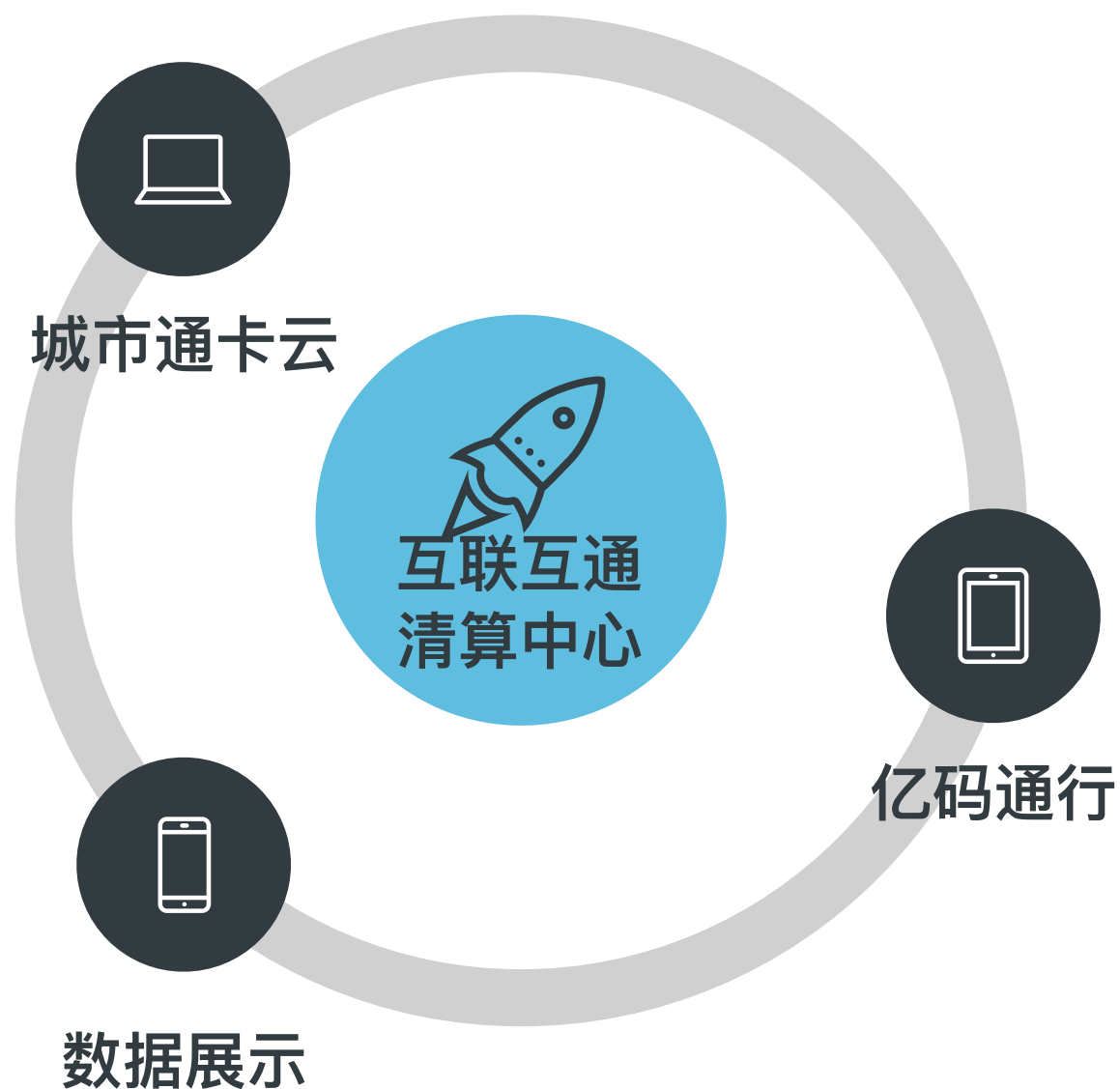


# 清分清算及通卡云平台 建设实施方案

北京亿速码数据处理有限公司

# 业务背景



- 为升级改造目前在运行的住建部互联互通清算中心平台，使之满足新城市接入的业务需要；
- 以及解决众多三、四线中小规模一卡通在系统建设和运营方面的诸多痛点问题；
- 业务系统需直观体现当前业务的发展趋势，需要数据展示系统给领导和经营提供决策支持。
- 公司对互联互通清算中心平台和中小城市通卡云平台进行项目立项。

进度约束：

- 10月份具备新互通城市的接入能力
- 11月底之前具备中小云平台试点城市落地、迎接12月初年会。

## 清算平台

- 互联互通城市的接入管理；
- 互联互通交易数据的交换、清分、对账、结算以及备付金管理

## 城市通卡云

- 中小城市的实体卡发卡、充值、消费的标准化功能；
- 与数据中心清分结算平台对接，实现互联互通交易清算；
- 与公司现有TSM平台对接，实现移动端的实体卡业务功能。

