ICS 33.050
CCS M 30

# 团　体　标　准

T/TAF 196—2023

# 移动互联网金融客户端技术要求

Technical requirements of mobile Internet application financial client

2023-11-24 发布　　2023-11-24 实施

电信终端产业协会　发布

# 目　　次

# 前　言

本文件按照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》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、阿里巴巴（中国）有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：李朋、汪辰、段虎才、周玉国、沈煜、刘献伦、郭隆庆、马蓁蓁、杨广贺、黄天宁、付晨、杨子琛、曹文浩。

# 移动互联网金融客户端技术要求

## 1 范围

本文件规定了移动互联网金融客户端的技术要求，包括配置管理系统、BFF、数据布局渲染引擎、用户体验、性能、安全方面的要求。

本文件适用于移动互联网金融客户端开发、部署、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 37092—2018 信息安全技术密码模块安全要求

GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

T/TAF 114—2022 移动应用适老化技术要求和测试方法

JR/T 0092—2019 移动金融客户端应用软件安全管理规范

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**体验适配层 Backend For Frontend**

主要是指承接适配角色，将内部复杂的微服务适配成各种不同用户体验(APP/Web/H5/第三方等)友好和统一的API，起到聚合裁剪适配的作用。

## 4 缩略语

下列缩略语适用于本文件。

BFF：服务前端的后端/体验适配层(Backend for Frontend)

URI：统一资源标识符(Uniform Resource Identifier)

CPU：中央处理器（Central Processing Unit，简称CPU）

IP：IP指网际互连协议，Internet Protocol的缩写

IMEI：国际移动设备识别码（International Mobile Equipment Identity，IMEI）

IMSI：国际移动用户识别码（英语：IMSI，International Mobile Subscriber Identity）

Bug：程序错误

APP：手机应用软件

FPS：每秒传输帧数(Frames Per Second)

