长城华西银行股份有限公司企业标准

Q/CCHX 003—2021

移动金融客户端应用规范

Standards of finance mobile client application

企业标准信息公共服务平台
公开 2021年08月05日 16点46分

2021-08-05 发布　　2021-08-05 实施

长城华西银行股份有限公司　　发布

目　次

企业标准信息公共服务平台
公开　2021年08月05日 16点46分

前　言

本标准按照 GB/T 1.1—2019 给出的规则起草。

本标准由长城华西银行股份有限公司提出并归口。

本标准起草部门：长城华西银行股份有限公司互联网金融部、科技部。

本标准主要起草人：唐卿莹、刘昌平。

企业标准信息公共服务平台
公开 2021年08月05日 16点46分

引　言

为强化标准引领作用，促进全面质量提升，长城华西银行股份有限公司制定《移动金融客户端应用规范》，对移动金融客户端应用提出要求，客户体验、服务规范、创新规范、机制保障四个方面。

本部分旨在有效提升移动金融客户端应用规范，促进移动金融客户端发展。本部分既可作为移动金融客户端应用的依据，也可作为各单位开展检查和内部审计的依据。本部分仅限于应用在长城华西银行股份有限公司。

企业标准信息公共服务平台
公开 2021年08月05日 16点46分

移动金融客户端应用软件安全管理规范

1 范围

本标准规定了移动金融客户端应用软件安全规范，以及客户端应用软件设计、开发、维护和发布的管理要求。

本标准适用于本行移动金融客户端产品。

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 0092-2019《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 术语和定义

下列术语和定义适用于本标准。

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

指在移动终端上为用户提供金融交易服务的应用软件，包括但不限于可执行文件、组件等。

3.2 资金交易类客户端应用软件 capital transaction client app lication software

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包括但不子手机银行、支付APP等。

3.3 信息采集类客户端应用软件 information collection client application software

指不直接向用户提供资金交易服务，但需采集个人敏感信息的移动金融客户端应用软件。

3.4 个人金融信息 personal financial information

指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，包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反映特定个人某些情况的信息。

3.5 支付敏感信息 payment sensitive information

支付信息中涉及支付主体隐私和身份识别的重要信息。

3.6 语音识别 automatic speech recognition

指通过网上银行进行资金操作交易，如转账、订单支付、缴费等。本人名下的投资理财、托管账户以及本人签订委托代扣协议的委托代扣等风险可控的资金变动不属于此范畴。

4 缩略语

以下缩略语适用于本标准：

APP:客户端应用软件(Application software)

URI:统一资源标识符(Uni form 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 总体要求

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。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。

6 移动金融客户端应用软件安全规范

6.1 客户端安全要求

a）客户端应用软件在运行时应具备对运行环境的检查能力，包括:系统是否被未经授权获取管理员权限、程序运行环境是否可信。

b）移动客户端应使用代码加壳、代码混淆等手段对客户端应用软件进行安全保护。

c）移动客户端应用软件应实现身份认证过程的防截屏、录屏。

d）客户端应用软件在展示个人信息时应屏蔽关键字段（必须由用户确认的除外）。

e）客户端应用软件应提供客户输入密码的即时防护功能，防止密码被截取。

6.2 用户身份认证

a）密码设置应支持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。

b）在修改密码前，应对用户身份进行重新验证，修改密码时新密码不应与原密码相同。

c）应严格限制使用初始密码，若设置初始密码，应强制用户在首次登录后修改初始密码。

d）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、生物特征识别等方式。

e）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。

f）若采用短信验证码作为验证要素，短信验证码应仅限于在规定时间内使用一次，短信验证码应具备长度和随机性的要求。

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。

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-次，图形验证码应由服务器生成，图形验证码不得作为独立的身份验证要素。

i）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。

j）在提示客户认证失败时，应模糊错误提示信息，防止错误提示信息中泄露用户敏感数据。

6.3 逻辑安全

a）客户端应用软件申请权限时，应遵循最小权限原则。

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，避免逻辑漏洞的出现，确保认证流程无法被绕过并防止越权访问。

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）当用户闲置在线状态超出时限时，应设计合理的账户登录超时控制策略。

6.4 传输安全

a）在外部网络内传输时实现全报文加密，保证交易数据的机密性，涉及信息交互的WEB页面应使用https协议。

b）实现数字签名等功能，防止交易中的抵赖发生，对于交易类信息需保证信息传输时的完整性。

c）数据交互应满足“最小必须”原则，仅交互完成相关交易所必需的数据。

6.5 算法及密钥管理

a）加解密密码算法宜采用符合国家密码主管机构要求的国产商用密码算法。

b）加密和签名宜分配不同的密钥，且相互分离。不应以编码的方式将私钥明文（或密文）编写在应用程序相关代码中，防止因代码泄露引发密钥泄露。

c）应依据应用程序接口等级设置不同的密钥有效期，并对密钥进行定期更新。

7 客户端应用软件管理要求

7.1 设计要求

a)客户端应用软件设计应遵循安全、可靠、易用、可维护和可扩展等原则，制定用于指导客户端应用软件设计与开发的总方案。

b)客户端应用软件应提供易用、风格统、体验良好的用户界面。

c)客户端应用软件应遵循合法、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。

d)客户端应用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，并经个人金融信息主体自主选择同意。

e)客户端应用软件不得以默认、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。

7.2 开发要求

a)客户端应用软件开发过程中应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，避免在请求、响应、存储、配置等功能中存在漏洞。

b)客户端应用软件开发过程中应建立并维护开发文档。

c)客户端应用软件开发完成后，应同步完成产品手册、用户手册或提供在线帮助说明功能。

d)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。

7.3 发布要求

a)客户端应用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和发布者，提供安全可靠的应用软件下载、发布、升级渠道。

b)客户端应用软件应当删除调试或测试中存留的敏感数据。

c)客户端应用软件安装过程中，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)客户端应用软件有新版本时，不能未经用户允许自动安装新版本。

e)若客户端应用软件支持动态模块更新,应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:动态模块更新后不得影响用户使用，不得修改用户有的安全配置。

7.4 维护要求

a)应制定科学、合理的管理策略和执行制度，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。

b)客户端应用软件应具有明确的应用标识符和版本序号，设计合理的更新接口，当某一版本被证明存在安全隐患时，应及时进行修复更新。

c)以SDK等形式对外提供金融交易类服务时，应记录SDK信息及引用本SDK的外部应用软件信息。

企业标准信息公共服务平台
公开 2021年08月05日 16点46分

参 考 文 献

[1] JR/T 0092-2019《移动金融客户端应用软件安全管理规范》
[2] JR/T 0171-2020《个人金融信息保护技术规范》

企业标准信息公共服务平台
公开 2021年08月05日 16点46分