## 亿码通行

- 码付平台已是闭环业务体系，保持独立运行
- 城市通云平台提供接口对接码付平台的移动端空开、空充业务

## 数据展示

- 对当前清算平台及城市通卡云的业务数据进行分析；
- 对清算平台及城市通卡云的业务数据分析结果进行多渠道形式展示。

# 功能清单

## 01. 通信前置系统

负责核心系统与外部系统之间的数据交换。主要包括与接入城市之间的文件传输和结算银行之间的报文交换。

## 02. 核心处理系统

交易数据处理、清分清算处理、差错争议处理、备付金管理、业务管理

## 03. 机构服务系统

提供给入网机构的查询服务；机构接入的传输客户端。

## 04. 数据分析系统

提供清算平台与卡云平台业务分析。

## 05. 数据展示系统

提供客户指定渠道的数据展示功能。

## 06. 密钥管理系统

对清算平台及卡云平台的密钥进行管理和维护

## 07. 卡管系统

负责IC卡产品配置、卡号段管理、制卡数据准备（住建部互通标准）、卡片个人化、卡片密钥管理等。

## 08. 核心交易系统

负责脱机消费类业务处理、联机售卡充值类业务处理、客服退换类业务处理，以及互联互通交易处理。在交易处理过程中完成相关账户处理。

## 09. 清分清算处理

完成本城市相关业务的清分清算处理，包括与本地商户的清结算、对账及差错处理、互通交易的对账等。

## 10. 客户服务系统

提供面向本地人工柜面的相关服务，主要是售卡充值、退换卡业务。

## 11. 互联网业务前置

提供面向移动互联网的业务渠道，主要是空中开卡、充值补登类业务。

## 12. 终端/机构接入前置

负责本城市的直连终端的接入、公交行业的POS前置对接以及与住建部清算中心平台的对接。

## 13. 一卡通业务管理

主要包括商户信息、黑名单、终端信息、业务参数等维护，以及交易数据查询与业务统计报表等。

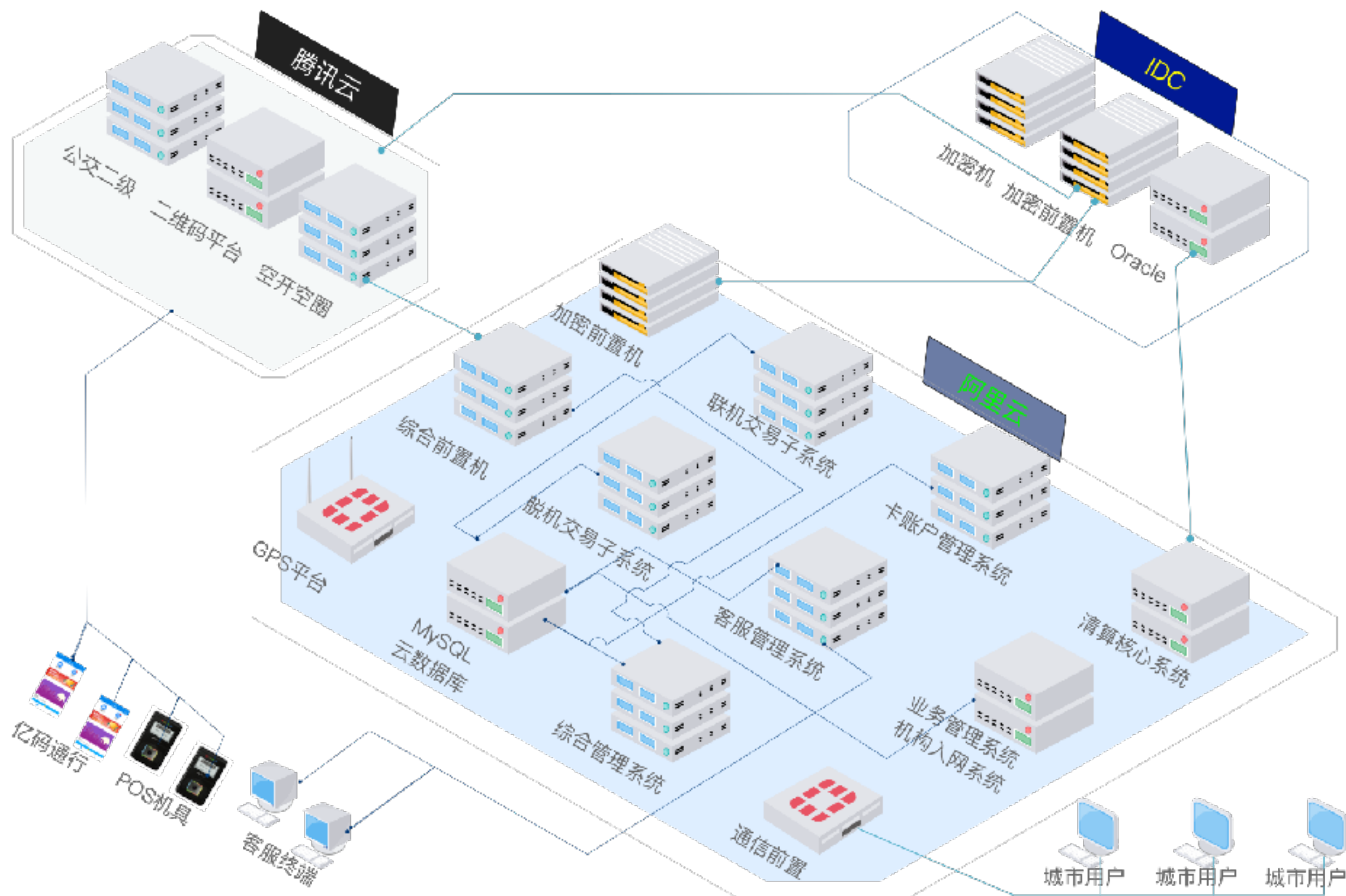
## 14. 公交业务管理

可选功能。适用于某些需要直接管理公交业务的客户。主要包括车辆、线路、票价等管理，以及运营统计报表。

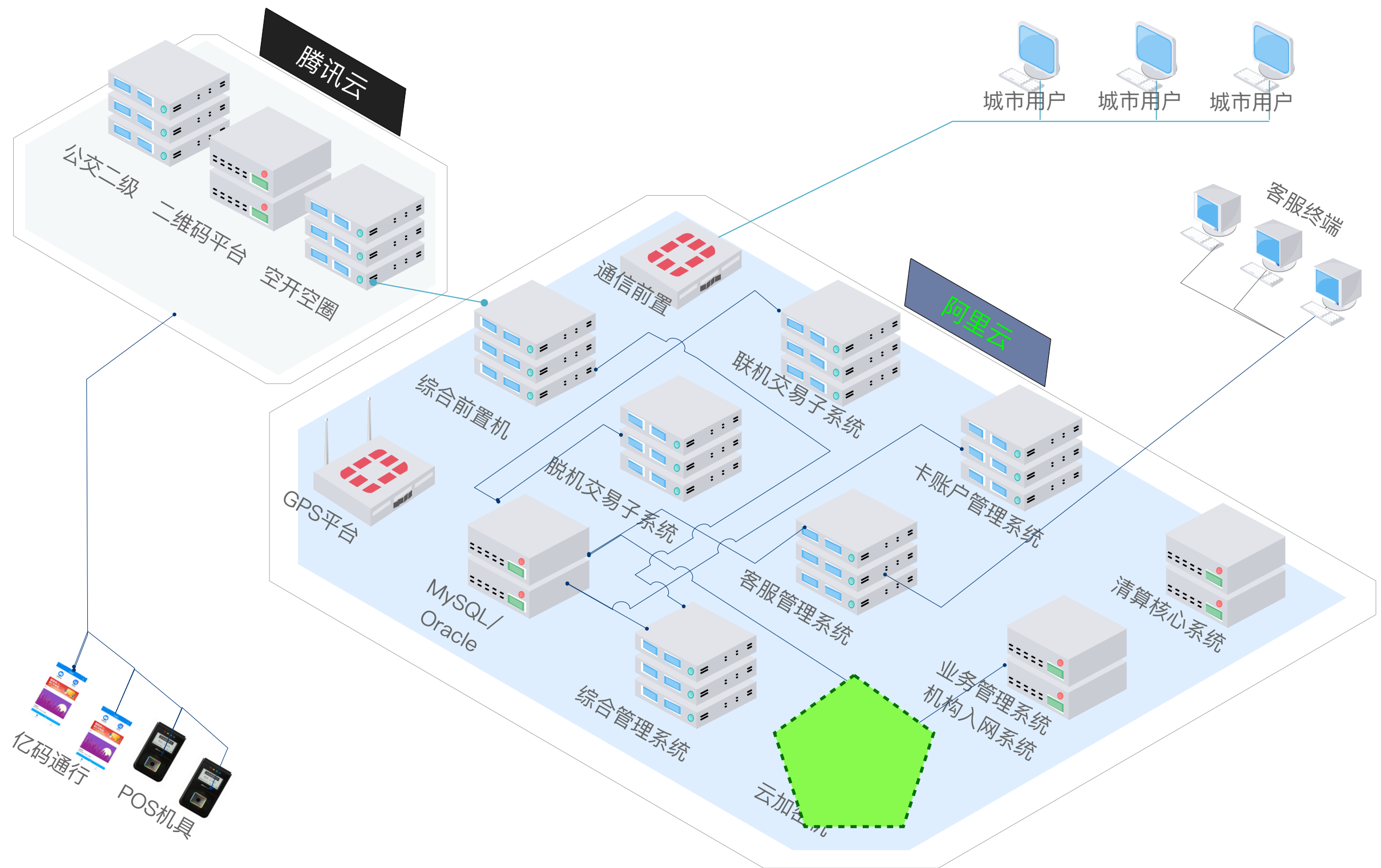
## 15. 云平台租户管理

对云平台的租户进行接入管理，主要包括租户信息管理、业务服务费率、用户权限管理等功能。

# 混合云方式



# 云加密及加密机托管

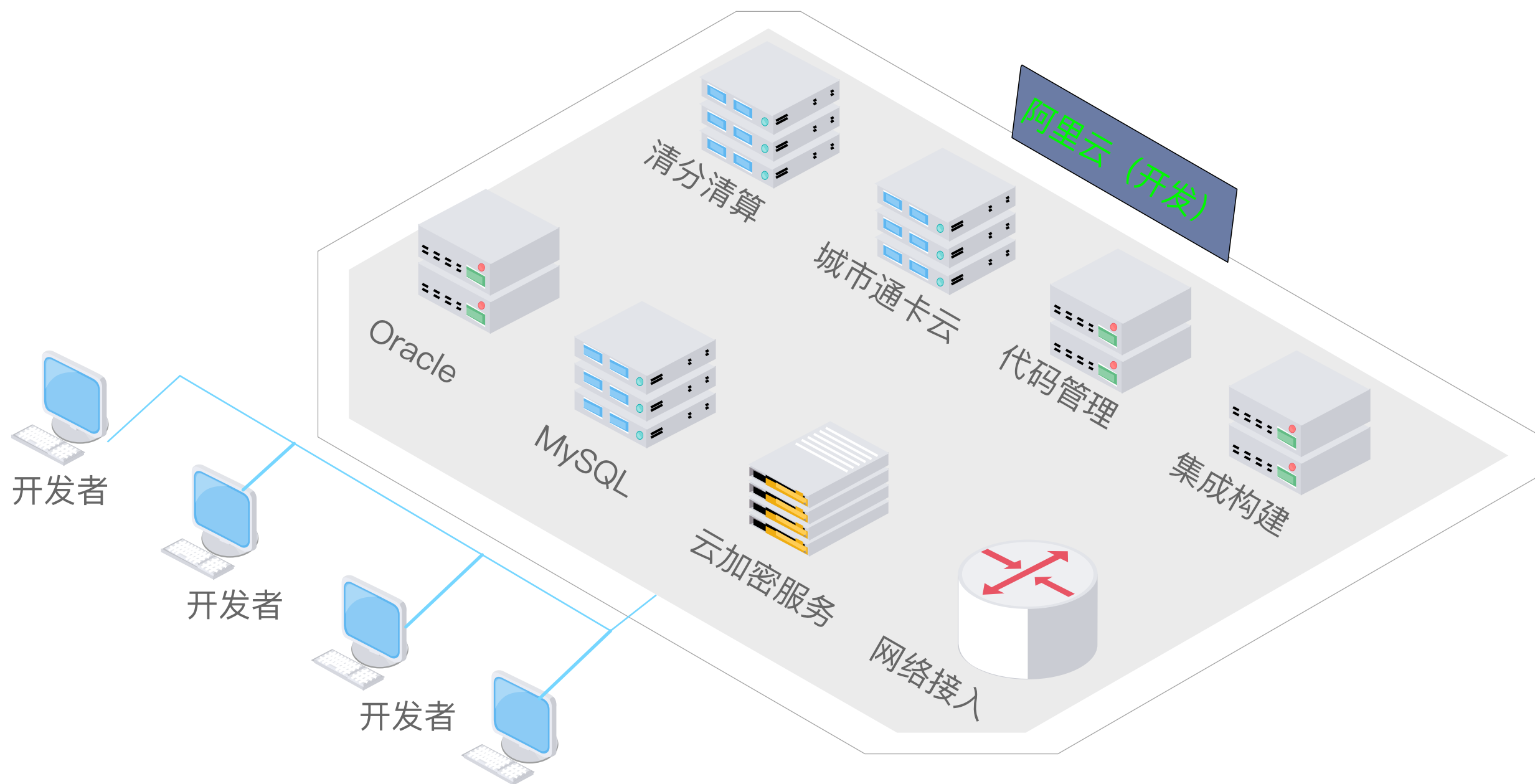




# 加密机连接比较

维度	混合云	加密机机房云托管	云加密服务
描述	通过物理专线在物理层面上连接本地数据中心到阿里云，然后建立边界路由器和路由器接口来连接数据中心与阿里云VPC。	将当前加密机部署在云托付机房内，通过专线和阿里云互联，搭建混合云。云托付提供优质的机房托管资源、云专线网络以及增值服务，并与阿里云公有云产品结合，为企业搭建混合云提供基础资源。	直接采购阿里云上的加密服务，与阿里云上的业务系统部署在同一个专有网络中，进行调用。加密服务产品通过了国家密码局的认证许可，在应用安全层面采用可靠的安全手段和认证方式，保证云平台方及加密服务原厂商都不可以操作用户自己的加密服务。加密服务归客户自己掌控。
成本	专线租用费：运营商收 专线初装费：15000（一次性） 资源占用费：7300（每年）带宽 1G	每年5000以内（按目前估计的5台加密机 + 10M专线）	一个加密服务费用为2000元/月
性能	距离远近有关，延迟在5ms以内	保证距离小于50KM，延迟在1 - 5 ms	性能与距离无关，由加密服务的性能决定，没有延时。
密码机形态	实体专用安全设备	实体专用安全设备，可以是传统密码机，可以是采用了虚拟化技术的云服务器密码机。	阿里云上的虚拟加密服务
部署模式	部署在本地机房	部署在阿里云托管机房	无需自己部署，加密服务由阿里云提供
安全	密钥安全由实体密码机保证，密码机安全由本地机房保证，业务系统调用传输安全由专线保证。	密钥安全由实体密码机保证，密码机安全由阿里托管机房保证，业务系统调用传输安全由专线保证。	密钥安全由加密服务保证，加密服务自有一套完整、完善的安全机制，保证其安全性等同于传统实体密码机，此套安全机制通过了国家密码局的评审，得到了专业认可，产品取得了国密局颁发的商用密码产品型号证书，密钥管理与密码运算与传统实体密码机完全一致。云下实体密码机迁移到云上加密服务根据具体情况会有完善、合规的方案。加密服务的安全由阿里云保证，平台保证满足合规要求，并提供99.999的高可用性。业务系统调用加密服务的传输安全由阿里云VPC保证，同时加密服务支持通讯模式密文传输。
监管	原来的监管模式	原来的监管模式 机房监控	加密服务使用通过国家密码管理局检测认证的密码机，让客户安全地生成、存储和管理用于数据加密的加密密钥，在不牺牲应用程序性能的情况下符合严格的密钥管理要求。
运维	方便运维 现场操作	方便运维 现场操作	远程运维 远程操作
比较	监管和运维方便； 一次性投入高，专线比较贵； 系统性能较低；	监管和运维较为方便； 一次性投入高； 系统性通较好；	监管不可控； 月运营费高； 系统性能高；

# 设备清单（研发环境）





# 设备清单

## 生产环境

生产环境	领域	用途	配置	数量
服务器-db(ECS)	清分清算	数据库服务器	16核 CPU   64GB内存  SSD, 2000GB	2
服务器-db_0001	清分清算	数据库服务器（高可用版本	8核   16GB SSD, 1000GB	2
服务器-dbbak(ECS)	清分清算	数据库备份服务器	2000GB	1
服务器-core(ECS)	清分清算	清算核心系统	16核 CPU   64GB内存  SSD, 1000GB	2
服务器-console(ECS)	清分清算	业务管理/机构入网子系统	8核 CPU   32GB内存  SSD, 500GB	2
服务器-pre(ECS)	清分清算	通讯前置	8核 CPU   32GB内存  SSD, 500GB	2
堡垒机	清分清算	堡垒机		1
云防火墙	清分清算			1
弹性负载均衡(SLB)	清分清算		10M/S	2
CA证书	清分清算			1
域名	清分清算			1
redis	清分清算	8G主从版		1
服务器-db_0001	城市通卡	数据库服务器（高可用版	8核   16GB SSD, 1000GB	2
服务器-core(ECS)	城市通卡	清算后台（文本文件）NAS	4核   8GB SSD, 500GB	2
服务器-kefu(ECS)	城市通卡	客服	4核   8GB   高效云盘, 200GB	2
服务器-综合管理(ECS)	城市通卡	综合管理系统、权限	4核   8GB 高效云盘, 200GB	2
服务器-综合前置(ECS)	城市通卡	二维码、APP后台等等	4核   8GB  高效云盘, 200GB	4
服务器-通讯前置(ECS)	城市通卡	车载前置、互联互通前置等(暂	4核   8GB  高效云盘, 200GB	2
服务器-数据备份	城市通卡	单独买存储	1000GB	1
堡垒机	城市通卡	堡垒机	10个以内	1
弹性负载均衡(SLB)	城市通卡	二维码、APP负载、客服	按流量10M/S	3
CA	城市通卡			1
短信	城市通卡	100000条套餐	24个月	1
redis	城市通卡	2G主从版		1
MySQL 5.6	城市通卡	4 核 8GB 1000GB存储空间		1
VPC	城市通卡			2
专线	城市通卡			2

# 设备清单

## 研发环境

开发环境设备	配置
清算-开发ORACLE数据库	4核   16GB 高效云盘, 500GB
清算-开发服务器	4核   16GB 高效云盘, 500GB
通卡云-开发服务器(ECS)	4核   16GB 高效云盘, 500GB
通卡云-db_MYSQL	8核   16GB SSD, 1000GB
开发管理服务器(ECS)	4核   16GB 高效云盘, 500GB
集成测试服务库(ECS)	4核   16GB 高效云盘, 500GB
网络设备	5M支持公网及VPN接入
Oracle 数据库软件	自行安装
DataV数据可视化	
开发台式机	2
加密机	5

## 接入测试

测试环境	配置
服务器-db(ECS)	16核 CPU   64GB内存  SSD, 1000GB
服务器-db_MYSQL	8核   16GB SSD, 1000GB
服务器-core(ECS)	16核 CPU   64GB内存 SSD, 1000GB
服务器-console(ECS)	8核 CPU   32GB内存  SSD, 500GB
服务器-motmng(ECS)	8核 CPU   32GB内存  SSD, 500GB
服务器-pre(ECS)	8核 CPU   32GB内存  SSD, 500GB
堡垒机	
云防火墙	10台
弹性负载均衡(SLB)	
分布式缓存服务 DCS	主备2G内存
CA证书	
域名	
redis	

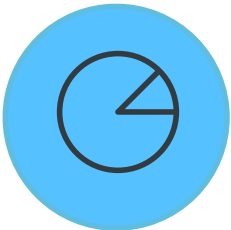
# 实施内容

- 确定加密机部署方案
- 搭建开发及生产运行环境
- 确定机具/卡片结构



## 总集成

## 清算平台



- 建设互联互通清算平台中心
- 平台中心投产及新城市接入
- 业务数据迁移

- 建设中小一卡通云平台软件
- 云平台部署上线投产
- 建设云平台租户的POS接入前置



## 城市通卡

## 分析展示



- 数据分析需求确定
- 数据分析结果渠道展示

- 云平台与码付平台对接IC卡业务对接
- 空开及空圈业务对接



## 对接业务

## 1.环境准备

指开发环境和云生产环境的规划、采购、系统集成等：

- 所有环境的规划设计、采购计划
- 本地开发环境设备（服务器、存储、网络）的采购、到货、安装
- 云平台供应商的选择 网络连接 云环境的采购、

## 2.资源协调

指需要开展业务对接和联调配合的相关方资源：

- 码付与手机端平台之间的协调，使码付平台能在APP实现空开
- 公交POS前置提供商的确定、对接联调资源的协调；
- 一部分现有接入城市的联调配合资源；
- 首个拟新接入的互通城市对接资源；云平台落地试点城市的资源协调、确定拟发卡片COS
- 财务、清算等内部其他部门的资源配合

## 3.清算平台开发

完成清算中心平台的关键业务闭环具备新城市接入联调能力：

- 清算中心平台核心闭环功能的分析与确认
- 核心闭环功能的开发、测试
- 现有系统迁移的数据分析、迁移工具开发
- 城市接入客户端的开发测试

# 工作任务

## 4.云平台开发

完成一卡通云平台的最基本的发卡充值、清算业务：

- 云平台标准功能范围的确认
- 发卡、充值功能的开发、内部测试
- 与互联互通清算平台对接开发测试
- 与码付平台联调空开接口

## 5.联调测试

完成一阶段清算平台系统功能的联调测试：

- 清算平台与城市接入客户端的联调
- 原有清算平台数据迁移的验证、测试；
- 清算平台关键管理功能的测试
- 云环境与本地的联通性测试、处理性能测试（需在云生产环境开展）

完成一阶段一卡通平台系统功能的联调测试：

- 基本发卡充值业务功能测试；
- 与清算中心平台的互通清算对接测试
- 发卡数据准备与码付平台的空开接口调试；

## 6.部署投产

完成一阶段功能的部署投产：

- 业务操作培训；
- 云生产环境的配置与清理，应用部署与验证测试；
- 数据正式迁移，新互通城市的接入；一卡通云平台试点城市的试运行接入。

## 7.功能完善

对一阶段尚未完成的清算中心平台和一卡通云平台的功能，进行开发完善：

- 清算中心平台的其他业务报表、辅助管理功能；
- 清算中心平台的互通交易数据的图形化展示；
- 一卡通云平台密钥管理、客服柜面、码付平台空充业务对接
- 一卡通云平台业务管理功能的完善

## 8.运维保障

由公司技术运维团队在系统投产后提供系统运维支撑：

- 环境信息管理、运维管理制度；
- 运维日常支撑
- 客户培训管理

## 9.项目收尾

系统投产运行稳定后对项目开展验收工作：

- 功能点验收；
- 技术资料移交验收；
- 代码验证并移交；
- 组织项目验收会。



# 进度计划



## 部署上线

- 清算中心平台上线部署
- 通卡云平台一期功能上线部署

2018.10.25

## 平台迁移

- 清算平台原系统迁移准备

2018.10.30

## 开发完善

- 公交云平台二期功能开发测试

2018.11.25

## 二期上线

- 清算中心平台二阶段功能完善开发
- 公交云平台二期功能上线

2018.11.30



## 项目领导小组



由业主方和开发方的项目主管领导或总监共同组成，主要职责：

- 1) 批准项目实施总体设计方案、实施计划；
- 2) 项目实施中有关重大问题的决策；
- 3) 协调外部资源推动进度。

## 业主项目经理



代表业主方对项目具体工作进行决策和协调 对项目总体进度负责 协调业主方有关部门以及外部合作方的资源，配合项目工作开展：

- 1) 业务财务等部门需求的收集整理、确认；
- 2) 内部技术部门的对接资源协调；
- 3) 其他外部合作方的配合协调；
- 4) 与开发方项目经理对接，共同按计划推动项目工作；
- 5) 向项目领导小组汇报项目工作，及时反映问题，协调上层资源

## 开发方项目经理



代表开发方对项目具体工作进行决策、人员的组织和任务安排，对开发方的进度计划、质量总负责：

- 1) 与业主方项目经理共同确定项目需求边界和范围、执行计划；
- 2) 协调内部开发组的资源，按计划完成开发测试任务；
- 3) 协调系统集成资源，完成系统规划、安装、调试等集成任务；
- 4) 组织系统联调、部署、培训、投产等实施工作；
- 5) 与业主方项目经理对接，安排其他合作方的对接工作；
- 6) 向项目领导小组汇报项目工作，及时反映问题，协调上层资源；
- 7) 处理项目实施过程中其他事项。