ROOT：管理员权限
TLS：传输层安全性协议（英语：Transport Layer Security，缩写作TLS）
TLCP：信息安全技术传输层密码协议

## 5 移动互联网金融客户端技术能力要求概述

本文件参考架构如图1所示。

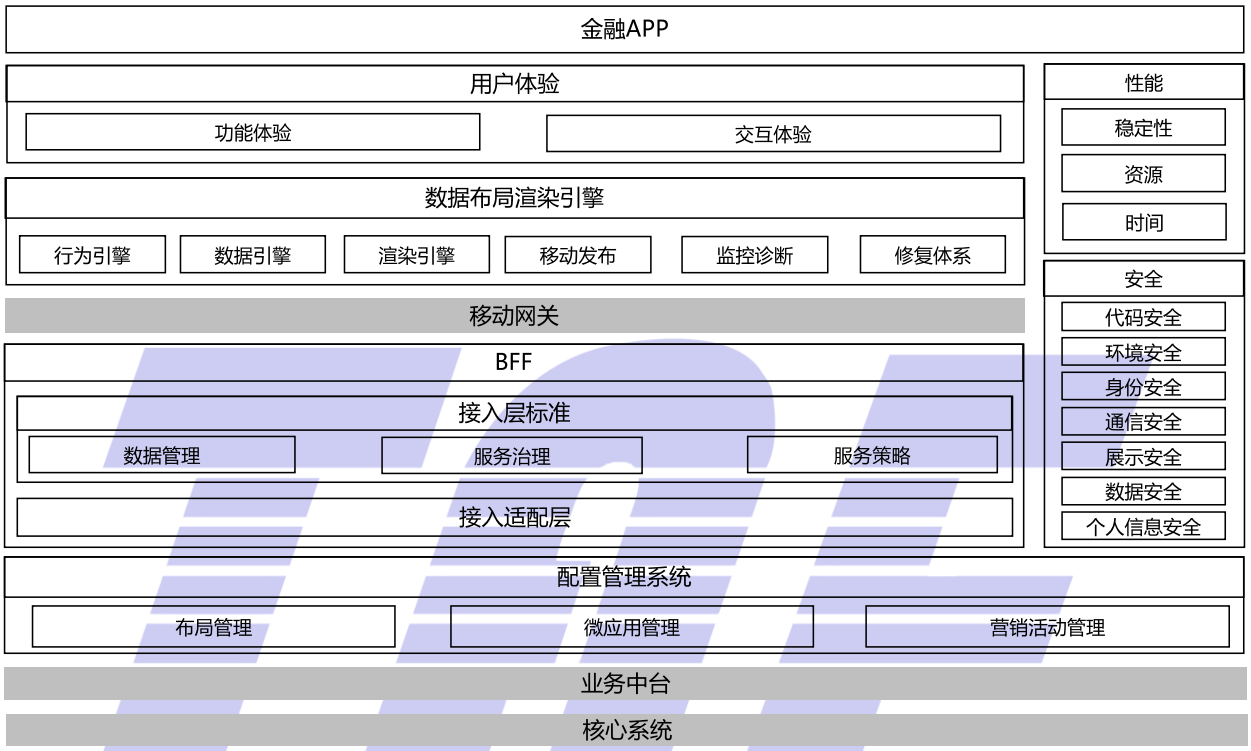


图1 移动互联网金融客户端技术能力要求

本文参考架构包括配置管理系统、BFF、数据布局渲染引擎、用户体验、性能、安全等模块。

配置管理系统包括布局管理、微应用管理、营销活动管理；BFF包括数据管理、服务治理、服务策略；数据布局渲染引擎包括行为引擎、数据引擎、渲染引擎、移动发布、监控诊断、修复体系；用户体验包括功能体验、交互体验；性能包括稳定性、资源、时间；安全包括代码安全、环境安全、身份安全、通信安全、展示安全、数据安全、个人信息安全。

## 6 配置管理系统要求

### 6.1 布局管理

#### 6.1.1 卡片管理

卡片管理能力要求如下：

a) 应支持卡片的样式配置，如字体、字号、背景色、卡片间距、图片等；

b) 应支持静态数据管理能力，如卡片标题、卡片副标题、按钮名称、卡片内容等；

c） 应支持动态接口，如接口名称、接口参数、接口版本号等；
d） 应支持多种自定义刷新机制，如压后台刷新、下拉刷新、页面切换刷新、定时刷新等；
e） 应支持多种卡片渲染形式的配置能力，如 H5、小程序、iOS、Android 等。

#### 6.1.2 页面管理

页面管理能力要求如下：
a） 应支持实时预览的能力，如手机端预览、控制台预览等；
b） 应支持定时发布上线、定时下线的能力；
c） 应支持主题的设置，如导航栏的颜色、主题类型、主题的状态、主题的素材等。

#### 6.1.3 模板管理

模板管理能力应支持卡片模板的配置，包括但不限于新增卡片类型、调整卡片的样式属性。

### 6.2 微应用管理

#### 6.2.1 应用管理

应用管理能力要求如下：
a） 应支持应用的创建、上传、发布、删除能力；
b） 应支持不同类型的应用入驻，如 H5、小程序、React Native 等；
c） 应支持应用的分组能力，如在客户端不同的展位显示不同的应用列表。

#### 6.2.2 审核管理

审核管理能力要求如下：
a） 应支持应用的多种审核状态，包括但不限于待审核、审核通过、审核失败等；
b） 应支持审核人员的管理。

### 6.3 营销活动管理

#### 6.3.1 投放管理

投放管理能力要求如下：
a） 宜支持多种展位类型的配置，如开屏、弹屏、公告、Banner、列表、浮标等；
b） 宜支持多种展位位置的配置，如页面顶部浮层、页面顶部、页面底部、列表头部、列表底部等；
c） 宜支持多种展位素材类型的配置，如文本、静态图片、gif 动图、lottie 动画、H5 页面等。

#### 6.3.2 活动管理

活动管理能力要求如下：
a） 宜支持活动类型的配置，如定向人群的投放、对未来发生行为时触发定向的投放；
b） 应支持多种活动周期的配置，如每天、每周、每月的设置；
c） 应支持活动有效期的配置，如开始时间、结束时间。

## 7 BFF 要求

### 7.1 数据管理

数据管理能力要求如下：

a) 宜支持批量请求的能力，如并发对多个卡片模块的下游系统进行调用；
b) 宜支持兜底数据的能力，如卡片下游数据不可用时返回默认的数据。

### 7.2 服务治理

服务治理能力要求如下：
a) 应支持版本控制的能力，如楼层模板版本的权重控制、默认模板的控制；
b) 宜支持降级控制的能力，如没有命中模板的降级、模板系统不可用的降级、限流降级。

