和随机性的要求，如：至少 8 位，由大小写字母、数字中的两种或三种符号组成；
c） 采用手势密码作为验证要素，手势密码应至少设置连续不间断的 6 个点；
d） 采用短信验证码作为验证要素，短信验证码应采用长度不小于 6 位的随机数字，认证成功后不可再次使用。发送短信验证码的短信中，应告知用户短信验证码的发送方、用途、开始时间、有效时间（建议默认 10 分钟）、联系方式、安全操作提示语等；
e） 客户端应用软件交易时应按照业务管理的要求，对客户身份进行认证，且根据业务规则和风险控制要求采取单因素认证或双因素认证，如：对应大额资金交易，应采取双因素认证；

5.7.3 认证失败处理

a） 客户端软件应提供认证失败处理功能，如：结束会话、限制失败登录次数和自动退出等措施；

b) 客户端软件在提示认证失败信息时，应模糊错误提示信息，防止提示信息中泄露敏感信息，如：登录失败，应提示“账号或密码错误”，不应提示为“账号不存在”或“密码错误”等。

5.7.4 重新身份认证

a) 在用户身份认证后，客户端应软件进入终端后台时，如果超过应用设定时限后被唤醒切换到前台，应采取措施对用户重新认证；
b) 在修改密码前，应对用户身份进行再次认证；
c) 在修改登录密码后，应销毁当前会话，并重新进行身份认证。

5.8 移动金融客户端软件逻辑安全

5.8.1 基于用户的控制

若客户端应用软件涉及用户敏感数据，则应对访问用户提供有效的授权机制。具体技术要求如下：
a) 授权用户访问的内容不能超出用户实际被授权的范围；
b) 对于认证、校验等安全保证功能的流程设计应充分考虑其合理性，确保认证流程无法被绕过；
c) 对于交易处理功能逻辑设计应充分考虑其合理性，避免逻辑漏洞的出现，保证资金交易安全；
d) 客户端应用应尽量避免使用不安全的函数或不安全的组件，避免敏感数据硬编码；
e) 限制应用用户账户的多重并发会话。

5.8.2 对应用软件的限制

客户端应用软件访问终端数据和终端资源应经过用户明确的许可，并遵循最小授权原则。具体技术要求如下：
a) 未得到许可前不应访问终端数据和终端资源；
b) 未得到许可前不应修改和删除终端数据，不应修改终端资源的配置。

5.8.3 风险控制

a) 应设计合理的登录风险控制策略，包括：
   1) 应限制多点登录，如切换设备登录，应给出适当的风险提示，如：您的账号已在别处登录。
b) 应设计合理的交易风险控制，包括：
   1) 针对不同的资金交易金额，应设计合理的身份认证策略，如：大额交易应采用双因素身份。
   2) 针对不同的资金交易业务场景，应设计合理的策略，如：限额控制、时限控制等。
c) 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。

5.8.4 回退及异常处理

a) 交易过程中如遇交易失败或在交易完成前用户进行撤销操作，应返回到交易前的有效状态；
b) 当交易出现异常时，客户端应用软件向用户提示出错等信息，但不应泄露用户的敏感数据；
c) 客户端应用软件发生故障产生的异常信息，不应包含用户的敏感数据。

5.9 移动金融客户端软件密码算法及密钥管理

5.9.1 密码算法

a) 客户端应用软件要求使用符合要求密码算法对资金有关交易或重要业务数据的保密性、完整性、真实性和不可否认性进行保护；

b） 密码算法、密钥长度及密钥管理方式应符合国家密码管理部门的要求。

5.9.2 密钥管理

a） 密钥在传输过程中应使用密码算法对密钥进行保护；
b） 随机生成的密钥具有一定的随机性与不可预测性；
c） 密钥需加密存储，确保存储位置和形式的安全；
d） 客户端应用软件推荐使用一会话一密的方式；
e） 密钥推荐在本地生成并加密保存，以减少密钥在生成设备上及密钥传输过程中的安全隐患；
f） 客户端应用软件经过专业加固处理，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；
g） 客户端应用软件经过专业加固处理，具备基本的抗攻击能力，能抵御静态分析、动态调试等操作，确保无法获取内存中的密钥。

