

标准研究

2022 年第 1 期（总第 20 期）

证标委秘书处

2022 年 4 月 12 日

摘 要

本期《标准研究》特别推出“2021 年企业标准‘领跑者’”专刊，主要由 2021 年证券期货基金领域企业标准“领跑者”上榜单位供稿，分享参与企业标准“领跑者”的活动心得，以及标准在企业内部的应用经验，有助于行业机构学习借鉴，提升对标准化工作的认识。

目 录

一、长江证券移动金融客户端开发规范.....	1
二、国泰君安证券区块链电子数据存证标准.....	3
三、中信建投证券移动金融客户端技术要求.....	7
四、中信建投期货移动金融客户端技术要求.....	12
五、工银瑞信基金移动金融客户端应用技术规范.....	16

一、长江证券移动金融客户端开发规范

为提升服务水平，提高市场竞争力，保证个人金融信息安全及客户权益，长江证券股份有限公司（简称长江证券）第一时间组织安排企业标准制定工作。在公司内部，组织安全、客户端、服务器、数据等各个方向的骨干员工针对相关标准的各个点进行深入的讨论和评判；在公司对外，协调安全、数据等开发商进行广泛咨询。最终确认了针对长江证券的“移动金融客户端应用”的企业标准，该标准主要从以下三个方面进行考虑和设计。

（一）标准的完善性

1.文档格式。严格按照模板进行编辑，对文档做好架构性的设计，从目录、字体、内容、格式等方面，严格按照标准规范进行排版和编写。

2.文档内容。按照标准规定的内容逐一核实规范，确认规范的基本要求，例如包含已有的国家标准的内容，在此基础上根据企业自身的评估，确认更加细化的内容。

（二）安全性及先进性

安全性是企业标准的核心内容，也是金融服务信息领域的核心要求。标准规定了移动金融客户端在设计、开发、运维过程中的安全要求，同时移动金融客户端在使用过程中，会对个人金融信息进行收集、传输、存储和使用，在各个环节做出企业要遵循的标准。在这个过程中，也可以梳理、审

视和规整企业本身在安全方面所制定规范的不足。

先进性方面，积极响应国家当前在金融领域着力推进的技术入手，比如国密、生物识别、无障碍使用、隐私及权限的最小化获取。同时，从企业的优势点出发，比如客户端的性能、安全标准等级等。

（三）覆盖客户端的全链条

“移动金融客户端”标准涉及到的不仅仅是客户端本身，还包括数据的传输、储存，客户隐私的保护和服务，应急处理、数据管理规定等。涉及的人员也不仅仅是客户端相关的开发人员，也包含服务器、数据、安全等工作人员，在制定相关标准时，需要全链条人员都参与进来。

通过本次企业标准的制定，对企业本身在“移动金融客户端”开发方面也有很大的现实指导意义。首先，职责更加明确，“移动金融客户端”的标准涉及全链条，各个环节的核心工作也都可以明确下来。其次，提升了安全性，不仅仅是客户端本身的安全，也涉及到数据的传输、存储、保存、管理等方面。第三，提高了客户端技术先进性，尤其是性能这块，在对相关标准梳理和制定的同时，也对企业本身客户端的使用体验和性能方面做了很大的改善。

后续，长江证券将在该企业标准的基础上进一步探索和研究标准研制工作，助力标准化真正成为行业“移动客户端”的推进器，引领行业移动金融客户端工作向高质量发展。

二、国泰君安证券区块链电子数据存证标准

2018 年 9 月，最高人民法院发布了《关于互联网法院审理案件若干问题的规定》（以下简称《规定》），明确提出“当事人提交的电子数据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认”。对于经区块链存证的电子数据，该《规定》明确了在政策、法律、科技的推动下，区块链存证越来越成熟并被金融机构应用。在证券公司内部，存在大量电子数据存证场景，例如客户在开户、业务办理、金融产品购买等流程中均需要使用电子合同，以国泰君安证券股份有限公司（简称国泰君安证券）为例，日均签署电子合同达 5 万份，同时国泰君安证券的投资研报、版权文章、客户对账单等都有进行存证保护的需求，这些电子数据都可以在区块链系统中进行安全、永久的存证保存并获得相应的司法保护。然而目前行业缺乏统一的规范性指导文件，面临着数据格式不一致、技术要求不统一、存证流程不完整等问题，使得区块链存证的有效性难以得到普遍认可。在此背景下，亟需统一的标准来规范企业区块链存证应用，引导行业在规范化的平台和环境下加速成长。

