|  |
| --- |
| 密级：保密 |
| **iCloud-IOT**  **<企业版IOT平台设计>** |

**修订历史记录**

| 版本号 | 版本日期 | 修改者 | 说明 |
| --- | --- | --- | --- |
| V1.0.1 | 2018年12月10日 | iByte | * 企业架构说明 |
| V1.0.2 | 2019年1月23日 | iByte | * 业务能力开放 |
| V1.0.3 | 2019年2月11日 | iByte | * 资产转移至开放平台 |

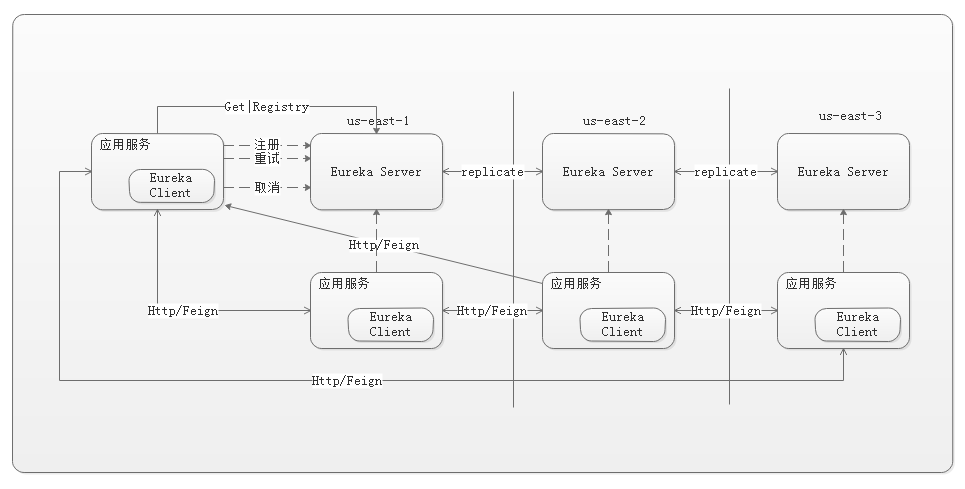
## 架构说明

基于IASS平台提供基础能力服务，IOT开放平台实现对外能力拓展和业务开放能力。业务聚合与资源整合实现业务开放平台化管理，达到"一云多端"，合作方自由平台管理、平台定制业务和自身业务系统拓展能力

### 注册中心

#### 工作原理

* 服务注册（Registers）、服务更新（Renewals）、服务取消（Cancels）,服务超时（Expirations）和服务状态变更（Status Changes）同步到集群的所有服务
* 新的Eureka Server节点加入集群后的影响
* 新服务注册(Register)注册时的影响
* 服务心跳(renew)配置，定时检查服务监控状态
* 服务下线和剔除机制，去除减少内部服务检查与和重试次数
* 自我保护模式，达到注册中心服务健康文档



注意事项：

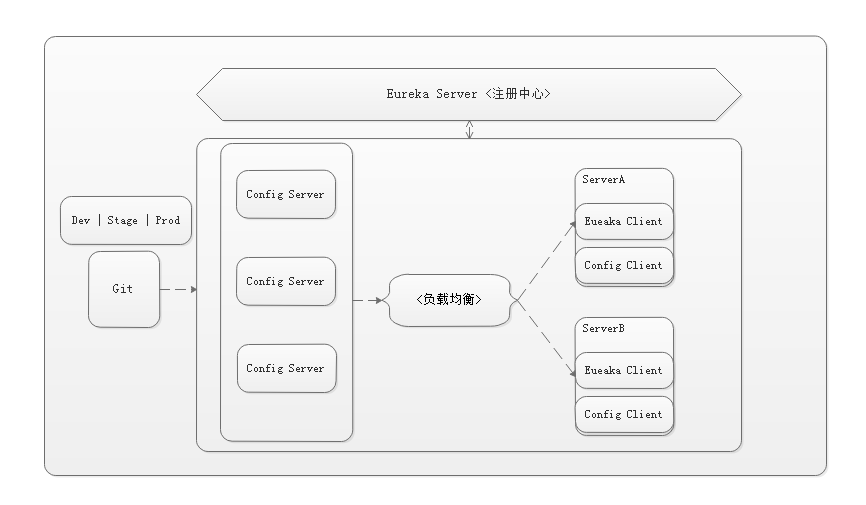
附：

* Eureka Server集群之间的状态是采用异步方式同步的，所以不保证节点间的状态一定是一致的，不过基本能保证最终状态是一致的
* 拉取服务间隔时间，服务心跳时间，自我保护模式，无效无法清理时间等相关配置查看配置文档

### 配置中心

#### 工作原理

* 通过配置服务(Config Server)来为所有的环境和应用提供外部配置的集中管理,这些概念都通过spring的Environment和PropertySource来抽象,所以他可以适用于各类Spring应用,它也能对应用的开发环境、测试环境、生成环境的配置做切换、迁移git服务器会从远程git拉取配置文件,并存入到本地git文件库,当远程git不可用时,会从本地git文件库拉取配置信息
* 配置信息依赖于，不支持跨集群和不同环境的数据隔离,数据更新基础基于spring-cloud-bus和webhook实现
* 不支持版本回滚和灰度发布后续切换为Apollo配置中心



