



# 双网融合下的高铁智慧出行服务

李世平 国铁吉讯CTO

## 一. 公司简介

## 国铁吉讯科技有限公司



- 国铁吉讯科技有限公司由中国铁路投资有限公司与吉利、腾讯携手共同组建。铁路占股51%，吉利、腾讯占股49%。
- 国铁吉讯科技有限公司的成立，是铁路部门深化国铁企业改革、积极发展混合所有制经济、推动高铁网+互联网“双网融合”取得的重要成果。
- 公司负责动车组WiFi平台建设和经营，将向旅客提供站车一体化、线上线下协同的出行服务，包括WiFi接入、行程服务、订票、订餐、休闲文化娱乐、新闻资讯、特色电商、联程出行、智慧零售等。



- 中国铁路官方WiFi入口、官方行程服务；
- 高铁年客流量超过20亿人次，用户发展潜力巨大；
- 高铁车站和列车封闭场景的全触点；
- 预计到2020年，覆盖全国3000+动车组列车。



## 定位与使命:

定位

智慧高铁服务商

### 双网融合

高铁网 + 互联网，在技术和服务上进行双向融合，采用下一代新技术、新模式，为铁路生产运营的智能化、数字化升级做贡献。

使命

让服务联网 让出行智慧

### 时空运营

将出行空间场景演化成用户体验中心，有效规划用户的时间、空间，以做好客运服务为宗旨，促进消费升级，不断满足人们对美好出行生活的需要。

出发地需求

铁路上需求

目的地需求

出发服务

线上/线下的在途服务

持续服务

信息提醒

预定信息/行程提醒

共享出行

网约车/租车/公共交通

商旅服务

商品订购/旅游攻略/进站服务

预约定制

预约挂号/订票酒店/景区

WiFi连接服务

车载硬件：车载天线确保信号覆盖；车载离线服务器确保内容体验

在线娱乐

视频/音乐

手机游戏

新闻/资讯

电商购物

车上点买送货

智能提货柜

配送到站

会员服务

会员积分

会员成长

会员权益

旅客服务

车、站内服务

增值服务

智能进出站

共享出行

网约车/租车/公共交通

智慧零售

商品订购/到站到家配送

定制服务

地接/引导/旅游/求医/急救/上学/就业/业内服务

票务信息  
需求预测

内容推荐  
广告营销

互联网+高铁网，为旅客提供门到门的一站式生活服务

离场服务  
应用营销

出行意向

再次出行

## 掌上高铁V2.0时代



## 乐享3.5小时高铁时光



## 二. 双网融合建设规划



## | 互联网+铁路智慧出行



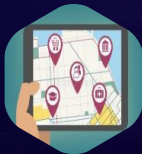
## | 互联网+铁路客运服务

### 特色服务 “互联网+”全面升级

铁路特色服务信息化、智能化、集约化

- 根据个人信息ID，对特殊旅客进行分类，针对分类旅客的需求快速响应处理；
- 集合智能机器人，减少人力的成本，智能化的提供相应的服务；
- 结合大数据分析系统，精准定位服务人群，更好的管理聚合的服务打通服务链。

站内导航



小红帽



行李寄存



重点旅客服务



遗失物品找回

贵宾室  
VIP LOUNGE

行李\宠物托运



VIP贵宾室

## | 互联网+铁路旅游

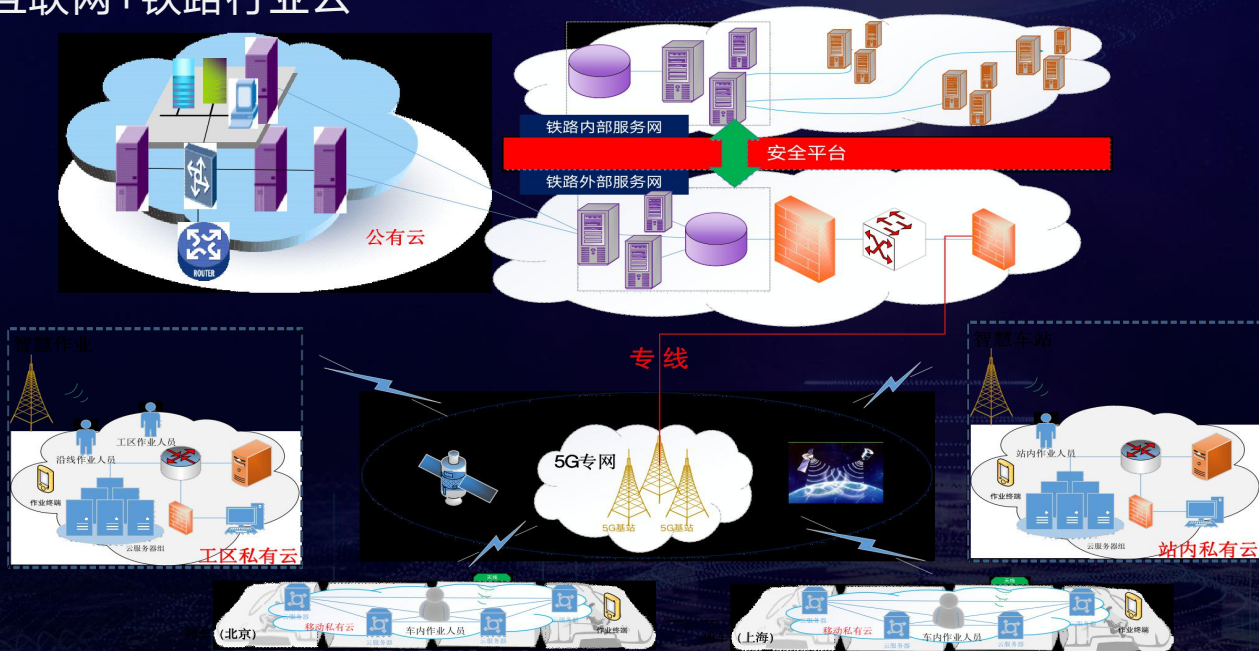


## | 互联网+铁路餐饮



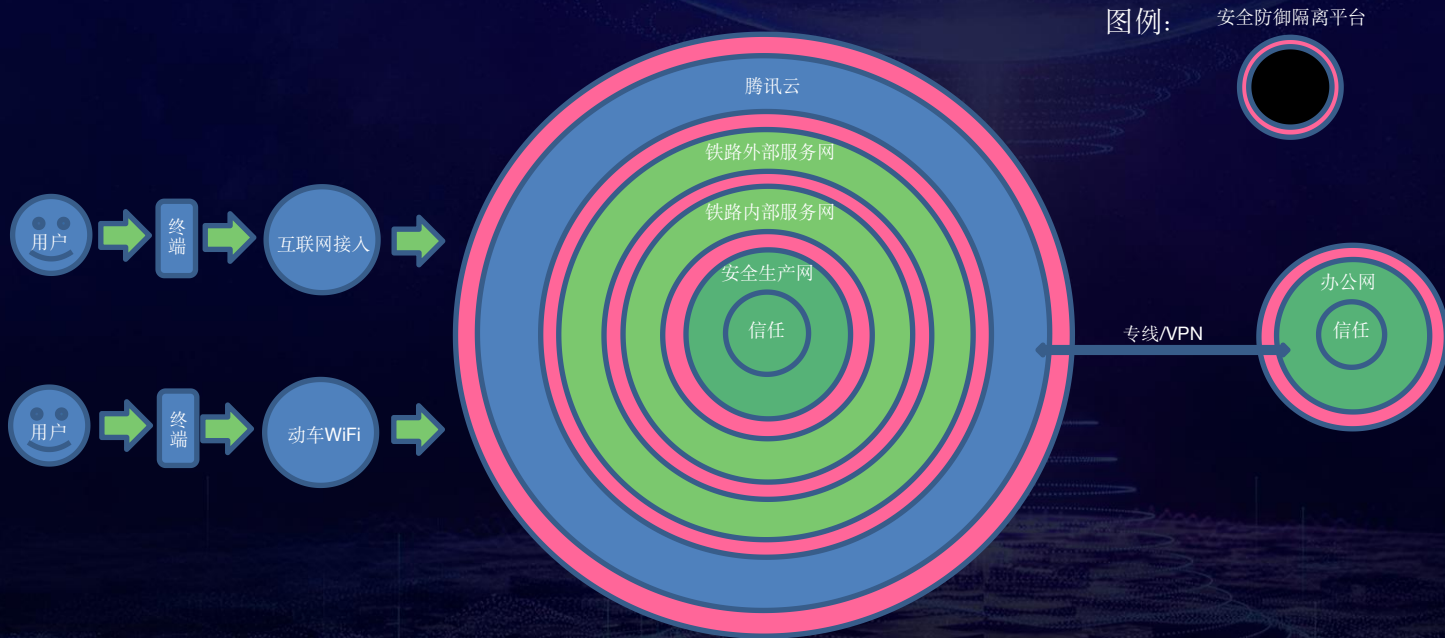


## | 互联网+铁路行业云





### 三. 双网融合安全思考



## | 目前我们(行业)的网络安全架构存在的问题:

默认内网安全, 预设了对内网中的人、设备和系统的信任, 从而忽视内网安全措施加强。

攻击者一旦突破企业的网络安全边界进入内网, 常常会如入无人之境

公有云、私有云、混合云, 云计算, 手机移动端等的快速发展导致传统的内外网边界模糊, 很难找到物理上的安全边界。

基于密码, SSL证书, AES 密钥等静态认证, 一旦密钥或者证书被泄露, 黑客可以横行无忌, 为所欲为

# 零信任

自动化学习  
自动化调整  
公有云  
混合云  
去网络中心化  
谷歌 Google BeyondCorp  
变革与演进  
持续检测  
持续身份认证  
以身份为中心  
机器学习  
安全与易用平衡  
传统边界正在消失  
零信任IT办公网安全架构实践  
ZeroTrust Security  
不影响生产  
智能身份分析  
最小授权  
动态访问控制  
业务访问主体  
时空变化  
业务访问代理

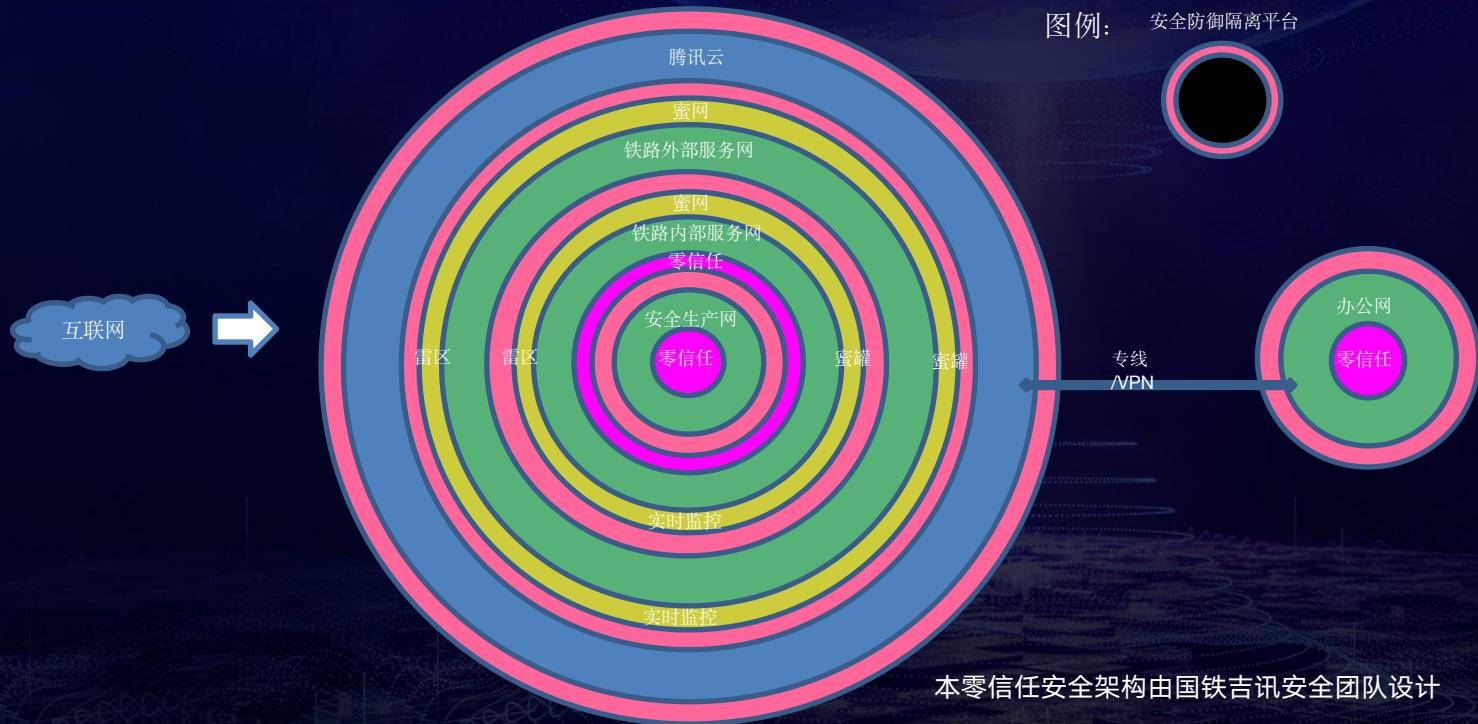
- 零信任  
默认内网和外网一样充满风险，不再相信任何内部人和内部设备
- 无边界  
网络安全架构从“网络中心化”走向“身份中心化”
- 蜜网雷区  
布置蜜网、雷区，通过蜜罐诱杀和洞察分析攻击者
- 以身份为中心  
建设智能身份平台，业务访问主体和访问代理分别通过与智能身份安全平台交互，并协商数据平面配置参数，来完成信任的评估和授权过程
- 持续身份认证  
零信任架构认为一次性的身份认证无法确保身份的持续合法性，即便是采用了强度较高的多因子认证，也需要通过持续认证进行信任评估
- 动态访问控制  
零信任架构下的访问控制基于持续度量的思想，是一种微观判定逻辑，通过对业务访问主体的信任度、环境的风险进行持续度量并动态判定是否授权。



# 零信任安全架构设想

## CRGT Ot Security Architecture

图例： 安全防御隔离平台



感谢聆听