ICS 35.240.40
CCS A 11

团　体　标　准

T/NIFA 11-2022

商业银行互联网开放平台架构规范

Commercial bank internet open platform architecture specification

2022-2-17 发布　　2022-2-17 实施

中国互联网金融协会 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》和GB/T 20004.1—2016《团体标准化 第1部分：良好行为指南》给出的规则起草。

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。

本文件由中国互联网金融协会提出。

本文件由中国互联网金融协会归口。

本文件起草单位：中国互联网金融协会、神州数码信息服务股份有限公司、中国光大银行股份有限公司、武汉众邦银行股份有限公司、四川新网银行股份有限公司、广发银行股份有限公司、华夏银行股份有限公司、恒丰银行股份有限公司、安永（中国）企业咨询有限公司、上海银行股份有限公司、广州银行股份有限公司、北京银行股份有限公司、湖南三湘银行股份有限公司、上海华瑞银行股份有限公司、秦皇岛银行股份有限公司、宜宾市商业银行股份有限公司、重庆富民银行股份有限公司、中信百信银行股份有限公司、中互金认证有限公司、京东科技信息技术有限公司、北银金融科技有限责任公司、广东华兴银行股份有限公司、晋商银行股份有限公司。

本文件主要起草人：陆书春、杨农、杨彬、刘绪光、苏莉、张维凡、陈宏鸿、李敏、舒秋东、马洪杰、于宏志、沈伟、韩东妍、王磊、袁春雷、杨涛、李耀、彭磊、张路路、蒋恩平、沈星、钟成鹏、丘佳成、曾以蓁、卢敏福、杨志强、赵毅、房效庆、李南、董铁军、徐启鹏、魏乾顺、赵志东、杨立、张汝成、王晖、王子航、费伟伟、张赫、赵盼、吴頔、刘昕、岳红超、黄鹏、边兰洲、巫山、赵爽、李增局、史汝辉、邬肖玢、刘英硕、朱晓光、吴可、朱采顺、陈强、潘红双、杨金彬、谭柱钢、熊钊隆、管晓军、吕恩涛。

引　言

近年来，随着金融科技的快速兴起，银行业乃至整个金融业正在发生深刻的变革，金融科技的应用和发展给银行业带来了机遇和挑战。科技与金融的关系，从支持、支撑，到驱动、引领，科技甚至开始改变金融服务形式。在此背景下，“开放、合作”成为银行业应对各类挑战的有益举措。中国人民银行在《金融科技（FinTech）发展规划（2019-2021年）》中进一步明确将“借助应用程序编程接口（API）、软件开发工具包（SDK）等手段深化跨界合作”作为金融科技“拓宽金融服务渠道”的具体措施之一。

为积极应对互联网业务的发展，国内多家商业银行都建设了“互联网开放平台”。但是，目前国内针对商业银行互联网开放平台的架构定位、架构设计等，都缺乏统一的标准体系和机制。为此，中国互联网金融协会牵头发起研制商业银行互联网开放平台架构规范，为商业银行提供参考和借鉴，在合规可控的前提下，减少参与各方的额外成本，实现互联互通。

商业银行互联网开放平台架构规范

1 范围

本文件规定了商业银行互联网开放平台的参考架构规范，本文件从架构定位及目标出发，明确了商业银行互联网开放平台的应用架构、技术架构、物理架构、安全架构的主要目标、关键能力及设计要点。

本文件不包括商业银行互联网开放平台的业务接入模式、业务产品定义、接口报文传输的内容。

本文件适用于商业银行互联网开放平台的建设，以指导从事或参与商业银行互联网开放平台建设的相关方开展相关工作。

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。

JR/T 0071（所有部分） 金融行业网络安全等级保护实施指引

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0185—2020 商业银行应用程序接口安全管理规范

3 术语与定义

下列术语和定义适用于本文件。

3.1

商业银行互联网开放平台 commercial bank internet open platform

基于API、SDK等标准化的应用程序接口模式，将银行的相关业务或技术能力向外输出，并使得外部程序安全地使用银行对外提供的金融服务能力。是银行金融服务能力输出的技术承载媒介，是对外提供金融服务以及对内提供服务管理和治理的应用接入平台。

注：本文件中，使用“开放平台”作为“商业银行互联网开放平台”的统一简称。

3.2

应用程序接口 application programming interface

一组预先定义好的功能，开发者可通过该功能（或功能的组合）便捷地访问相关服务，而无需关注服务的设计与实现。

[来源:JR/T 0185—2020,3.1]

3.3

应用软件开发工具包 software development kit

基于特定软件包、软件框架、硬件平台、操作系统等建立应用程序时所使用的软件开发工具集合。

[来源:JR/T 0185—2020,3.5]

3.4

应用方 application agency

调用商业银行应用程序接口的机构和个人。

[来源:JR/T 0185—2020,3.3,有修改]

3.5

应用方门户 application agency portal

银行提供给应用方的门户网站，用来展示银行对外的产品信息、帮助信息，实现应用方的注册、实名认证、应用注册、产品申请、报表查询等功能。

3.6

沙箱 sandbox

银行帮助应用方建立一个隔离环境，该环境通过建立挡板的方式模拟银行生产环境的关键业务流程，用于应用方与银行的联调测试。

3.7

应用 application

应用方对外提供的一个独立的产品功能，一般对应一种应用形态，如一款App，或者一个网站等。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