国泰君安证券直面行业痛点，组织区块链技术骨干及业务专家，结合行业要求和自身情况，制定符合企业规划和业务要求的存证标准，并从四个方面进行了充分考虑和设计。

应用模型有效性设计。本标准应用模型设计充分考虑了存证系统完备、证据有效、证明机构有效等方面，从规范完整的业务流程设计、完善的权限机制、技术机制以及应急机制等保障存证业务系统的有效性。通过电子证据摘要计算唯一性算法、存证取证可验证、多方验证等保证电子证据存取的有效性。引入独立授时机构作为可信时间源、对获取时间的程序模块存证和提供查询核验等保证电子证据存证时间的有效性。对于存证证明，标准还建议应用端与底层区块链通过加密方式通信，防止节点伪造或数据泄露。此外，标准还引入电子数据元信息的存证与核验机制，且要求按业务各环节先后发生顺序依次存证并支持核验。

技术先进性。系统设计充分考虑了基础环境、软硬件、网络环境的安全性，且标准中所有加密、摘要、签名算法均支持国密算法。包括安全的物理环境、安全计算环境、边界安全控制、网络防护等，以及从链基础功能、区块链证书、区块链浏览器的基础设施层和应用端安全要求。存证中涉及的哈希摘要计算推荐使用 SM3 算法、加密通信使用国密 SSL 等。

存证数据完整性设计。标准充分考虑了存证数据定义、传输、验证、检索及隐私保护方面。系统可根据不同业务类型定义不同存证数据模板。存证数据的验证、检索方式便捷多样。存证数据存储、应用需严格遵循法律合规要求，保障数据隐私。

存证流程完整性设计。标准充分考虑了应用原则、参与方及关键过程等方面，应用原则涵盖合规性、有效性、可追溯三个方面，涉及的参与方包括应用业务相关方和应用系统支持方。关键过程涵盖了区块链网络定义、存证模板定义、存证数据预处理、存证签名、上链存证和公示、司法鉴定、出证全流程，完整定义了存证业务流程的全生命周期。

标准自实施以来，已在理财、业务办理、官网等应用，提供了统一存证平台，实现了不同平台、不同格式的数据标准统一，进行流程化规范化的存证。系统可以基于场景定义不同的链式证据模板，并以理财为例设计了登录、产品详情、适当性匹配、签署、下单等关键步骤形成环环相扣的链式证据，增强了业务系统存证数据的法律效力。同时，通过定义统一的存证公共组件，便于业务快速接入存证应用，将存证业务的开发效率提升 60%。另外，提供规范的存证模板，存证数据的录入按模板检测，实现存证数据自动化检测，避免不规范或错误数据的录入。目前标准的应用效果良好，每日上链数据 5 万条，累计数据超百万。通过制定标准规范系统

存证应用，不但对于提升证据司法有效性认定具有重要价值，同时也降低各系统应用成本，提升了开发效率和数据治理水平，提高公司乃至行业整体的区块链存证应用水平。后续，国泰君安证券还计划在该企业标准的基础上进一步探索研究区块链存证行业标准，助力标准化真正成为行业数字化转型的推进器，引领行业科技工作健康发展。

三、中信建投证券移动金融客户端技术要求

在当前互联网金融浪潮中，信息系统建设与安全运行的压力越来越大，所面临的信息安全形势也日趋复杂，金融 APP 安全、管理和运营方面的问题尤为严峻。中信建投证券有限公司（简称中信建投证券）起草的《中信建投证券移动金融客户端技术要求》，遵循国家相关政策与标准的要求，紧贴行业需求与业务特点，从移动金融客户端（以下简称“金融 APP”）安全技术、软件管理、生物特征识别、无障碍服务等方面提出了标准要求，中信建投证券以蜻蜓点金 APP 为首的一系列金融 APP 均参考了该标准进行实施，减少设计缺陷和安全漏洞，提升 APP 研发的质量和安全运营水平，为金融客户提供更高质量的服务。

