附件1:

**重庆高新区金融创新线上综合服务平台**

**建设方案**

一、项目背景

重庆高新技术产业开发区于1991年3月经[国务院](https://baike.baidu.com/item/%E5%9B%BD%E5%8A%A1%E9%99%A2/343590)批准成立，是首批5个国家综合改革试点开发区，位于重庆都市发达经济圈核心区、两江半岛中心地带、成渝经济区重庆门户。近年来高新区经济大力发展，在过去五年中，重庆高新区新增高新技术企业、科技型企业、高新技术产品数量稳居全市第一！其中孵化公司有8家企业挂牌新三板和重庆股份转让中心。2017高新区科技服务大市场累计实现交易额超80亿元。市级及以上众创空间达8家，创新创业孵化面积超100万平方米。种子基金投贷项目50个、金额1723万元，3支产业专项基金规模达18亿元。科技金融产品助企融资达5亿元。

面对强大的金融需求以及高速增长的企业数量，政府部门的工作量也成倍数增加，加之政府部门目前没有相对完善的体系对企业和金融机构的供需进行管理，无法规范金融市场。为此，高新区为了更好地彻执行财务制度，按照政策组织财政收入，保证财政支出，管好用活地方的财政资金以及积极响应国家职能政务的口号，提高经济效益，高新区欲结合时代特点利用，云计算等先进技术，打造一个开放、公益、专业的金融创新线上综合服务平台，其作用于加快推进科技与金融有效结合，优化科技金融环境，缓解科技型企业融资难问题，方便企业发布获取政府补贴以及金融产品的需求，同时也让高新区和第三方金融机构积极对接其需求，形成一个良好的供需关系链。

二、需求分析

**（一）拓宽融资渠道**

企业需要依托高效便捷的线上金融服务平台寻找到适合的金融产品。中小微企业在孵化和成长到成熟的各个阶段都需要资金的持续供给和政策扶持，传统的模式是通过线下的方式寻找投资，成本高、时间长、效率低。因此，急需找到可提升企业在进行股权和债券融资效率的渠道。

**（二）提升产品竞争力**

除了通过纸媒电视等传统媒介渠道发布自身金融产品，银行（金融机构）也需拓展现有金融产品的发布和宣传方式，让市场更好地了解银行（金融机构）的优势产品的同时，银行也可以通过平台累积的企业需求资源对自身产品进行优化和创新，提升产品认同度的同时，也完成自身产品链的快速升级。

**（三）线上下审批结合模式**

为响应国务院关于印发2016年推进简政放权放管结合优化服务通知，提高政务服务效率。大力推行“互联网+政务服务”，为企业孵化和成长“点对点”提供政策兑现线上高速通道，是目前高新区政府部门的首要需求。

**（四）金融活动精准推送**

第三方金融中介机构需通过活动及其金融辅助业务的线上发布，为区内需要参与路演、展会和急需上市辅助的高成长类企业提供有效支持，与此同时，也有力促进第三方机构的良性和健康发展。

**（五）信息保密和平台安全**

金融创新线上综合服务平台在投入运营后，将会累积大量的企业基本信息、经营信息和融资需求数据。同样，高新区内的银行（或者其他金融机构）会对企业的产品申请进行审核和反馈，以及政府部门在政务审批中查看到企业填报的申请内容，都属于需要重点进行信息保密和平台安全维护的关键范畴。

三、项目目标

**本平台建设目标主要有以下两点：**

一是致力于通过PC端和移动端为企业特别是科技创业型公司提供创业扶持政策和金融产品线上服务，同时为区内各家银行（或者其他金融机构）提供集中性一站式产品发布渠道和平台。

二是通过智能化和便捷性的功能模块设计，在平台建设和运营阶段充分利用聚类分类分析、复杂网络匹配模型、自然语义分析等先进技术，最终把重庆高新区金融创新线上综合服务平台打造成具备科学、创新、高效理念的指标性和示范性的创业创新金融互动服务平台，为实现金融市场供需双方互利共赢，为着力提升高新区营商环境质量奠定坚实基础。

四、建设原则

为确保项目的建设成功与可持续发展，在平台的建设与技术方案设计时平台开发商将遵循如下的原则：

**（一）统一设计原则**

统筹规划和统一设计系统结构。尤其是应用系统建设结构、数据模型结构、数据存储结构以及系统扩展规划等内容，均需从全局出发、从长远的角度考虑。

**（二）先进性原则**

系统构成必须采用成熟、具有国内外先进水平，并符合国际发展趋势的技术、软件产品和设备。在设计过程中充分依照国际上的规范、标准，借鉴国内外目前成熟的主流网络和综合信息系统的体系结构，以保证系统具有较长的生命力和扩展能力。保证先进性的同时还要保证技术的稳定性、安全性。