App：应用（Application）

DevOps：开发运维一体化（Development Operations）

DMZ：（网络）隔离区（Demilitarized Zone）

HTTPS：以安全为目标的HTTP通道（Hyper Text Transfer Protocol over Secure Socket Layer）

H5：超文本标记语言5.0（Hyper Text Markup Language 5.0）

RA：数字证书注册审批机构（Registration Authority）

SDK：应用软件开发工具包（Software Development Kit）

SSL：安全套接层协议（Secure Sockets Layer）

URL：统一资源定位符（Uniform Resource Locator）

5 架构框架

5.1 开放平台架构定位

开放平台在商业银行IT架构体系中宜承担以下架构定位：

——资源与服务的整合者：基于开放平台所提供的资源整合能力，应用方可整合银行的金融服务能力和自身的非金融服务能力；

——场景金融服务提供者：基于开放平台的服务开放技术（API/SDK/H5/小程序等），银行可碎片化行内的金融产品，使其嵌入客户的生活、生产场景；

——服务组合与定制化平台：基于开放平台的服务组合能力，形成涵盖金融与非金融服务集市（服务接口资源池），为应用方提供产品定制与创新服务；

——业务场景数据获取者：基于开放平台的场景数据的通道能力，可获得大量的场景业务数据，反哺银行业务能力建设；

——外部平台接入安全管控中心：基于开放平台作为银行与外部平台对接的枢纽地位，可实现对外部接入的统一安全管控。

5.2 开放平台架构建设原则

开放平台除应满足银行整体架构原则外，还应遵守以下原则：

——标准化原则：应通过服务治理，输出标准化服务，减少应用方对接资源投入；

——服务化原则：应遵循高内聚、低耦合的服务化设计理念，降低平台组件间的耦合度；

——最小授权原则：对应用方的接口使用，应按照“最小授权”的方式进行访问控制；

——数据安全原则：数据在采集、交换和应用过程中，应采取必要的技术和管理手段确保数据安全；

——网络安全原则：内外部系统间网络应确保安全隔离，并设置必要的网络安全防护策略；

——高可用原则：应建立服务限流、熔断、降级等机制，保障业务的连续性；

——可扩展原则：应支持灵活扩展，及时响应市场、业务高峰等变化。

5.3 开放平台内部架构体系

本文件涉及的开放平台的架构体系包含应用架构、技术架构、物理架构和安全架构，其关系如图1所示。

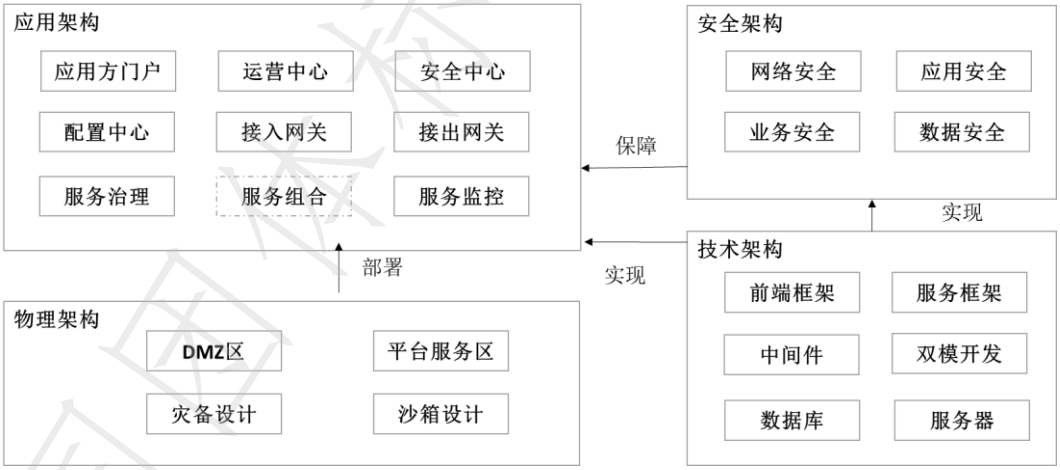

图1 开放平台内部架构体系关联参考图

5.4 开放平台外部关联体系

开放平台作为行内行外对接的枢纽，应与行内、行外的其他系统相互配合，共同实现开放平台的架构定位。其关联关系示意图如图2所示，主要关联关系要求包括：

——开放平台与应用方：开放平台直接对接应用方，为应用方提供一系列业务接入能力，同时也能实现应用方服务能力的发布代理；

——开放平台与银行自有渠道：二者共同构成银行主要的业务渠道，但分工不同，开放平台实现应用方的接入，自有渠道实现银行自有终端的接入；

——开放平台与基础支撑系统：开放平台在构建过程中，应实现对行内基础支撑系统的集成，如短信平台、加密平台；

——开放平台与行内业务整合类系统：开放平台可通过行内的业务整合类系统实现行内业务系统、行外系统的能力组装发布；

——开放平台与行内业务系统：开放平台应为行内业务系统对外服务能力开放提供通道。

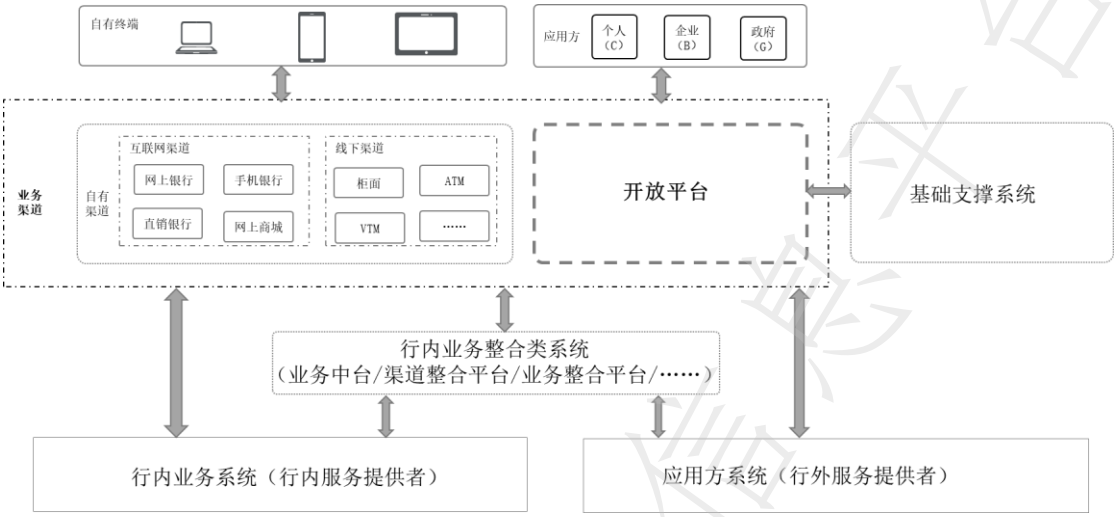

图2 开放平台外部关联体系参考图

6 应用架构

6.1 架构图

开放平台的应用架构参考图如图3所示，应包含的关键应用组件有：应用方门户、运营中心、安全中心、配置中心、接入接出网关。建议包含服务组合、服务治理、服务监控等组件或在全行架构体系内具备相应的能力。

图3 开放平台应用架构参考图

注：因为开放平台对服务组合组件并无特殊要求，可直接利用银行已有的相关能力，故本文件不再对其内容进行展开。

6.2 应用方门户

应用方门户主要使用对象是个人、企业、政府的应用开发者或运营运维人员，应用方可以在应用方门户上注册、申请、学习使用开放平台提供的产品功能。

