

**2015年支持安吉星二期业务现网改造工程**

**爱立信安吉星管理平台技术建议书**

****

**爱立信（中国）通信有限公司**

**2015年9月**

目 录

[1. 项目背景 3](#_Toc421783153)

[1.1 平台现状 3](#_Toc421783154)

[2. 项目需求 5](#_Toc421783155)

[3. 建设方案 6](#_Toc421783156)

[3.1 系统建设原则和策略 6](#_Toc421783157)

[3.2 平台定位 7](#_Toc421783158)

[3.3 系统软件需求 8](#_Toc421783159)

[3.4 系统架构 12](#_Toc421783160)

[4. 方案设计 13](#_Toc421783161)

[4.1 系统容量 13](#_Toc421783162)

[4.2 平台配置清单 14](#_Toc421783163)

[4.3 方案可靠性 14](#_Toc421783164)

[4.4 安全性 14](#_Toc421783165)

# 项目背景

上海移动与通用汽车谈定的安吉星车联网项目，安吉星车载设备上将安装移动的SIM卡进行语音通信、数据传输和短信业务，以及相应计费与账务服务。根据上海移动要求，由爱立信的安吉星车联网管理平台负责提供API接口与安吉星SOS进行通信，同时M2M平台提供WEB PORTAL工安吉星管理员使用。

## 平台现状

经过上期建设，上海移动安吉星车联网管理平台已经具备如下能力：

* 安吉星门户：用来为安吉星管理员提供管理界面，包括权限管理、套餐管理、查询、报表以及运维功能等；
* 安吉星网关：负责接收来自安吉星平台的请求，然后将相应请求转发给上海移动的相应网元；同时还需要负责接收网元的反馈，并且经反馈返回给安吉星平台。来自于安吉星的接口包括：
  + 基于SFTP的批量文件传输；
  + 基于HTTPS的SOAP消息

安吉星车联网管理平台现有网络拓扑：



安吉星车联网管理平台现有拓扑图

安吉星车联网管理平台目前运行于上海移动云平台，相应的服务器资源如下表所示：



# 项目需求

本期项目需求为基于爱立信M2M平台，为安吉星优化相应的车联网管理平台的供API接口和WEB PORTAL服务，主要新增和优化模块包括：

* 门户
* 接口
* 卡管理
* 业务监控
* 安全

# 建设方案

## 系统建设原则和策略

（1）标准性和开放性

系统的设计应符合国际标准和工业标准，采用开放式系统体系结构。

（2）实用性和继承性

采用成熟的、经实践证明其实用性的技术。能满足现行业务的管理，并适应将来业务发展的要求。保留原有系统的运作流程和需求特点，尽可能的不改变员工的使用习惯，在原有系统的基础上取长补短。

（3）可靠性原则

设计详尽的故障处理方案，保证系统运行的稳定性和可靠性。

（4）先进性

以先进成熟的计算机和通信技术为手段进行组网，遵循目前国际和国家的相关标准或规范。

（5）经济、实用性

在系统的组网建设中，要立足于实际情况，充分考虑到目前各种业务实际的需求，切实实现功能和性能方面的要求，并要切实结合目前现有设备情况，尽可能充分利用现有资源，节约投资。