**（三）高可靠/高安全性原则**

系统设计和数据架构设计中充分考虑系统的安全和可靠。

**（四）标准化原则**

系统各项技术遵循国际标准、国家标准、行业和相关规范。

**（五）成熟性原则**

系统要采用国际主流、成熟的体系架构来构建，实现跨平台的应用。

**（六）适用性原则**

保护已有资源，急用先行，在满足应用需求的前提下，尽量降低建设成本。

**（七）可扩展性原则**

信息系统设计要考虑到业务未来发展的需要，尽可能设计得简明，降低各功能模块耦合度，并充分考虑兼容性。系统能够支持对多种格式数据的存储。

五、建设方案

**（一）整体架构**

重庆高新区金融创新线上综合服务平台整体架构如图1所示：

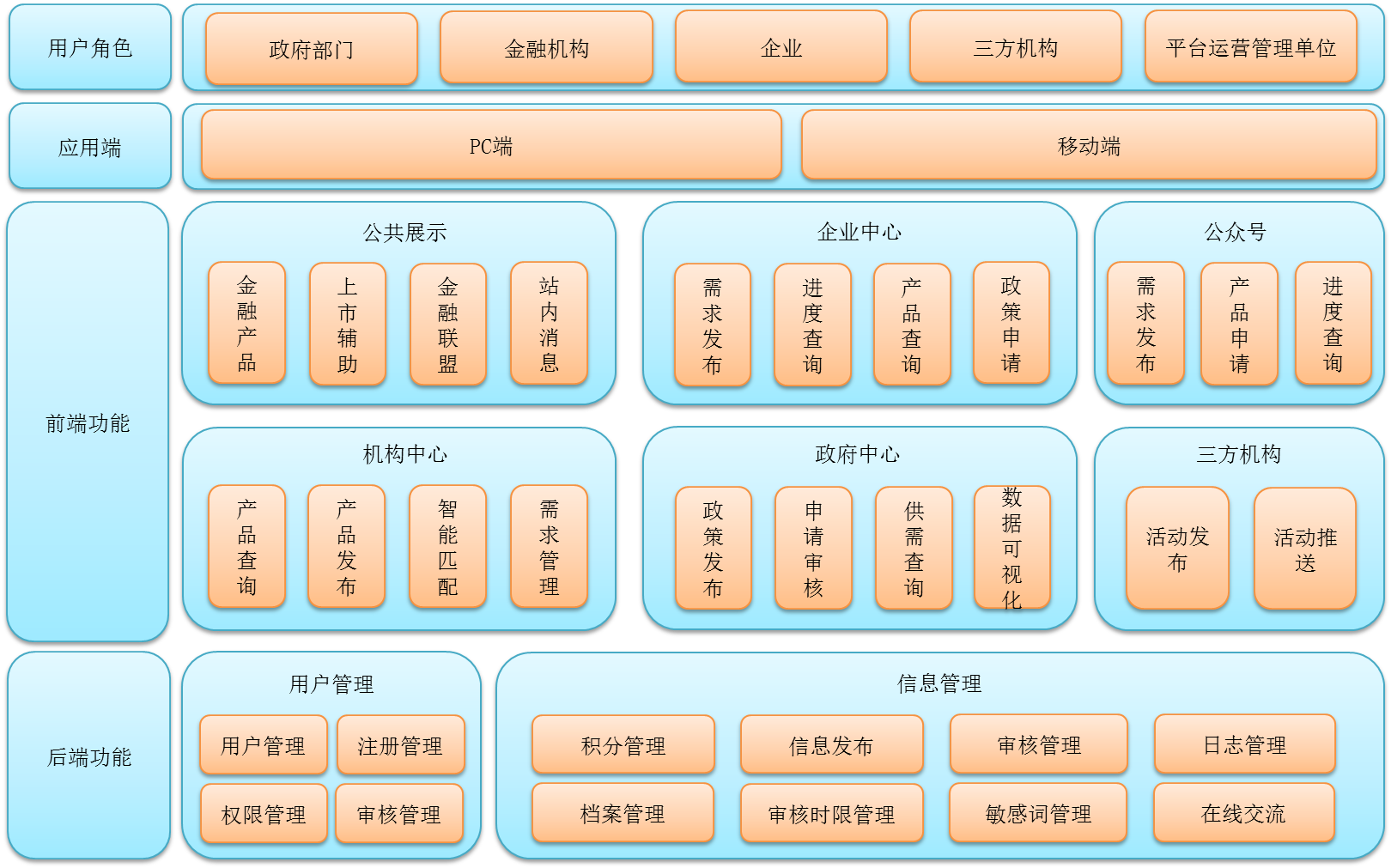


图1 平台架构图

本期平台整体架构整体上分为前端功能和后端功能。前端功能是面向普通平台用户包括社会公众、企业、政府、金融机构及平台运营管理单位的应用功能界面，不同的用户可以查看平台相关信息以及注册登陆后进行相关业务的处理流程，功能主要包括：

金融产品；

金融联盟；

上市辅助；

企业中心；

机构中心；

政府中心；

三方机构；

移动端公众号。

后端功能是面向平台运营管理单位用户的应用功能界面，不同的平台用户管理员可以进行不同的后台操作，包括：审核管理、权限管理和安全管理等相关操作管理功能操作，保证平台信息发布的合规性和稳定运行。功能主要包括：

用户管理；

信息管理。

**（二）用户说明**

金融创新线上综合服务平台的用户角色主要分为5个大类，包含：政府用户、银行（金融机构）用户、企业用户、 平台运营管理单位用户、第三方中介机构用户。针对这几类用户，平台分别提供下列业务权限：

1.政府用户可在平台中发布政策申请细则和申请条件，同时了解平台已发布的需求和产品，另外可通过大屏了解平台实时数据情况。

2.银行用户可发布金融产品，自动匹配企业融资需求，实现需求抢单，以及联合授信和二次授信等业务操作。订单中止和完成后提供评价功能，评分根据规则计入企业在平台中的积分明细。

3.企业用户可发布需求信息，申请相关政策补贴和金融产品，并可实时跟踪申请进度。针对三方中介机构发布的金融相关活动，可报名预约参与。产品申请中止或完成后，评分根据规则计入银行在平台中的积分明细。

4.平台运营管理单位用户可在后台管理中，进行账号角色和权限分配，注册和发布审核，积分管理等平台管理业务操作。

5.中介机构用户可以发布路演活动，进行上市辅助对接等操作，查看服务和活动申请企业详情等。

**（三）流程设计**

整个平台流程设计主要分为企业融资申请流程，企业政策申请流程和银行（金融机构）抢单流程和第三方机构活动发布流程。

**1.企业融资**

企业融资申请流程如下图2所示：



图2 企业融资申请流程

**2.政策申请**

企业政策申请流程如下图3所示：

图3 企业政策申请流程

**3.银行抢单**

银行（金融机构）抢单流程如下图4所示：



图3 银行（金融机构）抢单流程

**4.机构发布**

第三方机构活动发布流程如下图5所示：

图5 第三方机构活动发布流程

**（四）平台功能**

**1.公共展示**

公共展示功能模块主要分为平台首页、金融产品、上市辅助、金融联盟等主要板块：

（1）金融产品板块主要展示金融机构在该平台发布的债权和股权金融产品信息，企业用户登录后可以进行查询和申请，加大了线上金融产品的推广力度，并提高了申请效率。

（2）企业可以在平台发布融资需求，平台通过对需求数据智能匹配给存在适用产品的金融机构，由平台和机构向企业提供产品推介，实现“抢单”功能，为企业提供多种选择。有利于企业通过多方对比选择最优条件的金融产品。

（3）上市辅助和路演及展会活动相关的第三方机构，例如：券商、投行，会计事务所等相关企业也可在平台中发布最新的创新企业活动信息，并可通过选择特定行业实现精准推送，以提高业务促成率。

（4）平台运营管理单位可以在后台发布最新的政策资讯，展示在金融联盟板块中，便于企业及时查看到可能与自身发展有关的政策和新闻消息。

①平台首页

平台首页不仅展示了目前平台已入驻企业和机构的数量，已融资金额总量和供需两端的成交率等关键数据，也包含区内、市级和国家层面的重要政策新闻展示。

同时，首页也提供公众进入各公共模块的入口，例如：我要贷款和我要风投提供给公众用户查看平台中已发布的债权和股权融资产品。上市和申报则为有上市意向和政策申请需求的企业和公众提供资讯服务。

通过上述信息的集中展示和链接，为访问平台的公众了解高新金融创新线上综合服务平台的业务重心和服务项目提供快速直观的有效途径。

②金融产品

金融产品模块主要展示了银行（或者其他金融机构）发布的股权和债权融资产品，访问平台的用户可以通过产品各类属性进行查询，例如：产品类型、利率范围等，为公众和已注册的企业用户提供快速筛选和申请金融产品的快速通道。

③上市辅助

上市辅助模块主要展示了银行（或者其他金融机构）和券商为企业提供的上市辅助产品或联系信息，便于有上市需求的企业及时查阅和进行线上对接，同时也利于政府部门了解和掌握区内具有良好发展潜力的企业信息，为其提供针对性的上市和投融资服务。

通过平台的公共展示页面向公众推送的讯息、金融产品和第三方机构活动等重要信息，有利于平台后期的快速运营推广，吸引区内更多的企业和金融机构进驻平台，提升平台的知晓率和认可度。

