

文章编号: 1005-8451 (2018) 05-0023-05

# 集团型铁路企业移动智能融合平台及其应用

牛志亢

(华电集团北京燃料物流有限公司, 北京 100035)

**摘要:** 针对集团型铁路企业移动化、智能化、服务化管理需求, 研究并设计集团型铁路企业移动智能融合平台, 提出包括总体架构、网络架构和安全策略的平台总体设计方案, 详细阐述平台的服务端和移动端功能, 给出平台在铁路人力资源领域的应用场景与实现, 包括移动事务协同、移动投票、移动职工健康档案、移动继续教育培训等。目前, 该平台已经得到应用, 其中的关键技术得到了验证。

**关键词:** 移动; 智能融合平台; 集团型铁路企业; 人力资源

**中图分类号:** U29 : TP39 **文献标识码:** A

## Mobile intelligent integration platform for railway enterprise group

NIU Zhikang

(Huadian Beijing Fuel and Logistics Co. Ltd., Beijing 100035, China)

**Abstract:** Aiming at the management demand of mobile, intelligent and service, this article researched and designed the mobile intelligent integration platform for railway enterprise group, proposed the overall design scheme of the platform including overall framework, network architecture and security strategy, described the functions of server terminal and mobile terminal of the platform in detail, introduced the application scene and implementation of this platform in the field of railway human resources including mobile collaboration, mobile voting, mobile staff health management, and mobile continuing education training, etc. The platform is applied successfully and the main algorithms are validated.

**Keywords:** mobile; intelligent integration platform; railway enterprise group; human resources

集团型铁路企业存在多层级、分布广、业务与管理模式多样化的特点, 云计算、物联网、移动互联网等新一代信息技术已经渗透到企业的内部环境中, 为铁路企业转型升级提供强大的技术驱动力, 对集团型铁路企业的业务和协同、程序和制度、角色和责任、以及技术等各方面产生了重要影响。

在移动互联的驱动下, 打破传统的 PC 办公模式, 企业级移动应用被运用到行业内各业务领域, 将线性协作变成点状聚合, 在给企业用户带来便利、极致用户体验、业务创新加快的同时, 各铁路企业自行组织、分散建设的移动应用缺乏统一规划、统一标准、统一开发及统一管理, 产生使用上的差异以及维护上的困难, 并对网络信息安全方面带来了隐患。

搭建私有、自主、安全可控的移动应用架构及移动运用平台, 实现多业务系统移动化、智能化、服务化, 满足员工高效、个性化需求, 提升铁路企业横

向和纵向的沟通处理能力, 有力支撑企业业务管理创新改进和运营管控, 实现体系架构和服务模式的创新、可持续发展, 就显得尤为重要。

## 1 平台架构

集团型铁路企业移动融合平台架构主要由移动终端层、隔离区 (DMZ) 前置层、适配器层和企业业务层组成, 移动端通过 http 协议访问部署在 DMZ 区的服务接口, DMZ 区的服务通过端口映射的方式访问网闸内部的适配器层, 适配器层在对接业务层的各个系统。平台总体架构如图 1 所示。

### 1.1 移动终端层

提供已封装好的移动通讯录、移动企信、企业应用商店等移动融合平台的基础组件, 以及同事圈等可选组件, 组件之间调用采用 RESTful API 方式包含一系列的数据处理封装, 扩展界面组件以及网络通信组件, 可以使移动应用的开发人员尽可能规避底层相对复杂的开发。支持应用原生开发 (Native