注意事项：

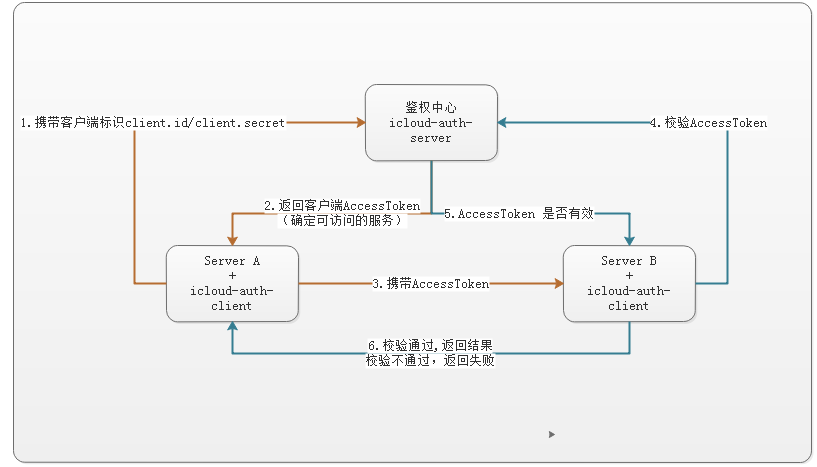
配置中心局限性

* 安全性：配置跟随源代码保存在代码库中，容易造成配置泄漏
* 时效性：修改配置，需要重启服务才能生效
* 局限性：无法支持动态调整：例如日志开关、功能开关

### 鉴权中心

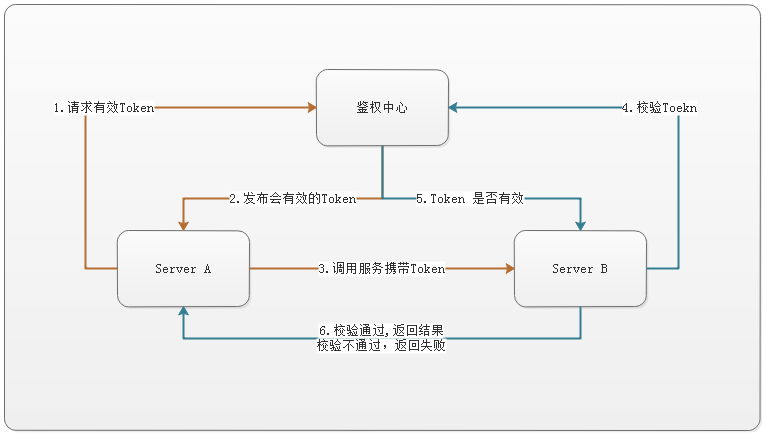
#### 客户端鉴权

* 微服务中,一般有多个服务,服务与服务之间相互调用时,有的服务接口比较敏感,比如资金服务,不允许其他服务随便调用,所以要进行服务调用的权限鉴定认证
* 客户端校验Token，解决服务划分治理与服务直接认证校验
* 服务治理解耦,对于开放，定制化业务,服务系统权限管理拼接

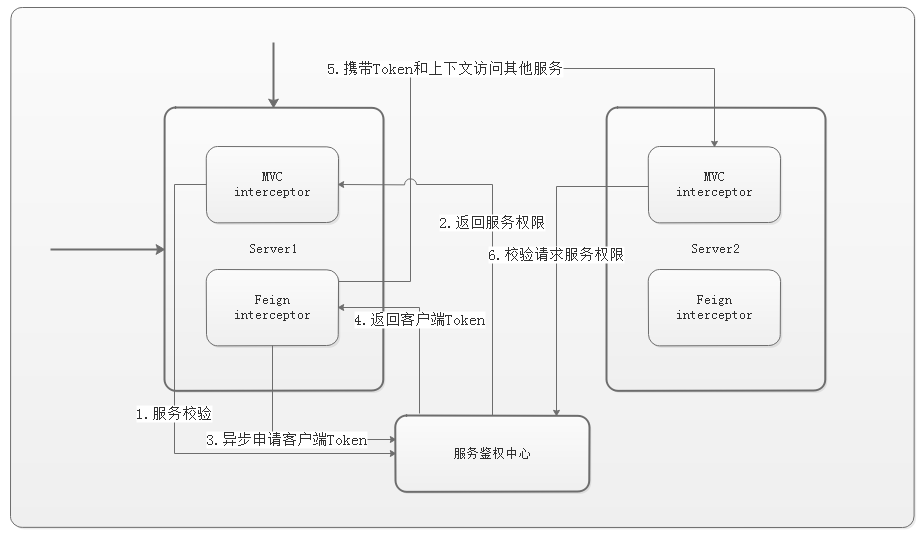


#### 用户鉴权

* 客户端请求服务时,根据提交的token获取用户信息,看是否有用户信息及用户信息是否正确
* 服务治理解耦,对于开放，定制化业务  
  如：短信、交易密码（类型有：只有密码面板 OR 带余额以及支付方式）、登录密码、指纹（TouchID）（目前仅仅适用于iPhone5S以上的用户）、上传资料审核、四要素鉴权（用户未绑卡，选择名字与身份证鉴权）、身份认证+银行卡信息确认