注：此处的产品，是指一组满足特定业务需要的 API 的集合。如电子钱包产品，包括开户、充值、消费、提

现等多个 API。

应用方门户建议主要包含以下模块。

——产品模块：产品模块宜提供产品相关信息及内容展示功能，包括：

- 产品列表展示：展示产品分类及其包含的产品名称列表；
- 产品详细信息展示：展示包括输入输出参数、错误码、调用方法说明、测试说明，包含的服务列表、测试工具、申请使用流程等详细信息。

——应用模块：应用模块宜提供应用方管理自身应用的功能，包括：

- 我的应用：查询应用方的所有应用；
- 新建/修改应用：应用方通过应用中心新建应用，并提出审核申请，待审核时可修改应用信息，申请后，银行方进行审核；
- 证书申请：应用方通过下载的证书生成工具生成并上传证书；
- 产品管理：应用方申请目标产品、查看使用产品清单、查看产品使用情况（如交易量、交易总额等）；
- 运营管理：提供运营报表的查询；
- 环境管理：查询测试地址、应用唯一标识的信息；
- 在线测试：可在线发送报文进行接口测试；
- IP 白名单管理：配置系统的 IP 白名单。

——应用方用户模块：应用方用户模块宜提供应用方用户的维护和管理功能，包括：

- 基本信息：查看和修改应用方用户的基本信息；
- 实名认证：应用方用户注册后，应通过实名认证申请和银行方审批；
- 计量计费：查询账单，绑定账户，进行计费的支付；
- 消息通知：查看系统提醒的通知；
- 角色管理：对同一应用方的不同使用用户提供角色管理；
- 应用方用户管理：对同一应用方的不同用户进行管理；
- 在线反馈：应用方可通过在线反馈，提交咨询问题并等待反馈。

——帮助模块：帮助模块宜提供流程说明、资源查找、手册下载等功能，包括：

- 开发指南：应用方可通过学习开发指南，了解开放平台的注册、接入、使用等要求；
- 测试环境：提供沙箱环境的使用说明，应用方可通过沙箱接入并实施测试；
- 工具下载：应用方可下载 SDK 等所需工具。

——新闻模块：新闻模块宜提供可查看和浏览开放平台新闻、消息等信息的功能，包括：

- 新闻列表展示：展示新闻的列表；
- 新闻详细信息：可查看新闻的详细信息。

6.3 运营中心

6.3.1 概述

开放平台应为运营人员提供管理控制台。基于运营中心，运营人员可进行开放平台基础信息管理、应用方维护认证、应用维护审核、计费管理功能。

6.3.2 开放平台基础信息管理

运营中心应为管理员提供维护开放平台基础信息的功能。具体包括：

——机构管理：运营中心机构管理功能应支持机构的管理维护操作，实现新增机构、修改机构信息、删除机构等功能；

——操作员管理：

- 运营中心管理员可对操作员信息进行维护，实现相关增删改查功能；
- 为操作员设置岗位和权限，设置登录用户名和初始密码。

——岗位管理：

- 运营中心管理员可对岗位信息进行管理维护，实现相关增删改等操作；
- 应实现岗位信息的条件查询。

——权限管理：

- 权限设置应遵循最小授权原则；
- 应对不同岗位的操作员设置与其对应的数据权限，运营中心的权限管理宜细化到菜单级别的权限管理，系统维护及操作；
- 应对不同机构的操作员设置与其对应的数据权限。

6.3.3 应用方维护认证

运营中心应提供应用方维护认证功能。具体包括：

——应用方维护：

- 运营中心应用方维护功能提供对于应用方的用户冻结、解冻、权限分配等功能；
- 复核人员对维护操作进行审核；
- 查看应用方详细信息，查看经办人和操作类型等。

——应用方认证：运营中心实名审核功能主要用于对应用方的用户实名认证申请的审核，如应用方资料审核、注册申请审核、身份认证审核等。

6.3.4 应用维护审核

运营中心应提供对应用的维护审核管理功能。具体包括：

——应用维护：运营中心应用维护功能提供对应用的维护操作，如应用上下线管理，权限分配，应用冻结、解冻等管理功能；

——应用审核：由运营人员通过应用审核功能，对应用方提交的申请，包括应用申请、产品申请、证书申请、应用上下线申请、沙箱环境申请等进行审核。

6.3.5 计费管理

运营中心宜提供服务使用计费管理功能。具体包括：

——计费维护管理：

- 运营人员对调用次数费用、流量费用的计费模式、计费类型、计费周期、计费限制，扣费方式进行审核管理；
- 运营人员管理和设置商业银行及应用方的收益分配方式。可按交易分类、商户类别、交易数量、交易金额、交易地区、卡类型等多种维度进行收益分润的设置。