### 7.3 服务策略

服务策略能力要求如下：
a) 应支持数据加工的能力，如对下游返回数据的剪切、拼接、过滤的能力；
b) 宜支持数据转换的能力，如将数据资源系统返回的数据模块、埋点模块、楼层模板数据转换为客户端可以识别的数据模型的能力。

## 8 数据布局渲染引擎要求

### 8.1 行为引擎

行为引擎能力宜支持根据服务端下发的数据协议，客户端做出相应的行为交互的机制，如强提示、弱提示、对话框、跳转等。

### 8.2 数据引擎

数据引擎能力要求如下：
a) 应支持数据缓存，如使用客户端数据库、本地文件等形式将楼层模板的数据缓存在客户端；
b) 宜支持多种请求形式的能力，如单一卡片请求、多卡片请求、总线请求等。

### 8.3 渲染引擎

渲染引擎能力宜支持多种渲染技术的能力，如 iOS、Android、H5、小程序等。

### 8.4 移动发布

移动发布能力要求如下：
a) 客户端应用软件宜支持多种技术栈的发布能力，如 iOS、Android、H5、小程序等；
b) 客户端应用软件宜支持灰度发布的能力，如用户维度、设备系统版本维度、设备机型维度、网络类型维度、城市维度等；
c) 若客户端应用软件支持动态模块更新，应使用加密通道与服务端通信传输更新模块并对更新模块进行签名校验。

### 8.5 监控诊断

监控诊断能力要求如下：
a) 应支持收集客户端性能稳定性数据，如启动速度、crash 堆栈、卡顿卡死堆栈等信息，并通过日志上传至监控后台，开发人员可对这些信息进行分析并针对性的进行改进；
b) 应支持不同事件类型的数据监控能力，如页面浏览、卡片点击、卡片曝光等；
c) 宜支持不同上报策略的能力，如自动上报、手动上报、根据开关上报等；

d) 应支持设备环境采集的能力，如公网 IP、IMEI、IMSI、设备型号、系统版本、网络类型、操作系统语言、CPU 核数、CPU 转速、内存大小、屏幕分辨率、客户端渠道号、客户端版本号；
e) 宜当对关键业务进行日志埋点，完善其他类型日志记录，预先制定异常日志识别规则，实时或定期对埋点日志进行分析，使用但不限于时间维度和用户维度分析异常操作行为。

### 8.6 修复体系

修复体系能力要求如下：
a) 在业务开发过程中，应考虑在某些应急情况下的降级策略，如后台不可用、业务限流等情况，给用户友好的提示信息；
b) 应用能够在无需重新安装的情况实现更新，帮助应用快速建立动态修复能力。如果是应用上线后出现 bug，宜支持使用补丁包修复而不需再发布新的版本；
c) 如果客户端软件某个模块在短时间内连续出现比较严重的问题，宜采取必要的熔断机制，机制包括但不限于业务暂时关闭等措施，在修复完成稳定后再放开使用。

## 9 用户体验

### 9.1 功能体验

#### 9.1.1 功能导航

应支持菜单导航的功能，如分类导航、常用功能、自定义菜单等。

#### 9.1.2 消息提醒

消息提醒能力要求如下：
a) 应支持多种类型的消息能力，如消息通知、消息中心、红点消息、角标等；
b) 宜支持多种活动类型的展示，如广告栏、公告栏、轮播图、弹窗、启动页等；
c) 宜支持消息状态的展示，如消息读取状态、消息删除、多设备消息同步等。

#### 9.1.3 社交分享

社交分享能力要求如下：
a) 宜支持多种分享的形式，如文字、图片、链接等；
b) 宜支持主流的分享渠道，如即时通信软件、社交软件、浏览器等；

#### 9.1.4 功能搜索

功能搜索能力要求如下：
a) 应支持搜索功能，如文字搜索、语音搜索等；
b) 应支持模糊搜索，如关键词的搜索；
c) 搜索结果应支持多种展示方式，包括但不限于纯文字、图文等；
d) 搜索结果宜支持互动，如购买、关注、收藏等。