④金融联盟

金融联盟部分主要公开展示全市及区内的最新新闻动态资讯，企业扶持政策和与企业创业创新发展相关的重要通知公告，以及第三方金融中介机构发布的活动信息，便于公众和注册用户及时了解高新区范围内正在发生的焦点信息，并提高平台已注册用户的互动性。

**2.企业中心**

企业中心模块是已注册企业用户，在登录平台后可查看和进行允许权限下的业务操作的个人中心页面，功能包括：企业融资需求发布，智能匹配银行（或者其他金融机构）产品，政府部门已发布政策申请，以及融资和政策申请的进度查询。

（1）需求发布

经注册的企业用户可在需求发布页面完成融资需求的标准化表单填写，同时，还能通过添加标签的方式，对企业自身进行自评，提高产品匹配精确度的同时提升申请成功率。

（2）智能匹配

通过企业填写的表单信息，平台为企业用户提供智能匹配服务，为企业实现债权和股权融资产品的精准推送和快速申请。提升企业用户的满意度和平台在供需两端的总体成交率。

（3）政策申请

针对高新政府部门发布的政策兑现项目，企业也可通过本平台进行线上申请，企业在提交申请的过程中，注册时填写的基本信息和在平台中产生的交易数据将被自动带入到申请表单中，从而大大提升企业政策申请的效率。

（4）进度查询

企业用户已提交的政策申请和融资申请，均可在平台进行实时查询，另外平台还提供站内短信推送功能，将企业申请项目的最新审批进展自动发送到企业用户的PC端和移动端当中，利于企业及时掌握并跟进申请提交的进展情况，提高申请一次成功的几率。

企业中心通过帮助企业智能搜集适合自身需求的金融产品，以及提供政府扶持政策的线上申请通道，支撑和拓宽区内亟待资金和政策支持的中小微企业的融资渠道，以开源的方式解决企业遇到各项难题。

**3****.机构中心**

机构中心主要是为平台已认证的银行（或者其他金融机构）提供个人中心页面，集中办理产品的发布、管理、企业融资申请审批和机构主账号与子账号信息维护。利于银行用户能即时知晓市场供需动态，为适应企业不断变化的需求，推动资金供给侧的推陈出新，提升产品竞争力。

（1）产品发布

银行（或者其他金融机构）能根据市场需要和自身产品策略，实时发布和更新债权和股权融资产品，同时平台可实现产品和企业需求的逆向智能匹配，便于银行（或者其他金融机构）能通过“抢单”的方式主动对接企业的需求，实现供需两端的双向选择。

（2）需求市场

需求市场供已认证金融机构查询和查阅企业已发布的融资需求，未经认证的金融机构无法查看到企业实名和真实需求，需企业确认对接后能完整查阅，保证了企业在平台中填报数据的安全性。

（3）需求管理

需求管理模块是银行（或者其他金融机构）处理企业融资申请的主要途径，该功能除可实时进行企业申请审核和评价之外，还提供订单反馈逾期提醒，避免其由于反馈超时影响积分和平台内评级。这样的设置机制，提高了银行（或者其他金融机构）反馈审核进度的积极性，维持平台供需两端良性互动。

（4）信息维护

该模块便于银行了解目前主账号现有积分评级明细，利于银行（或者其他金融机构）优化线上金融服务模式和效率，另外、银行（或者其他金融机构）可对子账号的数量和信息进行维护，便于其以多业务员角色的模式开展融资业务。

通过银行金融机构的有效参与，同时，利用部分约束原则保证资金供给端用户的线上规范操作，保证平台供需互动的合规性和高效性，有利于金融创新线上综合服务平台的平稳和可持续发展。

**4.政府中心**

金融创新线上综合服务平台的政府中心设立“政策发布、申请审核、供需查询、数据可视化”这四个功能板块。方便高新区政府部门发布政策，帮助企业实现线上政策申请，提高办事效率。

（1）政策发布

针对高新区政府部门发布补贴政策的需求，通过填写相应字段发布新政，政府部门也可以查看已发布和待发布的详细内容。政策发布有利于政府及时发布新政信息。

（2）申请审核

主要审核企业各项补贴的申请，当某个企业完成创业补贴的申请时，政府部门相关人员就会审核该公司的相关工商信息，其来源企业数据库（企业基本信息、企业经营状况，企业融资情况以及相关附件（可下载）），此时审核人员需要填写审核结果和审核意见，为了避免审核出错，在初审结束后还要再一次复审，最后完成补贴的办理。

（3）供需查询

分为产品查询和企业需求。产品查询主要用于政府部门管理人员查看金融机构发布的金融产品，并且可以按条件（产品类型，贷款渠道，贷款期限，担保方式，贷款额度）进行筛选。企业需求按时间先后显示企业的贷款需求，政府部门用户可以查看企业申请的贷款意向、担保方式、贷款期限、企业基本信息以及需求成功对接记录。方便政府部门用户把握供需情况，规范市场。

（4）数据统计

主要对债权产品、股权产品、企业需求、上市意向进行统计，并且记录平台企业数、服务企业数、当前产品数、累计成交额、平台机构数、当前需求总数（见图 企业及金融产品数据统计）。实时数据展示通过数据可视化，更加直观显示各个维度数据的变化。

这四个功能板块极大方便高新区政府部门向平台提供政策支持和平台运营管理单位案调整，助力企业快速成长。相应地，平台数据可以宏观辅助政府部门做经济决策，有效帮助政府部门用户把握区内宏观金融状况。

**5.三方机构**

重庆高新区金融创新线上综合服务平台的第三方机构包含活动发布和活动推送功能，方便第三方机构推送活动信息，例如：活动发布可以发布路演或会展活动，当第三方机构需要发布活动时，第三方机构须填写活动信息字段（见图25活动基本信息），确定活动主题、时间、地点、推送行业等相关内容，最后提交审核，交由平台运营管理单位进行审核。

活动推送会根据活动基本信息所选择的推送行业类型，把活动推送给目标行业企业。活动发布增强平台活力，增加企业获取行业最新信息的渠道；活动推送有利于活动的推广和企业知晓率和参与度。

**6.****后台管理**

后台管理模块主要包含：账户管理、权限管理、信息发布、审核管理、积分规则管理和在线交流等功能模块，为平台运营单位保证平台的合规合理化运营提供良好保障。

（1）账户管理

平台运营管理单位用户可以通过账号管理子模块为不同的平台角色用户新建账号，包含了政府用户、企业用户、金融机构用户、第三方机构用户、平台运营管理单位用户，并由系统自动分配唯一的账号编号，以供将来查询分辨。且还可修改账号信息，查看账号详情，启用或者停用该账号。

另外，平台实行分级账号管理制度，主账号可自行创建并管理子账号，方便上级管理下级工作，上下沟通更为便捷，有效提高工作效率，满足上层想了解下属工作动态的需求。

（2）权限管理

平台运营管理单位用户通过账号注册审核和管理，创建完成不同的角色用户账号之后，再通过权限管理模块为不同的平台用户角色配置不同的使用权限，使不同的用户角色具备平台对应的访问和业务操作功能。

（3）在线交流

为了使公众用户更了解平台基本业务操作流程，以及针对已注册用户的使用过程遇到问题，平台为运营管理单位用户提供了在线答疑反馈功能，以实现用户简单问题在线处理，提高平台的易用性，和用户满意度。

