**钱包O2O安全性设计**

**说明书**



华为技术有限公司

版权所有 侵权必究

修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 修订版本 | 修改描述 | 作者 |
| 2015-08-03 | v1.0 | 初稿 | 夏潘斌 |
| 2015-08-19 | v1.1 | 全文修订 | 夏潘斌 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目 录

[1 简介 7](#_Toc427847562)

[1.1 范围 7](#_Toc427847563)

[1.2 特性概述 7](#_Toc427847564)

[1.3 假设和约束 7](#_Toc427847565)

[2 Low Level威胁分析 8](#_Toc427847566)

[2.1 2层数据流图 8](#_Toc427847567)

[2.2 典型业务流程 9](#_Toc427847568)

[2.2.1 华为自有商品促销业务流程 9](#_Toc427847569)

[2.2.2 合作商户商品促销业务流程 10](#_Toc427847570)

[2.3 业务场景及信任边界说明 11](#_Toc427847571)

[2.3.1 典型业务场景 11](#_Toc427847572)

[2.3.2 信任边界说明 13](#_Toc427847573)

[2.4 外部交互方分析 13](#_Toc427847574)

[2.4.1 运营人员 13](#_Toc427847575)

[2.4.2 合作商户 16](#_Toc427847576)

[2.4.3 钱包APP 18](#_Toc427847577)

[2.4.4 CDN服务 20](#_Toc427847578)

[2.4.5 华为UP 20](#_Toc427847579)

[2.4.6 支付服务器 22](#_Toc427847580)

[2.4.7 收货地址服务器 23](#_Toc427847581)

[2.4.8 Push网关 24](#_Toc427847582)

[2.5 数据流分析 25](#_Toc427847583)

[2.5.1 与合作商户的数据流 25](#_Toc427847584)

[2.5.2 与钱包APP的数据流 26](#_Toc427847585)

[2.5.1 与CDN的数据流 28](#_Toc427847586)

[2.5.2 与支付服务器的数据流 29](#_Toc427847587)

[2.5.3 与UP的数据流 30](#_Toc427847588)

[2.5.4 与收货地址服务器的数据流 31](#_Toc427847589)

[2.5.5 与PUSH网关的数据流 33](#_Toc427847590)

[2.6 处理过程分析 34](#_Toc427847591)

[2.6.1 业务服务器 34](#_Toc427847592)

[2.6.2 分发服务器 37](#_Toc427847593)

[2.6.3 Portal服务器 40](#_Toc427847594)

[2.7 数据存储分析 43](#_Toc427847595)

[2.7.1 业务配置数据与日志 43](#_Toc427847596)

[2.7.2 MYSQL数据存储 46](#_Toc427847597)

[2.7.3 NFS共享文件存储 48](#_Toc427847598)

[2.7.4 REDIS缓存 49](#_Toc427847599)

[2.8 隐私设计规范Checklist自检 50](#_Toc427847600)

[2.9 缺陷特性汇总 51](#_Toc427847601)

[3 安全需求设计 51](#_Toc427847602)

[3.1 2015年8月安全需求设计 51](#_Toc427847603)

[3.1.1 签名字段算法要求从sha1增强到sha256 51](#_Toc427847604)

[3.1.2 意见反馈页面没有任何接入认证 51](#_Toc427847605)

[3.1.3 NFS的root权限修改 51](#_Toc427847606)

[3.1.4 Coverity扫描结果高、中风险项的清理 52](#_Toc427847607)

[3.2 2015年9月安全需求设计 52](#_Toc427847608)

[3.2.1 物理组网不能有单节点故障求 52](#_Toc427847609)

[3.2.2 Mysql数据库、Redis、Portal用户名和密码强度要求 52](#_Toc427847610)

[3.2.3 用户敏感数据加密存储&日志匿名化 53](#_Toc427847611)

[3.2.4 敏感信息加密算法的整改 53](#_Toc427847612)

[3.2.5 与应用客户端的认证鉴权 53](#_Toc427847613)

[3.2.6 软件版本的一致性，涉及升级完整性保护 54](#_Toc427847614)

[3.2.7 日志打印&日志保存策略管理 54](#_Toc427847615)

[3.2.8 新增订单接口采用sha256签名 54](#_Toc427847616)

[3.2.9 限制CDN访问NGIN的权限 54](#_Toc427847617)

[3.2.10 与Vmall的接口存在sha1的签名 54](#_Toc427847618)

[3.2.11 口令输入支持键盘安全控件。 55](#_Toc427847619)

[3.2.12 对于管理员分角色并赋予不同的管理权限，最小化权限原则. 55](#_Toc427847620)

[3.2.13 业务系统放DDos攻击 55](#_Toc427847621)

[3.3 安全红线 55](#_Toc427847622)

[3.3.1 安全红线要求 55](#_Toc427847623)

[3.4 应用安全 56](#_Toc427847624)

[3.4.1 应用安全要求 56](#_Toc427847625)

[4 各模块的分配需求 56](#_Toc427847626)

[5 各模块的接口描述 57](#_Toc427847627)

[6 备注和附录 57](#_Toc427847628)

[6.1 数据字典 57](#_Toc427847629)

[6.1.1 数据字典列表 57](#_Toc427847630)

Keywords 关键词：钱包 O2O 安全性

Abstract 摘要：

术语和缩略语清单：

| 术语/缩略语 | 描述 |
| --- | --- |
| O2O (Online To Offline) | 线上线下 |
| NFS |  |
| CDN |  |
|  |  |

# 简介

## 范围

云平台业务云涉及产品众多，比如钱包O2O、会员服务、音乐、视频、亲情关怀、手机服务等应用。

本文描述了钱包O2O产品服务端的安全性设计及其实现方案, 钱包O2O服务器与各业务模块之间的交互关系和影响范围如下所示：



## 特性概述

O2O服务器打造用户中心生活服务公共能力，通过集成或独立预置的方式落地到华为EMUI中，从而吸引更多用户并提升产品竞争力。

## 假设和约束

* **软件版本**

在部署O2O服务环境时必须满足以下软件版本：

| 软件列表 | 详细版本说明 | 备注 |
| --- | --- | --- |
| JDK | 1.7.0\_55 |  |
| DB | MYSQL：5.6.13 |  |
| REDIS | 2.8.20 |  |
| TOMCAT | 7.0.52.0 |  |

* **接口协议**

O2O与华为内部各部件的接口为http，与第三方商户域的为HTTPS；

接口求和响应报文都必须采用UTF-8编码。

# Low Level威胁分析

## 2层数据流图

O2O服务器的2层数据流图如下所示：



说明：

O2O服务器保存订单记录的目的是为了在客户端给用户展示消费信息，同时也是为BI进行统计分析提供数据。

数据流图元素及说明如下表所示：

|  |  |  |
| --- | --- | --- |
| ***元素*** | ***符号*** | ***描述*** |
| *外部交互方* |  | *能驱动系统业务，但不受系统控制的人和物(如用户，管理员，第三方系统等).通常表示目标系统的输入/输出* |
| *处理过程* |  | *一个过程执行一个任务时的逻辑表示，例如Web Server 、ftp server、LMT server* |
| *数据存储* |  | *数据存储表示文件、数据库、注册表项、内存等* |
| *数据流* |  | *数据在系统中的移动方向，如网络通讯、共享内存、函数调用等。* |
| *信任边界* |  | *当数据流穿越不同的信任级别(区域)时，就存在信任边界，例如从用户态到内核态，从客户端到服务端等。* |

## 典型业务流程

### 华为自有商品促销业务流程

以莫赛尔红酒为例，华为自有商品端到端的促销业务流程如下所示：



### 合作商户商品促销业务流程

以美团美食为例，第三方商户商品端到端的促销业务流程如下所示：



## 业务场景及信任边界说明

### 典型业务场景

O2O服务器的业务场景分为如下几类：

1. 运营人员O2O营销业务

* 首页管理(惠生活/NFC/负一屏)

运营人员通过管理门户配置各个机型展示的页面样式，荣耀钱包用户登录钱包应用后向服务器发起请求以获取最新的首页配置信息。

* 合作商户产品促销活动

运营人员制作HTML 5静态资源，并通过Portal上传到共享文件服务器，运营人员配置对应的业务APP跳转信息和首页信息，终端用户最后点击钱包APP的广告部分获取该静态HTML5资源并做对应的处理(可能会同步订单信息过来)。

* 华为自有产品促销活动

目前主要为华为手机优购码业务和1分钱促销业务，对于1分钱促销任务的流程如下：

首先服务器端预置1分钱的产品到服务器数据库中；

其次，运营人员通过Portal配置活动相关的静态资源；

运营人员配置首页广告，使得荣耀钱包APP能访问到静态广告资源；

用户点击1分钱广告页发起订购，并完成支付；

支付系统同步订单信息到O2O服务器;