#### 9.1.5 在线客服

在线客服能力要求如下：
a) 应支持电话客服；
b) 应支持在线人工客服，并提示用户前方排队的人数或预计等待的时间；

c） 宜支持智能客服，可根据问题匹配出相似的答案；
d） 宜支持视频客服；
e） 在线客服的功能入口应该是独立的、易发现的；
f） 应支持对客服服务的评价。

## 9.2 交互体验

### 9.2.1 交互引导

交互引导能力要求如下：
a） 有潜在危险的按钮应采用警示作用的背景颜色突出显示，如红色；
b） 应支持功能的引导能力，如新版本的更新说明、操作指引、温馨提示等；
c） 应支持表单填写的提示能力，包括但不限于必填项和非必填项的提示、错误信息的提示、重大影响的操作再确认提示等；
d） 应提供弹窗关闭的能力，如关闭按钮、点击弹窗外区域关闭、角标”X”等；
e） 页面无数据时，应展示引导性提示；
f） 重要的产品信息宜突出显示，如投资金额、产品收益率、投资期限等。
g） 针对业务术语，应提供准确易理解的解释说明。

### 9.2.2 交互反馈

交互反馈能力要求如下：
a） 宜支持操作流程的回退，如流程未结束点击返回则回退至上一步、流程结束后点击返回则不再回退至上一步；
b） 宜支持防重复点击，避免用户对用一个按钮的多次点击；
c） 应支持下拉刷新的提示，如文字、图标等；
d） 操作出现错误时，应引导和帮助客户进行修正；
e） 宜支持图片的查看，如下载、放大等；
f） 应支持用户等待时提供相关提示，如预计等待时间、加载图标、进度条等；
g） 应支持操作流程结束的反馈，包括但不限于成功、失败、异常的提示；
h） 应支持在数据获取时提供有效性校验功能，包括但不限于长度、数值范围等；
i） 若页面信息需要滚动才能展示完整，应支持页面到达底部的状态提示，包括但不限于已经到达底部、上滑加载更多、上滑跳转至其他页面等；
j） 信息填写未完成保存，点击返回时应提示当前信息不被保存，需确认后才能返回；
k） 应支持异常流程的反馈，包括但不限于页面加载失败、数据加载失败、网络异常等。

### 9.2.3 适老化

应支持适老化功能，应符合T/TAF 114—2022要求。

# 10 性能要求

## 10.1 稳定性

### 10.1.1 闪退率

APP的闪退率不宜高于0.5%。

#### 10.1.2 卡死率

APP的卡死率不宜高于0.2%。

#### 10.1.3 卡顿率

APP的卡顿率不宜高于0.2%。

### 10.2 资源占用

#### 10.2.1 CPU占用

用户在使用APP过程中，移动终端的CPU宜保持平均30%以下，不宜持续10秒钟出现峰值超过50%的占用。

#### 10.2.2 内存占用

内存占用能力要求如下：
不应存在内存泄露的情况；
退出页面内存应恢复到近似原始值。

### 10.3 时间

#### 10.3.1 冷启动响应时间

APP的冷启动响应时间不宜超过2s。

#### 10.3.2 操作响应时间

FPS最小值不宜低于30，平均值不宜低于50。

#### 10.3.3 页面可交互时间

页面可交互时间能力要求如下：
网络情况较好的条件下(Wifi或4G、5G),原生页面的可交互时间不宜超过2s，H5页面的渲染时间不宜超过5s；
网络情况不佳的条件下(3G、2G)，原生页面的可交互时间不宜超过10s，H5页面的可交互时间不宜超过20s。

## 11 安全要求

### 11.1 代码安全

代码安全能力要求如下：

a) 应具备基本的抗攻击能力，包括但不限于抵御静态分析、动态调试等；
b) 应采取代码加壳、代码混淆等反编译防护措施防止被破解、篡改、二次打包等，保护源代码安全；
c) 应避免使用存在已知漏洞的组件；
d) 应对组件权限进行限制，避免第三方移动应用随意调用组件内容；
e) 应对组件进行安全配置，避免发生劫持组件的安全问题；
f) 应禁止内部组件被外部程序调用，如需供外部调用，应检查调用者是否符合控制机制；

g） 应避免调用存在安全漏洞的函数，避免敏感数据硬编码；
h） 应删除冗余代码、调试代码等。

## 11.2 环境安全

环境安全能力要求如下：

a） 涉及敏感操作内容的客户端应能够对运行环境进行检测（如 Android 的 ROOT 机和 iOS 的越狱机），并对其进行相应的提示。例如可限制具有敏感操作行为的移动应用在 ROOT 或越狱等环境下使用。
b） 客户端运行过程中应能够监测运行环境的变化，防止移动应用程序被恶意劫持。
c） 客户端应用软件应实现敏感个人信息交互场景的防截屏、录屏，包括但不限于手势、登录口令、支付口令等。