（4）信息发布

为了使平台内容更加丰富，平台各类用户之间更多的互动，实时了解新闻资讯，后台提供了信息发布功能，平台运营管理单位可发布文章并推送至前端，主要包含新闻、活动、政策等类别的文章。

（5）审核管理

后台管理的审核管理子模块可以使平台信息规范标准，杜绝虚假无用信息，有效保障平台信息的安全性。主要包含了注册审核、发布审核、时限审核、敏感词管理审核等。

当用户注册新账号时，需平台运营管理单位审核其注册信息的真实性、全面性，审核通过之后方能注册成功；企业发布上市路演活动，金融机构发布金融产品，企业发布融资需求，都需平台运营管理单位用户审核通过之后才能发布；

对于金融机构审核企业贷款资料、授信、放款的期限规则也需平台审核，致力于做到金融机构在合理的时间期限反馈企业贷款申请情况；另外平台拥有敏感词库导入和录入功能，可批量加入如政治敏感词库、网络敏感词库，坚决杜绝平台出现垃圾敏感词汇。

（6）积分规则管理

后台还提供了积分规则管理功能，可用于政府对企业评级提供决策参考，也可促进企业、机构更活跃规范使用平台。新账号注册、每天第一次登录、产品和需求发布被审核通过、企业和金融机构被正面评价等行为均可增加积分，同样，企业和金融机构负面评价、企业授信未通过则扣减积分。

通过以上五个子功能模块，可方便平台运营管理单位高效管理平台，使平台信息标准规范，实现用户合规化访问，维持安全平稳运营。

**7.移动端**

平台应用端不仅有PC端，而且还搭配了移动端功能，企业用户关注线上金融创新线上综合服务平台微信公众号，成功绑定PC端账号之后，便可用手机实时查看PC端信息，方便快捷。

企业用户可直接用手机查看金融产品信息详情，申请意向金融产品，还可直接发布融资需求，实时查询金融产品申请进度，对于关键进度情况，公众号还可自动提醒推送，使企业用户及时知晓，快速处理。

平台PC端搭配移动端，使用户可实时办理相应业务，方便快捷，带来更好的用户体验。

**（五）开发方案**

**1.开发技术**

（1）开发语言以及框架

后端：java + Spring Boot

前端：（javascript，html，css） + ReactJS

（2）开发技术的特点

后端：java作为现在最流行的语言之一，它具有活跃的社区、安全性高、

丰富的类库、还有丰富的框架、对高并发的处理优于其他很多语言。

Spring Boot：Spring Boot 的优点快速开发，特别适合构建微服务系统，另外平台将封装各种经常使用的套件，比如mybatis、hibernate、redis、mongodb等。

Spring Boot 特性：

①使用 Spring 项目引导页面可以在几秒构建一个项目；

②方便对外输出各种形式的服务，如 REST API、WebSocket、Web、Streaming、Tasks；

③非常简洁的安全策略集成；

④支持关系数据库和非关系数据库；

⑤支持运行期内嵌容器，如 Tomcat、Jetty；

⑥强大的开发包，支持热启动；

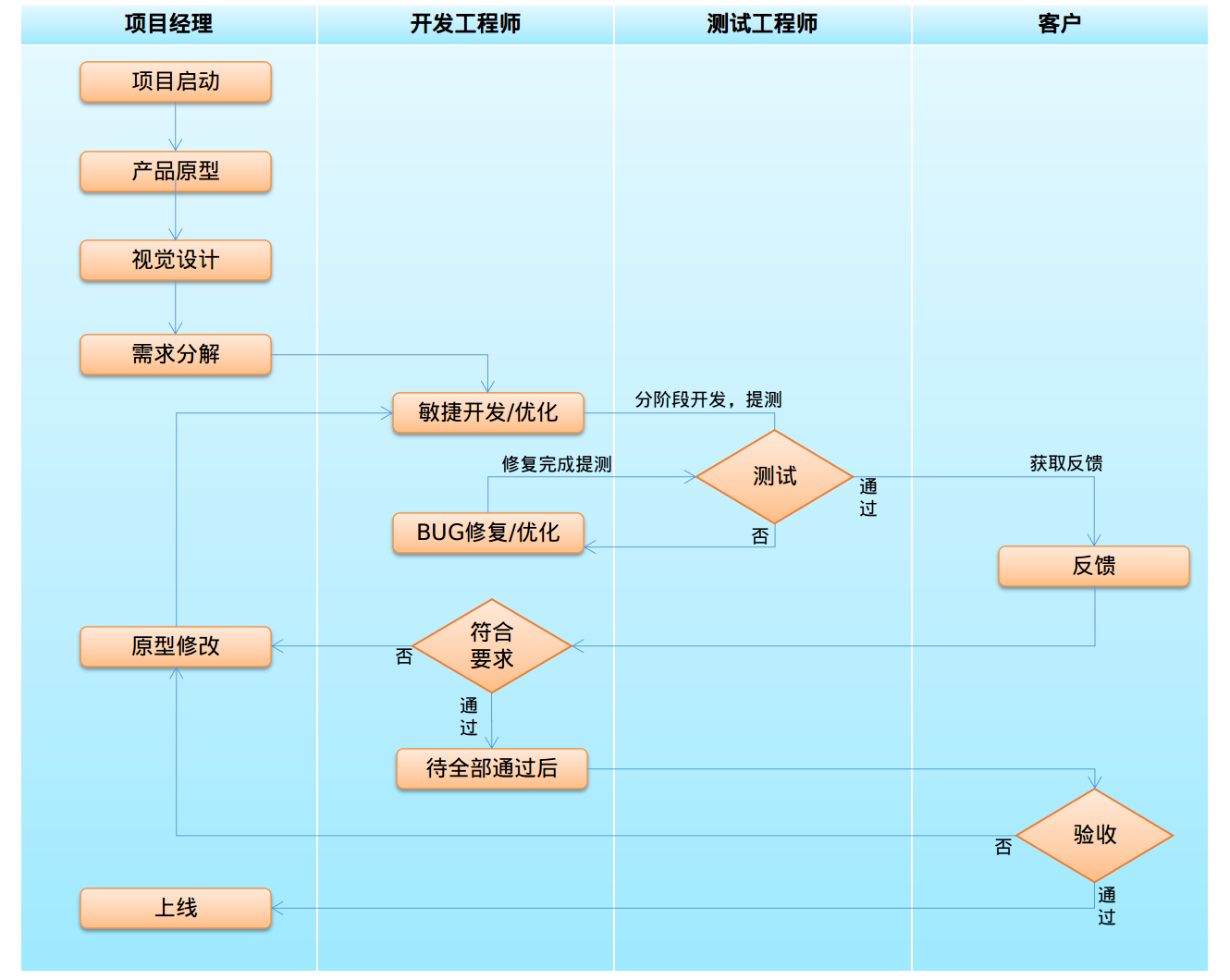
⑦自动管理依赖；

⑧自带应用监控；

⑨支持各种 IDE，如 IntelliJ IDEA 、NetBeans。

前端：前端流行语言js、html、css。

ReactJS：用于构建用户界面的JavaScript库。严格意义上来说，ReactJS更像一个工具，而不是框架。

**2.开发流程**

具体开发流程如下图6所示：

图6 开发流程图示

视觉设计：主要UI设计参与。

敏捷开发：项目初期会将系统分成各功能模块进行独立开发，并且这几个模块都具有可视化，可操作的特性，经过测试交给客户，等待客户的反馈。如果反馈良好，该模块进入可以交付。如果需要修改，再修改后进入反馈流程。

**3.质量管理**

质量管理主要分为功能质量和代码质量两个方面。

（1）功能质量

主要通过测试的手段保证功能的质量，包括以下几点：

单元测试：由开发人员自己完成，是一个自测的过程；

功能测试：功能测试检查实际的功能是否符合用户的需求。测试的大部分工作也是围绕软件的功能进行，设计软件的目的也就是满足客户对其功能的需求，该阶段主要由测试人员负责。

性能测试：根据项目的不同，提出不同性能指标。通过测试可以达到该性能指标就可以认定通过测试，也由测试人员负责。

（2）代码质量管理

设计和代码的检查准则：提供代码检查技术，自行检查，同时开发人员互相检查代码来发现bug和不正确的设计；

code review：管理者应该对代码质量负责；

开发完成后的代码质量管理：

依照标准化规范检测代码，提出修改意见；

提供接口测试用例，代码覆盖率、分支覆盖率、复杂度分析；

**（六）运行环境**

**1.WEB应用系统环境**

WEB应用系统环境主要是指：部署和运行金融创新线上综合服务平台web系统所需的硬件和软件，详细内容如表1所示：

表1：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 环境类型 | 形态 | 规格描述 | 数量 | 备注 |
| 1 | web服务器 | 硬件 | 1、8核CPU；  2、16G RDIMM DDR4 内存\*1；  3、300G 热插拔SAS硬盘(1万转) 2.5\*2；  4、主板集成千兆网卡\*2；  5、双口千兆网卡（RJ45接口）\*1；  6、双电源\*1；  7、标配导轨\*1； | 1 | 如果采用云主机（虚拟机）的环境，则需要满足：  CPU：8核；  内存：16G；  硬盘：300GB； |
| 2 | 操作系统OS | 软件 | Centos 7 | 1 |  |
| 3 | 中间件 | 软件 | Tomcat | 1 |  |

**2.存储系统环境**

存储系统环境主要是指，部署和运行存储系统所需的硬件和软件，详细如表2所示：

表2：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 环境类型 | 形态 | 规格描述 | 数量 | 备注 |
| 1 | 服务器 | 硬件 | 1、16核CPU；  2、32G RDIMM DDR4 内存\*1；  3、600G 热插拔SAS硬盘(1万转) 2.5\*3  4、主板集成千兆网卡\*2；  5、双口千兆网卡（RJ45接口）\*1；  6、双电源\*1；  7、标配导轨\*1； | 2 | 如果采用云主机（虚拟机）的环境，则需要满足：  CPU：16核；  内存：32G；  硬盘：1TB； |
| 2 | 操作系统OS | 软件 | Centos 7 | 2 |  |

**3.安全环境**

安全环境主要是指金融创新线上综合服务平台日常运行的过程中，需要提供的安全保障，详细如表3所示：

表3：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 环境类型 | 形态 | 规格描述 | 数量 | 备注 |
| 1 | 机房安全 | 硬件 | 根据IDC机房的硬件安全设计要求进行建设。 | N/A |  |
| 2 | 网络安全 | 硬件 | 提供防火墙、IPS、IDS、WAF防护。 | N/A |  |
| 3 | 数据安全 | 软硬件 | 提供数据存储安全，数据备份保障。 | N/A |  |
| 4 | 应用安全 | 软硬件 | 提供web防篡改、防攻击防护。 | N/A |  |
| 5 | 安全管理 | N/A | 具备完善的机房安全管理办法、规章制度、人员体制。 | N/A |  |

**4.机房环境**

机房环境主要是指用于部署软硬件的机房，以及web应用对外提供服务所需要网络带宽，详细如表:4所示：

表4:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 环境类型 | 形态 | 规格描述 | 数量 | 备注 |
| 1 | 机柜 | 硬件 | 预留10U空间 | 1 |  |
| 2 | 网络交换机 | 硬件 | 至少支持24个千兆以太网口 | 1 |  |
| 2 | 网络带宽 | N/A | 带宽≥30MB； | 1 | 后期根据企业注册数的增加进行相应的调整。 |

**（七）保密方案**

**1.协议约束**

平台运营管理单位、政府平台运营负责人、区内已注册和经认证的银行机构、平台已进驻的企业用户，都须签订用户保密协议或平台免责协议，以保证企业和银行数据的保密义务得到充分的履行，并受到法律法规的保护。

**2.用户隔离**

本平台设计遵循不同角色用户个人中心隔离原则，意味着公众用户、企业用户、银行（或者其他金融机构）用户都各自在登录后只能查看其对应角色下的个人中心页面，再进行平台允许的后续业务操作，这样既避免了用户的误操作，也保证了不同角色用户之间数据的独立性和保密性。

**3.后台配置**

金融创新线上综合服务平台除了设立各不同用户角色相互独立的个人中心和业务使用规范外，考虑到平台在运营期间的业务范围和流程变动，会导致功能权限和数据流转的对应调整，因此，平台设立了针对各不同用户角色可视化的权限调整功能，运用便捷的操作方式，使得平台运营管理单位相关负责人员能快速的启用、编辑、删减特定角色的前端展示功能内容，保证了平台的可靠性，以应对今后很长一段时间对平台保密性的扩展需求。

**（八）安全方案**

**1.整体架构**

重庆高新区金融创新线上综合服务平台是一个连接企业、金融机构（银行）、第三方服务机构，以及政府管理部门的综合性服务平台。不仅承载多种敏感的企业信息、金融信息，同时，还是政府部门的信息门户。因此，必须充分考虑平台的安全性，确保平台信息存储安全、访问安全、使用安全，维护政府形象。

本方案将根据GB/T25070-2010 信息系统等级保护安全设计技术的要求，从安全计算环境、安全区域边界、安全通信网络、应用安全、主机安全、安全管理等方面进行技术方面的设计。安全整体架构。