——结算管理：

- 开放平台按照设定的利益分配方式及计量统计结果，完成银行和应用方的收益分配计算、清结算；
- 开放平台宜支持灵活的结算方式，如事前包月、事中实时扣费、事后根据实际交易笔数或交易金额累计值的结算。

——计量统计：

- 统计商业银行与应用方、发卡方银行等机构发生的交易数量，交易金额，获得的收益分成，系统生成明细统计报表；
- 统计不同互联网企业应用及外部应用的流量费用、调用次数费用。运营中心对不同计费模式，计费类型的流量费用、调用次数费用进行统计分析，生成日/月/年报表；
- 费用明细账单，运营人员可以查看应用方账户的费用信息。

6.4 安全中心

6.4.1 概述

安全中心是开放平台的核心部分，应提供安全管理控制、安全数据服务方面的能力，包括证书管理、密钥管理、授权认证、安全传输、行为侦测。

6.4.2 证书管理

证书管理，应支持服务端证书管理、客户端证书管理、证书的生成、存储、上传和下发，对其具体要求如下：

——对于有能力的应用方，应建立自己的证书系统，生成自己的公私钥证书，然后通过应用方门户，将公钥证书上传给开放平台安全中心进行保管；

——对于能力欠缺的应用方，可以在应用方门户上填写申请资料，向开放平台申请自己的公私钥证书；

——如果行内有RA服务器，则将证书申请信息提交到RA服务器，通过RA生成可信任的合法证书；

——如果没有RA服务器，则请求安全中心自带的证书生成工具，生成不可信任的证书。

6.4.3 密钥管理

密钥管理的具体技术要求应符合JR/T 0185—2020中7.3.4的规定。为支撑以上要求并满足其他相关安全需求，开放平台应支持密钥的生成、存储、上传、下载、重置等功能。具体包括：

——商户可以在应用方门户上传已生成的密钥，上传后的密钥将由安全中心统一保管；

——应用方门户上应提供密钥的生成功能，商户可以通过应用方门户进行密钥的生成申请，此时密钥将由安全中心生成并保管；

——生成的密钥应展示在应用方门户上，应用方用户可以进行查看、下载；

——密钥应支持定期或主动地重置：

- 可以为密钥设定有效期，有效期满时开放平台自动进行重置更新；
- 当商户认为存在密钥泄露、被破解等不安全隐患时，可以在应用方门户上主动进行密钥的重置；
- 密钥重置后，旧密钥将失去作用，开放平台将使用新的密钥进行数据处理。

6.4.4 授权认证

授权认证的具体技术要求应符合JR/T 0185—2020中7.2.1、7.3.1、9.2.1、9.3.1的规定。为支撑以上要求并满足其他相关需求，开放平台应具备以下能力：

——支持通过APP_ID、App_Secret、数字证书、公私钥对，单独或组合进行身份认证；

——支持针对不同的服务场景，配置不同的身份认证策略；

——支持根据应用唯一标识APP_ID、应用的状态、产品的状态、应用申请产品的情况对应用方服务调用过程进行权限控制。

6.4.5 安全传输

安全传输的具体技术要求应符合JR/T 0185—2020中9.2.2的规定。为支撑以上要求并满足其他相关需求，开放平台应具备以下能力：

——应采用HTTPS协议，为浏览器和服务器之间的通信进行加密；

——应支持对报文中敏感数据进行加密处理，敏感数据不落地保存，并及时清理；

——应支持对报文中敏感数据进行脱敏与还原处理；

——应支持对报文整体的加签验签处理；

——应支持主流的加解密、加签验签算法，如国密算法等。

6.4.6 行为侦测

开放平台应记录必要的交易信息，如应用方标识、应用唯一标识、接口标识、时间戳等，对交易信息进行监控分析以及告警，并对第三方行为侦测分析。

6.5 配置中心

配置中心用于开放平台的参数配置，应满足参数高效获取、实时感知的要求。配置中心数据分类主要包括以下几种：

——服务配置：队列服务、缓存服务；

——开关配置：功能开关、业务开关、服务开关；

——业务配置：各类业务配置项。

6.6 接入接出网关

6.6.1 概述

服务网关是开放平台核心基础能力，企业将自身的服务能力封装成服务接口注册到网关，网关对服务进行管理，通过安全加密、流量控制、故障隔离等技术为应用方提供安全稳定的调用环境。

6.6.2 服务接入网关

服务接入网关应具备流量限制能力，根据预先设定的安全规则和业务规则将契合要求的流量过滤出来，然后根据接入的产品业务，将流量派发给后端业务系统进行处理。服务接入网关应具备以下主要能力：

——身份认证及鉴权能力：服务接入网关应具备识别使用者身份，防止其他人恶意冒充合法用户身份的能力，应能控制特定用户对服务能力的访问权限。

——数据安全防护能力：服务接入网关应确保数据在传输过程中的安全，通过加密算法，对数据进行脱敏、对称加密等安全处理，并且提供数据的完整性校验，确保数据在网络传输过程中的安全。

——多协议适配能力：服务接入网关应支持多种网络环境和常见传输协议，提供各类硬件及软件的快速接入能力，服务接入网关通过适配器将多种网络或数据协议进行适配统一后发送给业务系统使用。

——流量调控能力：服务接入网关应提供多种流量调控能力，根据不同的场景，设定相应的流量调控规则，从流量控制、熔断降级、系统负载保护等多个维度保护内部系统的稳定性，提高开放平台的整体可用性。