用户Token说明：

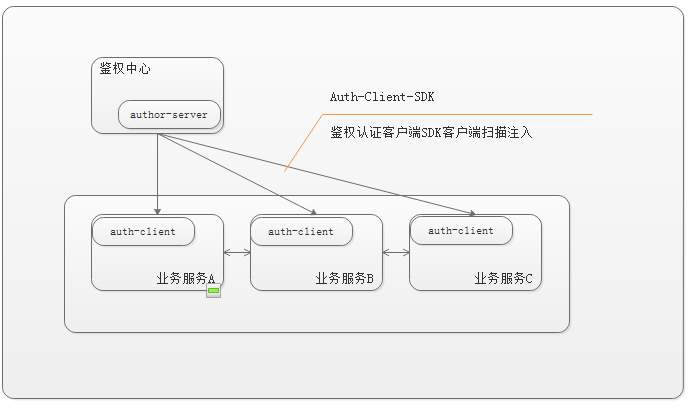


注：

被访问的服务，根据情况进行用户认证、服务认证。由 Request 的 Header 中携带

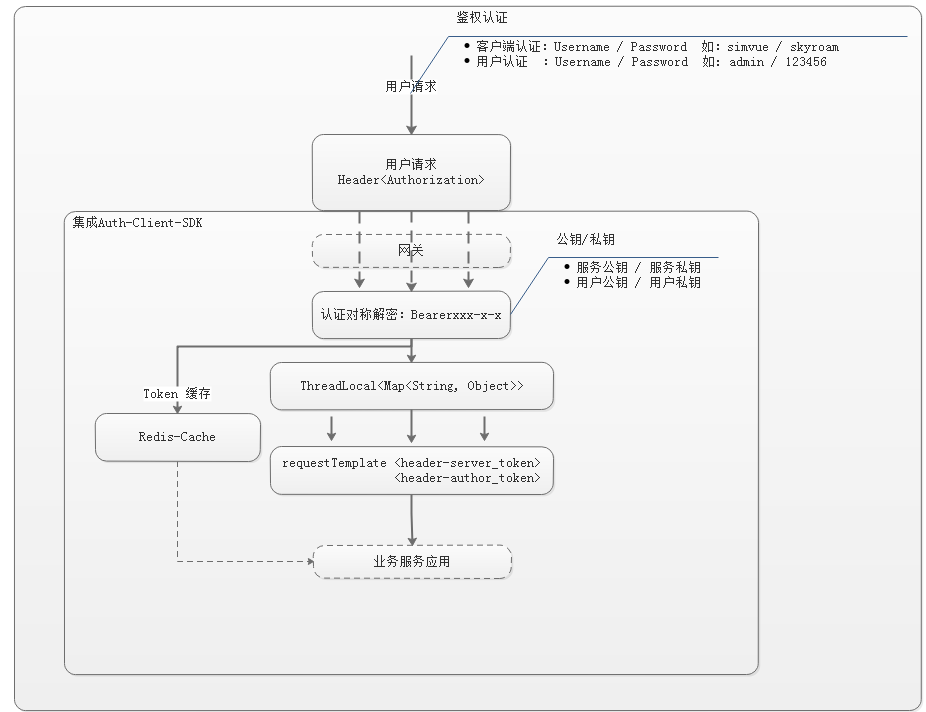
Authorization：用户认证token / client-token：服务认证token

#### 客户端认证SDK



客户端SDK说明：

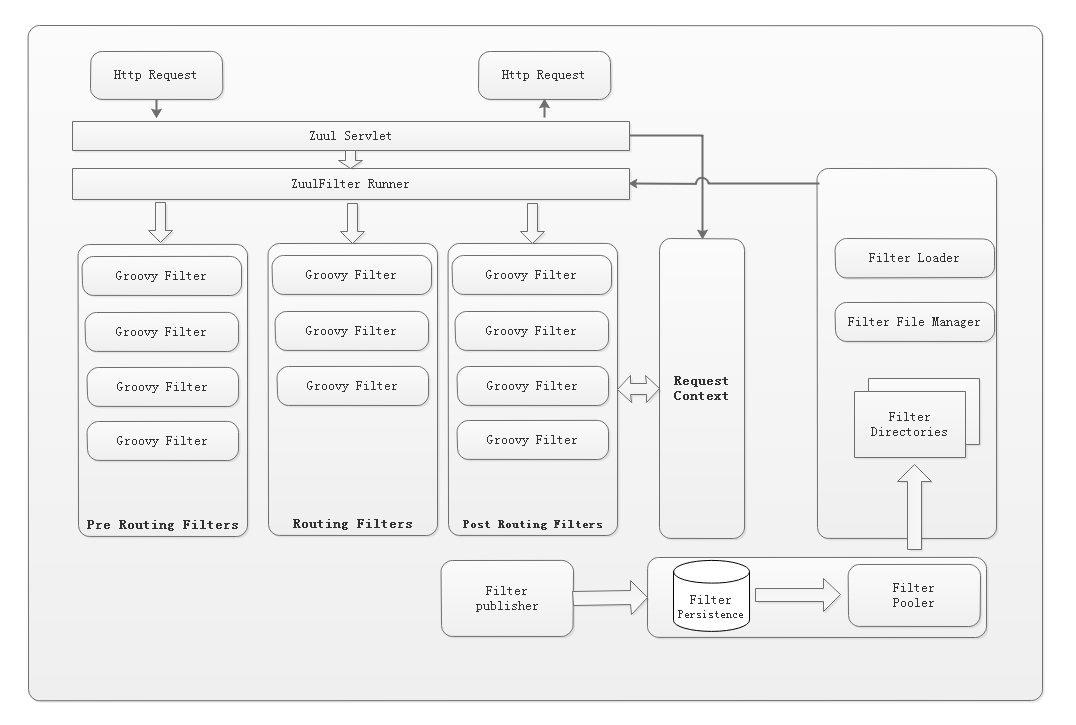
* 业务服务端集成认证SDK,对Token解密，数据权限(包含有效时间)、权限校验
* 自定义注解进行服务请求过滤拦截
* 用户认证token、服务认证tokenredis缓存与刷新机制



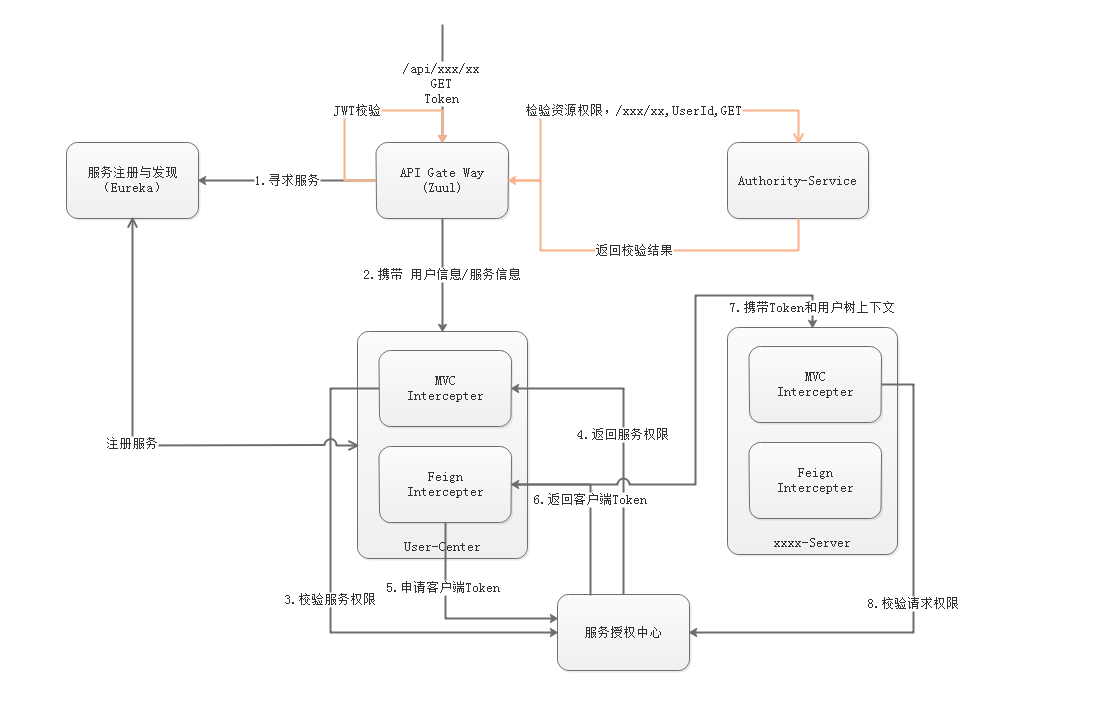
### 网关路由

Zuul在云平台上提供动态路由，监控，弹性，安全等边缘服务的框架。Zuul相当于是设备和 Netflix 流应用的 Web 网站后端所有请求的前门。

#### 工作原理



#### 流程步骤



* 默认所有的后端服务接⼝口都不不强制做认证校验的，即不不做⽤用户的token 和服务的token 认证
* 用户认证 @CheckUserToken、服务认证@CheckClientToken;   
  忽略用户认证@IgnoreUserToken忽略服务认证@IgnoreClientToken

简要说明:

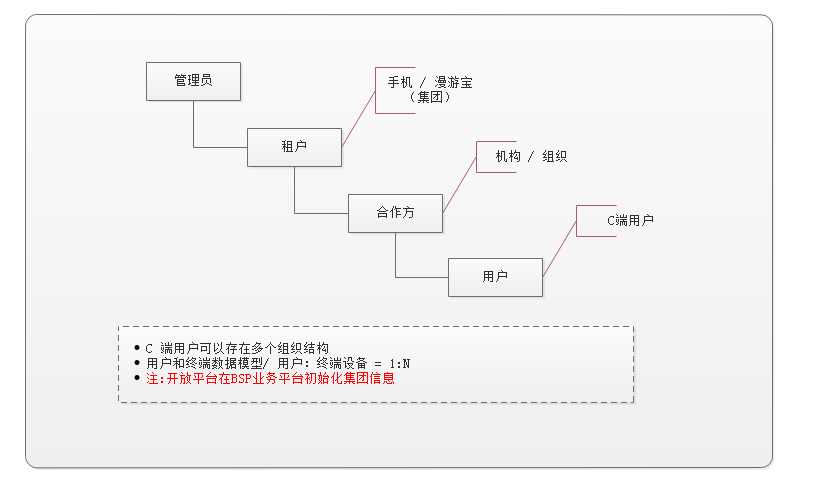
* 统一的系统入口
* 与服务治理框架结合，实现自动化的服务实例维护以及负载均衡的路由转发
* 统一的请求前置过滤，如：接口权限校验和签名比对等