## 平台定位

对于安吉星车联网管理平台方案的定位，如下图所示：

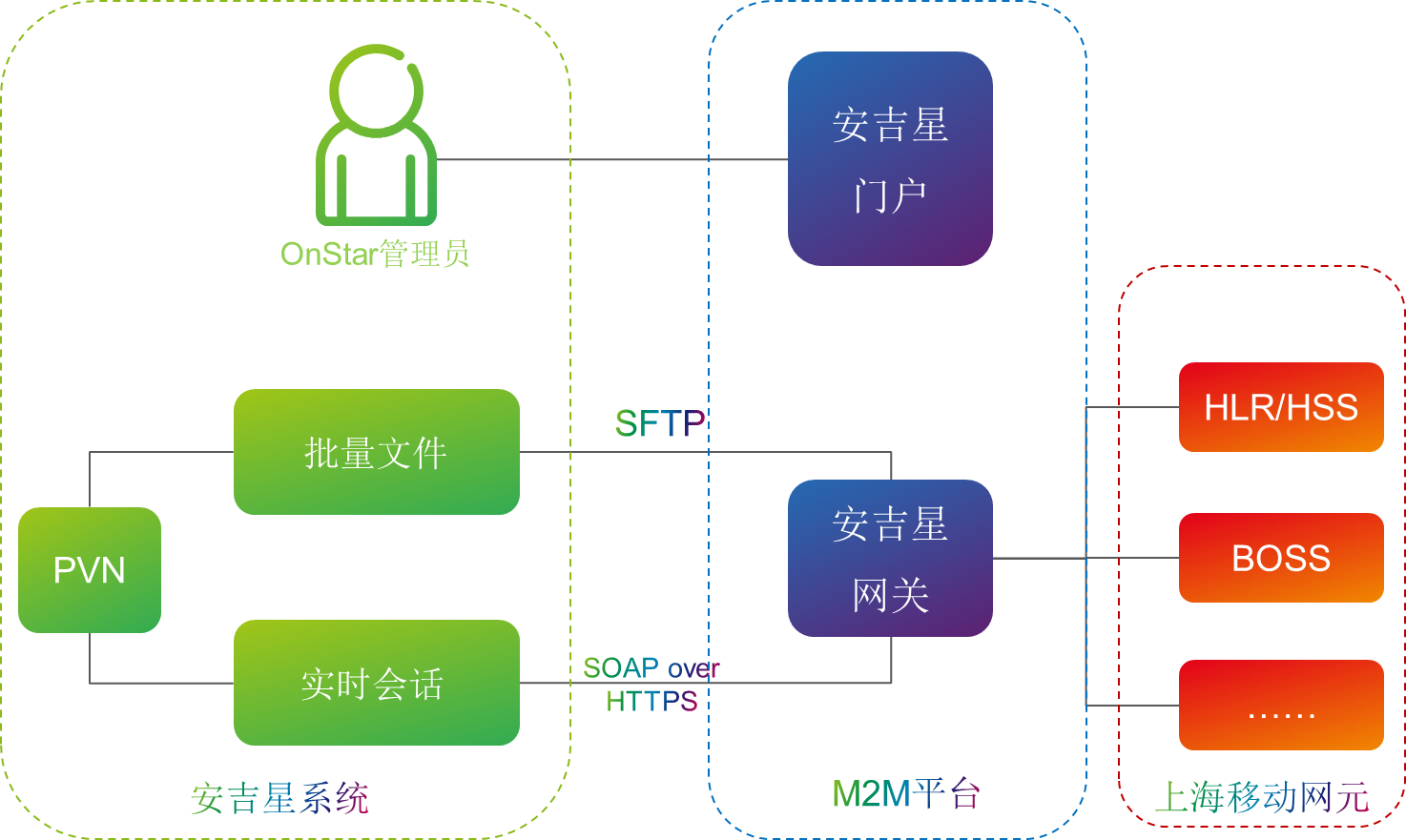


Figure 安吉星M2M应用平台的方案构成

## 系统软件需求

### 功能新增

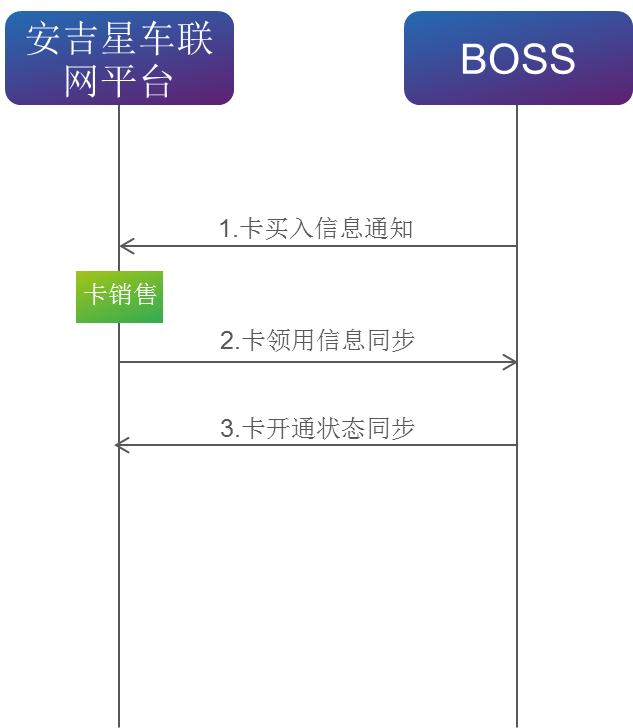
#### 门户功能新增

* 手机号码联想：车联网管理平台Portal页面中的所有搜索框，需要加入手机号码联想功能
* 手机号码历史搜索缓存：被搜索的手机号码至少需要输入7位，以天为单位，位数和时间限制可以通过配置完成；
* 单一号码集中操作：在车联网管理平台Portal页面中，需要在首页加入对于单个号码的所有操作的按钮（Button），同时在各个页面加入“回到首页”的按钮；
* 回到首页：在某个菜单项做了针对某个号码的操作后，通过“回到首页”，可以对这个号码做权限允许的所有操作；
* 英文版门户：车联网管理平台Portal页面，需要支持英文版门户。