## 11.3 身份认证

身份认证能力要求如下：

a） 移动应用软件应对访问用户进行有效的访问控制，保证授权用户访问的内容不能超出授权的范围；
b） 客户端应用软件登录时应采取适宜的验证要素，包括但不限于口令、短信验证码、手势密码、生物特征识别等；
c） 应确保采用身份验证的要素相互独立，即部分要素的损坏或泄漏不应导致其他要素的损坏或泄漏，如登录和交易验证的口令不能一致；
d） 客户端应用软件应配合服务端提供口令复杂度校验功能，避免采用简单交易口令；
e） 应严格限制使用初始口令，若设置初始口令，应强制用户在首次登录后修改初始口令，包括但不限于登录口令、交易口令、查询口令等；
f） 客户端应用软件交易时应对用户身份进行认证，如对于大额资金交易，应采用至少两种验证要素对用户身份进行认证；
g） 在用户身份认证后，客户端应用软件进入终端系统后台超过设定时限后切换到前台，应对用户身份重新认证；
h） 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、自动退出等措施；
i） 在提示用户认证失败时，应模糊错误提示信息，防止泄露用户账号、交易信息等敏感个人信息数据；
j） 在修改或重置口令前，应对用户身份进行重新验证，采用至少两种要素对用户进行身份验证，包括但不限于短信验证码、生物特征信息、数字证书等；
k） 修改口令时应对原口令输入错误次数进行限制，新口令不应与原口令相同；
l） 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。

## 11.4 通信安全

通信安全能力要求如下：

a） 客户端应用软件应具有和服务器端的接口双向认证机制；
b） 客户端程序处理与服务器交互重要数据和敏感个人信息时，应采用安全的密码算法技术保证数据的保密性、完整性和不可抵赖性；
c） 采用的密码算法应符合国家主管部门、国家标准和行业标准的要求，宜使用国家商用密码算法；
d） 对传输中的数据应采用安全的安全传输层协议进行保护，如 TLS 1.2、TLCP 1.1 等；
e） 通过客户端应用软件发起的身份认证或资金类交易报文，应具有重放攻击能力；

f） 客户端应用软件应对传入的 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。

### 11.5 展示安全

展示安全能力要求如下：

a） 客户端应用软件不应明文显示口令，包括但不限于银行卡口令、支付交易口令等；

b） 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；

c） 客户端应用软件处于未登录状态时，不应展示与用户主体相关的用户鉴别信息，包括但不限于卡片验证码、登录口令、支付口令等；

d） 客户端应用软件处于已登录状态时，与用户主体相关的用户鉴别信息不应明文显示，包括但不限于卡片验证码、登录口令、支付口令等；对于银行卡号、客户名称、手机号码、证件号码等可以直接或组合后确定信息主体的信息应屏蔽显示，或由用户选择是否屏蔽显示，如需完整显示，应进行用户身份验证，防范此类信息泄露风险。

### 11.6 数据安全

数据安全能力要求如下：

a） 客户端应用软件不应以任何形式存储用户的敏感个人信息；

b） 客户端应用软件运行日志中不应含有敏感个人信息，不应打印完整的敏感个人信息原文；

c） 客户端应用软件应在敏感个人信息使用完毕后，对其立即进行清除；

d） 客户端应用软件应支持页面返回后自动清除银行卡口令、网络支付交易口令、登录口令等支付敏感信息的机制；

e） 客户端应用软件应支持密码模块实现数据加密、数字签名、身份认证、防逆向调试等功能，采用的密码应支持符合 GB/T 37092 二级及以上要求。

### 11.7 个人信息安全

客户端应用软件对用户个人信息收集、存储、传输、使用和销毁等环节时应参考 GB/T 41391—2022 6.1–6.4 的要求。

# 电信终端产业协会团体标准

# 移动互联网金融客户端技术要求

T/TAF 196—2023

*



电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn