
Tencent 腾讯 | 腾讯安全
CSS
互联网安全领袖峰会
Cyber Security Summit
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。

产品版图

出行意向

出发地需求

出发服务

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

票务信息
需求预测

铁路上需求

线上/线下的在途服务

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	电商购物	会员服务	旅客服务
视频/音乐	车上点买送货	会员积分	车、站内服务
手机游戏	智能提货柜	会员成长	增值服务
新闻/资讯	配送到站	会员权益	智能进出站

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

目的地需求

持续服务

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

离场服务
应用营销

再次出行

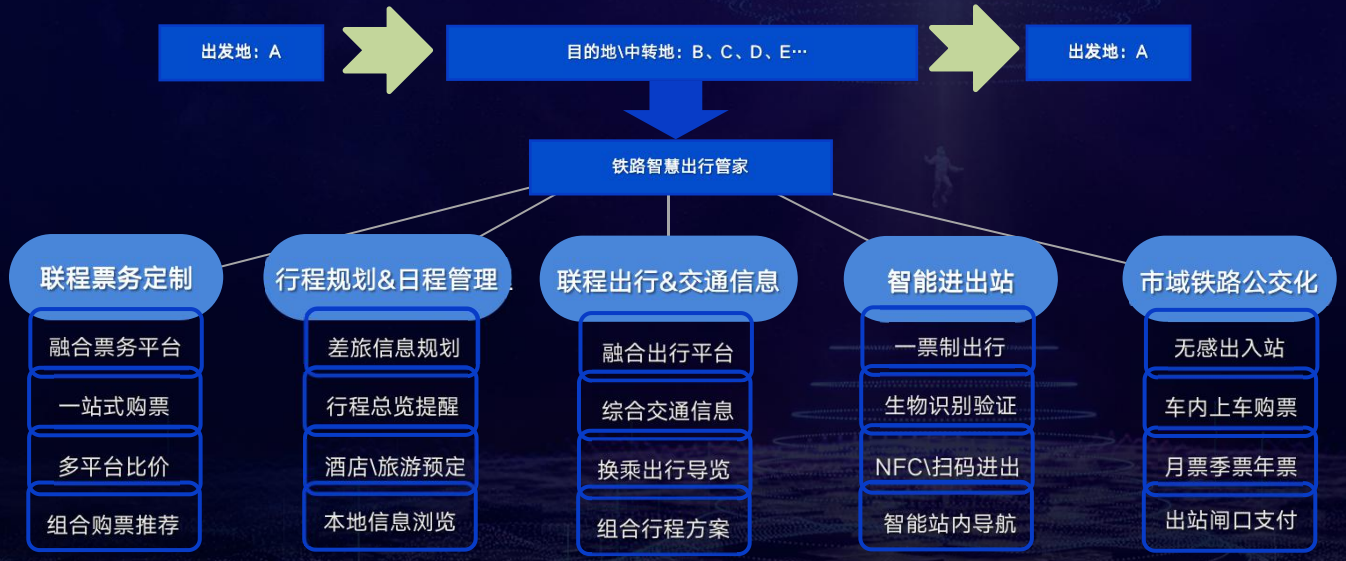
掌上高铁V2.0时代

乐享3.5小时高铁时光

CRGT 国铁吉讯

二. 双网融合建设规划

互联网+铁路智慧出行


出发地：A
目的地\中转地：B、C、D、E…
出发地：A
铁路智慧出行管家
联程票务定制
融合票务平台
一站式购票
多平台比价
组合购票推荐
行程规划&日程管理
差旅信息规划
行程总览提醒
酒店\旅游预定
本地信息浏览
联程出行&交通信息
融合出行平台
综合交通信息
换乘出行导览
组合行程方案
智能进出站
一票制出行
生物识别验证
NFC\扫码进出
智能站内导航
市域铁路公交化
无感出入站
车内上车购票
月票季票年票
出站闸口支付

互联网+铁路客运服务

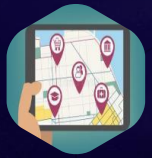
特色服务
“互联网+”全面升级

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。


小红帽

站内导航



行李寄存


重点旅客服务


遗失物品找回

VIP贵宾室


行李\宠物托运

互联网+铁路旅游


旅游票务
火车票
景点门票
生活票务（电影、演出、展馆）
01
旅游出行
旅游列车
自驾游
02
旅友社交
游记攻略
社交平台
06
国铁出行
旅游平台
旅游产品
铁路旅行社产品
第三方平台合作
自营特色主题产品
03
05
酒店住宿
铁路酒店集团化管理
资源整合，建立会员体系
04
旅游服务
电子导游
翻译系统
安全助手