重庆高新区金融创新线上综合服务平台整体部署架构设计，如图7所示：

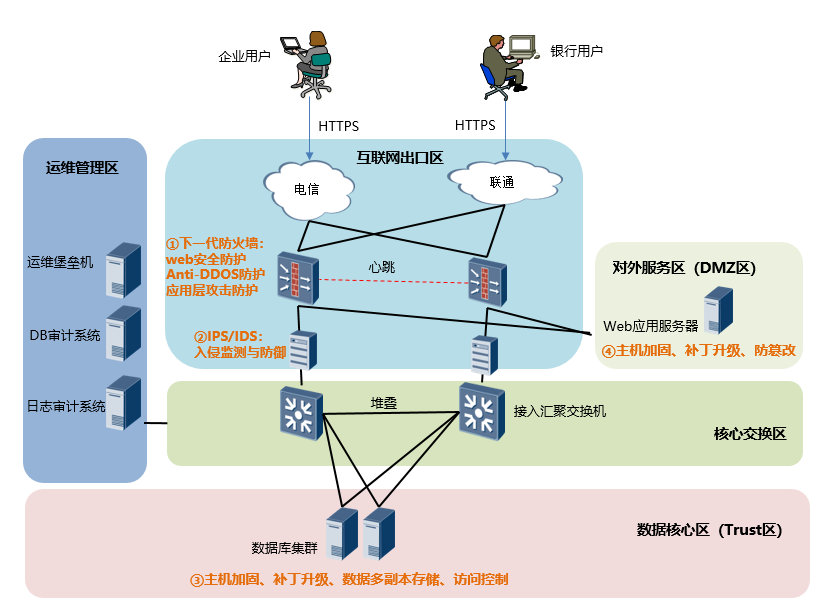


图7 整体部署架构

重庆高新区金融创新线上综合服务平台网络架构整体设计采用根据业务形态，以及信息安全等级保护的要求，将网络划分成不同安全等级的安全域。

安全域的划分是网络防护的基础，事实上每一个安全边界所包含的区域都形成了一个安全域。这些区域具有不同的使命，具有不同的功能，分域保护的框架为明确各个域的安全等级奠定了基础，保证了信息流在交换过程中的安全性。

在本项目中，将严格按照信息系统的重要性和网络使用的逻辑特性划分安全域，将划分如下确定的安全域：

互联网出口区域。在网络出口需提供多链路负载并自动匹配最优线路，保障网络可用性的同时实现快速接入；需在互联网出口边界进行隔离和访问控制，保护内部网络，从2-7层对攻击进行防护，实现对入侵事件的监控、阻断，保护整体网络各个安全域免受外网常见恶意攻击；利用网络防病毒，主动扫描web流量、阻止恶意软件到达并感染网络上主机等防护功能。

对外服务区域，该安全域内主要承载对外提供服务的计算能力，包括门户网站前端服务器、Web业务服务器、APP业务服务器等。同时，为保障区域的安全性，需对业务信息系统提供2-7层安全威胁识别及阻断攻击行为的能力，如SQL注入、XSS（跨站脚本攻击）、CSRF（跨站请求伪造攻击）、cookie篡改等，通过在对外服务区域边界设置合理的访问控制策略，提供针对应用层攻击检测与防护能力。

内网数据中心区域，该安全域内主要承载内网核心业务信息系统及核心系统数据库。同时，需对存储系统产生的数据访问权限进行划分，并对数据的相关操作进行审计；需对敏感或重要数据进行备份。

运维管理区域，该运维管理区域对业务环境下的网络操作行为进行集中管理与细粒度审计；需满足对运维操作提供最小权限控制以及安全接入需求。

**2.硬件方案**

（1）硬件购买

①硬件购买方案（等保三标准）如下表5所示：

表5：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品类型 | | 规格描述 | 数量 |
| 1 | WEB服务器 | | 1、8核CPU | 1 |
| 2、16G RDIMM DDR4 内存\*1 |
| 3、300G 热插拔SAS硬盘(1万转) 2.5\*2 |
| 4、主板集成千兆网卡\*2 |
| 5、双口千兆网卡（RJ45接口）\*1 |
| 6、双电源\*1 |
| 7、标配导轨\*1 |
| 2 | DB服务器 | | 1、16核CPU | 2 |
| 2、32G RDIMM DDR4 内存\*1 |
| 3、600G 热插拔SAS硬盘(1万转) 2.5\*3 |
| 4、主板集成千兆网卡\*2 |
| 5、双口千兆网卡（RJ45接口）\*1 |
| 6、双电源\*1 |
| 7、标配导轨\*1 |
| 3 |  | 下一代防火墙 | 1、吞吐量≥500M | 2 |
| 安全软硬件 | 2、支持透明、旁路牵引、反向代理部署等 |
|  | 3、提供防病毒功能 |
|  | 4、支持包括NAT、ACL等在内的防火墙功能 |
|  | 5、支持堆叠 |
|  | IPS | 1、吞吐量≥500M | 2 |
|  | 2、2U，含交流冗余电源模块，2\*USB接口，1\*RJ45串口，1\*RJ45管理口，6\*GE（Bypass）接口，1个接口扩展槽位。系统吞吐不少于4Gbps，最大并发不少于150万，每秒新建不少于4万 |
|  | 3、支持覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为7600种以上 |
|  | 4、能够有效抵御SQL注入等多种常见的应用层安全威胁 |
|  | 堡垒机 | 1U，含单交流电源，2\*USB接口，1\*RJ45串口，1\*GE管理口，4\*GE电口，2T SATA硬盘。授权管理50台设备 | 1 |
|  | 防篡改系统 | 产品支持Windows、Linux 、HP-Unix、IBM AIX等，支持IIS 、Weblogic、Websphere 、Apache 、Tomcat等中间件 | 1 |
|  | 支持根据操作类型进行文件防护，文件防护规则支持顺序匹配 |
|  | 告警类型包括：试图进行网页篡改的各种攻击行为；对可视内容的非法增加、删除、修改的行为 |
|  | 日志审计系统 | 1U，含交流冗余电源模块，2\*USB接口，1\*RJ45串口，2\*GE管理口，4个10/100/1000M电口，1个接口扩展槽位，4TB SATA硬盘，缺省授权接入40个日志源 | 1 |
|  | DB库审计系统 | 1U，含单交流电源，2\*USB接口，1\*RJ45串口，1\*GE管理口，6\*GE电口，1个接口扩展槽位，2T SATA硬盘 | 1 |
|  | 等保测评 | 等级保护测评，邀请具有测评资质的公司完成等保测评工作 | 1 |
| 4 | 网络设备 | | 1、至少支持48口千兆以太网卡 | 2 |
| 2、支持堆叠 |
| 5 | Internet线路 | | 带宽≥30MB | 租用 |
| 6 | 机柜租赁 | | IDC机房机柜：预留10U空间 | 租用 |

②硬件购买方案（一般标准）如下表6所示：

表6：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品类型 | | 规格描述 | 数量 |
| 1 | WEB服务器 | | 1、8核CPU | 1 |
| 2、16G RDIMM DDR4 内存\*1 |
| 3、300G 热插拔SAS硬盘(1万转) 2.5\*2 |
| 4、主板集成千兆网卡\*2 |
| 5、双口千兆网卡（RJ45接口）\*1 |
| 6、双电源\*1 |
| 7、标配导轨\*1 |
| 2 | DB服务器 | | 1、16核CPU | 2 |
| 2、32G RDIMM DDR4 内存\*1 |
| 3、600G 热插拔SAS硬盘(1万转) 2.5\*3 |
| 4、主板集成千兆网卡\*2 |
| 5、双口千兆网卡（RJ45接口）\*1 |
| 6、双电源\*1 |
| 7、标配导轨\*1 |
| 3 |  | 防火墙 | 1、吞吐量≥500M | 2 |
| 安全软硬件 | 2、支持透明、旁路牵引、反向代理部署等 |
|  | 3、提供防病毒功能 |
|  | 4、支持包括NAT、ACL等在内的防火墙功能 |
|  | 5、支持堆叠 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | IPS | 1、2U，含交流冗余电源模块，2\*USB接口，1\*RJ45串口，1\*RJ45管理口，6\*GE（Bypass）接口，1个接口扩展槽位。系统吞吐不少于4Gbps，最大并发不少于150万，每秒新建不少于4万 | 2 |
|  | 2、支持覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为7600种以上 |
|  | 3、能够有效抵御SQL注入等多种常见的应用层安全威胁 |
|  | 防篡改系统 | 产品支持Windows、Linux 、HP-Unix、IBM AIX等，支持IIS 、Weblogic、Websphere 、Apache 、Tomcat等中间件 | 1 |
|  | 支持根据操作类型进行文件防护，文件防护规则支持顺序匹配 |
|  | 告警类型包括：试图进行网页篡改的各种攻击行为；对可视内容的非法增加、删除、修改的行为 |
| 4 | 网络设备 | | 1、至少支持24口千兆以太网卡 | 2 |
| 2、支持堆叠 |
| 5 | Internet线路 | | 带宽≥30MB | 租用 |
| 6 | 机柜租赁 | | IDC机房机柜：预留10U空间 | 租用 |

