Q/027CJSC001

. . . . . 企 业 标 准

Q/027CJSC001—2023

长江证券
移动金融客户端开发规范

The enterprise standard of financial mobile application of ChangJiang Securities

2023-08 发布 2023-08 实施

长江证券股份有限公司发布

目　　次

前　言

本标准按照GB/T 1.1-2020给出的规则起草。

本标准由长江证券股份有限公司提出。

本标准起草单位：长江证券股份有限公司。

本标准主要起草人：潘进、蔡夏丰、陈晓磊、张仁松、谭小虎、明亮，张清，严文波。

引　言

移动金融客户端是金融业机构在提供金融产品和服务的过程中面向客户的最前沿也是最重要的一个环节，关系到客户能否便利、高效、安全地参与到金融体系中。作为安全防范的第一个重要环节，移动金融客户端一旦被攻破，不但会直接损害金融客户主体的合法权益，影响金融业机构的正常运营，甚至可能会带来系统性金融风险。同时，作为金融客户主体参与金融体系的最主要环节，移动金融客户端的质量、体验、技术先进性等也直接影响到我国金融体系的运行效率、我国金融体系在国际中的地位以及参与主体对我国金融体系的信心。为提升金融科技创能力和综合治理能力水平，持续强化金融科技安全与质量管理，使移动金融客户端技术水平与产品标准一致性水平同步提升，编制本规范。

长江证券股份有限公司移动金融客户端企业标准

1 范围

本标准对移动金融客户端的安全性、无故障使用、安全规范性、缺陷、兼容性、性能、更新、共存、开发管理等方面提出了规范要求。

本标准适用于提供金融产品和服务的金融机构。

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

GB/T 37076-2018 信息安全技术指纹识别系统技术要求

GB/T 38671-2020 信息安全技术远程人脸识别系统技术要求

JR/T 0192-2020 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 定义和术语

JR/T 0092-2019、JR/T 0171-2020、GB/T 37668-2019、GB/T 37076-2018、GB/T 38671-2020界定的以及下列术语和定义适用于本文件。

3.1 缺陷 Defect

程序中存在的某种破坏正常运行能力的问题、错误或者隐藏的功能缺陷。缺陷的存在会导致软件产品在某种程度上不能满足用户的需要。

3.2 崩溃 Crash

移动金融客户端由于代码不严谨造成程序中断并强制退出的一种异常，会严重影响用户使用体验。程序开发过程中需要避免这种情况。

3.3 兼容性 Compatibility

兼容性是指移动客户端在不同手机上按照最初设计的逻辑运行及界面正确展示的程度。在移动端开发中，由于不同型号的手机具有不同的机器属性，移动金融客户端在编制过程中需要针对多种属性进行完整的适配，以满足移动金融客户端更好的兼容性。由于Android厂商较多，ROM定制化也较多，Android移动金融客户端更容易出现兼容性问题。

3.4 冷启动 Cold Start

当应用启动时，后台没有该应用的进程，系统会创建一个新的进程分配给该应用，该过程就是冷启动过程。与之对应的启动方式是热启动，即后台已有该应用的进程。

3.5 响应 Response

移动金融客户端对于用户操作的反馈，重要指标是响应时间和响应速度，主要与UI设计以及向后台的数据请求有关。

3.6 性能 Performance

移动金融客户端运行过程中，运行稳定性、运行速度、内存占用、电池耗电这四个方面指标，决定着移动金融客户端的性能高低。

3.7 升级 Application Upgrade

移动金融客户端的内容不是固定不变的，随着时间推移会不断地改变，去掉无用内容，完善已有内容，增加新的内容。每一次移动金融客户端内容变化，都需要升级移动金融客户端。移动金融客户端的升级主要是在各应用市场中完成，同时，公司也提供自己的移动金融客户端升级方式。

3.8 系统权限 System Permissions

Android中限制特定进程进行具体操作的安全机制。

3.9 组件 Components

应用组件是Android应用的基本构建块。每个组件都是一个入口点，系统或用户可通过该入口点进入应用。Android系统有四种不同的应用组件，每种类型都有不同的用途和生命周期，后者会定义如何创建和销毁组件。