——灰度与MOCK支持能力：服务接入网关应能支持灰度发布及MOCK测试工作的开展。

——服务注册访问能力：

- 服务接入网关对内应提供服务的发布注册能力，服务接入网关根据服务接口提供的业务能力建立产品级的金融服务目录，通过发布注册模块将服务注册到网关中，配置相应的业务安全策略后，开放给应用方使用。
- 服务接入网关对外应提供服务的访问能力。

6.6.3 服务接出网关

服务接出网关为开放平台提供对外开放连接，应主要包含两方面功能：首先是用于开放平台整合应用方的服务；其次是用于行内系统通知应用方，具体业务由异步服务处理完成后通知应用方结果及其他主动通知交易。

服务接出网关应具备以下主要能力：

——模块化的开发及部署能力：模块化的开发及部署能力主要针对外部平台的接入条件的多样性，和接入平台相反，应将内部统一的数据及传输协议适配成为外部平台多样的数据及传输协议，所以应具备模块化的开发及部署能力来支撑和适配外部的多样化接入协议；

——证书等凭证的管理能力：服务接出网关在对接外部时，应使用不同的证书，对于证书的合法性及有效性进行管理，对于不合法、过期的证书要及时更换，确保接出系统的连贯性和稳定性。

6.7 服务治理组件

服务治理是整合服务的关键，通过服务治理可以有效地对业务服务、接口、元数据等进行管理和控制。使用自动化导入功能，可以对服务进行导入导出，避免重复冗余的工作，同时还能将整合后的服务下发到网关运行态，使得服务的治理、导入、下发一体化自动化。

因此，建议开放平台配套建设服务治理组件，或完善行内统一的服务治理组件使其满足开放平台服务治理的要求。

开放平台服务治理组件应补充完善以下功能：

——服务分类：遵守JR/T 0185—2020附录B.3.5的要求对服务进行分类管理。

——服务分类维度：可以对服务分类进行管理，预置服务分类及扩展服务分类；

——接口管理：对需要发布到互联网上的接口资源进行管理，如统一识别码、接口URL、API安全级别、接口功能描述、输入输出参数及其他技术信息等；

——服务发布：服务发布是指将服务发布到应用方门户，供应用方申请调用；

——产品管理：根据不同的业务需求对服务进行分类，形成一个个产品，发布到门户上供应用方调用；

——调用关系管理：支持在服务治理平台维护应用方与产品、API之间的调用关系，并可下发至运行态作为权限控制的依据。

6.8 服务监控组件

为遵守 JR/T 0185—2020 中 7.3.3、10.1 的要求，建议开放平台配套建设服务监控组件，或完善行内统一的服务监控组件使其满足开放平台服务监控的要求。