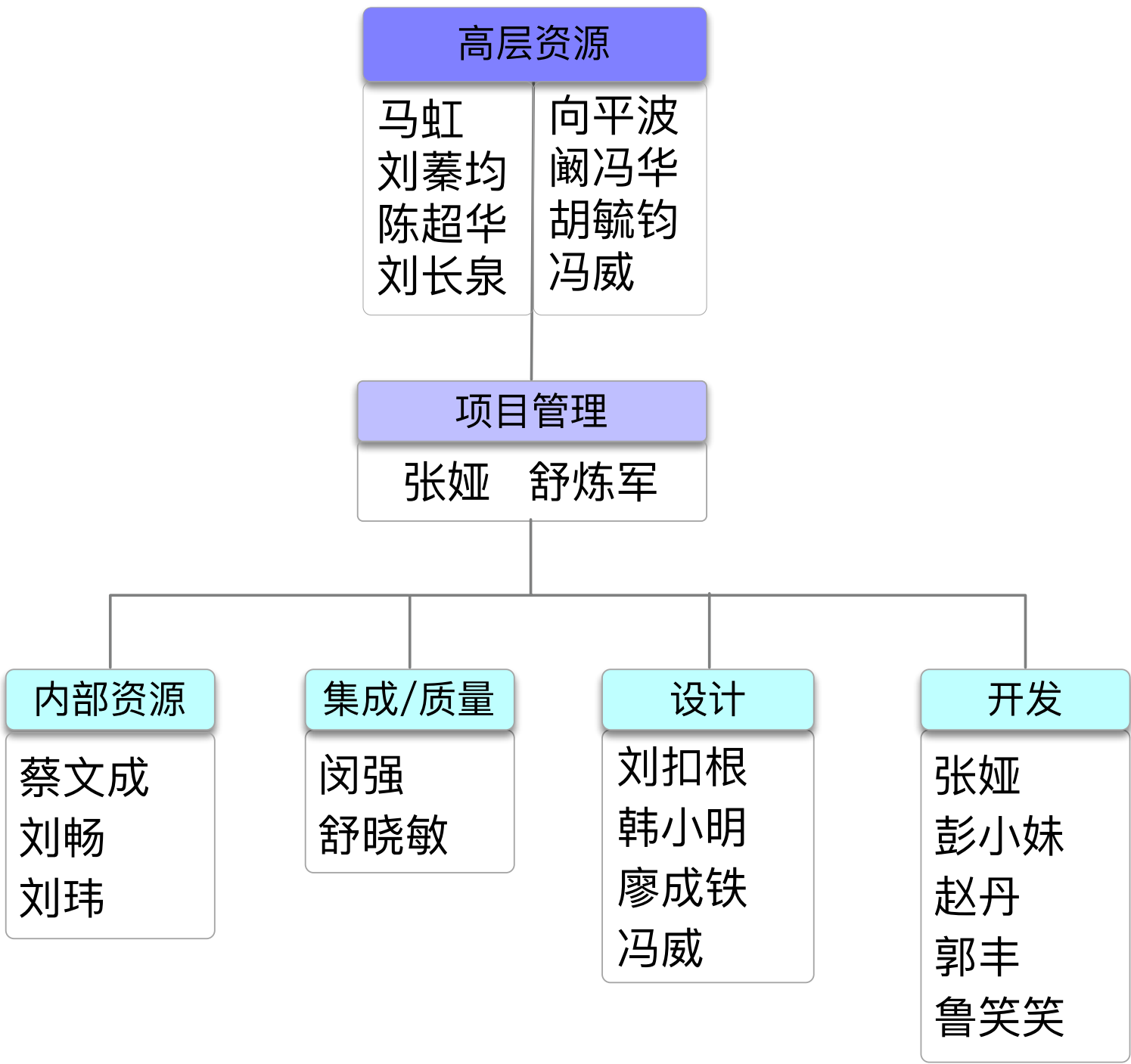
## 其它合作方



由业主方项目经理负责协调，配合本项目相关的对接、联调测试工作。

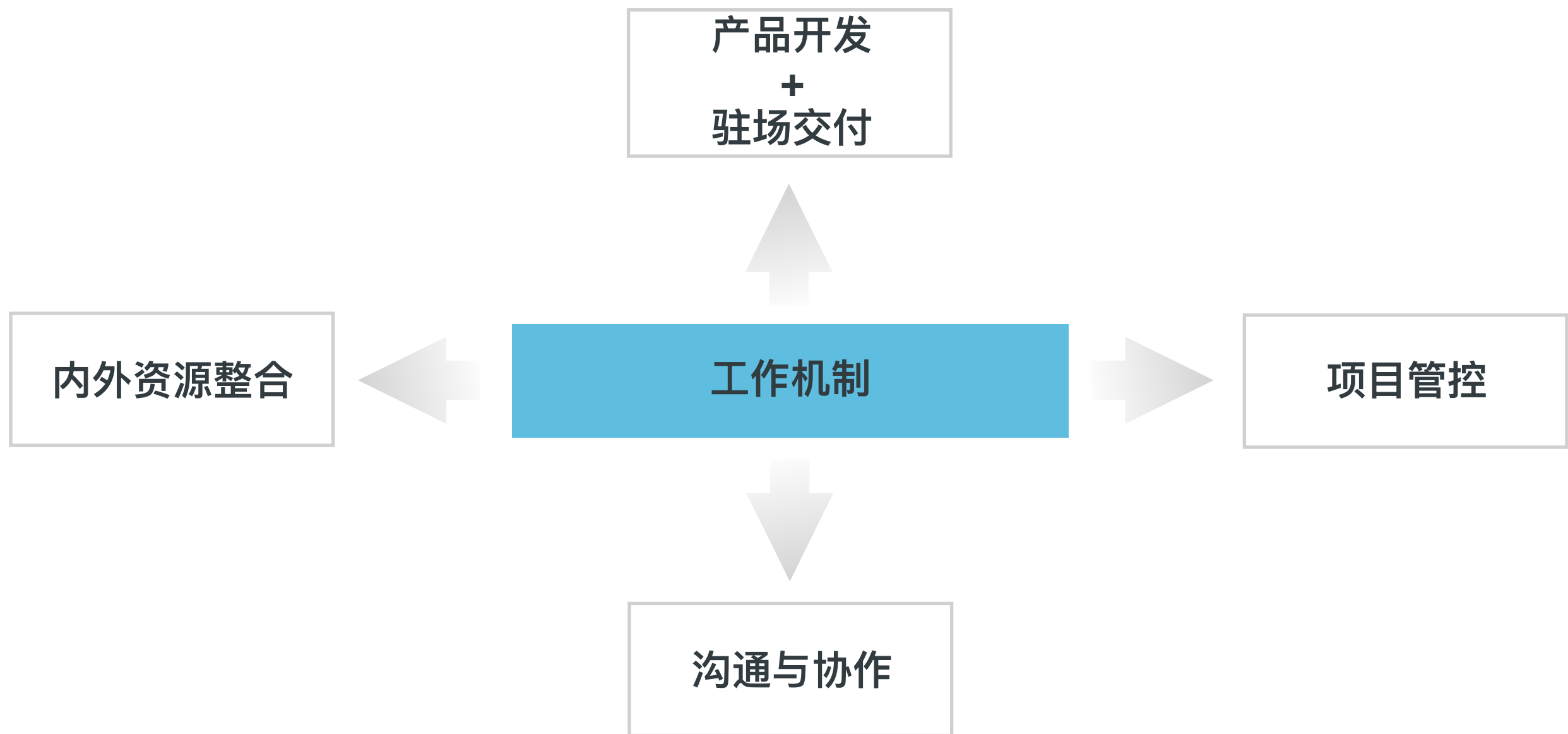
- 1) 互通城市方，与清算平台对接联调、迁移切换配合；
- 2) 公交POS前置厂商，提供云平台的POS接入能力；
- 3) 手机空开平台，与码付平台对接实现空开业务；
- 4) 卡片COS商，云平台试点城市的发卡；