3.10 安全加固 Safety reinforcement

在不改变移动金融客户端代码的情况下,将针对应用各种安全缺陷的保护技术集成到移动金融客户端内，为应用开发、打包、发布、运行全生命周期提供一体化安全保障服务，有效防止针对移动应用的反编译、二次打包、内存注入、动态调试、数据窃取、交易劫持、应用钓鱼等恶意攻击行为。

3.11 误识率 FAR，False Acceptance Rate

误识率是指被误识的输入模式的数量占被识别的所有输入模式的总数的百分比。是衡量模式识别系统性能的重要指标，其值越高则误识率越高，系统性能越差。

3.12 拒识率 FRR，False Rejection Rate

拒识率是指没有被识别的输入模式的数量占被识别的所有输入模式的总数的百分比。是衡量模式识别系统性能的重要指标，其值越高则拒识率越高，系统性能越差。

3.13 创新服务 IS，Innovation Service

符合现行法律法规、部门规章、规范性文件等要求，基于新技术，向金融用户提供的尚不具备管理细则的产品或服务。

3.14 小程序 MP，Micro Program

功能相对独立、完整的不需要下载或者更新App即可使用的应用。

3.15 数字人 MH, Meta Human/Visual Human

基于计算机图像技术，创造的一种数字化的虚拟人类形象。

3.16 安全键盘 SK，Secure Keyboard

具有和原生键盘功能相同的自定义键盘，可以拦截对安全软键盘界面的截屏、录屏攻击，防止恶意代码通过后台调用系统截屏、录屏API非法窃取用户输入数据。

4 移动金融客户端应用软件安全规范

移动金融客户端的安全要求主要涉及两个方面，一方面是移动金融客户端的设计、开发和运维过程中的安全要求，另一个方面是金融主体在使用移动金融客户端过程中产生的个人金融信息本身的安全。

4.1 客户端系统架构安全

金融业机构应以“权责一致、目的明确、选择同意、最少够用、公开透明、确保安全、主体参与”的原则，设计并实施覆盖个人金融信息全生命周期的安全保护策略。

a) 在产品设计阶段，应严格相关规范，切实保护个人信息。需在个人金融信息的收集、传输、使用、删除、销毁等各个环节考虑产品的安全性。
b) 在产品开发阶段，从用户信息的输入，用户信息的展示，认证失败处理，用户信息传输，及客户端运行环境，加固防逆向等方面，遵循相关标准进行开发。
c) 在产品运维阶段，保证客户端的正常运行，各个环节做到合理的监控，规范日常运维流程。做到自动化测试及动态感知，及时尽早发现系统漏洞，并做好修复和回退工作。对于第三方 SDK，应保证相关 SDK 符合国家安全标准。
d) 在产品设计开发运维阶段，需要考虑客户端的逻辑安全设计，并随着产品功能的不断丰富，对于一些老的基础性的逻辑需要回头分析看是否有更优化的空间。

4.2 客户端使用安全性

4.2.1 身份认证信息

该部分主要遵循JR/T 0092-2019的基本要求，对于规范中的增强要求，会结合实际需求进行规范。

a) 移动金融客户端应用软件涉及到交易，个人信息展示等安全规定的场景时，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，同时还应考虑多维度验证，包含无感身份认证、智能风控、设备认证。
b) 如果使用口令密码验证，应保证密码不可与用户身份信息相似（身份信息包含：身份证号、手机号码）。
c) 图形验证码、短信验证码应具有时间限制并仅能使用一次，都需要在后台生成，图形验证码不得作为独立的身份验证要素。
d) 移动金融客户端应用软件应保证输入的密码等敏感信息的安全，应满足 JR/T 0092-2019 的要求。
e) 个人金融信息在移动金融客户端的展示，应满足 JR/T 0092-2019 的要求。
f) 客户端在支持密码登录的同时，应提供其它方式登录（如指纹登录，人脸识别登录等），从而保证用户两种以上的验证方式。

4.2.2 密码算法

a) 移动金融客户端应用软件应使用密码算法对资金有关交易或重要业务操作进行保护。
b) 密码算法、密钥长度及密钥管理方式应符合国家密码主管部门的要求。
c) 密码设置重置阶段,需要对弱密码规则进行动态调整并给出禁止使用提示,不断满足安全要求,包含但不限于连续数字，重复数字，身份证号相关，手机号相关等弱密码规则。
d) 密码进行传输时，应采用非对称方式进行加密。
e) 如果设计密钥（session，token），需要考虑密钥的实效性，跟密钥相关接口的一致性，防篡改性，重放性等方面进行考虑。

4.2.3 客户端运行环境安全

移动金融客户端应用软件在运行时应具备对运行环境的检查能力，检查的范围可包括: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(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信息等。

a) 移动金融客户端需要进行安全加固才能发布。
b) 移动金融客户端切换到后台时，应给予用户提示。
c) 检查当前程序运行环境如果为模拟器或者 Root 过系统，则给予用户提示。
d) 需要对客户端进行加固,并对加固方案在特定周期内进行升级,从而提升客户端的抗攻击能力,抵御静态分析，动态调试等操作。

4.2.4 数据安全

a) 保证数据在收集，传输，存储的安全，并考虑数据的时效性。
b) 尽量减少对用户权限的索取，即使索取，使用后，提示用户关闭相关权限的获取。
c) 保证数据的完整性，主要考虑在数据传输存储阶段，防止数据篡改。

4.2.5 生物识别安全

移动金融客户端使用较多的生物识别技术有指纹识别、人脸识别以及占比较低的虹膜识别。这些都是跟具体的设备的识别效率有关,具体的指标有误识率和拒识率。在使用生物识别技术应满足以下安全：

a) 不上传保存用户的生物识别信息到服务器上。
b) 不保存用户的交易密码到设备中。
c) 用户在使用生物识别技术时，因为误识率和拒识率的原因，导致三次以上错误后，应切换到其他认证方式，保证用户的正常交易。
d) 提供客户删除生物识别技术的途径及用户认证的替换入口。
e) 涉及客户交易，密码，资金页面，应具备防截屏和录屏的能力。

在涉及客户核心资产隐私页面，需要使用键盘的空间，如客户交易登录需要输入密码的页面，应使用自定义安全键盘，该键盘应具备以下功能：

a) 具有系统原生键盘功能，对用户实际使用无影响。
b) 支持对用户输入数据、输出数据的加密保护。
c) 支持在安全键盘运行期间的动态数据加密保护，不能被截取和录屏；

4.3 个人信息安全技术要求

个人信息的收集、传输、存储和使用均需要在个人隐私协议说明中进行完成清晰的描述。

4.3.1 个人信息收集

根据JR/T 0171-2020标准规定的信息类别，针对移动金融客户端的特点，跟个人信息收集相关的技术要求主要有：

a) 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。
b) 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。
c) 移动金融客户端收集 C3 类别信息时，应使用加密等技术措施保证数据的保密性，防止在移动金融客户端被第三方 SDK 获取。
d) 对于交易密码等敏感信息，应采取具有有信息输入安全防护、即时数据加密功能的安全控件对支付敏感信息的输入进行安全保护，并采取有效措施防止合作机构获取、留存支付敏感信息。

4.3.2 手机权限申请

a) 应根据“业务需要”和“最小权限”原则，进行手机系统权限的申请。
b) 在申请手机权限前，应弹框明确提示该申请的用途，不得提前将相关功能的手机权限用途统一提示，也不能提前申请还未将使用到的权限。
c) 用户不同意相关隐私政策或者权限，不得退出 App 或者造成整个 App 功能的禁止使用。
d) 遵循使用时才申请使用相关权限，并提示用户，相应功能使用后，可以在系统设置中关闭该权限。
e) 关于存储权限，默认使用不需要申请存储权限私有存储空间，如需要一些跨应用的权限（如访问相册，分享图片），只需要临时申请，并提示客户，该相关功能使用后，可以关闭该存储权限。
f) 关于访问设备信息权限，默认使用不需要申请权限的 AndroidId 的设备码信息申请。
g) 严格控制第三方 SDK 对敏感权限的申请，升级到最新的相应的符合《全国信息安全标准化技术委员会发布信息安全技术移动互联网应用收集个人信息基本规范的征求意见稿》规定的第三方 SDK 版本。

4.3.3 个人信息传输

个人金融信息传输过程的参与方应保证信息在传输过程中的保密性、完整性和可用性，具体技术要求如下：

a) 应建立相应的个人金融信息传输安全策略和规程，采用满足个人金融信息传输安全策略的安全控制措施，如安全通道、数据加密等技术措施。
b) 传输个人金融信息前，通信双方应通过有效技术手段进行身份鉴别和认证。
c) 通过公共网络传输时，C2、C3 类别信息应使用加密通道或数据加密的方式进行传输，保障个人金融信息传输过程的安全；对于 C3 类别中的支付敏感信息，其安全传输技术控制措施应符合有关行业技术标准与行业主管部门有关规定要求。
d) 应根据个人金融信息的不同类别，采用技术手段保证个人金融信息的安全传输；低敏感程度类别的个人金融信息因参与身份鉴别等关键活动导致敏感程度上升的（如，经组合后构成交易授权完整要素的情况），应提升相应的安全传输保障手段。
e) 个人金融信息传输的接收方应对接收的信息进行完整性校验。
f) 应建立有效机制对个人金融信息传输安全策略进行审核、监控和优化，包括对通道安全配置、密码算法配置、密钥管理等保护措施的管理和监控。
g) 应采取有效措施（如个人金融信息传输链路冗余）保证数据传输可靠性和网络传输服务可用性。

4.3.4 个人信息存储

a) 客户交易密码禁止以明文形式保存在本地，加密保证不可逆。
b) 不缓存或保存客户的交易等敏感信息；如需保存，需采用技术手段保证个人金融信息的存储安全，并对存储的信息提升保障手段，防止第三方读取。
c) 应将去标识化、匿名化后的数据与可用于恢复识别个人的信息采取逻辑隔离的方式进行存储，确保去标识化、匿名化后的信息与个人金融信息不被混用。
d) 用户可以便捷删除保存在移动金融客户端中的个人金融信息；移动金融客户端被卸载后，所保存的信息应全部从移动金融客户端中删除。

4.3.5 个人信息使用

a) 个人敏感信息展示需要在经过个人身份信息验证后才能展示，如券商展示的个人资金、总市值及个人的资产分析类数据。
b) 个人敏感信息不应明文全部展示，如资金账号。
c) 应采取技术措施防范个人金融信息在展示过程中泄漏或被未经授权的拷贝。

4.3.6 第三方平台管理规范

终端在登录或者其它用途需要使用个人信息到第三方平台时，应保证以下几点：
a) 需要与安全负责人讨论保证个人信息的安全。
b) 使用的个人信息保证不落地到第三方服务器上。
c) 应保证个人账号信息作为主体唯一信息提供给第三方使用,可以在后台生成唯一对应串传给第三方使用。
d) 涉及到设备信息（设备码、IP、位置信息、MAC 地址等）需要经过用户授权才能使用。
e) 在上线后，定期检查第三方的使用情况，防止滥用用户个人信息数据。

4.4 无障碍使用

针对移动金融客户端的特殊场景，该部分主要遵循GB/T 37668-2019的一级要求，提供基本的无障碍功能，即用户可利用自己适用的交互方式使用移动金融客户端的主要功能。
a) 移动金融客户端如果存在非文本验证码，则应提供可被不同类型器官（视觉、听觉等）接受的替代表现形式，以适应不同的残疾人群使用。
b) 移动应用中的链接，在使用特殊颜色标注的同时，还应为该链接提供链接目的和用途。
c) 在输入框处，应提供语音输入的入口。
d) 至少提供两种对比度大的皮肤供用户使用。
e) 提供多种字体大小的设置。
f) 在移动金融客户端页面中，文本颜色不应作为传达信息、表明动作、提示响应等区分视觉元素的唯一手段。
g) 在移动金融客户端中，如果有多媒体，应为多媒体信息提供概要。
h) 在移动应用中，所有可见的非纯装饰性组件均应被辅助工具正常访问。在页面局部更新后不可见组件应不可访问；在页面局部更新后新出现的可见非装饰性组件应能被用户代理正常访问。
i) 如果有广告页面的话，应提供“跳过”功能按钮。
j) 引导页应提供多种切换方式，如互动，按钮切换。
k) 所有交互性组件应容易聚焦，不应因为键盘等辅助工具遮挡；在页面局部更新后不可见的组件应不可聚焦；在页面局部更新后新出现的可见非装饰性组件应能被辅助工具正常聚焦。

l) 用户输入的错误信息应能被自动检测并且以文本形式向用户描述错误信息。
m) 实时及离线推送消息应提供多种方式的提醒，如弹框，声音，震动等方式。
n) 在移动应用中，界面风格应保持一致，在多个界面重复出现的元素应该采用一致的布局。布局变化后，应提供引导页面进行引导说明。

5 移动金融客户端应用软件技术规范

5.1 缺陷解决率

缺陷率包含功能性缺陷和崩溃率。
功能缺陷应从项目开发的各个环节尽可能杜绝。
崩溃率需要从以下几个角度进行评估：
a) 崩溃率，崩溃率应保证在 0.05%之下。
b) 单个错误影响人数，超过总人数的 0.01%的需尽快解决。
c) 修复率需要保证上面的崩溃率和影响人数。

5.2 兼容性

兼容性主要是指设备、屏幕尺寸、平台版本三个方面的兼容性。
a) 目前移动金融客户端的设备主要有 iPhone、iPad、Android 手机、Android 平板，目前根据市场占有情况，移动金融客户端应至少满足 iPhone、iPad、Android 手机三种类型的设备。
b) 平台版本支持 iOS 需要支持 9.0 及以上的版本，Android 需要支持 5.0 及以上版本，基本可以满足市场上 95%的主流机型。
c) 需要适配满足各个平台的各种屏幕尺寸的手机，基本覆盖市面上的所有机型。
d) 网络接入支持 IPv4/IPv6 双栈使用。
e) 客户端全面兼容鸿蒙系统。

5.3 性能

主要对移动金融客户端的大小，冷启动时间、内存占用、服务器响应时间提供参考：
a) 安装包不宜过大，影响客户的更新时间和流量，建议控制在 100MB 以内。
b) 安装耗时时间在 20s 以内（各种机型平均时间）。
c) 冷启动时间根据一些统计平台的数据应控制在 2 秒以内。
d) CPU 占用保证在 5%以内。
e) 内存占用保证在 200M 以内。
f) 服务器响根据服务类型响应时间不同。交易相关服务器响应在 300ms 以内，行情相关服务器响应时间在 100ms 以内，总线相关服务器响应时间在 500ms 以内。

为保证以上性能的持续优化，需要在代码、资源、打包各个环节进行优化：
a) 对 lib 文件下的 so 文件进行瘦身，目前应用市场支持 64 位 apk 的单独上传，因此客户端在打包过程中可以将 64 位 APK 包单独生成，从而减少 lib 下 so 文件的大小。
b) so 文件动态加载。在使用频率较低的功能且 so 文件较大的情况下，可以在用户使用时，动态从服务器上下载并加载 so 文件。
c) 版本迭代发布前，检查 res 文件，删除无用的资源文件。打包时，gradle 开启 shrinkResources，移除无用资源文件。

d) 根据屏幕尺寸下载相应尺寸的图片。对于清晰度要求不高的图片，仅保存一份 xh 目录线的图片文件即可。
e) 尽量使用共用的标准的资源文件。
f) 优化启动流程，减少启动时同时大量的初始化功能模块，采用延迟或动态触发的功能加载相关模块。如定位 SDK 功能，可以在使用该功能时，才初始化相关 SDK。
g) 减少 dex 文件的大小。尽量减少第三方库的引用，避免重复功能模块的重复加载。
h) 减少进程间通信的使用。

5.4 移动金融客户端更新

a) 移动金融客户端更新需要对更新内容进行详细描述。
b) 需要在应用内响应位置提示升级到最新版本。
c) 如果对最低版本限制，需提前通过短信、消息、弹框等通知客户，让客户更新最新版本。
d) 尽量减少动态更新（苹果系统有下架风险），对动态更新包的大小控制在 1MB 以内。
e) 动态更新的下达率及更新的成功率后台需要有监控并据此分析移动金融客户端升级更新的必要性。

5.5 应急处理机制

由移动金融客户端、服务器等缺陷导致大规模客户无法正常使用移动金融客户端时，需要制定多方位的应急处理机制，至少但不限于以下机制：

a) 服务器站点切换，这个环节既要求移动金融客户端根据网络情况的主动切换，也包括服务器对站点监控后通知移动金融客户端进行切换。
b) 热更新或者便捷升级方案。
c) 移动金融客户端在紧急情况下切换为应急版本以满足客户的关键使用功能，尤其是相关交易功能。

5.6 软件共存

a) 为了保证安全，应杜绝同一个移动金融客户端（包括同一移动金融客户端的不同版本）在一台设备上安装及运行，可通过安全检测、移动金融客户端或者后台对签名和包名信息进行验证。
b) 金融客户端需要保证自己的独立性，不因除收集系统层面的其它 App 的影响（如杀毒软件）。

5.7 接入三方 SDK

a) 保证三方SDK的安全性，需经过安全部门的检测，才可以面向客户使用。
b) 满足隐私的合规要求，需有相关的隐私政策文档说明，并满足最小申请和使用客户权限的标准。
c) 在非必要的情况下，三方SDK不做启动时的初始化工作，仅在使用时进行SDK功能的初始化。
d) 三方SDK的数据传输应满足4.3章节所列的安全措施，以保护用户的个人信息。
e) SDK的对接功能应满足最小的需求边界性，而不是整体无差别的全部接入使用。
f) 非必要的情况下，不暴露给第三方用户针对客户的任何隐私数据，确实需要暴露的，应做好加密、脱敏或者私有化部署的方案。

6 移动金融客户端创新性技术及创新服务规范

6.1 生物识别系统技术规范

目前我司使用到的生物识别系统主要包含：

a) 指纹登录。
b) 活体/人脸识别。

6.1.1 指纹登录

a) 指纹信息验证基于设备自带指纹验证系统。
b) 用户标识应具有唯一性。
c) 用户标识以用户名和可区分标识符实现。
d) 用户更换、删除设备指纹验证后，金融客户端应给客户合理的提示，并引导客户进行重录或者删除指纹登录逻辑。
e) 用户删除后，删除相关指纹绑定的信息。
f) 指纹识别失败后，引导客户使用其它方式进行登录。

6.1.2 活体/人脸识别

a) 活体识别采用主动配合活体检测，通过指令要求用户进行相关动作并判断人脸的真实有效性，指令包括但不限于点头、抬头、左右转头、张嘴、眨眼等。
b) 活体识别系统采用本地验证，需要保证该过程在可信环境中进行，防止相关数据采集过程中个人信息等数据不被泄露，保证不在网络上传输相关活体识别信息。
c) 应对每次活体识别过程进行留痕。
d) 本地不保存活体识别采集过程中的数据，如果是留痕或者其它合规要求的需要保存截图等相关信息的，数据保存在应用内的存储空间内。
e) 留痕或者其它合规要求的需要保存截图等相关信息需要上传到服务器的应采用满足数据传输安全策略相应的安全控制措施，如数据加密等。
f) 保证本地人脸识别库的更新，减少活体识别的错误率。
g) 活体识别失败时，应告知客户失败的错误代码或错误值。
h) 针对不同识别失败原因进行相应处理。如果是因为硬件或者本地库的原因引起的，应采用其它符合合规和安全的方式进行代替。

6.2 IPv6 实施改造技术规范

a) 以保障系统安全稳定运行为前提，应用系统改造与软硬件基础设施升级相结合递进式推进与增量式推进相结合。
b) IPv4 和 IPv6 站点需同时返回，移动金融客户端需要根据当前网络情况，使用合适的算法逻辑选择最快的站点进行连接。不可以一刀切只返回 IPv6 站点。
c) IPv6 工作不仅仅涉及网络、应用、安全、运维、监控、安全保障等技术方面，还牵涉外部运营商、域名服务商、合作厂商等诸多干系方，相关工作方案要集思广益 N 充分讨论、全面论证。
d) IPv6 推进工作要规范有序，必须经过充分的功能性、可用性、安全性等全方面的验证，测试通过后方可正式上线。
e) 在做好 IPv4/IPv6 全双栈支持的同时，要好应急准备和回退处置方案，确保紧急情况下快速响
f) 应并恢复业务运行，确保不造成重大信息安全事件。

6.3 国密改造技术规范

a) 以保障系统安全稳定运行为前提，应用系统改造与软硬件基础设施升级相结合递进式推进与增量式推进相结合。

b) SSL证书应满足国密要求，应有失效时间及失效时终端的处理逻辑，客户也可以选择更新本地使用的证书。

c) App与后台网关建立连接时应采用国密SSL，基于《GM/T 0025 SSLVPN 网关产品规范》，通讯协议采用基于ECC_SM4_SM3密码套件，进行双向认证握手，建立安全连接通道。

d) 应采取保护措施防止客户端和服务器之间的会话被窃听、篡改、伪造和重放。措施如下：

1) 采用TLS1.2安全通信协议；

2) 采用校验Token的方式对登录后所有的请求进行合法身份鉴别；

3) 数据包有签名字段，对请求数据进行签名处理，保证数据的完整性；

4) 采用校验Token的方式防止重放。

e) App退出登录后，终端与后台的会话请求应被终止。

6.4 跨平台/跨系统小程序开发技术规范

该系统平台涉及到的主要模块有：

a) 小程序前端开发模块。

b) 小程序后台管理模块。

c) 小程序鉴权中心模块。

d) 小程序微服务模块。

以上模块的关系如图 1 所示。

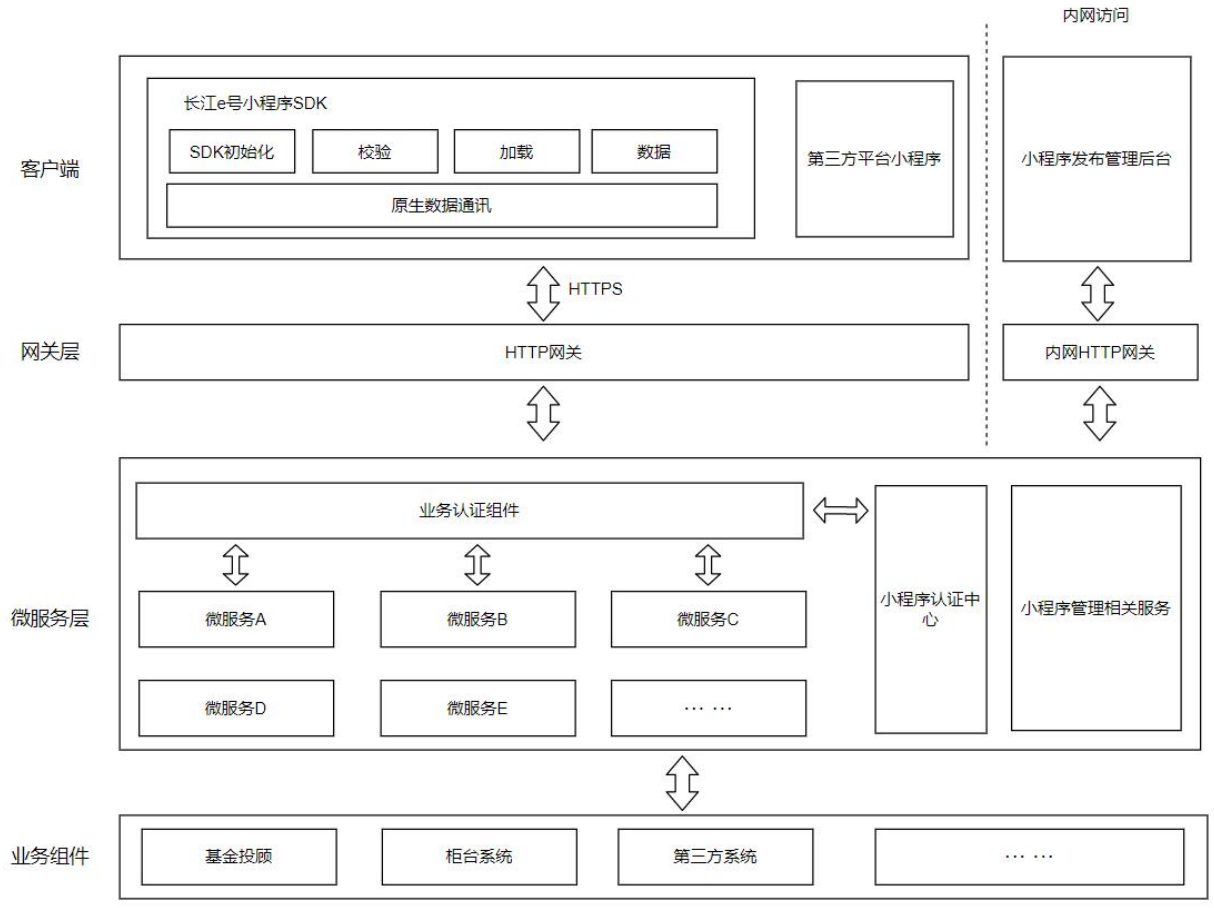

图 1 小程序系统模块示意图

6.4.1 小程序前端管理模块

小程序前端管理模块主要负责小程序前端的下载、更新、加载、通信及安全防护。

a) 小程序下载通信应满足通信安全。
b) 小程序资源包应在应用内存储空间内，保证其它应用不能访问控制和修改。
c) 小程序资源包应为加密包。
d) 小程序需要满足通信独立、跨平台、跨应用、动态更新等特征。
e) 小程序要有合理的灰度、版本回撤、版本删除等逻辑功能。

6.4.2 小程序后台管理模块

小程序后台管理模块主要负责小程序的创建，成员管理，权限管理，小程序版本管理，小程序版本开发质控流程，小程序上线，灰度发布及上线流程。

6.4.3 小程序鉴权中心模块

小程序鉴权中心模块需要满足以下规范：

a) 网关 Token 认证。
b) 网关防篡改功能，通过签名算法请求包体计算签名，通过教研签名防止请求包体篡改。
c) 网关防重放功能，基于时间戳和随机数防止请求重放。
d) 权限管理。
e) 数据传输基于 HTTPS 安全通道进行传输，一些敏感数据进行加密传输。
f) 数据传输不设计用户的敏感数据。

6.4.4 小程序微服务模块

该模块主要负责小程序功能号的转发和路由功能。

6.5 数字人功能

数字人做为智能化的终端交互工具，可以为用户提供更便捷、人性化的服务。数字人在金融领域使用的场景有很多，有营销类的，客户服务类和宣传类等方面。使用数字人时可以是播报型，也可以是交互型。在使用数字人业务，应满足下面的使用标准：

a) 确保数字人的设计和使用符合隐私法规和最佳实践，应满足 4.3 章节所列的安全措施，以保护用户的个人信息。
b) 数字人场景应提供清晰的信息，明确告知用户正在与一个虚拟数字人互动，而不是真实人类。该透明度有助于消除不准确期望。
c) 数字人应该遵守明确的伦理指南，确保其行为和决策是合乎道德的，并避免传播虚假和误导性信息。
d) 用户应该有权选择是否与数字人互动，以及何时终止互动。
e) 有严格的日志和数据统计模块，保证数字人的行为和决策是可以追溯的，并保证数字人提供的服务能够满足客户的实际需要。
f) 所涉及的知识库和大模型应保证私有化部署，并保证返回的内容符合法律法规及可以过滤相关内容的返回。