



FinClip 小程序技术白皮书

2021 年 11 月更新

版权所有 © 凡泰极客 2021。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



和其他商标均为凡泰极客技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受凡泰极客商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，凡泰极客对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1	背景.....	1
1.1	无界与开放的必然联系	1
1.2	打造金融业小程序生态	2
2	术语.....	4
3	总体架构	9
3.1	FinClip 小程序运行时与安全沙箱 SDK.....	12
3.2	FinClip 小程序管理后台	13
4	FinClip 小程序生态	17
4.1	小程序中心运营商.....	17
4.2	程序开发者	18
4.3	小程序引擎 SDK 提供商	20
4.4	小程序 SDK 插件提供商	22
4.5	小程序上下架审核管理者	23
4.6	小程序云端服务提供商	23
4.7	多方协同的行业数字生态	24
5	信息安全与隐私保护	25
5.1	端侧用户设备信息留痕	25
5.2	云侧数据安全性与隐私保护	25
5.3	网络访问控制	26
5.4	实时安全应急管控.....	26
5.5	审计	27

1 背景

最近十年来，移动互联网极大程度的改变了社会生活面貌，让消费者突破时间和空间的限制，随时随地获得网络连接的能力，不仅改变了自己的消费行为，也逼迫商家改变提供服务的方式。智能手机、移动支付、二维码、小程序给消费场景带来了 O2O，新的营销方法与手段成为可能，例如消费者在线下门店的消费能非常便利的获得积分或者消费积分，而商家则把消费者的线下足迹顺利转化为数据。

从 2017 年初，微信创始人张小龙宣布小程序正式上线开始，很多行业都在摸索着开发小程序，且取得了不错的成绩，小程序已经生长出一个相对完整的生态圈。在轻应用混战的当下，小程序已经成为巨头们角逐的焦点，支付宝、百度、今日头条、京东都先后发布各自的小程序生态平台。

在小程序爆炸性发展的前景下，可以在外部 App 上运行的小程序平台，开发者一次开发就可以多端运行，开放小程序生态的诉求变得越来越强。小程序在券商业内开始得到应用是顺应了某些需求，“这些年，各类券商 APP 在功能上不断做‘加法’，导致 App 越来越重、功能越来越多，而有的用户可能觉得返璞归真更好，或许现在是到 App 试着做‘减法’的时候了。”

1.1 无界与开放的必然联系

数字化时代这已经成为了各行各业的必由之路，在各行各业互联互通的环境下，彼此与客户、合作伙伴均通过网络进行连接与交互，传统商业组织的边界发生了变化 — 在线上，数字化边界由软件定义。

消费者的线上消费场景、活动场景，都封装在一个个应用、一堆堆代码中。在这里，应用与小程序不再是主角，而是隐藏在应用背后的支撑性服务，是场景闭环的“最后一公里”。技术上如何让我们的基础服务“输出”到这些丰富多彩的第三方应用中？又如何开放边界让

第三方合作伙伴主动“入驻”到我们的空间提供产品、内容与服务为我们的消费者客户所用？

无界的根本目标，是最大程度发展商业场景的提供者 — 合作伙伴，通过他们去触达消费者。要做到无界，就必须开放。这里的开放，我们特指：

- 在数据安全、隐私保护的前提下，才能把基础服务功能向互联网开发；
- 基于标准、主流的技术规范，避免采用封闭技术，才能降低第三方应用场景与我们集成、融合时的技术成本，从而吸引商家、合作伙伴的支持配合；
- 必须有规模化管理第三方合作伙伴的应用场景、实现连接的能力。受限于规模化能力，也谈不上开放；

1.2 打造金融业小程序生态

不仅各行各业都有着“开放与无界”的必然联系，在金融与证券行业中，也有着迫切的诉求。

在移动互联网时代之前，银行发行的一张塑料小卡片，让消费者在各种线下门店获得无现金的消费活动便利。但是，消费者只能从预生成的电子账单甚至纸质账单获得关于自己的消费行为信息，只能通过短信获得交易提醒，只能通过网银等工具查询自己的消费积分，只能通过商家张贴的广告或者店员的提醒得知使用某张特定的信用卡所获得的消费折扣或积分激励。

券商也在逐渐试水微信这样的第三方小程序平台模式，改变了原先把 App 外包给第三方的模式，并在证券行业中率先引入了小程序平台，以支持公司在金融创新业务上的各类尝试，同时又不会影响到行情和交易模块的稳定性。实现了高度模块化，让敏态模块和稳态模块各自独立、互不影响，既保证 App 在业务服务上利用小程序的灵活性快速试错、迭代，也能保证行情交易等基础服务的稳定性要求，让产品升级变得更为便捷。

本白皮书提出的方案，是把它实现成一个“小程序运行沙箱”，即借鉴腾讯、百度等公司的相关技术，建立一个类似于微信小程序的平台，公司一些业务办理功能和创新业务的尝试都可以通过小程序的形式在 App 上发布，用户无需更新 App，就可以获得最新服务。

腾讯通过其微信平台率先引领了小程序技术，阿里、百度、头条等互联网巨头均陆续跟进，各自发展出自己的小程序生态，让自己的平台更加生态化、更加开放。本文所提出的方案首先借由证券行业进行实践，并通过证券行业所必需的合规监管属性进行衍生，提供更加安全、开放的小程序运行技术。相比纯粹的 HTML5 内嵌，小程序类技术有一些显著的优势：

一、性能更佳，页面渲染不基于 DOM 而是通过 WebView 堆栈中的多个实例切换实现页面转换；尤其是在 Android 端，运行时通常可自主控制采用性能更高的 Chromium 而不是系统缺省的 WebView 进行界面渲染；

二、业务功能独立上架到服务器端经合规审批才发布，出现任何问题可以随时下架；

三、可以在即时通讯技术中进行分享、转发，真正促进人与人基于场景的交流；

四、极其松散耦合的架构，释放金融机构生产力——App 的原生部分可以做得非常稳定、简单，因为业务功能都以轻应用的方式独立在 App 之外实现。

下文将详细介绍 FinClip 小程序技术标准与平台，并尝试以金融或证券行业举例，帮助您对产品获得更深的了解。如果您对 FinClip 小程序引擎技术感兴趣，也欢迎访问我们的产品官网，或者致电咨询热线获得更多信息。

产品官网：<https://www.finclip.com/>

咨询热线：400-066-0021

2 术语

为了便于描述方案，本节先就所涉及概念术语进行定义。通过这些定义，也基本上描述了整体方案本身。

名词	解释	其他称呼
FinClip	一个轻应用技术解决方案，涵盖一个“应用商店”（FinClip App Store）、一个多设备应用运行安全沙箱（FinClip Mini-App Runtime）、一个开发工具（FIDE）、一个移动端开发助手（FinClip Mobile Assistant）	
轻应用（Mini-App）	一种区别于传统原生应用软件的技术形态，它的特点（1）免安装，使用时动态下载；（2）自动升级更新；（3）运行在设备端安全沙箱中，仅能对所在设备的资源通过沙箱作有限访问授权，并仅能建立沙箱许可的网络连接；（4）便于在社交网络中进行分享转发；（5）以 HTML5/JavaScript 为开发技术；（6）在云侧应用商店上架，即可以端侧设备使用，在应用商店下架，则端侧也消失；（7）它与互联网主流小程序技术兼容	FinClip 小程序，有时简称小程序，但需避免与微信小程序等混为一谈
应用商店（App Store）	一个轻应用的集散中心，可以对轻应用进行上下架管理、标签管理、排序、搜索、推荐。应用商店由应用商店服务（App Store Service API）和应用商店前端（Front-end）组成，前端可呈现轻应用列表不同的展示方式——视乎所在的终端设备而定，例如一般手机 App 中可能没有明显的形态，主要视乎所在 App 的需要而定；在车载系统、游戏平台中有相应的“陈列”界面；在桌面端和 Web 端则可能类似于主流应用商店	应用市场——视乎应用商店中应用的提供者参与者是一个生态群体还是独家企业小程序中心
管理账户	使用者通过应用商店的管理账户登录，访问应用商店的管理后台，对小程序与应用进行日常管理。可以在其中进行小程序上下架，应用绑定与关联，增加或编辑安全策略等操作；	
运营账户	对企业端行为进行审核管理。运营端用户可以在其中审核小程序上下架，应用绑定与关联，对安全域名进行加白或加黑	

	操作；	
开发者账户	轻应用开发者，申请获得应用商店的开发账户，从而获得向应用商店申请提交应用上下架、进行灰度发布、获得应用使用数据	
应用灰度发布	一个轻应用在上架后，可以进行一定用户范围内的发布试用，以便于业务试水、AB 测试、低成本试错	
轻应用运行沙箱、运行时 (Runtime)	又程为小程序运行时，运行的载体，为轻应用提供安全隔离的运行环境，对轻应用的代码进行解释和渲染执行。以 SDK 的形式存在，并可以被第三方集成；	FinClip Mini-App Runtime, 小程序 Runtime, 小程序 SDK, 轻应用虚拟机
FinClip SDK (Runtime SDK), 简称 SDK	上述运行时的物理形态，是一个二进制组件，供设备端原生应用的开发者嵌入至原生应用中从而获得运行轻应用的能力。因为轻应用运行时是一个设备端操作系统上指定格式的二进制库 (Library)，并且暴露一定的接口供集成者使用，所以它具备 Software Developer Kit (SDK) 的特点，对于开发者来说，是一个 SDK	FinClip Runtime SDK, 小程序 SDK
宿主	嵌入运行时 SDK 的设备端软件，是 SDK 的宿主。宿主包括但不限于 iOS Native App、Android Native App、Windows/MacOSX/Linux Desktop Application、IoT 的 Embedded OS 等等	
SDK 扩展 (Plug-in)	因为宿主环境五花八门，宿主开发者所选择集成的第三方技术包括但不限于支付、视频、人脸识别等等不可假设，为了便于这些外部技术能被运行在运行沙箱中的轻应用进行调用，运行时 SDK 提供了“插件”机制，供宿主开发者或者其所选用的第三方技术提供者把相关功能开发成插件方式注入到 SDK 中，扩展 SDK 的能力，供轻应用开发者使用。注意插件的安全漏洞能导致 SDK 的安全隔离遭到破坏，所以宿主方开发者需要对之进行严谨的安全认证与把关。一个插件以一个二进制组件的形态存在。宿主开发者需在构建宿主	

	时，把插件与 SDK 一起作为开发组件进行编译打包。	
用户	本方案范围内，特指 FinClip 轻应用的终极使用者，通常也就是嵌入了 FinClip 轻应用运行能力的宿主软件的直接用户	
宿主软件用户	iOS/Android/Windows/MacOS/Linux/车载系统/IoT 原生软件的直接使用者。这些软件嵌入了 FinClip 技术后获得轻应用运行能力，从而让该软件用户享受到轻应用的良好体验	
轻应用开发者	基于 HTML5/JavaScript 遵循主流小程序技术的开发规范，进行前端开发，并通过应用商店开发者账户获得申请轻应用上下架的权限和调用应用商店相关 API 的权限。轻应用后端，也由开发者自行负责	
插件开发者	利用 SDK 的插件机制，向 SDK 注入额外的扩展功能，供宿主进行集成，供轻应用调用。插件由插件开发者提供	
宿主开发者	设备端原生应用的开发者，也是 SDK 及插件的直接使用者	
应用商店运营者	使命是丰富应用商店的内容，发展应用商店中”商品“（轻应用）的”供应商“，并对轻应用触达用户、增加曝光率和使用频率提供一定的运营推广手段。	
技术平台运营者	把 FinClip 视作一个技术平台，以调度、运转平台多方（宿主开发者、插件开发者、轻应用开发者、用户、应用商店运营者）以促进形成生态多边、产生生态环境中各方的良性互动，从而推动生态的发展	
FIDE	FinClip 为轻应用开发所设计的开发者工具，全名为 FinClip Integrated Development Environment；	
FinClip Mobile Assistant	可实时扫码预览、测试小程序，查看小程序历史版本，一键体验凡泰小程序 DEMO 与亮点功能的移动应用；本质上是一个移动端 FinClip App Store	凡泰助手

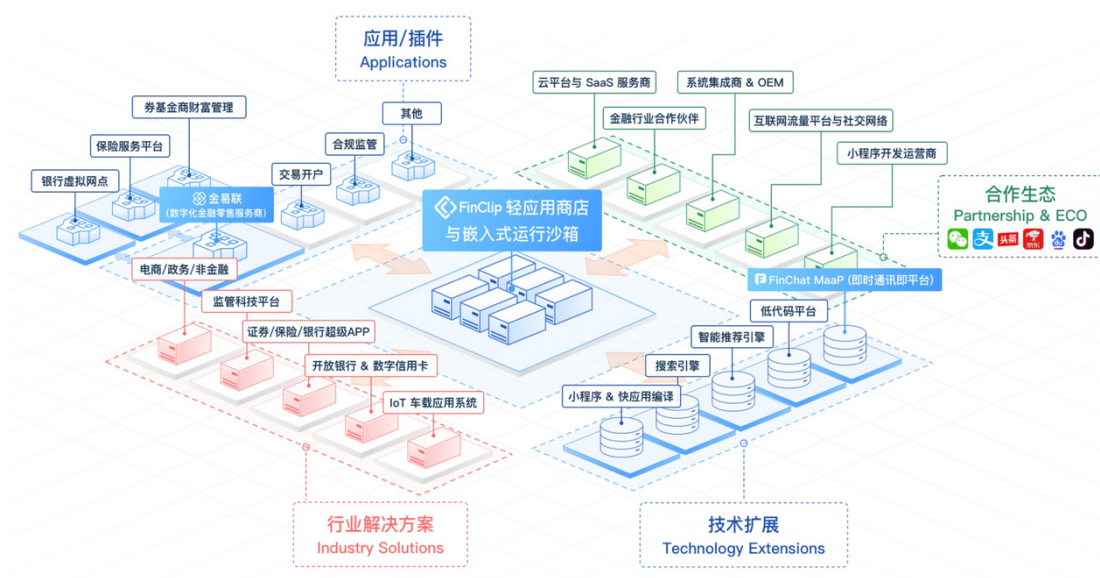
APP ID	小程序的唯一身份识别码，作为小程序运行时向服务器申请访问小程序的唯一识别码；	
Bundle ID	第三方应用的唯一识别码，在安卓应用市场表现为 Application ID，在 iOS 应用市场表现为 Bundle ID；	
SDK KEY	由第三方应用的 Bundle ID 生成的识别 ID，作为小程序运行时向服务器获取 APP ID 的识别令牌。一个运行时只有一个 SDK KEY，第三方应用集成小程序运行时 SDK 后，必须写入对应 SDK KEY，方能访问对应小程序；	
SDK SECRET	同样是由第三方应用的 Bundle ID 生成的，与 SDK KEY 配套使用的安全密钥。在集成小程序运行时 SDK 时，需与 SDK KEY 一同写入	
API SERVER	是小程序与小程序管理后台进行服务请求的服务器地址，需在集成小程序运行时 SDK 的时候进行写入；在 finclip.com 中的默认地址为 https://api.finclip.com	
白名单域名	白名单域名实际与备案的域名一致，但白名单域名是由平台运营方直接进行设置，开发者无需配置校验文件即可访问；	
平台成员	是指小程序开放平台的账号成员，拥有使用平台功能的权限；	
开发成员	是指客户端 APP 账号导入到平台后设置为开发者的成员，有打开开发版小程序和体验版小程序的权限；	
体验成员	是指客户端 APP 账号导入到平台后设置为体验者的成员，有打开体验版小程序的权限；	
开发版小程序	是开发者通过小程序平台企业端或者 FIDE 工具上传到「代码包管理」模块中的小程序版本。开发版可以直接提交审核，也可以被设置为体验版；	

体验版小程序	是从开发版中选择一个版本，让指定人员才能打开的「测试版本」，一次只能有一个开发版做为体验版，且人员数量有一定的限制，体验版无需提交审核；	
审核版小程序	从开发版或体验版中选择小程序进行提审，提交审核通过后，即可将审核版小程序发布为线上版小程序；	
线上版小程序	线上所有用户使用的小程序版本，该版本的代码在新版本代码发布后会被覆盖更新；	
关联微信小程序	将 FinClip 小程序与微信小程序进行关联，并更新小程序的二维码。用户如果用微信扫描，将会直接打开微信小程序；	
小程序插件	可被添加到小程序内直接使用的功能组件。小程序开发者可直接在小程序内使用插件，无需重复开发，为用户提供更丰富的服务。	
MD5 指纹	根据特定内容生成的不可逆验证码，开发者可通过比对指纹内容校验所下载文件与源文件是否一致。	

3 总体架构

FinClip 小程序开放平台借鉴目前主流微信小程序、支付宝小程序等互联网成熟的小程序技术方案，再结合中国证券行业的合规监管的业务场景，逐步的发展起来。它由 FinClip 小程序 SDK、FinClip 小程序管理后台、监控与合规工具以及小程序云端运行环境共同组成。

它同时也是一个生态性的协作平台，可以由金融机构本身、SDK 的提供商、小程序开发者（通常为金融机构的 IT 人员或其指定合作伙伴）、合作渠道（通常提供了 SDK 嵌入的“宿主”）进行协作。



总体架构包括：

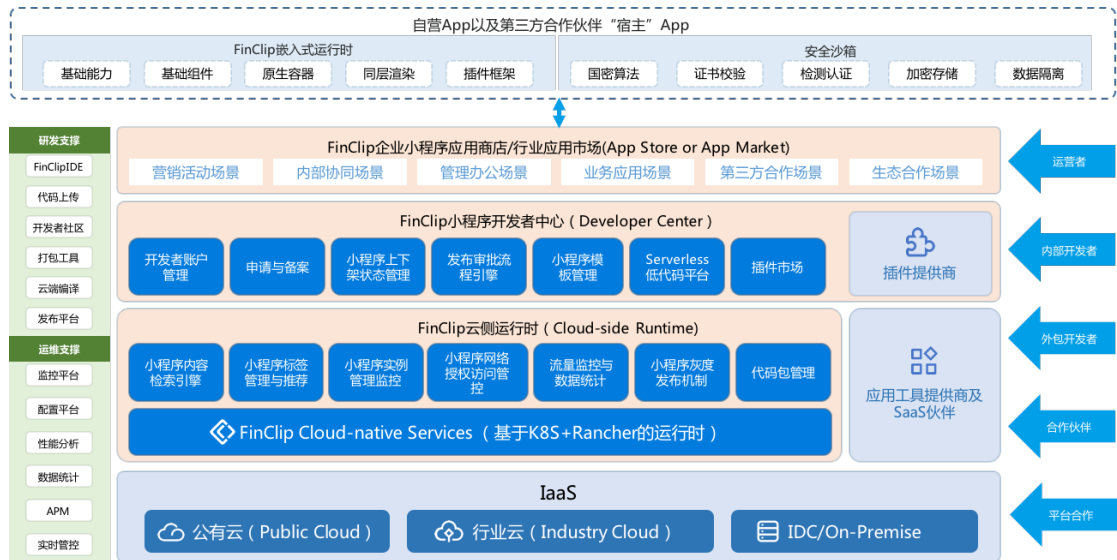
- SDK——通用 SDK 开发包，提供给 App（“宿主”）进行打包
 - 为应用提供安全沙箱机制，保证嵌入应用的安全性
 - 兼容微信小程序和一般 H5 应用
 - 完全继承小程序“用完即扔”，轻量小巧的特性
- 小程序——业务应用以小程序的形式发布到金融机构自有小程序应用中心(应用商

店的模式)

- 持牌机构小程序开发团队计划嵌入到 App 中的业务应用采用微信小程序的形式发布
- 小程序与相应的业务后端系统协同完成特定的服务
- 小程序应用管理后台——成立小程序应用管理后台
 - SDK 开发/维护/升级/安全
 - 运营小程序应用中心
 - 宿主 App 应用证书签发管理
 - 小程序 SDK 证书管理
 - 提供运营统计数据、运营支撑
 - 小程序开发管理

下图是 FinClip 小程序技术架构的示意图，中间的红色区域主要是 FinClip 小程序的核心部分，即由应用商店，开发者中心与云侧运行时三者组成，左侧的绿色区域是 FinClip 为研发与运维人员提供的主要支撑能力，顶部虚线中的蓝色区域是指 FinClip 的客户所需要在自有 App 中集成的部分。

小程序前端框架借鉴了主流前端框架 Vue 的设计思路，从小程序的应用形态，提供了简洁的编程模型，定义了一套组件和 API 接口的规范，降低了学习门槛，方便开发者快速开发小程序。



在小程序框架内部提供了小程序的生命周期管理，通过事件的方式把小程序每个阶段都注入到小程序里面，开发者可以通过这些事件来处理小程序每个阶段需要完成的业务逻辑。同时框架内部使用了虚拟 DOM 来处理页面的每次更新，提升了页面的渲染性能。

前端框架下面是小程序 Native 引擎，包括了小程序容器、渲染引擎和 JavaScript 引擎，这块主要是把客户端 Native 的能力和前端框架结合起来，给开发者提供系统底层能力的接口。

在渲染引擎上面，凡泰小程序不仅提供 JavaScript + WebView 的方式，还提供 JavaScript + Native 的方式，在对性能要求较高的场景，可以选择 Native 的渲染模式，给用户更好的体验。示意图左边和右边分别是面对开发者提供的研发支撑和运维支撑服务，可以帮助开发者更有效率的开发小程序，在上线后也提供众多的工具帮助开发者管理和运营线上的小程序。

3.1 FinClip 小程序运行时与安全沙箱 SDK

FinClip 小程序集中行业力量打造并维护一个通用的、安全可靠的、App 接入 SDK 及与之配套的应用技术规范，明确持牌机构、App 渠道和机构服务组织的角色关系，促进机构小程序应用生态的健康有序发展：

对持牌机构，可以：

- 直接使用通用 SDK，不需要投入研发资源，自行开发安全沙箱
- 基于应用小程序规范，一次开发完成后，即具备与多家 App 对接的能力
- 自主控制与 App 渠道的业务合作关系，可以自由、灵活的控制是否允许 App 渠道访问小程序服务

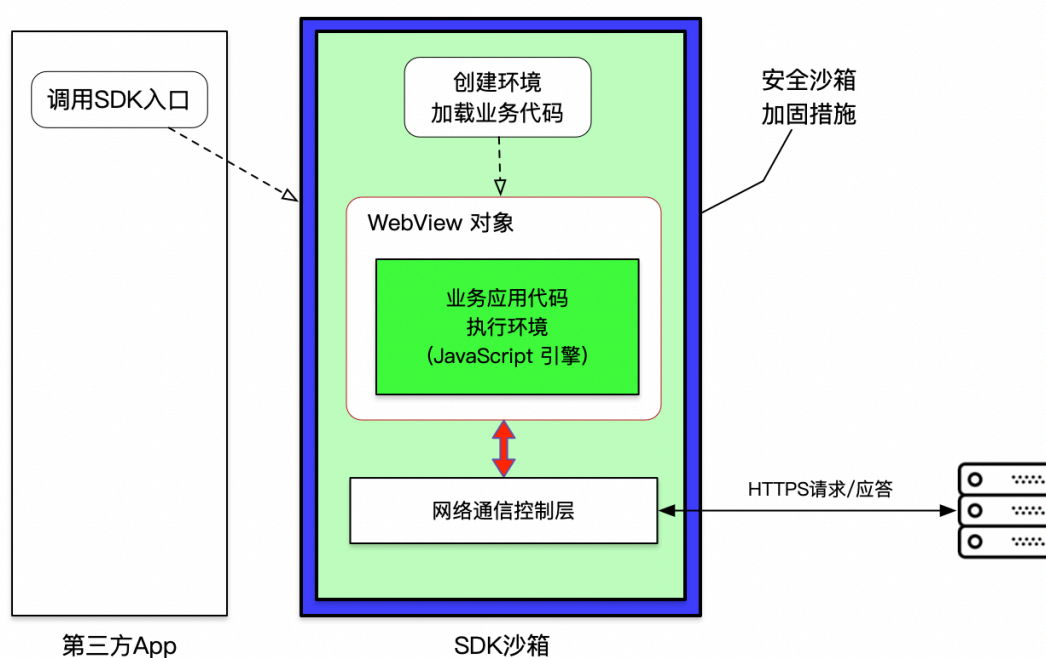
对 App（“宿主”）提供者：

- 只需要对接调试一次
- 极大降低与机构的合作实施难度(只需要进行 UI 层面的整合)

SDK 的主要功能包括：

- 安全沙箱，保护沙箱中的 H5 应用和小程序应用不被宿主 App 干扰、窃听
- 运行环境，提供在宿主 App 内安全执行小程序/H5 应用的环境
- 合规留痕，在法律框架内为 H5/小程序提供合规留痕所需要的设备识别信息
- 支持第三方以 SDK 插件形式扩展 SDK 服务 API（如智能音识别插件等）
- 指标采集，应用性能指标（APM）

SDK 为业务代码提供一个封闭的安全沙箱,有效对抗外部代码的干扰和数据泄露风险;第三方 App 只能通过 SDK 暴露的接口启动 SDK,SDK 完全管控对业务代码所需要的运行环境以及业务代码所有对外通信,可以通过多种机制保证网络通信不被拦截和干扰;SDK 内部使用独立的浏览器内核,运行环境与系统浏览器完全隔离(在 Android 上)。

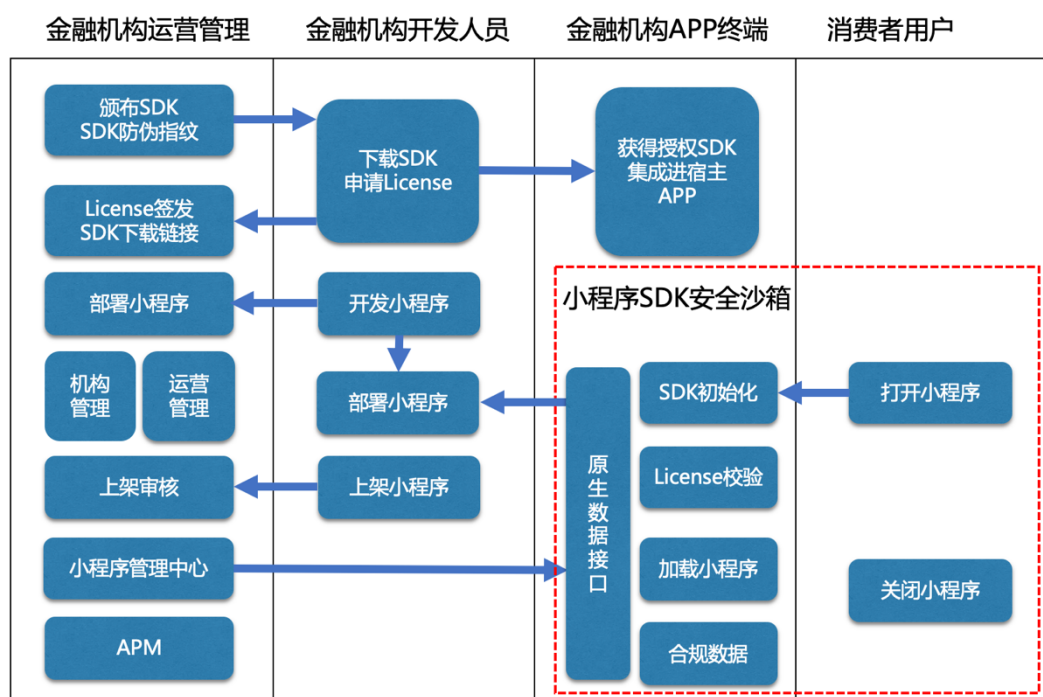


3.2 FinClip 小程序管理后台

FinClip 小程序管理后台是搭建在金融机构私有化机房上面的小程序服务平台,是面向金融机构、全生态的中心化平台。通过管理后台,金融机构不同利益诉求者可以达到多方协同、互利共赢的生态平衡。

FinClip 小程序管理后台的运营者,扮演类似腾讯在微信小程序世界里的角色,履行对上架的小程序进行审核、管理、监管的职能,业务上中立,充当证券业数字化生态的促进者、赋能者。由于是私有化在金融机构内部机房其满足金融信息系统安全合规要求,其数据隐私保护承诺,高于微信、支付宝、百度、字节跳动的类似生态。