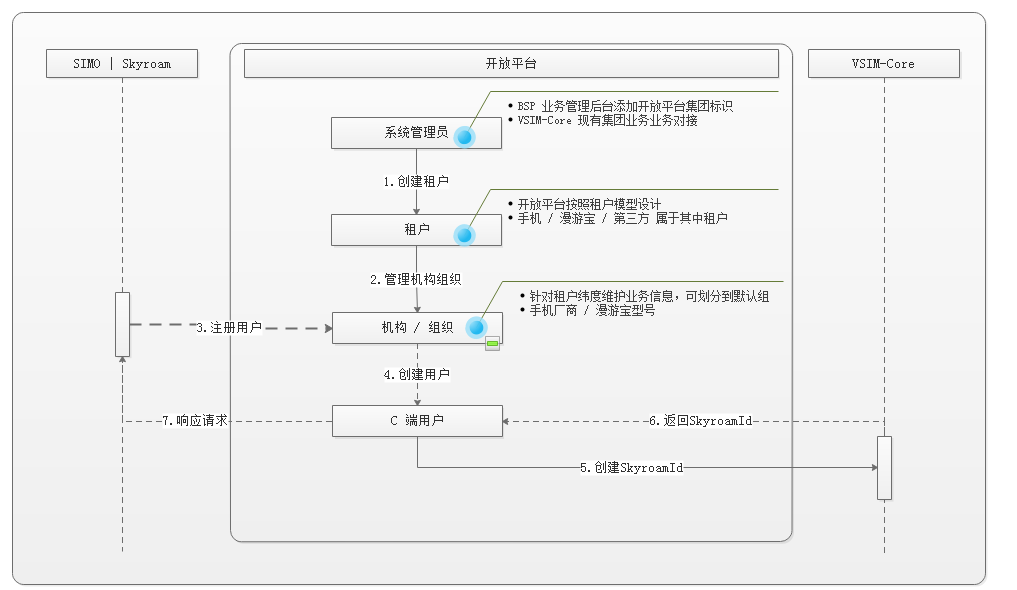
### 基础业务服务

#### 用户管理

##### 业务说明

* 开放平台以平台入租的设计理念设计，手机、漫游宝、第三方产品接入以租户身份管理相关内置业务
* 基于VSIM-CORE 原有业务调整，现有的BSP 系统需要在集团管理创建开放平台，满足现有的VSIM-CORE业务流程
* 客户端 / SIMO APP 注册用户，开放平台新建用户存入到默认组织或机构