开放平台服务监控组件应补充完善以下功能：

——服务和产品监控：基于服务和产品的运行情况监控；

——应用方运行监控：针对应用方的交易调用情况、流量进行监控；

——异常事件监控：开放平台应用各种异常事件监控；

——异常告警：支持对应用方进行告警、设置告警的方式和告警的策略，包括邮件告警、短信告警等；

——日志记录：应能完整记录接口访问日志，日志内容应遵守JR/T 0185—2020中7.3.3中关于日志的要求；

——权限检测：应满足JR/T 0185—2020中10.1.2的要求，建立未授权和冒用商业银行应用程序接口的检测机制，发现问题及时处置。

7 技术架构

7.1 架构图

开放平台整体技术架构参考图如图4所示：

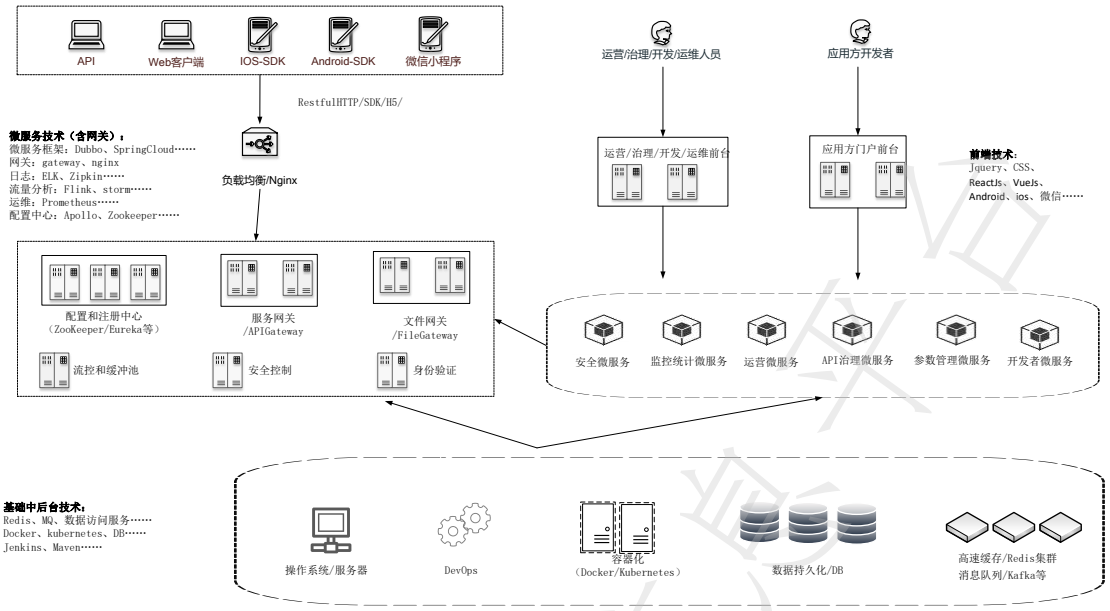

图4 开放平台技术架构参考图

开放平台的技术框架为分层体系架构，涵盖前端、中台和后台等各类技术。

7.2 前端框架

前端框架宜满足以下技术要求：

——应使用前后端分离技术。前端服务负责提供最外围的服务展示、服务接入、服务流程等内容，后端服务提供运营服务、产品服务等内容；

——应采用基于组件和模块化的开发方式，页面的加载采用异步嵌入技术；

——开发技术框架的选择上，可使用高性能渲染框架以及统一的标准脚手架工具，标准化应用结构，流水线式开发；

——可使用可定制的标准化web组件库；

——在构建上应使用成熟的工具，解决代码分割，压缩等问题；

——配有高性能I/O中间转发服务层，实时监控应用运行状态。

7.3 服务框架

开放平台服务面向互联网，基于互联网流量的不确定性，宜采用微服务框架。服务框架建议包含以下组件。

——注册中心：应具备服务注册发现能力，应记录当前可用的服务实例。

——负载均衡：应支持服务提供方使用多实例方式发布服务，支持服务调用方动态、自动连接到合适的服务节点。

——服务网关：应包含完整的通讯框架，实现服务的路由转发。

——限流、熔断和降级：限流器应限制访问后端的流量，起到缓冲和保护作用；熔断器应确保依赖的服务出现故障时，其他服务正常运行；在业务高峰时，可通过手动或自动方式完成低优先级服务的降级配置，保障高优先级服务的运行。

——配置中心：应具备将本地设置的配置信息在配置中心中发布注册的能力，实现多节点实时同步全局信息，同时保证配置过程在开发、测试、生产环境的无差别性。配置中心宜使用高可用的分布式方案，确保一个配置服务出现问题时，其他节点也能够提供配置服务。

——服务集成框架：应具备不同服务框架、服务组件的整合能力。将服务组件集成在统一的服务框架上协同工作，集成框架应提供可用的服务运行环境，并实现各类业务的配合工作。集成框架应能够让用户在统一的界面使用系统。

——调用链：应能够跟踪记录完成一个业务逻辑时调用到的服务链路，并将这种串行或并行的调用关系展示出来。应能够利用调用链在系统出错时快速定位故障点，并可统计各个服务的调用次数，确保热点服务能够被分配更多的资源。

——监控组件：应具备指标监控、链路监控和日志监控等监控能力，应提供快速集成的方式，将多维度的统计指标进行汇总分析和统一展示，自定义告警阈值，与其他组件联动实现动态扩容、主动隔离，线性伸缩等功能。

7.4 中间件

在开放平台技术架构中，为高效地开发和集成各应用组件，建议引入中间件。开放平台框架使用的中间件建议包含以下几种。

——Web服务器中间件：Web服务器中间件用于承载前端应用程序，应可以处理HTTP协议，响应针对静态页面或图片的请求，进行页面跳转，或者把动态请求委托给应用服务器。