收稿日期: 2017-12-24

基金项目: 中国铁路总公司科技研究开发计划重点课题 (2016X004-1)。

作者简介: 牛志亢, 助理工程师。

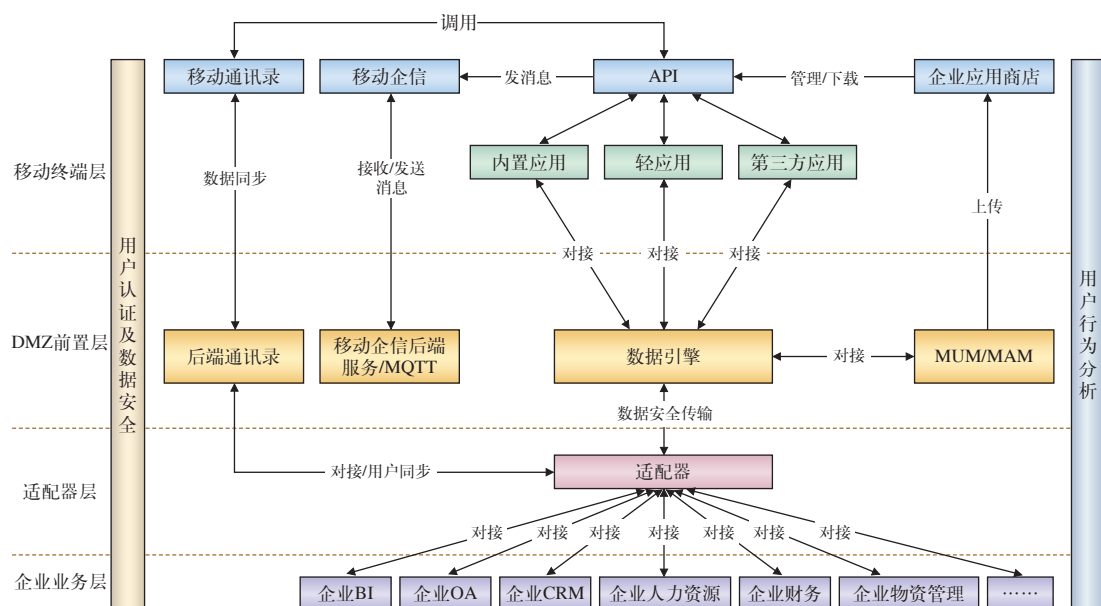


图1 铁路企业移动融合平台总体架构

APP)、HTML5 开发 (Web APP)、混合开发 (Hybrid APP) 的开发模式下, 内置应用、轻应用和第三方应用等多种应用类型, 结合铁路企业实际管理需要, 采用其中一种或多种应用组合<sup>[1-2]</sup>。

## 1.2 DMZ前置层

搭建和部署移动应用系统所需的前置访问服务器, 仅为链接点, 不在该层部署数据库和移动应用服务, 主要实现对移动终端层的数据传输、数据处理、加解密等功能, 并与部署在企业业务层的移动应用进行数据交互。

## 1.3 适配器层

整合铁路企业内部业务系统, 统一延伸原有 Web 应用系统, 并进行统一适配接入, 协助业务系统发布远程服务, 供移动终端进行调用。

## 1.4 企业业务层

在铁路企业内网服务区, 部署各业务系统数据库服务器和应用服务器, 移动应用与 Web 应用使用相同的数据库, 单独部署移动应用的核心逻辑。

## 2 网络架构

铁路企业网络分为内外两张物理隔离的网络, 网络结构如图 2 所示。其中, 外网通过防火墙、入侵防御、流量控制、链路均衡器等设备连接互联网, 内网通过专线连接其他铁路企业, 内外网间的信息交换由安全平台完成。内外网核心层主要由核心交换

机与核心防火墙组成, 负责各网络区域间的数据转发与访问控制。内外网办公终端区主要由楼层接入交换机与楼宇汇聚交换机组成, 各楼宇中的办公终端根据办公需求的不同接入外网办公终端区或内网办公终端区。内部服务网与安

全生产网分别部署有为铁路内部提供一般性服务的信息系统和直接关系铁路运输生产的信息系统, 移动接入部署于外部服务网。

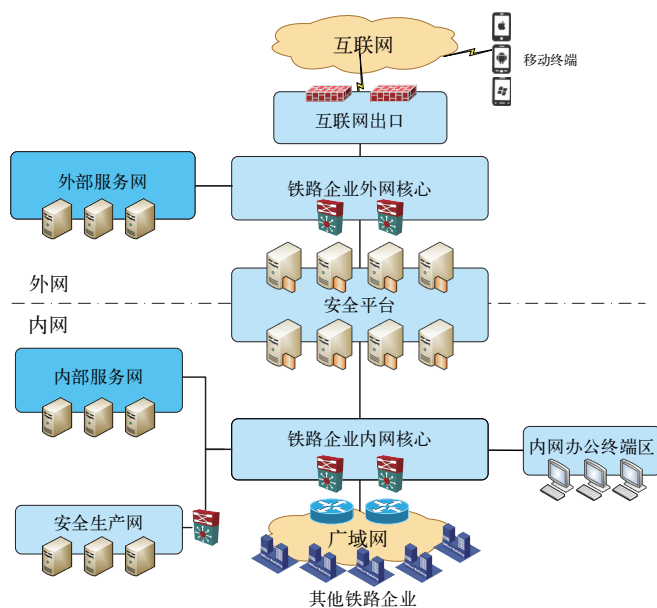


图2 网络架构图

## 3 安全策略

安全策略如图 3 所示。

### 3.1 系统安全防护

(1) 利用网闸的数据摆渡技术和防火墙的数据检测技术实现外部服务网、内部服务网安全隔离条件下的互联互通;