#### 客户经理管理

#### 卡管理

* 卡信息获取：客户经理登录门户后，从工作流中获取新购卡
* 卡选择：客户经理通过界面选定指定的手机卡号，确定这些卡销售给安吉星
* 卡实名信息导入：安吉星为领用新开卡，需要导入卡用户实名信息
* 卡开通：客户经理通知BOSS，新卡分配给安吉星使用，要求开卡
* 卡状态查询：客户经理获取开卡状态
* 卡开通确认：平台获取卡的实名信息和BOSS的开卡状态，确认这些卡为安吉星开通成功
* 卡状态控制：安吉星的新开卡包括如下状态：
  + 新卡 - 移动新购卡，可以为安吉星使用；
  + 领用 - 客户经理占用SIM卡，这些卡不能被BOSS分配给其他用户使用，卡网络开通成功，通信资源开始计时
  + 开通 - 导入卡实名信息，正式开通
  + 暂停 - 安吉星通过门户或接口要求暂停相关卡



#### 套餐订购

* 套餐订购：客户经理可以通过门户为安吉星的卡管理特定套餐订购(目前仅限于“APN2经销商套餐”)，并对该套餐的属性进行限制(例如限定人数等)
* 套餐与优惠选择：客户经理在订购套餐时，需要同时选择套餐和优惠信息(可以为空)
* 资费计算：结合套餐和优惠计算资费(优惠为空时，优惠幅度为100%)
* 套餐用户数限制：控制套餐可订购用户只能小于3000
* 优惠管理：客户经理可以在门户设定优惠额度，额度范围为0-1(以百分比形式显示)，优惠可以在套餐的设定时与套餐相绑定
* 保持套餐订购原子性：由于客户需求，在安吉星为用户订购套餐(100003,Basic Package B(APN1正式套餐B)),平台向BOSS发起两个套餐订购，车联网平台负责保证订购的原子性：
  + 当两个子套餐都订购成功时，100003套餐才被认为订购成功；
  + 任一子套餐订购失败时，100003套餐订购失败，车联网平台负责向BOSS发起退订请求
  + 对于退订操作，也遵循同进同退的退订原则

#### 系统管理新增

* 新增角色：上海移动客户经理，针对该角色可创建不同的用户，每个用户可执行下列操作：
  + 卡销售
  + 开卡确认
  + 优惠管理
  + 套餐订购
* 新增角色：上海移动运维人员，负责系统维护

#### 安全需求

* 业务门户与管理门户相隔离：车联网平台的管理门户和业务门户相隔离，业务门户供业务部门和安吉星使用，业务门户仅对需要访问的IP地址开放；
* 管理门户限制内网IP登录：车联网平台的管理门户供运维人员使用，管理门户内容与部署与业务门户相隔离，同时管理门户只允许通过内网访问
* 业务门户使用SSL证书，使用互联网登录：车联网平台供上海移动的客户经理使用时，可以通过互联网域名的访问，同时车联网平台提供SSL证书(5年版)
* 接入SOC平台：车联网平台需要接入SOC平台
* 接入防篡改系统：支持互联网访问时，车联网平台需要接入防篡改系统

接受安全扫描等操作：平台入网前应完成内网、公网漏洞扫描、网站渗透测试、安全配置扫描（合规）、防火墙策略评估。

根据扫描和评估结果完成系统整体安全加固。

### 接口功能变更

基于系统现状和功能需求变更，目前与安吉星侧系统接口无变化，需要调整与上海移动内部网元接口

具体的接口功能调整：

* BOSS
  + 卡销售同步接口 – 安吉星车联网平台通过BOSS获取已购入的新卡信息，由客户经理确认销售给安吉星的SIM卡信息，并同步给BOSS进行开卡操作。建议使用文件over FTP
  + 开卡信息同步接口 – BOSS侧确认与安吉星开通SIM卡后，需要定期(按天/小时)，将SIM卡开卡信息同步给车联网管理平台。建议接口形式为文件 over FTP
  + 套餐变更信息 –当套餐信息发生变更时，需要BOSS/车联网平台协同工作，一起定义套餐的相关参数并确保同时上线
  + 套餐优惠信息 – 当有套餐优惠信息变更时，需要BOSS/车联网平台协同工作，一起定义套餐优惠的相关参数并确保同时上线
* SGSN/HLR – 需要上海移动定期(按月)上传/同步SGSN/HLR对应的区域映射关系表到车联网管理平台