# 团队成员



姓名	部门	岗位
刘长泉	亿速码	副总经理
蔡文成	亿速码	部门经理
舒炼军	亿速码	项目经理
刘畅	亿速码	系统管理
向平波	上海捷羿	总经理
胡毓钧	上海捷羿	部门经理
刘扣根	上海捷羿	技术总监
韩小明	上海捷羿	技术总监
廖成铁	上海捷羿	工程总监
冯威	上海捷羿	技术总监
张娅	上海捷羿	研发经理
彭小妹	上海捷羿	研发
赵丹	上海捷羿	研发
郭丰	上海捷羿	研发
鲁笑笑	上海捷羿	研发
舒晓敏	上海捷羿	测试

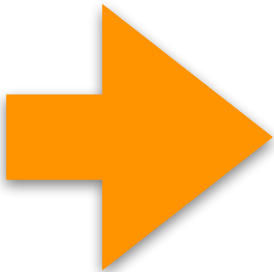
# 工作机制



1. **开发模式**采用现场交付+远程产品开发结合的方式开展工作
- 现场完成需求确认、客制化开发等需要有效沟通的工作
  - 现场完成迁移分析、验证工作
  - 远程完成基础产品层开发、云环境的集成、部署与联调等工作

2. 双方项目经理各自**协调其内部资源**，保证总的进度计划
3. 由双方项目经理**组织每周项目例会**，汇总进度和问题
4. 会议纪要、需求变更、项目决策等沟通采用邮件形式传递
5. 其他合作方的资源，统一通过业主方项目经理**协调**

- 开发商公司出现问题?
- 项目遭开发商技术锁定?
- 希望需求得到及时响应?



对核心的开发技术路线管理!  
项目过程的管控!  
项目交付物的质量管理!

项目准备

调研/采购

设计/开发

实施/集成

上线/初验

关键活动

- |        |             |            |             |             |
|--------|-------------|------------|-------------|-------------|
| - 建立组织 | - 开发环境准备    | - 系统设计与评审  | - 制定集成部署方案及 | - 双方测试及环境确认 |
| - 前期调研 | - 需求调研分析方案  | - 数据库设计评审  | 评审          | - 投产准备部署    |
| - 资料收集 | - 集成方案      | - 标准方案设计与代 | - 设备集成调试    | - 发布系统      |
| - 范围确定 | - 设备采购、到货验收 | 码审查        | - 用户测试      | - 进行试动行     |
| - 制定计划 |             | - 开发测试     |             |             |

主要成果

- |          |          |           |            |            |
|----------|----------|-----------|------------|------------|
| 《项目实施方案》 | 《项目需求报告》 | 《系统设计方案》  | 《系统部署方案》   | 《上线部署操作手册》 |
| 《项目实施计划》 | 《设备采购清单》 | 《数据库设计方案》 | 《系统技术标准规划》 | 《系统试动行问题》  |
|          | 《项目集成方案》 | 《架构设计方案》  | 《UAT测试方案》  | 《系统移交手册》   |
|          |          | 《代码编写规范》  |            | 《系统运维手册》   |
|          |          | 《项目测试方案》  |            |            |



# 预算方案

投资项目	成本预估 (万)		
软件研发 (捷羿)	200	200	200
云服务	阿里云 65.863	腾讯云 77.557	华为云 104.1111
硬件 (加密机+开发机)	30	30	30
汇总	295.8	307.557	337.111

# 需要解决问题

## 加密机方案



加密机方案未定，设备采购清单、总集与部署方案难以最终定版。

## 云服务提供商



未确定云服务商，云部署的技术方案不能确定，使用的相关云产品不能确定。

## 设备及服务采购



开发设备及开发的云环境不具备，开发商无法进场。

谢谢