（2）硬件租赁

①硬件租赁方案（等保三标准）如下表7所示：

表7：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品类型 | | 规格描述 | 数量 |
| 1 | DB云服务器 | | 1、16核CPU\*1； 2、32G RDIMM DDR4 内存\*1 3、600G 热插拔SAS硬盘(1万转) 2.5\*2 | 1 |
| 2 | 云Web服务器 | | 1、8核CPU\*1 2、32G RDIMM DDR4 内存\*1 3、300G 热插拔SAS硬盘(1万转) 2.5\*2 | 1 |
|
|
|
|
|
|
| 3 | 安全服务 | 防火墙服务 | 1、支持透明、旁路牵引、反向代理部署等 | N/A |
| 2、提供防病毒功能 |
| 3、支持包括NAT、ACL等在内的防火墙功能 |
| IPS服务 | 1、支持覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为7600种以上 | N/A |
| 2、能够有效抵御SQL注入等多种常见的应用层安全威胁 |
| 堡垒机服务 | 保障网络和数据不受来自外部和内部用户的入侵和破坏 | N/A |
| 防篡改服务 | 支持根据操作类型进行文件防护，文件防护规则支持顺序匹配 | N/A |
| 告警类型包括：试图进行网页篡改的各种攻击行为；对可视内容的非法增加、删除、修改的行为 |
| 日志审计服务 | 监控整个IT系统的运行情况，及时发现系统异常事件；通过事后分析和丰富的报表系统，高效地对信息系统进行有针对性的安全审计 | N/A |
| DB库审计服务 | 对数据库遭受到的风险行为进行告警，对攻击行为进行阻断 | N/A |
| 等保测评服务 | 等级保护测评，邀请具有测评资质的公司完成等保测评工作 | N/A |
| 4 | Internet线路 | | 带宽≥30MB | 1 |
|
|

②硬件租赁方案（一般标准）如下表8所示：

表8：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品类型 | | 规格描述 | 数量 |
| 1 | 租用DB云服务器 | | 1、16核CPU\*1； 2、32G RDIMM DDR4 内存\*1 3、600G 热插拔SAS硬盘(1万转) 2.5\*2 | 1 |
| 2 | 租用云服务器 | | 1、8核CPU\*1 2、32G RDIMM DDR4 内存\*1 3、300G 热插拔SAS硬盘(1万转) 2.5\*2 | 1 |
|
|
|
|
|
|
| 3 | 安全服务 | 防火墙服务 | 1、支持透明、旁路牵引、反向代理部署等； | N/A |
| 2、提供防病毒功能； |
| 3、支持包括NAT、ACL等在内的防火墙功能； |
| IPS服务 | 1、支持覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为7600种以上 | N/A |
| 2、能够有效抵御SQL注入等多种常见的应用层安全威胁 |
| APT检测防护服务 | 针对明确目标的持续的、复杂的网络攻击提供防护服务 | N/A |
| 网关杀毒服务 | 病毒杀除、关键字过滤、垃圾邮件阻止等服务 | N/A |
| WAF服务 | 执行一系列针对HTTP/HTTPS的安全策略来专门为Web应用提供保护 | N/A |
| 流量清洗服务 | 针对对其发起的DOS/DDOS攻击的监控、告警和防护 | N/A |
| 4 | Internet线路 | | 带宽≥30MB。 | 1 |
|
|

（3）物理安全

这里的物理安全主要是指承载金融创新线上综合服务平台软硬件设施的IDC机房的安全，IDC机房应具备高安全建设水准，包括：具备完善的消防系统、温度控制系统、门禁和监控系统、可靠的电力供应系统、标准机柜、安全管理制度，以及抗地震能力等。本方案建议采用水土IDC机房或者平台运营管理单位的IDC机房作为平台的运行环境。

（4）边界安全

通过在网络边界部署下一代防火墙，实现对于网络边界的统一访问控制、流量攻击、病毒攻击、XSS攻击、SQL注入攻击防范等。

（5）主机安全

①病毒防护

本方案的Web服务器主机、数据库主机均采用基于开源的Linux系统。Linux系统具备良好的“病毒免疫”和“漏掉免疫”特性可以很好实现病毒防护。

②主机加固

通过对服务器的OS（Linux系统）进行安全加固，例如：裁剪多余的服务、禁止不用的端口、强化密码策略等。同时，启用服务器操作系统本身的审计功能，实现对于主机层面的安全审计要求。

③接口管控

通过对包括WEB服务和DB服务在内的物理服务器的外设接口，包括：USB、VGA、串口等进行打封条，严厉禁止使用，避免不法人员通过外部操作对系统和数据进行任何拷贝，确保平台安全。

（6）数据安全

①数据传输安全

本系统将采用HTTPS的方式进行数据加密传输，HTTPS（全称：Hyper Text Transfer Protocol over Secure Socket Layer），是以安全为目标的HTTP通道，简单讲是HTTP的安全版。即HTTP下加入SSL层，HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL。 它是一个URI scheme（抽象标识符体系），句法类同http:体系。用于安全的HTTP数据传输。现在它被广泛用于万维网上安全敏感的通讯。

②数据操作安全

通过部署数据库审计系统，实现对用户行为、用户事件及系统状态加以审计，即可通过定期对数据库的操作进行日志审计，评估操作的规范性，实现对用户行为、用户事件及系统状态加以审计，范围覆盖到每个用户，从而把握数据库系统的整体安全。

③数据容灾

数据容灾主要是指当数据发生安全威胁时，比如：宕机、系统故障等，可以通过相应的容灾机制实现数据的快速恢复，并确保应用系统可以正常的使用。本方案从软件和硬件两方面进行数据保护。

存储数据的数据库服务器通过采用raid技术，对硬盘的数据进行保护。当发生某一硬盘故障时，raid技术确保了数据的可用，因为，数据除了在已经损坏的硬盘上存储，同时，还在其他的硬盘上进行有效的备份，即便是不更换坏硬盘的情况下，数据也不会丢失，系统也可以正常使用。通过更换坏的硬盘，raid技术可以实现数据有效恢复至新硬盘中，从而恢复服务器的数据安全保障等级。