互联网+铁路餐饮

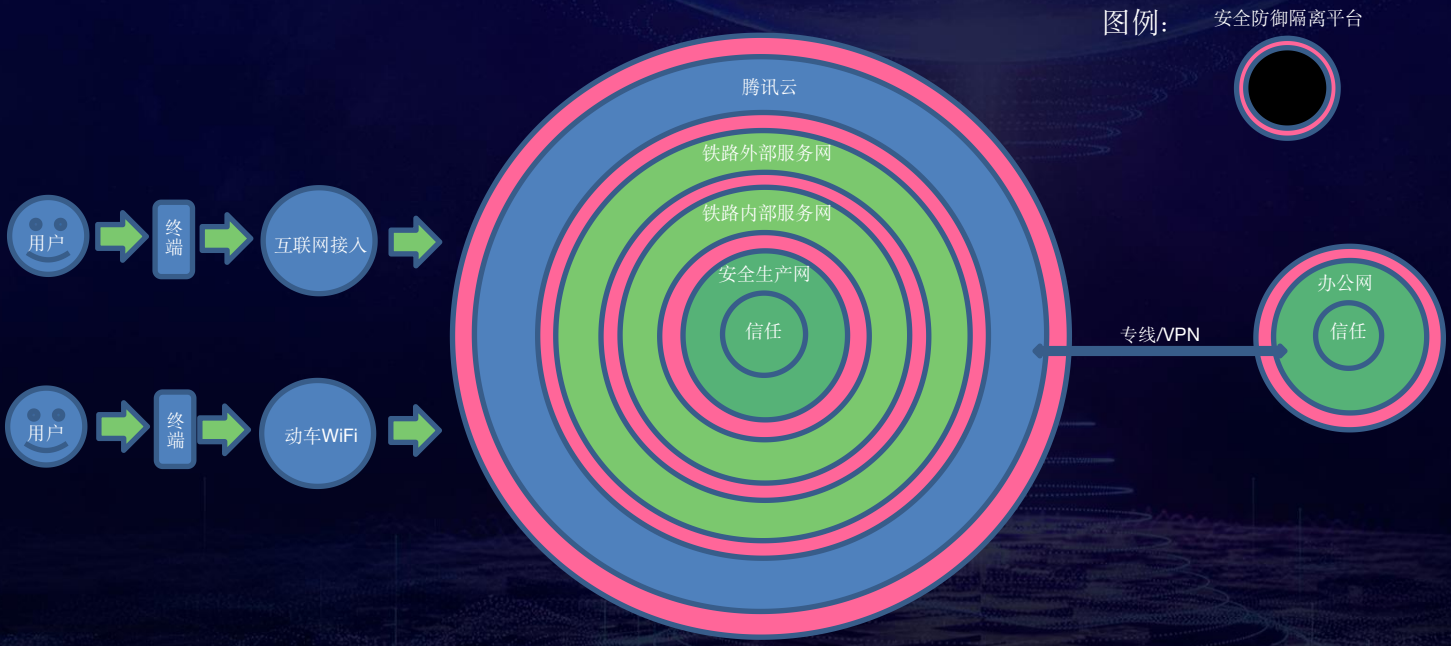

线上线下联合运作
线上
站外内联合配送
自动机械分拣
智能化信息配送
配送链路实时跟踪
联合
多样性选择资本化运作
标准系统安全管控
智能配送省时省力
环节监控平台化运营
线下
统一内外商务合作
配送中心与分拣系统
自动配送链与智能机器人
标准生产与配送线

互联网+铁路行业云


公有云
铁路内部服务网
安全平台
铁路外部服务网
专线
5G专网
5G基站
5G基站
工区作业人员
沿线作业人员
作业终端
云服务器组
工区私有云
站内作业人员
作业终端
云服务器组
站内私有云
(北京)
移动私有云
车内作业人员
作业终端
(上海)
移动私有云
车内作业人员
作业终端