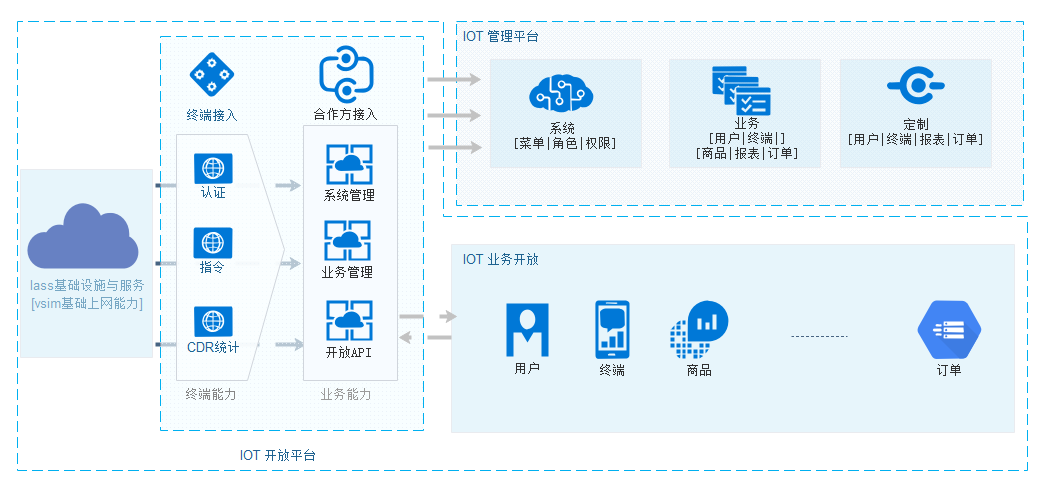


#### 菜单管理

#### 角色权限管理

### 字典服务服务

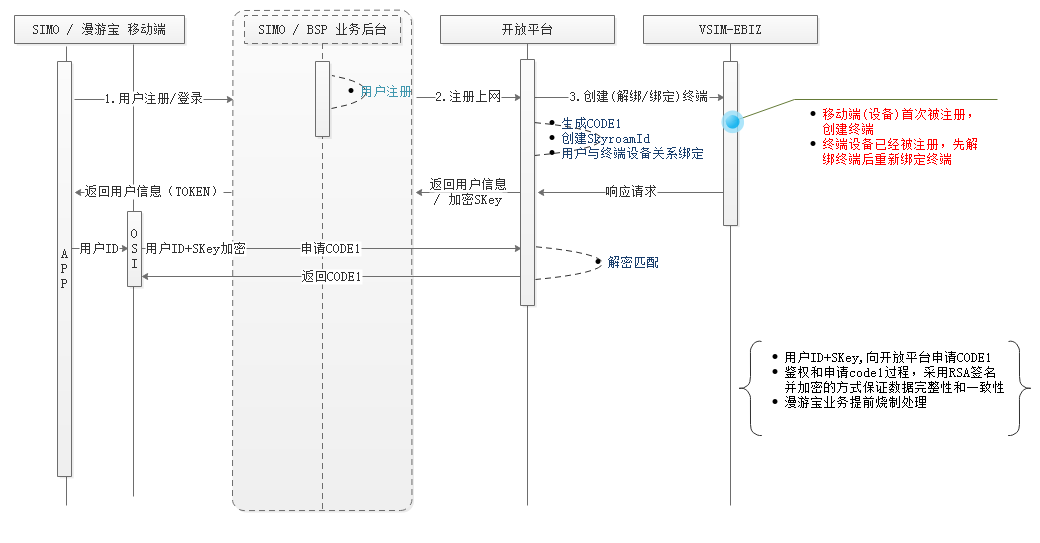
### VSIM业务中心



#### 终端管理

##### 业务说明

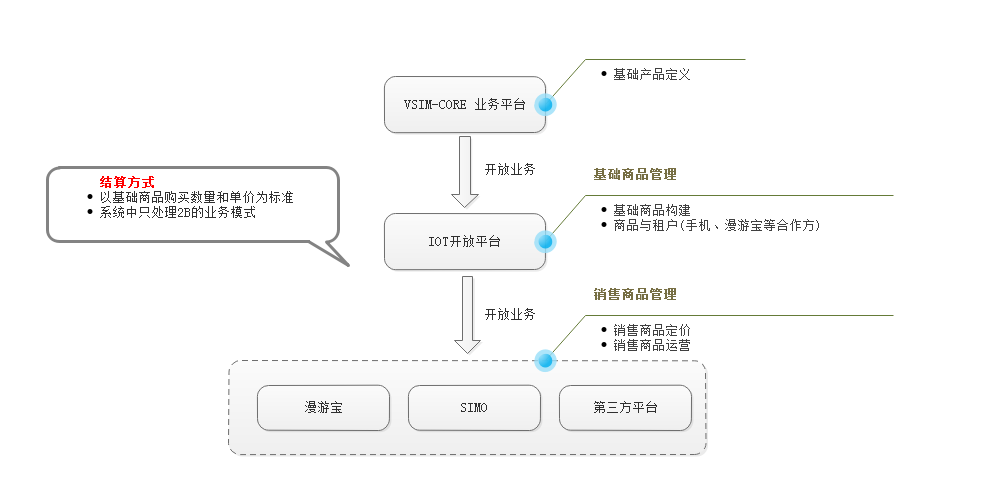
* 新用户注册时，先从开放平台获取SID与SKey，用于完成后续鉴权与申请code1
* 本地验证SID与SKey无问题后，移动端向开放平台发起连接，请求鉴权，同时申请code1。后续终端要与后台传输加密业务数据，是在以code1建立的加密通道内进行
* 鉴权和申请code1过程，采用RSA签名并加密的方式保证数据完整性和一致性。



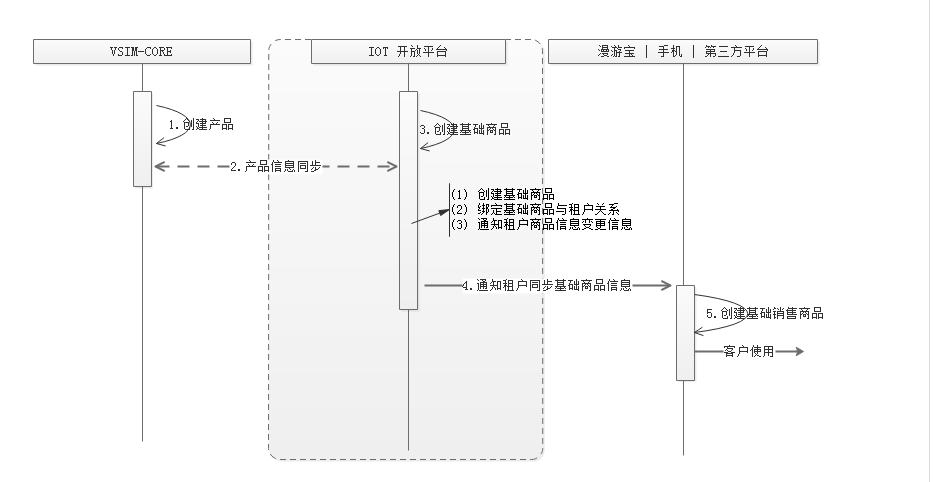
#### 商品管理

##### 基础产品管理

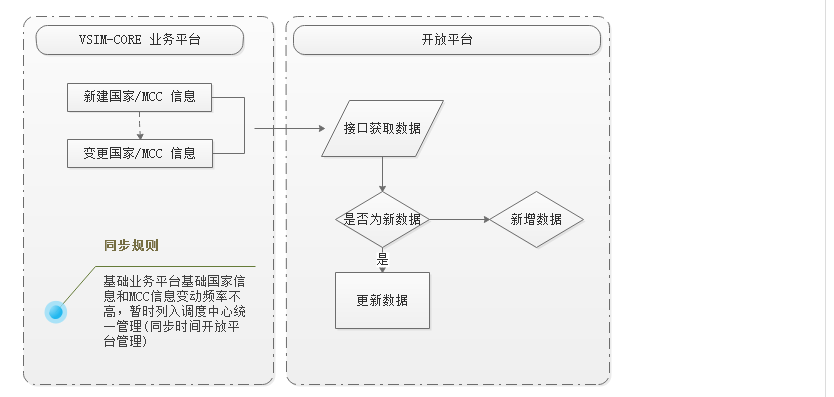
###### 业务说明



* VSIM-CORE 在业务平台创建基础产品信息，定义有效时间
* 全网流量、定向流量流量基于能力（开放平台基础能力+VSIM-CORE基础能力+业务平台附加能力）实现
* 开放平台同步产品信息
* 开放平台根据基础产品信息创建基础商品，绑定租户关系，相对应租户所相关的基础商品变更通知到对应租户业务管理平台
* 基础商品Flow决定用于那种终端产品
* 结算方式：对内事业部以使用流量为单位结算，接入方以套餐数量和“流量”为结算单位，实现第三方接入利益最大化



国家和mcc信息管理



* 业务说明

Vsim创建信息的国家和mcc信息，icloud-vsim主动定时同步vsim的国家和mcc的信息，时间间隔为1小时。

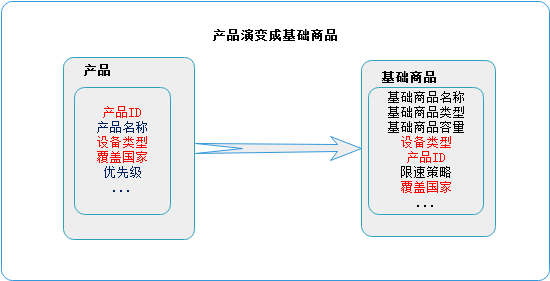
注意：因为主外键关系，同步mcc的任务要比同步国家的任务晚5分钟，确保国家信息先入库。

产品信息管理

* 实现同[国家和mcc 信息管理](#_国家和mcc信息管理)一样

##### 租户基础商品管理

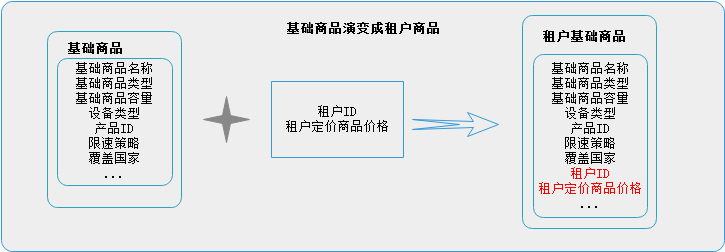
###### 业务说明



* 根据现有的一个产品创建对应一个基础商品，基础商品包含了产品的设备类型、覆盖国家等属性
* 基础商品类型包括：Data Plan / 流量套餐，DP/ Day Pass 套餐
* 一个产品已经建了一种商品类型的基础商品，不能再用这个产品建另外一种商品类型的基础商品（简之而言，一个产品不能创建2种类型以上的商品）
* 设备类型决定于哪款设备可使用
* 基础商品可上下架，不可物理删除

##### 租户定价商品管理

###### 业务说明



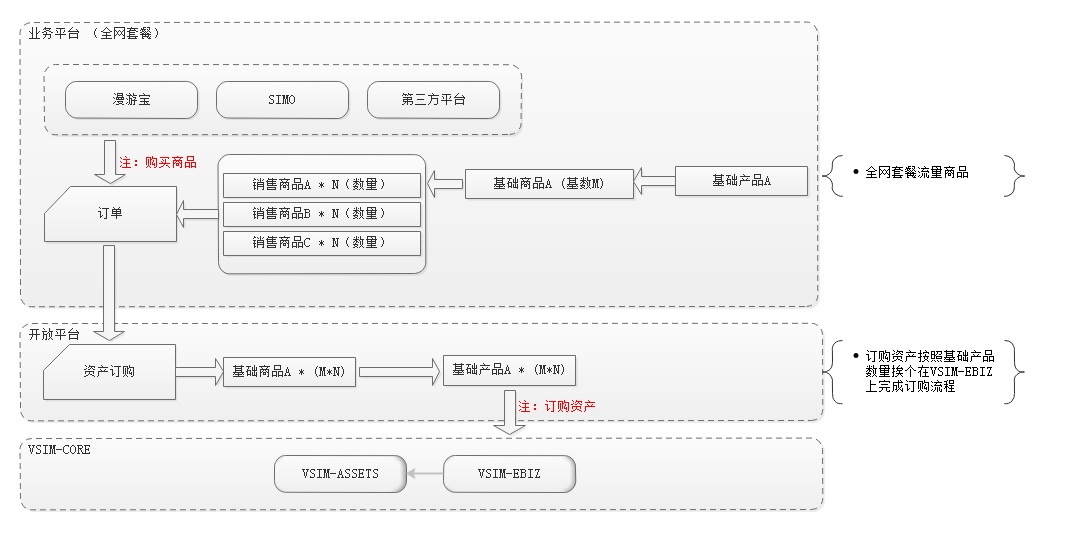
* 根据现有的基础商品信息，绑定租户并定价，租客即可查询到平台开放的基础商品
* 租户商品可上下架，不可物理删除
* 基础商品下架后，租户商品也会同时下架