更重要的是，数据库存储系统采用master-slave架构，实现业务数据的热备份。当发生DB服务器宕机、存储系统异常时，可以实现秒级切换，确保业务的正常运作。

（7）应用安全

通过在网络边界部署下一代防火墙，可以有效地防护针对web系统七层攻击，例如：黑客攻击、流量攻击、跨站点攻击、病毒攻击等。同时，在web服务器上部署防篡改系统，可以进一步确保web系统平台不可能被篡改，进一步保障平台数据的真实、完整、可信。

（8）运维安全

通过部署运维堡垒主机，实现对于运维人员管理服务器、网络设备、安全设备、DB维护等运维操作的审计。同时，通过建立科学的运维管理流程，根据不同的运维人员的等级和工作职能在平台系统中设置不同的维护权限，例如：普通运维人员职能DB进行查看操作，技术负责人可以对DB进行读写操作等，结合日志审计机制，可以有效地规避针对系统的运维风险。

（9）统一日志平台

通过部署日志审计系统，实现对于全网日志的收集和统一分析，通过事件关联分析，预警分析，可以及时发现和定位网络中发现的安全风险，并采取相应的安全措施。

六、运营运维

**（一）运营方案**

重庆高新区金融创新线上综合服务平台的主要运营工作，包括：新闻运营、政策运营、用户管理、平台数据运营、以及平台工作报告。

**1.新闻运营**

通过转载和原创两种方式完成新闻运营工作，转载新闻的来源包括人民网等国内网站以及从重庆高新区官方网站获取（每周至少2篇默认新闻）。原创新闻由平台运营管理单位和高新区管委会合作选题，写稿完成新闻发布（每月1篇），发布在金融创新线上综合服务平台官网首页。

**2.政策运营**

政策运营主要是发布高新区政府机构出台的相关政策，高新区财政局运营方对接人向平台运营管理人员实时反馈最新的政策兑现信息和调整动向，便于运营人员及时在平台中完成更新。

**3.用户管理**

在金融创新线上综合服务平台正式运营阶段，平台运营管理单位须组织运营人员与区内各认证银行（或者其他金融机构）讨论每月就金融产品发布和成交情况进行讨论，并与平台已注册企业进行沟通，收集企业用户对平台产品和运营的意见。

将上述两类用户反馈情况进行汇总，并通过电子邮件的方式告知平台运营管理工作人员和高新区政府部门对接人。

另外需要对平台进行日常信息维护，包括银行（或者其他金融机构）的注册及发布信息审核，权限分配等相关工作，还须处理公众用户咨询、注册企业用户和机构用户投诉、反馈等。

**4.数据运营**

通过每周对平台前端用户行为分析，平台数据挖掘，进而优化平台主要业务流程，例如：对用户量、交易量、交易额、对接成功率等数据维度进行统计分析，并将分析结果呈报高新区政府部门。

**5.运营月报**

每月的第一个工作周，平台运营管理单位负责人应出具平台在上一个月的运营月报。

为完成该月报的制作工作，平台运营管理单位负责人应登录用户管理后台核查各项指数信息，将其填入表格的相应位置中。

月报制作完成后，以电子邮件的方式发送给平台的相关运营人员。

**6.人员体制**

发布与审核人员1-2名，主要工作为：

平台的新闻、政策、公告发布；

账号注册审核，银行（其他金融机构）认证；

企业发布的融资需求内容、银行（其他金融机构）发布的债权和股权金融产品，第三方机构发布的金融活动和上市辅助信息审核。

开发方对接人员1-2名，主要工作为：

负责与平台开发商项目经理对接，处理平台在开发过程中的各类问题；

收集平台测试版的相关问题，反馈给平台开发商项目经理；

平台运营维护阶段，与平台开发商对接，反馈需要处理的问题给平台开发商运维工程师。

平台日常管理人员2-4名，主要工作为：

负责与公众用户和已注册用户在线交流，对平台操作不熟悉或需要业务咨询的用户进行答疑；

与已认证的银行（其他金融机构）对接，商讨并处理资金供给方反馈的各类问题，例如：银行进度反馈时限修订，积分规则的修改等；

收集需要反馈给高新区政府部门的平台数据，积分规则管理，用户角色对应的权限管理，银行（其他金融机构）和企业的子账号个数设置等。

平台管理监督人员1-2名，由高新区政府部门指定，主要工作为：

负责监督平台运营管理人员在日常管理过程中进行的数据导出和使用；

负责监督平台权限设置合理性和合规性，例如检查银行（其他金融机构）用户是否只被赋予了应有的权限，没有超出核定的范围等；

平台运营异常情况上报。

**（二）运维方案**

**1.免费质保期内服务承诺**

平台开发商承诺在质保期内为用户提供多种售后服务：

专人负责：平台开发商承诺为本项目指定专门联络人和负责人，在质量保证期内定向为本项目进行跟踪服务，包括跟踪对用户提供问题的解决情况以及后续应用情况，专门的负责人需由符合技术要求及资质的人员组成，其技能水平能够覆盖本次项目建设所涉内容。

现场响应：用户遇到使用及技术问题，电话咨询不能解决的，平台开发商承诺：8小时内提供上门服务，确保系统正常工作；无法在8小时内解决的，提供后备解决方案，包括进行数据恢复、系统重装等操作，使用户业务能继续开展。

技术服务：平台开发商承诺定期对全系统的运行情况进行检查与评估，包括系统运行环境、系统状态、数据存储情况、安全运行情况、异常操作等进行记录、汇总与报告，并协助用户对系统进行维护，包括数据备份、数据清理、设备清障、运行调优、数据初始化等。

培训服务：平台开发商承诺对用户方操作人员提供正式的培训服务，包括集中培训、分层次培训，并在服务期内，对用户方因机构人员调整所需要的零星培训提供及时支持。

技术升级：在质保期内，如果平台开发商的产品技术升级，平台开发商承诺及时通知用户方，如用户方有相应要求，将对采购人进行升级服务。

远程在线诊断和故障排除：对于电话咨询无法解决的问题，工程师经用户方授权通过远程登录到用户方网络系统进行免费的故障诊断和故障排除；

故障协排：对于系统运行之外的原因而产生的故障（如通讯链路中断、火灾、自然灾害、人为破坏等），平台开发商承诺协助用户方共同完成故障的清除或危害情况的限制，平台开发商承诺按用户方的要求投入专业人员、提供专业服务进行故障排除。

**2.免费质保期后服务承诺**

免费质量保证期过后，平台开发商承诺同样提供免费电话咨询服务，并提供产品上门维护服务，指定具备相应技术能力的专人负责联络。

免费质量保证期过后，如果用户方需要继续由平台开发商提供售后服务的，平台开发商承诺以优惠价格提供售后服务。

**3.服务范围**

质保免费期的免费范围：实施、培训、维护、集成、升级、需求范围内的客户化开发。

在质保期内，如有质量问题或质量缺陷，我公司会免费予以更换或修复，以保证使用人正常运行。

免费保修期内产品质量经权威机构鉴定不符合质量要求的，或者不符合投标条款的，按合同约定承担违约责任。