下图以金融机构管理者角度，说明其多方协作原理。



FinClip 小程序管理后台运营者：

- 对金融机构的开发者账户进行开立与管理
- 对金融机构所申请上架的小程序进行审核
- 对金融机构潜在违规或有技术缺陷、安全漏洞的小程序进行下架
- 响应合规请求，对任何存在潜在技术与合规风险的小程序进行实时下架，从而杜绝任何第三方入口带来的风险
- 对符合 FinClip 小程序运行标准的 SDK 进行审计、认证、颁布。SDK 可以由多家开发商提供，但是需符合隐私保护、信息安全、合规管控等方面的要求。并对符合要求的 SDK 颁布进行数字签名以保障该 SDK 是安全、无后门、未经污染的版本。任何采用 SDK 的机构，均需从 FinClip 小程序管理

后台下载官方颁布的版本

金融机构开发人员：

- 到小程序管理后台申请一个开发者账户（类似于申请微信小程序开放者账户）
- 让 IT 人员把希望嵌入到第三方合作伙伴网络空间(例如一个 App)的代码，以 H5 或者类似微信小程序代码规范的方式进行开发，打包成 FinClip 小程序
- 提交至 FinClip 小程序管理后台，通过 FinClip 小程序管理后台提供的“小程序开放助手”工具进行测试
- 测试无碍申请上架发布
- 小程序的服务器端代码开发、运维部署，这与当前微信小程序的开发生态无异

金融机构 APP 终端：

- 在 FinClip 小程序管理后台，下载“FinClip 小程序引擎开发组件”（即含有安全沙箱及 FinClip 小程序运行时的 SDK）
- 把该 SDK 打包至自己的 App
- 在 App 的某处，提供一个能点击打开该金融机构小程序的入口，其用户在首次点击时，该小程序将从 FinClip 小程序管理后台远程加载至本地，由 SDK 进行渲染执行。该小程序通过 SDK 所的网络黑白名单设置，连接到此前金融机构所提供的服务器端地址

FinClip 小程序管理后台是 FinClip 小程序生态与开放平台的核心组成，应由金融机构私有化基础设施服务机构负责运行与管理。

4 FinClip 小程序生态

FinClip 小程序作为一个证券行业的小程序开放平台，通过建立标准与规范把多个参与方融合在一起，共同构建一个既开放又合规可控的数字化生态。



此生态的主要参与者有以下各方。

4.1 小程序中心运营商

如前所述，小程序中心运营商由金融机构基础设施 IT 运营人员进行管理，对整个小程序管理后台承担运营、管理、维护职责，其职责范围包括：

- 维护小程序管理后台的软件服务功能，确保多方可以正常、高效地在平台完成业务诉求
- 进行审核管理，包括小程序上下架审核等
- 拓展小程序管理后台的参与者，让更多开发人员加入 FinClip 小程序生态

- 维护 FinClip 小程序的健康生态，确保小程序生态符合监管需求

运营商负责对小程序上下架进行审核，确认小程序的安全合规；

1. 根据平台运营规范和国家法规，对已提交审核的小程序的基本信息、代码、页面内容进行安全合规审查；
2. 通过平台的公告和文章，及时向开发者同步平台功能和 SDK 的更新情况，为开发者提供更优质的服务；
3. 定期监控和统计平台的小程序数据，分析平台稳定性和运营状况，不断完善平台功能和制定新的运营方针。

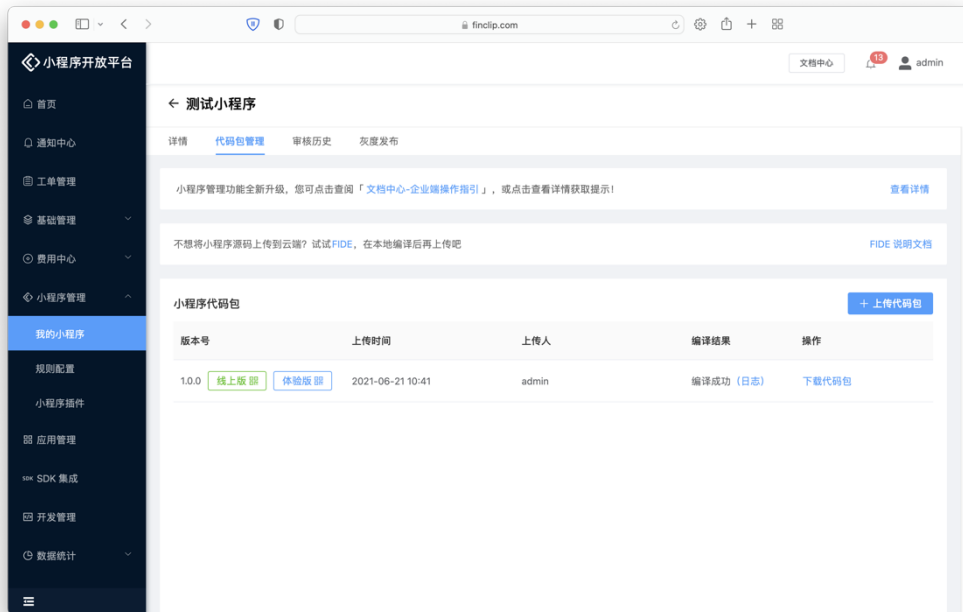
4.2 程序开发者

小程序开发者以金融机构为主，可以在小程序管理后台中完成以下业务：

以核心的小程序上架为例，金融机构若想成为小程序平台的开发者并开发上架小程序，需要在平台上申请企业账号并按照下图的流程完成小程序的开发和上架。

1. 创建小程序：开发者可在平台创建小程序，获取小程序 APP ID；
2. 下载开发工具：小程序平台兼容微信小程序，推荐使用微信开发者工具进行开发；
3. 配置服务器：开发小程序前需要配置服务器域名以确保小程序能够正常访问服务器；
4. 开发小程序：建议参考本平台的开发文档或微信开发文档进行开发，如需使用第三方框架，推荐使用 mpvue 或 Taro 进行开发；