（一）安全技术

随着国家对个人信息保护的力度不断增大，各监管部门相继出台了监管政策。本标准的制定中依据相关监管要求，主要关注以下几点。

1. 国家密码技术应用

标准关注对身份鉴别、通信数据传输、证书管理等进行规范，确保客户的身份真实性，通信数据机密性和完整性。

2. 个人信息保护

标准关注个人信息的采集、使用、传输、存储等过程中的个人信息保护，从个人信息全生命周期管理的角度规范 APP 中权限获取、个人信息收集范围等。

根据以上关注点，该部分标准从以下方面提出技术要求：

1.开发安全：标准主要防范攻击者对客户端程序的调试、分析和篡改。

2.逻辑安全：标准对风险控制、避免业务逻辑漏洞等方面提出要求。

3.数据安全和个人金融信息安全：标准对通信安全、本地存储、输入验证、隐私政策、权限申请进行规范。

4.身份认证安全：标准对密码复杂度、安全输入控件、多因素认证进行规范。

5.密码算法和密钥管理：标准要求密码算法应使用 SM2、SM3、SM4 算法，关键密钥管理应使用硬件密码设备。

6.运行环境安全：标准提出了开发、测试、仿真、生产环境应有效隔离，对 SDK 的使用应符合要求。

（二）应用管理

证券行业数字化转型和高质量发展离不开安全稳定的软件应用和系统。为了给每位用户提供极致服务体验，金融 APP 多采用敏捷开发模式，更新迭代较快。标准从缺陷管理、兼容性要求、性能要求、应用更新等方面制定要求，致力于

提高稳定性和研发效能，提升客户体验，为用户提供系统先进、功能强大、体验良好的移动应用软件。标准主要从以下几个方面进行规范：

1.缺陷管理：标准对金融 APP 软件缺陷修复提出要求，要求缺陷按照分级管理的策略，不同级别的缺陷对应不同的修复时限。

2.兼容性要求：移动客户端的品牌、型号众多，不同的操作系统、不同的尺寸经常面临不同的适配要求。标准对金融 APP 软件兼容性进行规范，要求对主流的 android、ios 和鸿蒙操作系统予以支持，对 IPV6 网络予以支持，能够识别无网或弱网状态并提示下一步操作。

3.性能要求：移动网络、客户端硬件性能、页面复杂程度、服务端响应是性能影响的主要因素，直接关系到客户体验。标准对以上性能指标进行了明确定义。

4.应用更新：标准从保护客户权益和体验方面，对更新过程进行了规范。

（三）生物特征识别

得益于互联网金融在证券行业的快速发展，生物特征识别技术在证券金融 APP 中的应用场景遍地开花，被广泛应用于移动身份认证、身份识别。业务办理过程中的活体检测、指纹、人脸登录等功能，为客户带来了方便。结合证券业务