#### 订单管理

#### 资产管理

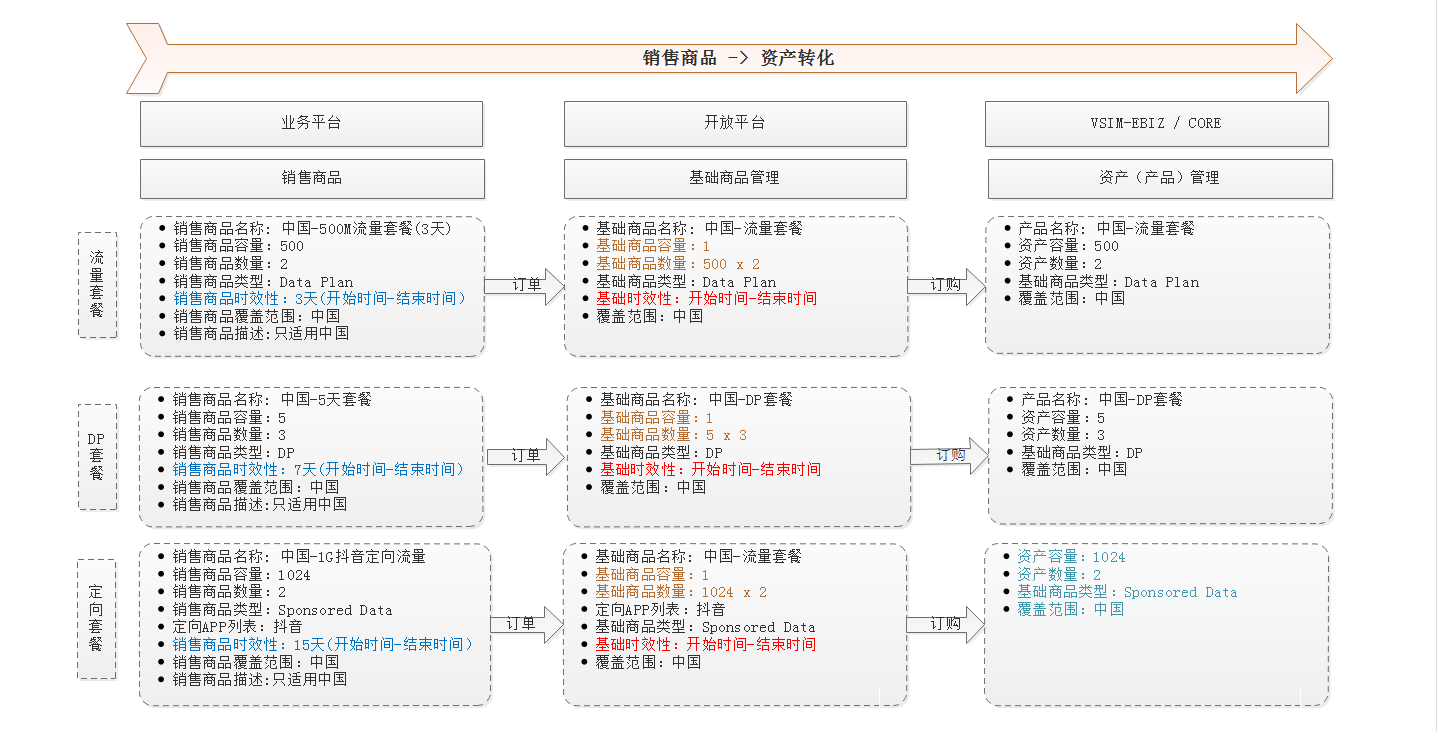


###### 业务说明



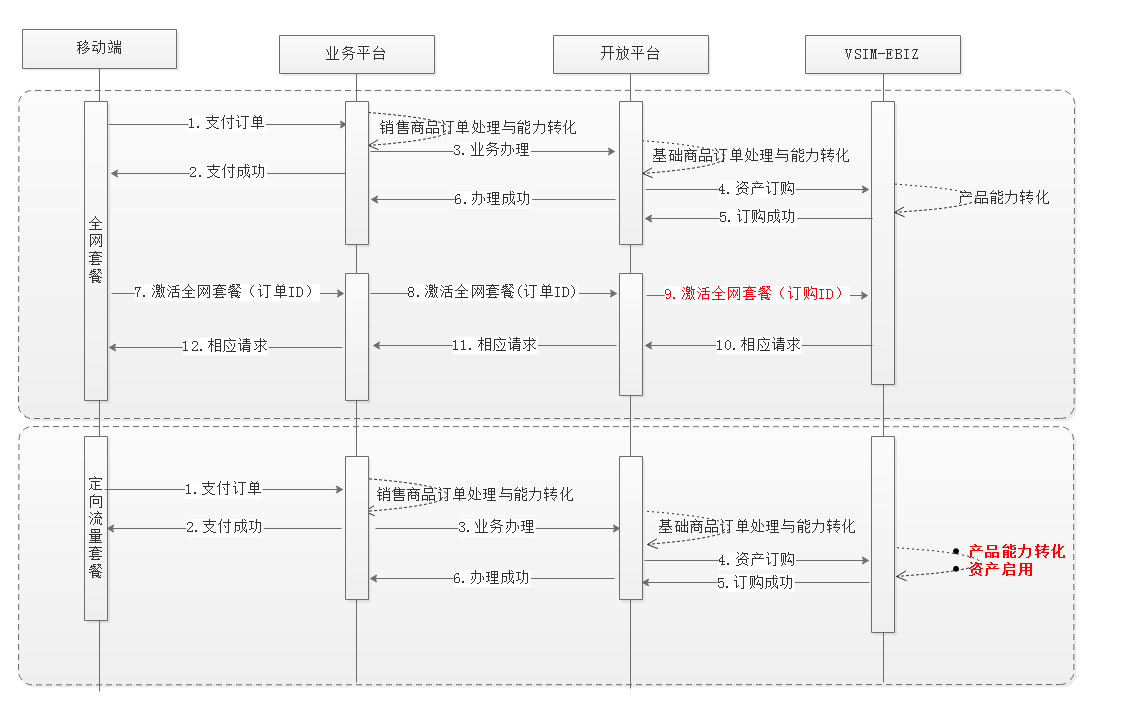
* 业务平台下了一个订单，购买了N个全网套餐，转换成M\*N个基础商品向开放平台起订购资产请求
* 开放平台接收到业务平台订购的请求，转换成M\*N个基础产品向VSIMCORE发起订购资产
* VSIMCORE接收到订购请求，给对应的用户订购资产

###### 资产转化



###### 资产激活

* 全网套餐（包含Data Plan / 流量套餐，DP/ Day Pass 套餐），购买后选择性激活
* 定向流量套餐（Sponsored Data）即买即用无需选择激活（后续有变动-可选择）



## 存储说明

## 数据库表字典

### 认证中心服务表设计

#### 数据模型

### 基础字典服务表设计

#### 数据模型



### 基础业务系统表设计

#### 数据模型



## 监控说明

### 基础服务链路监控(Zikpin)

## 服务架构说明