——应用服务器中间件：应用服务器中间件用于承载后端应用服务程序，应屏蔽服务器的复杂性，使得应用程序在此基础上可以方便快捷地部署和运行。

——缓存中间件：缓存中间件应提供数据的高速访问能力，减少数据库访问的次数，加快应用程序响应速度。

7.5 数据库

开放平台的数据包括两类，一类是开放平台的应用方信息、应用信息、产品信息、服务信息等业务类信息；另一类是服务运行过程中的调用流水信息。

基于应用场景，开放平台对数据库要求建议如下：

——业务类信息不需要复杂的逻辑运算，建议采用传统关系型数据库；

——针对调用流水信息，需要支持流水信息的高效写入，需要具备时间维度的表分区及清理能力，可采用时序数据库；

——采用开放式架构，能够在不同的软硬件环境中便捷切换；

——提供完善成熟易于配置的数据备份、数据清理、数据恢复和数据库监控方案，并提供相应的工具或程序。

7.6 服务器

开放平台面向互联网的特性，要求其服务器资源具备较强的扩展能力、伸缩能力。因此，建议如下：

——服务器资源应考虑通过云化资源池，采用虚拟机的方式进行基础单元部署；

——虚拟机应支持分组处理，保障接口类请求、文件传输类等不会互相干预；

——应部署代理服务器，如Nginx，进行负载均衡，以提高服务防风险抗压力的能力。

7.7 双模开发

开放平台宜同时兼顾敏态和稳态的双模开发模式。敏态注重定制化开发，如对报文、通讯协议个性化适配开发等；稳态更注重产品的标准化开放。建议采用以下方式支撑双模开发：

——Devops体系：从开发、测试、运维等方面与稳态模式分开，实现快速交付；

——灰度发布：灰度发布能有效降低版本发布的风险，是开放平台对外稳定输出服务能力的体现；

——沙箱：沙箱是与生产环境基本一致，提供给应用方联调测试用的测试网关，在敏态和稳态模式下的沙箱可分离部署，降低交易开发的耦合度。

8 物理架构

8.1 架构图

开放平台的部署架构参考图如图5所示：

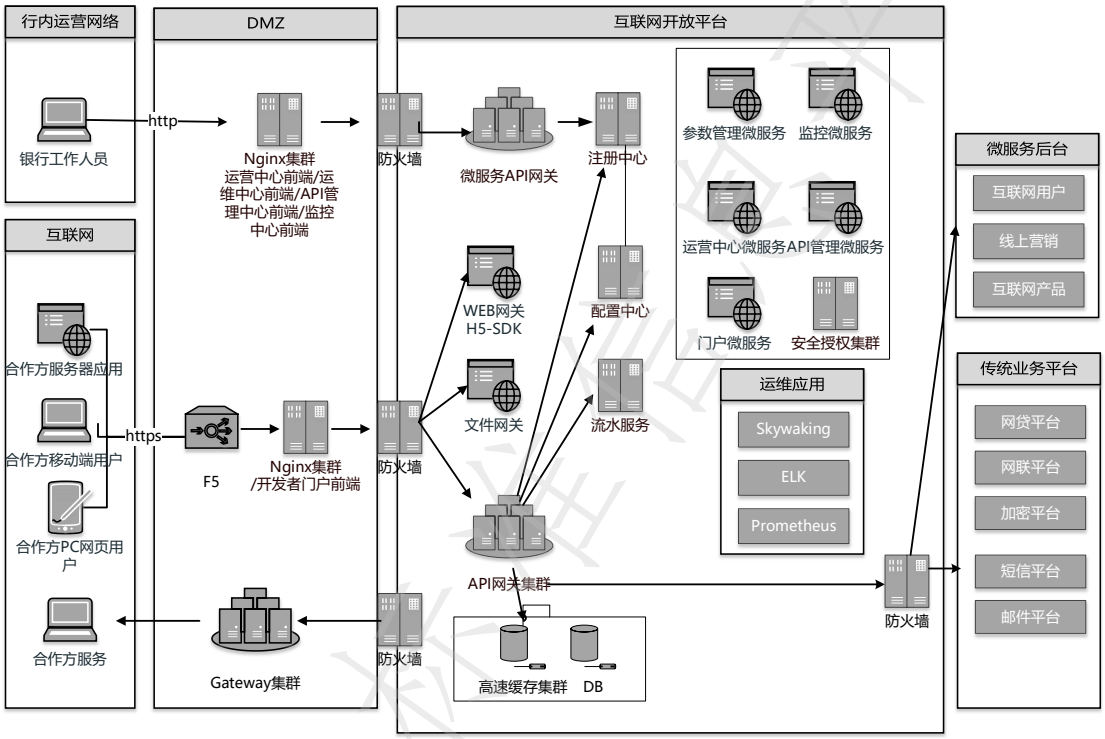

图5 开放平台部署架构参考图

开放平台的部署架构采用分区分域的方式，在网络区域划分上应划分为网络接入区（部署在DMZ网络的部分）和平台服务区（部署在核心网络的部分）。不同网络区域使用屏蔽子网防火墙进行隔离，DMZ区域与互联网、城域网或专网通过外网防火墙设置连接策略，并采用银行统一的安全架构和安全设施保证接入安全。

8.2 DMZ 区

DMZ区负责与外部互联网环境的直接对接，要求如下：

——根据应用方的网络架构不同，DMZ区域仍可以划分为多个独立的子区域，为不同的网络连接模式提供接入点；

——应为不同安全需求的接入模式提供互不干扰的策略和独立的网络环境，应在每一个区域内部署开放平台网络接入区的全部逻辑节点，并保证每个区域的服务都是高可用的；

——在DMZ区，各组件完成接入点的功能，执行链路加解密、（通讯级）身份验证、完整性校验、通讯报文形式检查等工作，并将通过校验的合法请求报文路由至下一个处理节点；

——接入点应通过负载均衡器实现流量动态分配和反向代理等功能；

——开放平台门户页面的静态资源宜驻留在DMZ区。

8.3 开放平台服务区

开放平台的核心组件建议部署在开放平台服务区，其中包括：

——交易网关：包括API网关、WEB网关、文件网关等。
——开放平台服务：包括应用方门户、运营中心、配置中心、运维监控组件等。
——银行IT基础设施：开放平台的运行时环境和依赖的基础中间件、操作系统、数据库能力，属于IT基础设施，由各银行按照本行IT架构规划统一使用。

8.4 灾备设计

开放平台应采取必要的灾备策略保障开放平台运行的安全稳定，具体要求如下：
——开放平台应支持多中心部署，数据库、应用应至少保证同城主备（一主一备）部署，必要时需实现同城双活，异地灾备；
——开放平台应支持分布式部署方式；
——整个部署架构不应存在单点：所有节点均可以通过硬件负载设备或者软负载工具，实现集群多节点部署，部署节点也可以随业务量的增加横向扩展，且所有应用都是运行状态；
——开放平台应具备运行时安全控制策略，如流量控制、故障隔离、服务熔断。

8.5 沙箱设计

开放平台应使用沙箱提供应用方测试验证能力，具体要求如下：
——若使用挡板（数据桩）的方式，则沙箱应为开放平台服务中的一类应用，部署在核心网络区；
——若使用仿真业务环境，应将所有仿真环境独立搭建子网，开放平台节点应在该子网中再次部署；
——配置有限的防火墙策略，使得仿真测试子网的开放平台服务节点与生产环境的开放平台服务节点进行数据和文件交换。

9 安全架构

9.1 网络安全

开放平台的网络安全应遵守JR/T 0071中有关网络安全的要求，同时满足JR/T 0185—2020中8的要求。

同时针对开放平台的特性，补充以下内容：
——应建立网络隔离区，实现与互联网环境的连接；
——网络隔离应采用双层异构网络防火墙进行保护，分别是互联网和DMZ区设置一道防火墙，DMZ区和内网应用区设置一道防火墙，通过防火墙中设置的安全策略，确保网络流量的合法性；
——DMZ通常应放置一些不包含机密信息的公共设施，主要包含web服务器、反向代理、FTP服务器、第三方网关等；
——互联网HTTPS请求应先经过SSL加速器卸载HTTPS到HTTP进入DMZ区，然后经过反向代理，基于统一资源定位符（URL）负载路由到指定的内网应用，反向代理可以选择性地将内网服务对外进行暴露。

9.2 应用安全

9.2.1 身份验证/认证

开放平台应按照JR/T 0185—2020中7.2.1、9.2.1、9.3.1的规定进行身份验证/认证。此外，还宜满足以下条件：
——应支持集中管理授权和认证，如基于OAuth2.0的授权标准；