5. 上传代码包：小程序开发完成后可在平台中上传代码包进行编译，并可以下载平台提供的测试助手 APP 进行功能的测试；



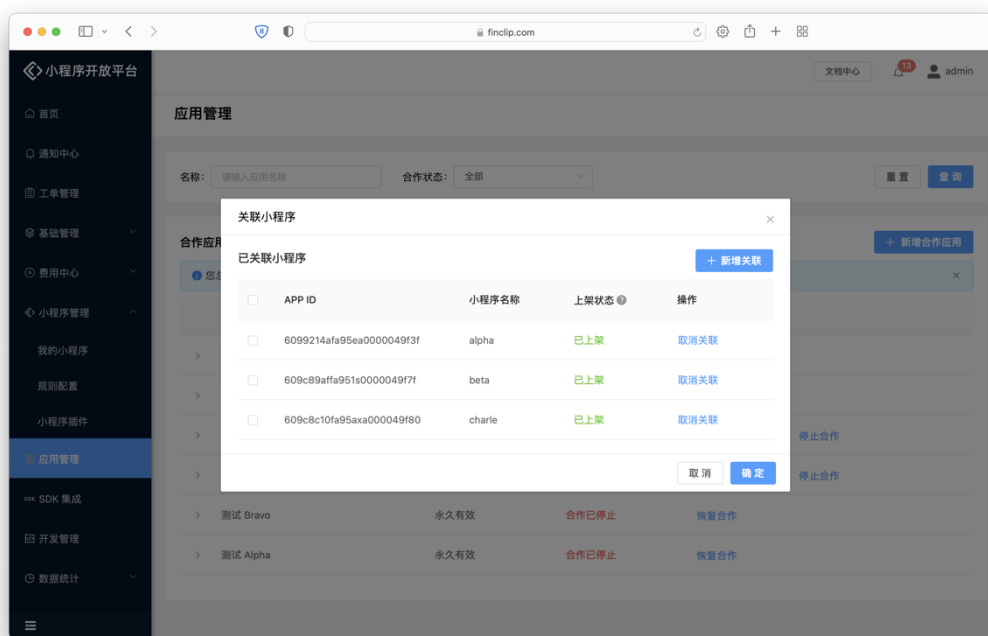
6. 提交审核：小程序上架前，开发者需要完善小程序的基本信息并提交至运营方进行合规审核；



7. 上架小程序：审核通过后，小程序的上架由开发者自行控制，运营方仅负责上

架前的合规审核；

8. 关联应用：开发者需要将已上架的小程序关联至 APP 应用，当两者关联后，用户才能在 APP 应用中打开小程序。



4.3 小程序引擎 SDK 提供商

FinClip 小程序引擎 SDK 主要负责小程序运行时环境构建与隔离、第三方 App 的身份校验、小程序代码的更新与版本管理、小程序的网络访问控制及其他权限控制、小程序的行为监控等功能。

提供 SDK 的厂商，必须遵循以下准则来保证小程序引擎的安全性。

- SDK 自身需要对抗篡改/跟踪/逆向工程的能力。小程序引擎需要运行在第三方 App 内，要保证自己不被第三方破解导致 SDK 被篡改或跟踪。对于破解/逆向工程，SDK 核心代码需要使用 C/C++/Object-C 实现，提高反编译的难度，同时对其他代码进行混淆处理，提高反编译后的破解难度；对于篡改 SDK 的

攻击方式，SDK 需要提供签名的哈希值并在运行前校验代码的完整性；对于跟踪行为，SDK 需要尽量运行在单独的进程中，与宿主 App 保持隔离。

- SDK 需要与宿主 App 保持隔离。为了保持小程序引擎的独立性，SDK 需要运行在单独的进程/线程中。这样既可以保证小程序引擎作为沙箱的独立性，避免一些行为被宿主应用监控，同时隔离的进程也避免 SDK 与宿主 App 发生异常时相互影响。
- SDK 需要完善的安全测试流程来保障健壮性。SDK 提供商需要组织专门应用安全团队/外部安全服务商对 SDK 不同版本进行安全测试和攻击测试，及时修正安全漏洞，发布新版本
- SDK 需要数据监控能力。SDK 要将小程序引擎的运行状态等行为数据和性能数据定时上报到服务中心，以便服务中心对小程序引擎的使用情况进行监控。服务中心通过对大量 SDK 激活和使用情况的监控，可以及时感知 SDK 版本异常和行为异常并作出快速反应。SDK 要拥有远端控制引擎的能力，当某个版本的 SDK 出现漏洞时，通过集中式的控制，在服务中心端限制某些有安全漏洞的 SDK 版本的特定功能，包括完全停用
- SDK 运行时接管所有对外网络通信。在小程序的 WebView 中禁用了传统 DOM 的访问和网络访问的 API (XMLHttpRequest)，所以小程序无法直接发起网络请求，小程序对外网络通信均必须通过 SDK 提供的 API 完成。SDK 提供的 API 对小程序的网络请求进行了过滤和拦截。小程序必须在管理后台配置 IP 地址/URL，小程序启动时运行时会加载小程序配置的域名信息并限制小程序只能访问对应的域名或 IP
- SDK 不应收集运行在其中的小程序的业务场景相关信息，包括但不限于用户行

为数据、交易数据、账户数据、以及小程序提供者（金融机构）的任何商业内容

- SDK 不应收集其所处于的外部环境（“宿主”）的相关信息，包括但不限于宿主的用户行为数据和其他隐私数据
- SDK 需遵循国家等级安全保护标准

SDK 引擎提供商的职能应包括：

- 专职团队对 SDK 进行开发更新维护
- 根据业务场景的需求对 SDK 进行定期升级
- 负责 SDK 的安全漏洞检测和对第三方 App 开发团队的安全/更新提示
- SDK 官方下载页面和数字指纹（MD5/SHA Digest）
- 通过 SDK 在线验证服务，确保不符合安全要求的 SDK 版本在指定期限内停用

4.4 小程序 SDK 插件提供商

SDK 本身只是一个隔离的、安全的小程序运行时。与微信、支付宝不同，它出厂时并不知道自己将被打包嵌入到什么“宿主”环境中，所以它无法预先内置一些原生的技术能力。这些能力，可以插件的方式，由“宿主”自行选择，注入到 SDK 中，从而让运行其中的小程序获得对该些扩展能力的调用。FinClip 小程序生态应欢迎任何有能力的开发商参与进来，一同打造一个开发、多元的生态系统。

一些证券业常用的插件包括：

- 用于开户的语音、视频双录技术

- 语音识别、人脸识别技术
- 自行开发并开放 API 接口, 允许小程序通过 API 调用的方式获得特定服务, 例如证券行业中高频使用的行情功能
- 其他因业务场景所需的设备端原生功能

与小程序引擎 SDK 提供商相同的是, 所有开发出来的插件均需通过运营方审核, 只有在代码安全、业务合规的基础上, 方可在 FinClip 小程序管理后台中上线。

4.5 小程序上下架审核管理者

小程序上架审核管理者可以金融机构 IT 运营管理职能部门负责, 其职责是对小程序上架进行审核, 确保其安全性、合规性。

管理职能包括审核小程序的名称、图标、简介等信息是否符合应用基本信息规范, 审核小程序的内容是否存在恶意营销、违法犯罪、血腥暴力等违反平台规范和国家法规的内容。

4.6 小程序云端服务提供商

金融机构可以选择把自己的小程序服务器端托管在行业云提供商 (例如深证通) 机房, 行业云提供商需具备高规格的基础设施托管环境, 保障客户系统安全稳定运行, 且需满足合规监管诉求。

金融机构也可选择仅把小程序的前端入口 (例如 API 网关) 或部分服务部署在云端, 通过 VPN、专线等任何方式再连接到自己内部的机房。

金融机构也可以选择完全在自有机房部署服务, 不采用任何金融云服务商的资源。

4.7 多方协同的行业数字生态

FinClip 小程序生态是由多方协作、各司其职、共同打造出的全新的、更高效、更合规的行业生态。在这一生态中，多方均可获得收益，生态才能健康可持续发展。

5 信息安全与隐私保护

FinClip 小程序生态，在合规、安全与隐私保护方面，需做到高于微信小程序等互联网平台。

5.1 端侧用户设备信息留痕

FinClip 小程序 SDK，在所在“宿主“的设备端收集硬件指纹等信息，供小程序开发者收集、留痕，作为用户交易行为不可抵赖的存证。这类似于当前证券公司手机交易 App 所依法收集留痕的信息。

这类数据，由金融机构的小程序开发者，通过 SDK 接口获得，并把数据上传到该金融机构的机房，以记录其客户在第三方宿主 App 使用该金融机构小程序时的设备信息。这样，即使用户不是通过金融机构自有的 App，其交易行为所发生的设备也能被留痕。

SDK 开发商及 SDK 插件开发商，不能私下收集和传输该类信息。这在 SDK 软件、SDK 插件提交 FinClip 小程序管理后台时，将被管理后台运营商检查、审计，以确定其符合规定。此外，FinClip 小程序管理后台运营商以及小程序上下架的审核机构，亦不收集此类用户设备信息。在发生合规审计需要时，由监管机构向相关金融机构调查相关数据。

金融机构应存储用户设备信息并关联相应的交易行为（与目前证券公司手机证券 App 中设备端信息留痕要求一样）。

5.2 云侧数据安全与隐私保护

金融机构所开发的 FinClip 小程序，其服务器端无论托管在行业云服务商（例如深证通）或运行在自有机房，均需严格遵循互联网上应用服务的安全规范。以证券公司为

例，券商对自己的手机证券系统信息安全负责，其 FinClip 小程序的安全等级应与手机证券无异，虽然小程序前端发布在 FinClip 小程序管理后台，但服务器端自行维护、所暴露的接口应自行安全加固。

FinClip 小程序管理后台运营商，除了审核发布金融机构的小程序代码、让其可被远程加载到允许的第三方宿主，并不参加到持股金融机构具体的小程序业务场景的链路中，不收集金融机构或其第三方合作伙伴的任何业务信息、用户信息，服务器端业务逻辑不发生在其管辖的网络空间内。

5.3 网络访问控制

每一个上架的 FinClip 小程序，在第三方宿主内嵌的 SDK 中加载后，其网络请求只能连接到申请上架时备案的服务器端地址，无法在 SDK 内随意连接到互联网上任何其他地方。

5.4 实时安全应急管控

FinClip 小程序管理后台可在任何时候作以下应急处理：

- 金融机构因其开发的 FinClip 小程序发现缺陷，主动下架该小程序
- 小程序中心监控到某 FinClip 小程序信息安全问题，让其下架
- 小程序中心监控到某金融机构在某第三方合作伙伴的入口的信息安全风险，下架在该合作伙伴的小程序
- 金融机构终止与某第三方合作伙伴的合作，小程序监控中心注销该金融机构与该第三方机构的关系数字证书，使该第三方机构的宿主 App 无法再通过其嵌入的 FinClip 小程序 SDK 加载该金融机构的小程序。这等同于

以数字化方式解除双方的合作备案

- 发现某个版本的 FinClip 小程序 SDK 安全漏洞，迅速终止这个版本的 SDK

有效加载小程序的能力，迫使第三方宿主 App 们升级 SDK 版本

5.5 审计

在 FinClip 小程序平台上，开发者的登录日志、操作日志、服务器安全基线文件变更、访问权限、变更日志都会被记录，通过自动化检测实时审计非法访问和风险操作，并进行告警。FinClip 小程序开放平台对数据的操作均有详细日志记录，并区分不同操作者角色，授予不同的权限。平台会永久存储这些日志以方便后续的审计追踪。