三. 双网融合安全思考

国铁吉讯网络安全现状


图例:
安全防御隔离平台
腾讯云
铁路外部服务网
铁路内部服务网
安全生产网
信任
用户
终端
互联网接入
用户
终端
动车WiFi
专线/VPN
办公网
信任

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的加强。

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

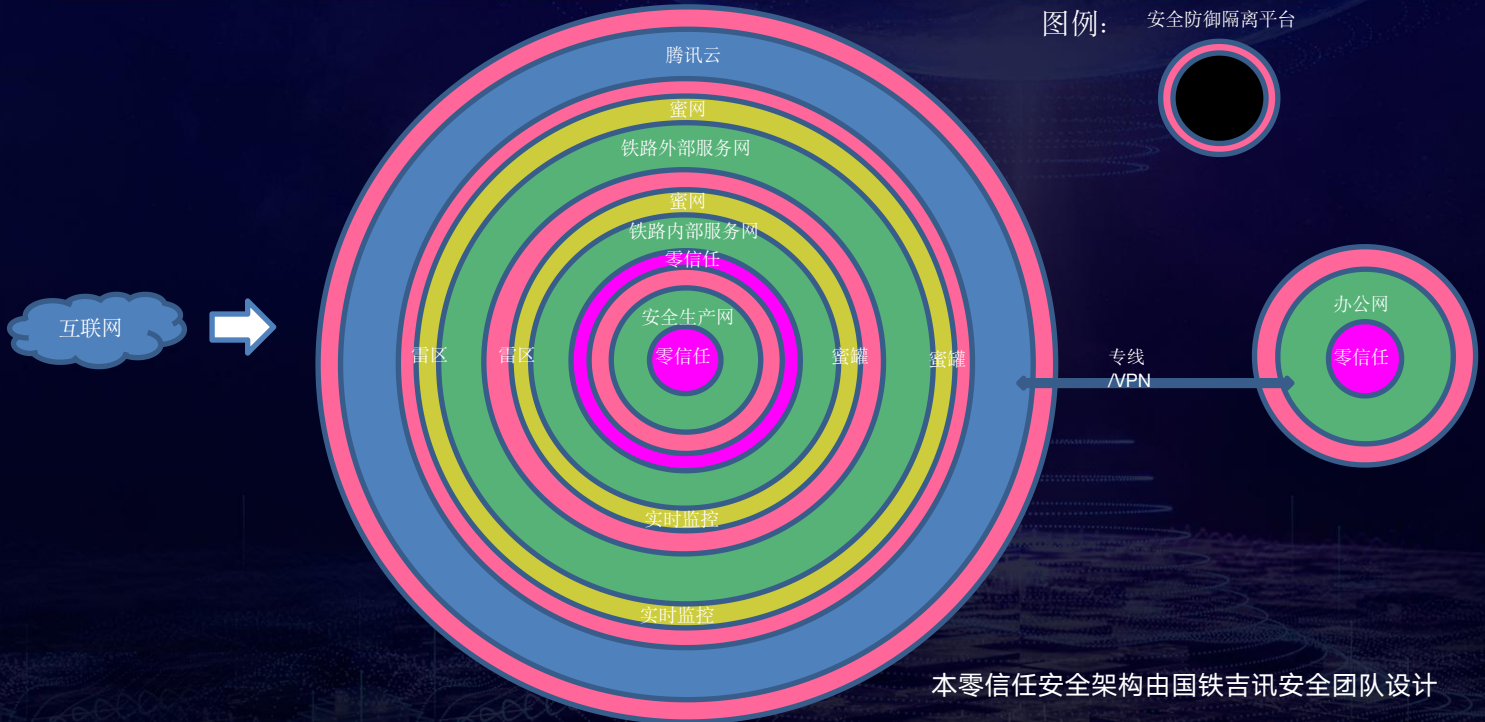
谷歌 Google BeyondCorp
零信任IT办公网安全架构实践
自动化学习
变革与演进
ZeroTrust Security
传统边界正在消失
自动化调整
持续检测
不影响生产
公有云
持续身份认证
智能身份分析
最小授权
以身份为中心
混合云
动态访问控制
业务访问主体
机器学习
时空变化
去网络中心化
安全与易用平衡
业务访问代理

解决方案设想

- **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 0t Security Architecture



本零信任安全架构由国铁吉讯安全团队设计

感 谢 聆 听