1. 合作商户管理和订单管理

* 合作商户及其产品管理(信息管理和接入认证管理)

运营人员在管理门户Portal上配置合作公司的基本信息，终端钱包用户通过获取首页信息接口获取这些配置的信息并在界面显示。运营人员对于公司基本信息的操作有：增、删、改、查。

* 订单同步及订单查询

华为惠生活有很多合作商户，例如美团、大众点评等，华为荣耀钱包为其提供一个分发业务的渠道。当荣耀钱包用户通过荣耀钱包入口进入美团首页后，用户在美团进行各种订购、支付等功能，其中当用户在美团发生订购行为后，美团会将这些信息同步到华为的O2O服务器，用于信息统计汇总。

1. O2O理财业务

* 理财首页配置管理

运营人员通过VPN接入到O2O服务器的Portal，配置理财的应用、容器、首页这三层信息， 荣耀钱包APP用户进入到精品理财入口调转到精品理财的首页.

* 理财公司管理

理财作为荣耀钱包的一个重点业务，理财公司的信息较O2O其他合作商户的信息要多一些，所以针对理财公司专门制作了一个理财公司管理的业务。运营人员通过VPN，使用浏览器在O2O管理Portal上进行理财公司的增、删、改、查操作。荣耀钱包用户通过获取理财公司列表的接口获取配置的所有理财公司信息。

* 理财公司产品管理

合作理财公司通过O2O服务器开放的数据同步接口，将其旗下的理财产品信息同步到O2O服务器。例如，对于兴业银行，其旗下的理财产品有产品A、产品B和产品C，这些产品本身在O2O服务器不提供录入功能，都是开放接口给理财公司自行管理。荣耀钱包APP用户进入精品理财首页即可获取这些产品的信息。

* 理财公司个人收益信息管理

合作理财公司通过O2O服务器开放的数据同步接口，将使用华为账户购买其理财产品的用户收益信息同步到O2O服务器。O2O服务器接收到这些用户数据后保存到后台文件系统，并将最近一周的信息存储到数据库中。荣耀钱包用户可以通过O2O服务器开放的查询接口查看昨日收益信息。

1. 华为自有商品促销业务

* 华为自有商品管理(增/删/改/查)

目前华为自有商品作为O2O业务的一种，主要提供：莫塞尔红酒、手机预购、手机优购码、1分钱活动等产品。运营人员通过VPN访问O2O的门户Portal进行产品分类配置，产品配置和产品支付渠道配置。

* 华为自有商品分类管理

荣耀钱包APP用户获取华为商品列表和商品详情，接着向O2O服务器发起订购业务，订购成功后向华为支付服务器发起支付，支付成功后支付服务器会将支付结果信息反馈给O2O服务器并更新订单状态。

* 华为支付渠道管理
* 华为自有商品订单管理

1. 用户经营类业务

* 权益管理

运营人员针对机型配置对应的权益信息，权益的产生可以是针对特定机型的，也可以是通过购买优购码以后产生的权益。荣耀钱包APP用户通过点击“我的权益”跳转到对应权益领取页面并进行领取权益操作。对应领取余额的操作，荣耀钱包APP会发送消息到O2O服务器，O2O服务器将发送消息给支付服务器进行实际的支付。

* 消息管理

用于参与荣耀钱包业务，例如购买手机，该过程会促发某些用户有中奖的消息。用户点击“我的消息”后依据消息的设置进行消息处理。

* 信息反馈

用户通过荣耀钱包APP向O2O服务器提交信息反馈。

### 信任边界说明

1. 信任边界

信任边界涉及华为域的内部部件，包括UP、收货地址服务器、支付服务器和Push网关

1. 非信任边界

第三方商户的服务器和CDN、应用客户端与O2O服务器都存在边界信任问题；

运营人员通过浏览器来配O2O的数据，存在信任边界，目前现网通过VPN方式访问，提升了安全性；

## 外部交互方分析

针对数据流图中外部交互方进行威胁分析，外部交互方需要分析仿冒和抵赖两种威胁.