有强合规、高安全的特点，对于生物特征技术的应用，标准重点规范了以下几个方面：

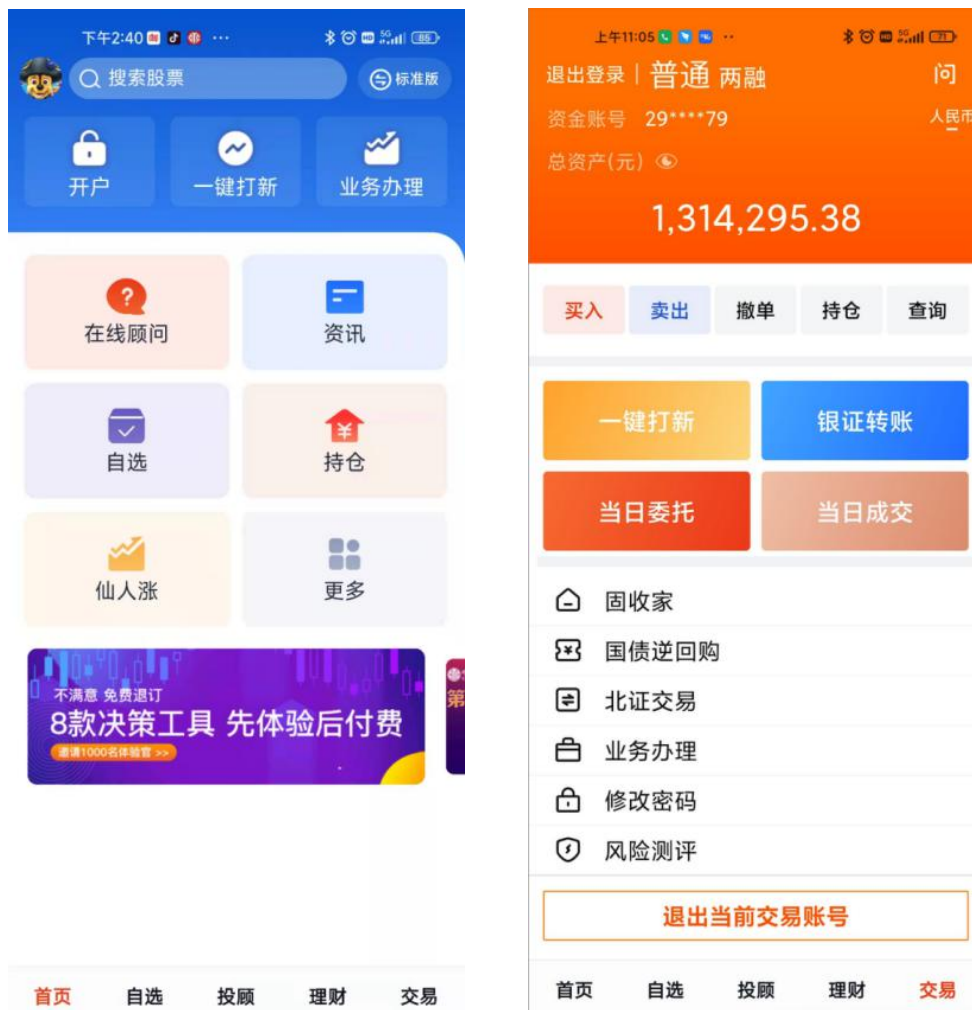
1.安全性：标准对错误率、失效处理等方面提出要求，确保所用户信息安全。

2.准确性：根据不同的业务场景，标准定义了不同的阈值，包括错误接受率、错误拒绝率等。

3.合规性：根据不同的应用业务特点，标准对多特征绑定校验、其他身份证明组合检验等模式提出了要求。

（四）适老化

随着金融 APP 的逐渐普及，全面延伸了普惠金融的广度和深度，提升了信息化建设水平和力度，极大地方便了社会公众，也提升了金融服务效率。然而，对于诸如老年人、视障人士等人们而言，由于该群体的特殊性，现阶段其金融需求需要得到更好的满足。标准遵循《证券期货业移动互联网应用程序适老化服务规范》，对适老化提出了明确要求。



后续，中信建投证券将持续以“领跑者”活动为标杆，推动企业标准化建设，不断研究和跟进国家标准和行业标准，关注新技术和新场景，并注重同实践的结合。未来，中信建投证券将不断强化企业标准化意识，提升金融服务能力，助力行业高质量发展，致力于为用户带来更好的体验。

四、中信建投期货移动金融客户端技术要求

随着互联网+金融模式的深入探索，金融服务的重心已逐步向移动端倾斜，“移动金融客户端应用”在功能上日益丰富，在服务能力上迅速提升，目前已成为各类金融机构全方位融入生活场景、提供便捷金融服务的主要入口。

近年来，全球范围内数据安全问题频发，个人信息安全和隐私保护形势严峻。自 2017 年 6 月 1 日《中华人民共和国网络安全法》正式施行，个人信息安全保护国家保准体系等配套规章、政策文件相继出台，同时，国家各执法机构也在加大执法力度，陆续开展多次移动端的安全性相关检查，主要涉及移动端应用的自身安全性及移动端用户权益保障。在此背景之下，中信集团也要求各子公司对移动端 APP 进行摸排整改，建立健全个人信息安全管理的长效机制，开展 APP 安全认证和中信认证，提高数据安全保护能力，在严峻的执法形势下，确保公司合规以及业务健康发展。

中信建投期货有限公司（简称中信建投期货）在 2018 年上线移动端-金建投 APP，面向用户提供网上开户、期货行情、期货交易、公司研报等功能服务，金建投经过近 3 年的更新迭代，功能日益完善，下载及使用人数逐步增多。因此，金建投作为中信建投期货唯一自主研发的综合性 APP，对其设计开发、安全性能、客户端发布更新、用户身份认证、个人信息保护、数据通信安全等方面提出了更高的要求。中信

建投期货也根据一系列监管措施制定了部分移动端相关的规范，但是没有形成体系文件，缺乏导向型管理制度，急需对移动端应用程序的软件安全、管理及运营方面等统一规范要求，减少设计缺陷和安全漏洞，强化个人金融信息风险识别和监控，提升安全运营水平。

中信建投期货在内部组织专业团队牵头，并邀请第三方专业机构，结合行业要求和自身情况，制定符合监管要求、具有前瞻性及可执行性的移动端企业标准。中信建投期货在《移动金融客户端技术要求》企业标准制定过程中，参考及引用《移动金融客户端应用程序安全管理规范》、《证券期货业移动互联网应用程序安全规范》、《个人金融信息保护技术规范》和《证券期货业软件测试指南软件安全测试》四份文件编写。同时整理汇总中信建投期货金建投 APP 在安全性、身份鉴别、网络通信安全、数据安全、开发安全等方面的各项数据及资料，保证所制定的企业标准在符合各相关制度规范要求的前提下，具有企业自身的可执行性，并且该标准也要具备一定的创新性和前瞻性，使中信建投期货移动金融客户端在企业标准的规范下能够更安全更可靠。

中信建投期货《移动金融客户端技术要求》主要从两大方面进行考虑和设计，分别是移动端应用程序的安全性要求和管理性要求：

一是移动金融客户端应用程序安全要求。标准分别从身

份认证安全、个人金融信息保护、逻辑安全、安全功能设计、缺陷解决率、数据安全及网络通信安全等方面进行考虑。在业务流程的设计上充分考虑其合理性，避免逻辑漏洞的出现；在用户认证环节通过对关键类业务增加二次认证，对用户进行多重提醒，对密码的存储、传输、显示方式、长度和复杂度等方面进行明确的规定；建立健全有效的缺陷处理机制，保障故障的及时修复；在数据安全及通信管理方面对数据的获取、访问、存储、展示以及客户端与服务器的交互作出了要求，从 APP 前端对各项安全指标都进行了全面严格的规范，保障客户端的安全性。

二是移动金融客户端应用软件管理要求。标准分别从设计要求、开发要求、开发环境要求、安全测试、发布和更新要求、兼容性、性能、软件共存、系统维护、安全审计及创新和前瞻性等方面进行考虑。在 APP 设计上，遵循安全、可靠、易用、可维护和可扩展等原则，为客户提供易用、友好的用户界面；从开发角度对 APP 开发流程、项目管理及编码安全等提出了要求，开发环境有效隔离，防止账户在不同环境的混用；APP 正式上线前必须进行安全测试和安全加固，且必须由第三方安全厂商来完成；从 APP 发布和更新流程上作出了规范，保障版本更新发布的安全性；且要求 APP 兼容市面上大多数主流机型，也必须由第三方测试机构来完成；本标准也从创新及前瞻性方面结合公司实际情况作出了要

求。

标准实施以来，金建投 APP 在开发、测试、安全、发布及缺陷处理等方面严格按照标准执行，对金建投用户权限最小化及权限仅在使用时才进行声明和获取进行了改造，使之更贴合标准要求，进一步满足合规性和安全性要求。同时金建投在兼容性方面虽然已经达到标准要求，但仍然具有优化空间，可进一步提升。下一步，中信建投期货将通过企业标准提升公司移动端安全及管理要求，也会通过移动端自身的改造优化来促进企业标准的优化和完善。

五、工银瑞信基金移动金融客户端应用技术规范

当前移动互联网、人工智能等新技术领域快速发展，推动金融产品、金融服务等创新不断涌现。工银瑞信基金管理有限公司（简称工银瑞信基金）充分借助技术进步，助推自身业务的发展，并针对不同的技术领域形成了不同的内部规范。工银瑞信基金发布的《Q/ICBCCS 001—2021 工银瑞信移动金融客户端应用技术规范》企业标准，规定了移动金融客户端在产品应用设计、应用安全等方面的总体原则和基本要求，从移动金融客户端安全、管理、创新等方面着手，在对主要评估领域进行覆盖之余，还创新性的补充了个人信息安全和服务端技术相关规范，在 19 个细分领域对移动客户端应用技术进行规范，涵盖了客户端软件项目的全生命周期。

工银瑞信基金在整个标准撰写的工作中，收获良多。在标准的行文起草、结构设计方面，工银瑞信基金详细学习了《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》，在标准命名、编号、章节安排方面，严格按照导则执行；在安全方面，工银瑞信基金充分借鉴了安全领域相关国家标准和金融行业标准，结合工银瑞信基金自身的业务特点和场景，从软件安全和个人信息安全两个角度出发进行了详细的规范说明；在客户端研发管理方面，工银瑞信基金以公司内部的软件项目研发管理办法为主体，参

考了监管机构相关的要求，从设计、性能、质量保障、软件发布管理、缺陷修复、运维保障等维度进行了基本的规范阐述；在创新方面，工银瑞信基金则是从产品创新和技术创新两个视角来体现自身对创新的思考。工银瑞信基金通过规范人脸识别、指纹识别、**ORC** 识别、智能问答等应用方式，依托于大数据、人工智能等核心技术，结合多个业务场景，实现满足客户的需求，为用户带来全新的体验。