——应采用高速缓存存储授权认证信息，进行统一的授权管理和认证；
——交易在运行中，应可以基于多个层面进行安全认证，其中一个环节认证失败，则整个交易失败。

9.2.2 权限控制

商业银行应遵守JR/T 0185—2020中9.3.2的要求控制相关权限。此外，还应满足以下条件：
——应用方可以通过签约的方式申请服务的访问权限，经过开放平台运营人员后台审核、复核后获得相应的访问权限；
——签约获取的访问权限应设置有效期，并提供有效期管理，签约内容变更时应提示应用方重新完成签约；
——开放平台应为应用方提供主动撤销访问权限，注销应用程序的功能；
——开放平台应具备运营管理功能，运营人员可以通过管理端对开放平台进行管理控制；
——应用方门户应针对不同的运营人员设定不同的角色和权限，不同角色登录展示不同的菜单内容；
——应用方门户应支持登录超时控制，运营人员可设定、修改默认登录超时时间。

9.2.3 安全传输

商业银行应符合JR/T 0185—2020中9.2.2的规定设计信息传输方案。根据使用场景不同可选择HTTPS单向认证或双向认证。有条件的应用方可以搭建虚拟专用网络或物理专用网络。

9.2.4 流量控制

开放平台应提供多维度的流量控制机制，包括应用方、应用程序、服务接口、服务系统、吞吐量等维度，各维度可以自由组合。当服务单位时间访问量或并发量超过预设的流量阈值时，应立即启动预先设定的处置流程。

9.2.5 故障隔离

为满足故障隔离要求，开放平台应具备以下能力：
——应提供完备的故障隔离机制，支持人工隔离或自动隔离模式，当有异常情况发生时，能快速有效地隔离故障点，避免异常扩大化对其余正常部分造成干扰破坏。
——应具备健康监测模块，能够及时响应负载均衡设备发送健康探测报文，当系统集群中某一路状态出现异常或处于关闭状态时，负载均衡设备能够及时切断该路系统的流量，避免影响对外服务的可用性。
——应具备统一异常定义和处理模型，对服务接口和服务系统的异常进行完整记录和监控。当异常统计信息满足设定的规则时，能够通过监控平台发出告警，并对故障服务或故障系统迅速隔离，避免局部故障导致资源过载、服务阻塞，影响整个系统的可用性。

9.2.6 服务熔断

开放平台的服务访问请求，应根据服务系统的服务响应时间和返回状态，判断服务状态是否正常。当服务系统发生异常达到预先设定的阈值时，应采取自动拒绝交易或暂停服务等措施，避免某一服务的故障影响其他服务的正常调用。

9.2.7 SDK 加固及代码混淆

开放平台对外发布的SDK初始化时，后台应对SDK的信息做出校验，确保SDK的准确性以及对SDK代码混淆和加固，防止被恶意反编译修改和核心代码流失。

9.2.8 安全审计

开放平台应能支撑商业银行的安全审计需求，并符合JR/T 0185—2020中12.3的规定。

9.3 业务安全

9.3.1 用户安全

对用户安全的要求如下：

——用户数据侦测：银行应通过必要的流程设计及技术手段，对用户交易行为数据、资产数据进行侦测，掌握用户资金的实际去向，保障用户的资金安全及使用合规（如通过受托支付形式发放贷款、获取钱包账户交易明细等）；

——用户信息保护：

- 用户数据授权：应在业务流程中做好关键信息的授权管理；
- 用户数据传递：应尽可能减少客户信息的传递；
- 用户数据使用：应加强风控能力建设，按照最小可用原则向第三方提供数据，同时对数据采取必要的脱敏处理。

9.3.2 交易安全

商业银行应符合JR/T 0185—2020中10.2.2、10.2.3的规定实现对交易安全的管理。此外，还应满足以下条件：

——交易风险控制：应对应用方行为侦测与预警，应在调用过程中校验API的调用顺序；

——开放形式控制：对外开放形式采用API直接连接时，应遵守JR/T 0185—2020中6.2中的要求；

——业务合规性保证：应确保业务产品的合规性以及业务产品的长期生存和可持续发展。

9.4 数据安全

依据《数据安全法》《个人信息保护法》规定，商业银行必须对数据进行分类分级管理。商业银行应遵守JR/T 0171-2020规定的数据分类分级要求，实现对数据收集、传输、存储、使用、删除、销毁的全流程管理。

商业银行应遵守JR/T 0185—2020中7.2.2、9.3.3的要求对数据进行管控。

可参考方法包括但不限于以下内容：

——数据加密解密：互联网业务的开展应符合行业标准的信息安全与加密方案，并支持国密算法，具体要求如下：

- 在互联网数据传输时，应具备数据加密及传输加密机制，使整个系统数据传输的各个环节无明文数据；
- 为防止数据在传输过程中被拦截获取，应用方在请求互联网业务时，应对上传的数据进行加密，形成密文，在互联网数据通过密文进行传输，银行收到密文数据后进行解密，转换成明文，再进行后续处理。

——数据加签验签：从互联网进入的数据请求，经过加密和加签处理，以验证数据是否被篡改过，并防止数据被拦截泄露。通过数字签名技术防止数据被非法访问、篡改、丢失。

——数据脱敏还原：与第三方平台进行数据交互时，涉及到企业内部用户隐私数据的请求，应按照最小授权原则，采用数据脱敏和脱敏还原机制，保障用户的个人信息安全不被泄露。其中，数据脱敏及脱敏还原可采取标记化技术实现，可参考JR/T 0149-2016的要求。

——数据备份与恢复：应建立本地或异地灾备的数据系统，该系统对主系统关键应用数据实时复制，当灾难发生时，本地或异地灾备系统可以快速接管主应用系统。

参考文献

[1] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[2] GB/T 25069-2010 信息安全技术 术语

[3] JR/T 0149-2016 中国金融移动支付 支付标记化技术规范

[4] 中国银行保险监督管理委员会.商业银行信息科技风险管理指引（银监发〔2009〕19号文印发），2009年3月3日

[5] 中华人民共和国数据安全法.2021年6月10日

[6] 中华人民共和国个人信息保护法.2021年8月20日