5.10 身份认证安全

5.10.1 认证方式安全

移动金融客户端从身份认证安全角度满足以下要求：

a） 客户端应用软件登录应采用两种或两种以上的维度对用户身份进行认证。包括但不限于无感身份认证、智能风控、设备认证等服务端鉴权方式以及口令、手势密码、生物特征识别等传统或创新型身份认证方式；
b） 应确保采用的身份验证要素相互独立，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，如：用于登录验证的口令和用于交易的口令不能一致；
c） 客户端应用软件交易时应按照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，客户端应采用两种或两种以上要素对用户身份进行认证等；
d） 对于手势密码、短信验证码、生物特征信息作为验证要素或验证要素组合中的一种时，应满足如下要求：
e） 若采用手势密码作为验证要素，手势密码应至少设置连续不间断的 6 个点；
f） 若采用短信验证码作为验证要素，短信验证码应仅使用一次，仅限于在规定时间内使用，短信验证码应具备长度和随机性的要求；短信验证码所在的短信内容中，告知用户短信验证码的用途；
g） 若采用生物特征识别作为验证要素，应当符合国家、金融行业标准和相关信息安全管理要求，防止非法存储、复制和重放。
h） 若采用图形验证码作为验证的辅助要素，图形验证码应具有使用时间限制并仅能使用一次，图形验证码应由服务器生成，客户端源文件中不应包含图形验证码文本内容；
i） 图形验证码不得作为独立的身份验证要素；
j） 在用户身份认证后，客户端应用软件进入终端系统后台时，如果超过设定时限后被唤醒切换到前台，应采取措施对用户身份重新认证。

5.10.2 认证信息安全

客户端应用软件应提供客户输入银行卡交易密码的即时防护功能，客户端应提供以下安全控制措施，或其他经攻击测试无法获取明文的安全防护措施：

a） 采取替换输入框原文；
b） 逐字符加密、字符加密；

c) 防范键盘窃听；
d) 采用自定义软键盘；
e) 客户端应用软件的口令框应默认屏蔽显示，屏蔽显示时应使用同一特殊字符（例如*或•）代替；
f) 客户端应用软件不应明文显示银行卡密码和网络支付交易密码；
g) 客户端应用软件展示个人金融信息时，应符合以下要求：处于未登录状态时，不应展示与个人信息主体相关的用户鉴别信息（如：卡片验证码、卡片有效期、登录密码、支付密码等）；处于已登录状态时，个人金融信息展示的技术要求如下：
   1) 除银行卡有效期外，用户鉴别信息（如：卡片验证码、登录密码、支付密码等）不应明文展示；
   2) 对于银行卡号、客户法定名称、手机号码、证件类或其他识别标识信息等可以直接或组合后确定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，应履行客户端身份验证，并做好此类信息管理，防范此类信息泄露风险；
   3) 涉及其他信息主体的信息时，宜进行屏蔽展示，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。
h) 客户端应用软件应提供认证失败处理功能，可采取结束会话、限制失败登录次数和自动退出等措施；
i) 客户端应用软件应配合服务端提供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，避免采用简单交易密码或与客户个人信息相似度过高的交易密码；
j) 应严格限制使用初始登录密码与初始交易密码，若设置初始密码，应强制用户在首次登录后修改初始密码；
k) 在修改密码前，应对用户身份进行重新验证；
l) 修改密码时应对原密码输入错误次数进行限制；
m) 修改密码时新密码不应与原密码相同；
n) 在密码重置时，应使用短信验证码、用户注册信息校核等方式，对用户身份进行校验；
o) 在进行修改密码或密码重置时，应采用两种或两种以上要素进行身份认证，如：数字证书、生物特征信息、智能风控等。

5.11 个人金融信息安全

5.11.1 数据获取

通过移动金融客户端收集客户个人金融信息时，具体技术要求如下：
a) 客户端应用软件应保证内存中不应存在完整的银行卡密码明文；
b) 客户端应用软件的临时文件中不应出现支付敏感信息，临时文件包括但不限于 Cookies、本地临时文件等；
c) 客户端应用软件程序应禁止在身份认证结束后存储支付敏感信息，防止支付敏感信息泄露；
d) 客户端应用软件运行日志中不应打印支付敏感信息，不应打印完整的敏感数据原文；
e) 应采取技术手段防止内存中加密的敏感数据被还原为明文；
f) 客户端应用软件应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；
g) 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，应采取防篡改机制保证数据不被移动终端的其他程序篡改；

h) 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。

5.11.2 数据访问控制

移动金融客户端应对可获取客户个人金融信息的操作应进行访问控制：

a) 应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；
b) 客户端应用软件在授权范围内，不应访问非业务必需的文件和数据。

5.11.3 数据传输

移动金融客户端与服务端进行数据传输时，具体技术要求如下：

a) 应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，协议版本应及时更新至安全稳定版本；
b) 应确保采用的安全协议不包含已知的公开漏洞；
c) 客户端应用软件与服务器应进行双向认证，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；
d) 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，应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，则应评估敏感数据调用的风险，并设计补救措施；
e) 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，应采取加密等措施确保其保密性；
f) 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，应采取措施（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，则应评估关键数据传输的风险，并设计补救措施；
g) 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、身份证号码等，在通过公共网络传输时，应采取措施（如：数字签名、MAC 等）确保其完整性；
h) 通过客户端应用软件发起的资金类交易报文，应确保交易报文的不可抵赖性，在有条件的情况下应采用数字证书技术；
i) 通过客户端应用软件发起的身份认证或资金类交易报文，应能够防止重放攻击。

5.11.4 数据存储

移动金融客户端存储个人金融信息时，具体技术要求如下：

a) 客户端应用软件不应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；
b) 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；
c) 客户端应用软件应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。

5.11.5 数据使用

信息展示

应用软件的后台管理与业务支撑系统，对个人金融信息展示具体技术要求如下：

a) 除银行卡有效期外，C3 类别信息不应明文展示；
b) 应采取技术措施防范个人金融信息在展示过程中泄露或被未经授权的拷贝；

c) 后台系统对支付账号、客户法定名称、支付预留手机号码、证件类或其他类识别标识信息等展示宜进行屏蔽处理，如需完整展示，应做好此类信息管理，采取有效措施防范未经授权的拷贝；
d) 后台系统不应具备开放式查询能力，应严格限制批量查询；
e) 对于确有明文查看需要的业务场景可以保留明文查看权限，后台系统应对所有查询操作进行细粒度的授权与行为审计；
f) 应防止通过散列碰撞等方法推导出完整的数据，若使用“截词”的方式进行部分字段的屏蔽处理，不应用散列代替字段被截词的部分。

共享和转让

移动金融客户端软件在对个人金融信息进行共享和转让的过程中，应充分重视信息转移或交换过程中的安全风险，具体技术要求如下：

a) 在共享和转让前，应开展个人金融信息安全影响评估，并依据评估结果采取有效措施保护个人金融信息主体权益；
b) 在共享和转让前，应开展个人金融信息接收方信息安全保障能力评估，并与其签署数据保护责任承诺；
c) 支付账号及其等效信息在共享和转让时，除法律法规和行业主管部门另有规定外，应使用支付标记化技术进行脱敏处理（因业务需要无法使用支付标记化技术时，应进行加密），防范信息泄露风险；
d) 应根据“业务需要”和“最小权限”原则，对个人金融信息的导出操作进行细粒度的访问控制与全过程审计，应采取两种或两种以上鉴别技术对导出信息操作人员进行身份鉴别；
e) 应定期检查或评估信息导出通道的安全性和可靠性；
f) 使用外部嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）进行信息共享与转让时，应定期检查或评估信息共享工具、服务组件和共享通道的安全性和可靠性，并留存检查或评估结果记录；
g) 应执行严格的审核程序，并准确记录和保存个人金融信息共享和转让情况。记录内容应包括但不限于日期、规模、目的、范围，以及数据接收方基本情况与使用意图等，并应确保对共享和转让的信息及其过程可被追溯；
h) 应采取有效技术防护措施，防范信息转移过程中被除信息发送方与接收方之外的其他个人、组织和机构截获和利用。

公开披露

个人金融信息原则上不得公开披露。金融业机构经法律授权或具备合理事由确需在移动金融客户端进行公开披露时，具体技术要求如下：

a) 应事先开展个人金融信息安全影响评估，并依据评估结果采取有效的保护个人金融信息主体权益的措施；
b) 不应公开披露个人生物识别信息；
c) 应准确记录和保存个人金融信息的公开披露情况，包括公开披露的日期、规模、目的、内容、公开范围等。

汇聚融合

个人金融信息汇聚融合的技术要求如下：

a) 汇聚融合的数据不应超出收集时所声明的使用范围。因业务需要确需超范围使用的，应再次征得个人金融信息主体明示同意；

b) 应根据汇聚融合后的个人金融信息类别及使用目的，开展个人金融信息安全影响评估，并采取有效的技术保护措施。

开发测试

个人金融信息在开发测试过程中的具体技术要求如下：

a) 应对开发测试环境与生产环境进行有效隔离；
b) 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。

删除

个人金融信息在删除过程中的具体技术要求如下：

a) 应采取技术手段，在金融产品和服务所涉及的系统中去除个人金融信息，使其保持不可被检索和访问；
b) 个人金融信息主体要求删除个人金融信息时，金融业机构应依据国家法律法规、行业主管部门有关规定以及与个人金融信息主体的约定予以响应。

数据销毁

个人金融信息在销毁过程中的具体技术要求如下：

a) 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；
b) 客户端应用软件进程被结束时，应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；
c) 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；
d) 客户端应用软件应确保无法通过技术手段恢复已清除的敏感数据；
e) 客户端应用软件应支持页面返回后自动清除银行卡密码、网络支付交易密码、登录口令等支付敏感信息的机制；f)客户端应用软件应对后台任务列表中的预览界面采取模糊或其他防护措施；
f) 当客户端应用软件从前台进入后台时，超过设定时限后应清除页面中已输入的敏感数据；
g) 客户端应用软件在安全退出登录时，应向服务器发送会话结束请求，使当前会话状态失效。

6 移动金融客户端软件备案认证

6.1 对标自查

每年根据监管要求，组织对移动金融客户端进行对标自查，对不符合要求的制定整改计划并确保当年完成整改工作。

对标自查项目包括但不限于：

a) 数据安全：数据防监听、防篡改、有效性校验、外接键盘输入设备的安全性、完整性、保密性、抗抵赖性、使用安全、删除安全、访问控制安全、异常处理安全；敏感/个人信息存储安全；
b) 通讯安全：安全协议通道，双向认证，会话超时/退出，实体间通信安全；
c) 加密算法和密钥安全：加密算法安全，密钥加密/解密安全，应用软件/后台系统的密钥管理安全；
d) 应用软件自身安全保护：第三方组件安全，H5 页面安全，接口安全，抗攻击性，环境校验，下载更新安全，审计安全；

e) 身份认证安全：防绕过，图形验证码安全，双因素认证，密码复杂度，修改/重置密码安全；
f) 应用软件生命周期管理：软件的开发、测试、发布、升级维护的安全性；
g) 二维码业务安全：二维码的申请、显示、解析、支付的安全，脱机二维码的安全，监控要素的采集与上送的安全。

6.2 备案认证

按监管要求组织开展移动金融客户端的备案、移动金融认证和银联支付应用软件认证。

a) 移动金融客户端软件应根据中国人民银行《关于发布金融行业标准加强移动金融客户端应用软件安全管理的通知》（银发[2019]237 号）要求，由业务主办部们组织向中国互联网金融协会进行备案；
b) 移动金融客户端软件备案后发生重大变更需要更新发布的，应当事先向中国互联网金融协会办理备案。重大变更包括但不限于以下情形：
   (1) 客户端软件名称、主要功能、技术架构、建设标准、建设内容发生重大变更的；
   (2) 对客户端软件运行安全产生重大影响的；
   (3) 可能对客户资金安全产生重大影响的；
   (4) 可能对客户个人信息保护产生重大影响的；
   (5) 可能造成客户端软件长时间中断服务的；
   (6) 变更实施技术难度较大的；
   (7) 有关管理部门、中国互联网金融协会认定的其他情形。
c) 移动金融客户端软件备案后，出现影响资金安全、信息保护或其他重大安全风险的情况，需要进行紧急变更的，可以先进行客户端软件的修复和发布，事后 10 个工作日内补办变更备案，并说明紧急变更原因。

7 技术先进性

7.1 兼容性

7.1.1 软件兼容性

移动金融客户端软件兼容终端型号数量>=50。

7.1.2 系统兼容性

移动金融客户端软件安全运行支持的操作系统最低版本为安卓 4.4 以及 iOS 9。

7.1.3 网络环境兼容性

移动金融客户端软件兼容IPv6网络环境。

7.2 性能

移动金融客户端应用服务应满足以下要求：

a) 移动金融客户端软件安装包文件大小不应超过 150MB
b) 移动金融客户端软件冷启动时间<=1 秒；
c) 移动金融客户端软件的后台服务器响应时间<=1 秒；
d) 移动金融客户端软件的后台服务器支持并发>=300；
e) 移动金融客户端软件 CPU 占有率<=0.1%；

f） 移动金融客户端软件内存占有率<=5%。

7.3 移动金融客户端更新

移动金融客户端需从服务端下载文件或补丁文件时，应保证下载通道的安全性，动态安装文件或补丁文件前应校验文件的完整性。

7.4 软件共存

a） 移动金融客户端软件在安装时与其它正在运行的移动金融客户端软件之间允许共存。

b） 支持与其它独立移动客户端软件（移动客户端杀毒软件等）共存。

企业标准信息公共服务平台
公开
2020年09月30日 10点33分