(2) 利用虚拟专用网 (VPN) 隧道技术, 实现

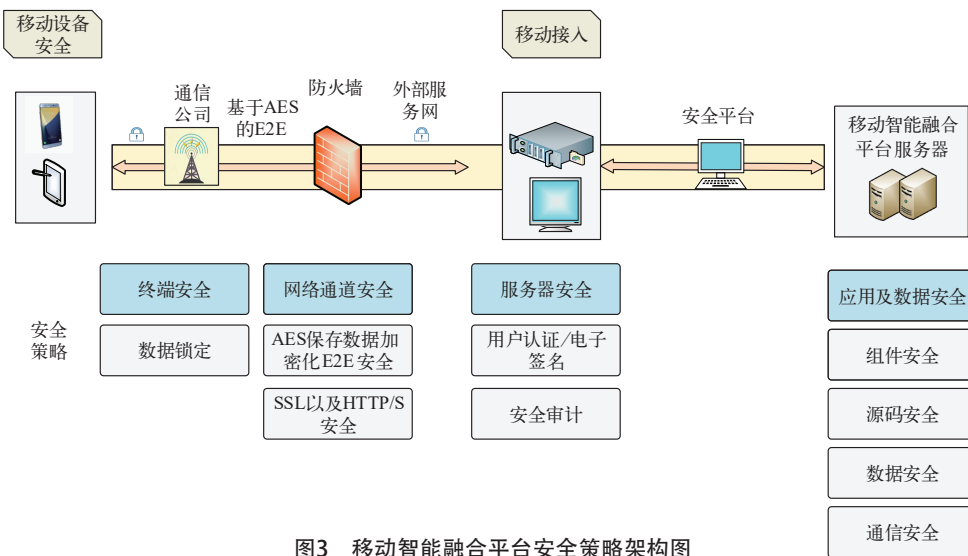


图3 移动智能融合平台安全策略架构图

的早期树立移动应用的安全保障。从以下几个方面进行规范：

（1）在组件安全（Activity、Broadcast Receive、Content Provider、Intent 等）、Webview 安全（禁止明文存储等）、访问控制（权限最小化保护等）、摆渡安全（第三方移动应用入口安全鉴别和校验等）、应用发布安全（上线、下载、升级安全测试与检测机制）等方面进行

数据从访问终端到服务器的全路径加密；

（3）利用 VPN 的身份鉴别机制和 PKI/CA 的证书认证技术，实现用户身份的双因子认证（CA 认证 + 用户名 / 强密码口令认证），保证数据访问源的可鉴别性。

3.2 内容安全防护

- （1）建立从终端、应用、传输到服务的全链条端到端安全防护措施；
- （2）应用水印、在线文档解析与加密、移动终端缓存清除等技术，有效控制移动端数据的使用、存储、传递、销毁的过程，防止移动端信息泄漏；
- （3）为避免在移动终端留存任何和用户安全相关的信息，阅读后自动回收销毁，在移动终端没有任何信息留存；
- （4）服务端可以配置信息备份的策略，定时对服务器上的信息做备份；
- （5）严格用户统一身份认证与管理，分类终端安全接入方式，严格限制非授权终端的非法接入，自动对移动终端进行监控和安全管理。

同时，平台对用户的操作进行严格的审计和报警，保证管理员和用户可以查看以往的系统和操作日志，可以对集中日志进行分析，查看系统是否曾遭到攻击。

3.3 安全编码

为提供移动应用客户端和服务端的整体安全能力水平，必须进行安全编码，从安全开发生命周期

- 应用安全规范；
- （2）在程序保护（加固保护、反盗版 / 二次打包能力等）、代码安全（安全编码、避免漏洞等）等方面进行源码安全规范；
- （3）在数据录入、访问、存储、传输、输出等方面满足数据完整性和保密性的数据安全需要；
- （4）在网络通信协议、会话安全、认证安全、抗抵赖等方面保证移动端与服务器端安全通信<sup>[3]</sup>。

4 平台功能

4.1 服务端功能

平台服务端采用面向服务的集中式控制和协调架构，将计算和数据处理在服务端执行，智能手机等移动终端通过应用接口或 Web 浏览器方式访问服务端，为移动端提供基础、管理、运营统计、应用商店、文档转换、消息推送等一系列管理和数据处理服务。帮助集团型铁路企业高效低成本地完成移动应用的开发、测试、发布、部署、运维和管理工作，并提供完整的信息安全体系。

4.1.1 基础核心服务

服务端的核心服务组件，负责移动端对接、应用执行、对接业务系统，数据集成等工作，同时，负责根据具体请求调用其他子服务。

4.1.2 企业管理门户

支持应用插件管理、应用管理、设备鉴权、系统配置等功能。

### 4.1.3 移动企信

搭建集团型企业内部跨组织、跨业务的沟通、协同、社交化平台,实现员工间即时通信,包括:即时消息、音视频通话、群组聊天、多媒体会议等,建立各部门服务号,通过同事圈,员工可以发表自己的动态,并可进行点赞和评论。使移动智能融合平台从简单的协同工作应用转化为拥有社交元素的综合应用,有效增强用户粘性<sup>[4-5]</sup>。

### 4.1.4 应用商店

通过应用商店方式进行集中管控和运营服务多个移动应用,提供版本、发布、升级、下载等功能,通过角色权限设置,可对每个移动应用进行权限控制。

### 4.1.5 运营统计分析服务

(1) 建立运营数据指标体系,进行用户分析,包括:新增用户、活跃用户、用户构成、启动次数、版本分布等。

(2) 留存分析,包括:留存用户统计、用户新鲜度统计、用户活跃度统计等。

(3) 渠道、终端、功能使用及错误统计分析,包括上线崩溃分析、应用程序无响应(ANR)分析、错误分析等运营数据统计与综合分析,分析结果既提供给移动应用开发者快速发现并解决异常,又提供给铁路企业管理者及时掌握移动应用运营动态,帮助铁路企业实现数据化运营和管理。

### 4.1.6 集中日志监控服务

针对系统运行时产生的一些错误信息、系统的负载信息、用户访问路径,以及响应时间、用户搜索关键字、接口的调用等日志数据,基于ELK(Elasticsearch+Logstash+Kibana)设计和实现集中式的日志数据收集和分析服务,在Logstash Agent层每台机器部署一个进程,负责对日志收集、过滤、数据源封装,并发送给部署在中心服务器上的分布式消息队列Broker(Redis或Kafka等),Logstash Agent将日志收集在一起交给全文搜索服务ElasticSearch,进行索引等处理,最后通过Kibana结合自定义搜索进行可视化的日志数据查询和分析。

### 4.1.7 文档转换服务

业务数据采用不落地模式,提供附件文档,包括:Office文档、PDF文档、方正文档、图片格式、

书生文档、压缩文档等,转换成图片、html的功能,并在所有界面提供水印功能。

### 4.1.8 消息推送服务

提供系统内、短信、移动企信等方式应用推送功能,使各类业务、事务消息可按事件、时间等条件自动推送,用户可以及时处理工作任务。

## 4.2 移动端功能

### 4.2.1 身份认证与登录服务

基于统一身份认证系统,平台提供多重安全认证策略,基于应用的不同安全等级,采用不同的安全认证组合,包括用户名与密码、手势密码、PKI/CA认证、设备绑定/解锁、短信认证、人脸识别、指纹识别等方式。

### 4.2.2 智能适配服务

移动设备存在多样性和差异性的特点,如:设备类型、屏幕尺寸、操作系统、支持的网络协议、运行环境并发模型等,移动端采用流体布局,以增强适配性,并提供全方位操作。

### 4.2.3 调用服务

对用户的地理位置信息、通讯录、摄像头、文字输入控件等进行合理合法的利用,使产品应用能够为用户提供更加智能、更加个性化的内容及功能。

### 4.2.4 用户数据采集服务

通过埋点采集用户活跃度、使用频率、使用时长、跳出率、访问深度、页面访问路径等用户与移动应用交互行为数据,以及移动终端串码、品牌、型号、操作系统及版本、存储空间等终端数据,为移动应用监控与分析提供数据支撑,为进一步提升设计、发展个性化服务。

## 5 铁路企业移动人力资源管理应用

基于集团型铁路企业移动融合平台开发的铁路企业移动人力资源管理系统,主要功能涉及人事管理、招聘管理、考勤管理、薪酬管理、社保管理、教育培训等多个方面<sup>[6-7]</sup>,以下为部分应用场景。

### 5.1 移动事务协同

通过移动技术加强铁路企业员工和管理层的协同。通过内置的业务流程,将基层员工、中层管理者、高层管理者和人力资源管理者进行在线沟通,改善



不同角色间的协同体验,帮助人力资源管理部门推进人力资源管理的各项业务。主要功能包括人力资源公告发布与查询、劳动合同审批、入职/离职申审、人员调动申审、招聘计划申审、外出/休假申审、出差申审、培训计划申审、人事材料借阅申审、社保缴费基数确认、加入企业年金申审、补充医疗保险报销等<sup>[5]</sup>。

## 5.2 移动投票

在铁路企业人力资源管理中涉及大量的民主投票过程,如职称评定、干部评选、职代会投票、党代会投票、工会投票等,研发的移动投票系统应用功能包括:(1)管理终端:导入候选人员名单,随机生成唯一投票验证码,查看投票详情,投票统计,根据业务场景不同,可匿名或实名;(2)移动终端:在线投票、在线计票。

## 5.3 移动职工健康档案

铁路企业越来越重视维护员工的身心健康,采用包括健康调查、定期体检、健康随访等多种方式,应用现代医疗和信息技术从生理、心理角度对企业员工的健康状况进行跟踪、评估,收集职工健康数据,建立职工健康档案,并对重点人群(如火车司机)进行健康评估预警。其应用功能包括:(1)健康管理部门:发布和收集调查问卷、管理体检数据、健康风险预警分析、管理指导处方、管理岗位工作调整建议等;(2)职工:填报调查问卷、查询体检报告信息、查询指导处方。

## 5.4 移动继续教育培训

铁路行业具有工作连续性强、人员所在地域分散等特点,造成了技术人员长时间脱产学习和集中培训难度较大等诸多问题。借助移动培训模式,学员可以打破时间和地域限制,通过移动终端,参加固定时段的直播学习,随时选择视频点播课件学习,并能够与教师、参培同学在线互动和共同学习。应用功能包括:(1)学员模块实现在线报名、选课、学习等功能;(2)培训机构系统模块实现教学日程安排、课件管理、成绩统计、学习问卷、授课教师评估、课程体系评估、主办单位评估、培训机构评估等功能;(3)授课教师模块实现在线答疑、考试成绩批复等功能。

可以看到,集团型铁路企业人力资源管理涉及内容繁多,各企业需要结合实际和业务场景,采取“核心先行、逐步完善、稳步推进”策略,应用移动智能融合平台,安全、快速的将各项业务应用移动化,为企业的发展提供强有力的信息化支撑。

## 6 结束语

在移动互联时代,集团型铁路企业的信息化应用建设正快速向移动化迁移,并成为信息化战略核心之一,通过设计与应用移动智能融合平台,在移动应用规划、设计和实现方面提供统一、安全、规范的移动应用开发标准,可以在保障铁路企业业务应用安全的基础上,为管理者与员工提供随时、随地便利的移动工作体验,现已具备将集团型铁路企业传统应用系统的部分应用扩展到移动终端的技术条件,经过近些年来的实践,取得了成功案例,为铁路企业的深入改革发展提供了强有力的技术支撑。

### 参考文献:

- [1] 张向阳,朱建生,刘承亮,等.铁路企业移动应用平台的研究与开发[J].铁路计算机应用,2017,26(3):43-45.
- [2] 王忠凯,史天运,张惟皎.动车组管理信息系统便携式移动终端的设计与实现[J].铁路计算机应用,2012,21(2):31-33.
- [3] 中国铁道科学研究院.移动互联网应用安全防护技术要求:Q/CR-TKT-00 0024-2018[S].北京:中国铁道科学研究院,2018,1.
- [4] 贾军营,王月鹏,王少华.基于MQTT协议IM的研究和实现[J].计算机系统应用,2015,24(7):9-14.
- [5] Silva, Carlos, et al. Secure push notification service based on MQTT protocol for mobile platforms[C]//12th Ibero-American Conference on Software Engineering and Knowledge Engineering, 2017:69-84.
- [6] Pilarski, Björn, Schumann, Matthias. Mobile applications in human resource management-a task-technology-fit perspective[C]//Tagungsband Multikonferenz Wirtschaftsinformatik, 2014:1526-1538.
- [7] 中国铁道科学研究院.中国铁路总公司人力资源管理系统社会保障管理应用总体方案[R].北京:中国铁道科学研究院,2015,10.

责任编辑 王浩