### 平台监控维护

* 数据库运行状态监控

CPU、MEMORY、DISK、表空间、进程状态、实例状态、连通性的监控和告警，可设置告警阈值，告警方式也可配置（监控门户、短信方式）。

* 服务器运行状态监控

CPU、MEMORY、DISK、进程状态、连通性等的监控和告警，可设置告警阈值，告警方式也可配置（监控门户、短信方式）。

* 平台业务状态监控

包括服务器接入情况、信息流量变化情况等的监控和告警，可设置告警阈值，告警方式也可配置（监控门户、短信方式）。

* 监控信息告警

对平台侦测到的故障和异常通过维护界面和短信（短信功能建立在新申请的短信接入号码和短信通道的基础上）进行告警，便于维护人员和用户及时发现问题，并进行处理。

* 监测、告警维护功能

监控还包括告警设置、维护人员、企业用户信息维护功能，如告警信息接收人员的手机号码，告警信息级别的维护和管理

* 对外接口状态监控

监控平台与外部接口运行状态

* 平台数据比对工具

平台还需要为运维人员提供数据比对工具，通过工具，运维人员可以实现平台数据的导出(按指定格式，包括用户/套餐等信息)，运维人员将导出文件交由其它平台进行数据比对。

## 系统架构

根据目前的功能需求和容量需求，系统架构无变化

# 方案设计

## 系统容量

系统容量无变化

但是需要添加测试平台，测试平台支持10000台车

### 测试平台计算能力和数量

忙时处理能力要求： 10，000 x 2 x 0.3/3600 = 2 TPS

按照单个VM处理能力200 TPS，则需要1个VM即可(同时提供数据的接收和发送)，不提供HA，共计1个VM负责测试平台与安吉星的接口

### 测试平台存储能力

* 会话存储能力要求：

10000 x 2 x (1+1+2) x 3 /1024x1024/0.6 = 0.38 G bytes

* 话单存储能力要求：

500,000 x 20 x 2 x3 /1024x1024/0.6 = 1.85 G bytes

* 数据库存储要求： 120 G bytes

总体存储要求 0.38+1.85 + 120 = 122.3 G bytes

### 测试平台功能要求

测试平台的功能要求与安吉星车联网平台保持一致，除容量差异外，不提供新功能。同时提供外网访问能力

## 平台配置清单



## 方案可靠性

本期项目中所有关键设备均具有双机冗余备份或负载均衡机制，具体描述如下：

* 主机的HA： 采用双机备份，两台机器之间有心跳机制，以Active-standby方式运行。
* 测试平台：不提供HA机制

## 安全性

本期工程平台的物理安全要求、系统架构安全、系统基础安全、敏感用户信息安全、日志安全、应用账号安全、网站安全、系统防病毒、集中安全管控、业务安全等要求参见《中国移动上海公司安全技术规范要求条款（试行）v1.2》及《中国移动上海公司安全技术规范书（试行）V1.2》。平台安全域划分、网络边界隔离与防护要求参见《中国移动支撑系统安全域划分与边界整合技术要求》。

* 系统具备防病毒能力，应是其安全内容建设的重点。系统的防病毒系统能够防止以http、https、邮件等多方式的病毒入侵。防病毒系统应具先进的检测、清除病毒的多层次能力；应具备全面查杀病毒，查杀病毒准确无误，管理方便，安装简单的特点；病毒码和扫描病毒引擎的自动更新功能；并能够提供报警机制等功能。由于本期工程服务器架构在内网，内网需经防火墙与外网相连。
* 同时系统的门户界面，管理界面，操作维护功能，日志，数据库等部分均采用了分组分权限的方式进行管理，不同权限的用户能够完成的操作也不同，从而最大限度的保证了系统的安全性。
* 客户信息相关系统操作日志记录要求：
  + 日志应当不区分操作的类型、来源和途径，记录所有重要操作，包括通过维护终端进行的本地操作。日志应当记录单次操作，记录的内容至少包括：操作帐号、操作时间、登录IP地址、详细操作内容和操作结果等。日志不应明文记录帐号的口令、通信内容等系统敏感信息和客户信息；
  + 日志仅能由超级用户和审计用户访问。日志应能够统一管理。所有涉及客户信息的操作的原始日志至少在线保留3个月，离线保留1年。所有涉及客户信息的操作的原始凭据应真实有效并至少保留1年；
  + 日志的格式和内容应当易于阅读，日志中如涉及大量指令或代码，应配有必要的使用手册，帮助审计人员快速理解日志的含义；
  + 系统应当支持日志的批量导出功能，至少单次能够导出500M以上或是一个月的日志数据，导出的格式应为可被excel或数据库导入的格式，文本格式的日志应当行列清晰，易于阅读。
* 客户信息相关系统安全防护要求：
  + 严格限制客户信息相关系统的互联互通能力，将系统中的客户信息置于核心区进行保护。安全域边界应部署防火墙、IDS等防护手段。