### 运营人员

|  |  |  |
| --- | --- | --- |
| 元素名称 | 运营人员 | |
| 元素概述 | 运营人员通过VPN登陆管理Portal进行首页配置，理财业务配置，商品管理，合作商户管理，营销活动等基本操作。 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | 级别：中  影响：如果仿冒人员绕过VPN、破解口令进入管理门户，那么O2O的首页和理财首页数据可能被乱修改导致业务不可用，另外对于理财公司KEY等敏感信息会泄露，该用户甚至可以修改Portal管理员的密码，导致真正的管理员不可用。  可能性：  用户必须获取如下信息才能发起攻击：   1. 用户获取访问的VPN账户 2. 用户通过VPN接入后能够获取O2O Portal的用户名和对应的密码。 |
| 已有消减措施 | 1. 传输通道加密和访问控制  用户必须通过VPN通道才能接入网络，并操作O2O的  管理门户，也就是传输通道被加密；  2. 用户认证  系统不存在特殊方式直接访问系统，用户必须通过用户名和密码来登录。  3. 口令管理   1. 口令复杂度已按照安全要求进行限制、默认口令首次登陆时必须重新修改密码、口令使用SHA256(userName+pawd)加密存储、密码验证操作数据库时使用了预编译防止SQL注入、密码过期失效、修改密码时需要口令确认。 2. 输入口令使用“.”代替明文、口令输入域不允许拷贝、不支持记住密码功能、日志中未打印口令明文。   4. 会话管理   1. 会话标识必须使用安全随机数算法生成，且有效长度不低于247个字符，至少保证64bit的完全随机 2. 用户名和口令认证通过后，必须更换会话标识 3. 必须使用cookie 用于维持会话 4. 会话cookie的属性要设置为HttpOnly 5. 通过在服务器上使用访问控制，保护服务器端会话数据免受服务器其他用户的未授权访问 6. 必须使用会话Token对敏感或关键的操作进行校验，会话Token必须使用安全随机数算法生成、有效长度不低于24个字符，且需要设置有效期 7. 会话使用过程中，会话信息必须在服务器端存储和维护 8. 服务器需要结合sessionid、IP地址以及其他的会话信息对每一个会话进行身份校验，判断该会话是否合法 9. 禁止在URL、错误信息或日志中暴露会话标识符 10. 所有登录后才能访问的界面都必须提供主动退出501、选项，当用户退出时，服务器端必须清除该用户的会话信息 11. 必须设置会话超时机制，在超时过后必须要清除该会话信息   **5. 防暴力破解措施**   1. 采用识别码，使用“验证码识别”工具（1.4版本）进行测试，工具识别率低于5%   验证码.png   1. 密码连续输入失败次数达到阀值则锁定账号 |
| 建议消减措施 | 1. 口令存储建议使用PBKDF2，建议盐值至少选取8字节（64bit完全随机）且每个用户不同，PBKDF2算法默认至少迭代50000次。用户修改口令时，系统自动更换盐值。  2. 口令输入支持键盘安全控件。  3. 对于管理员分角色并赋予不同的管理权限，最小化权限原则. |
| 产品落地计划 | 9月份版本 |
| 抵赖（R） | 风险（Risk） | 级别：中  运营人员操作错误或者恶意操后抵赖，会造成无法迅速确认操作的影响范围和审计操作者。  可能性：  1，重复的日志也会被记录，若存储空间满只能通过运维人员手工方式删除操作日志文件；  2，运营人员操作日志数据库存储篡改数据，未考虑其完整性校验；  3，日志备份文件没有备份策略或者只是存放在文件服务器上，未对防篡改、防删除、保留期限做严格管理控制。 |
| 已有消减措施 | 1. 用户认证  用户的操作必须拥有合法的用户名密码才能进行操作.  2. 操作日志  所有登陆用户的操作，涉及修改、删除、增加的变更操作都必须记录详细的操作日志。操作日志包括操作者、操作时间、操作内容、操作结果。  3. 操作日志存储访问控制和定期备份  严格控制操作日志访问权限，当前只有运维才有权限进行访问和清理操作。运维人员定期备份操作日志。 |
| 建议消减措施 | 合理安排日志文件备份周期，控制访问权限，并对备份日志文件进行完整性保护，防止被篡改。 |
| 产品落地计划 | 计划落地9月份版本 |

### 合作商户

|  |  |  |
| --- | --- | --- |
| 元素名称 | 合作商户 | |
| 元素概述 | 合作商户通过钱包入口导流到商户的门户来向终端用户提供服务。  理财公司作为合作商户之一，其合作模式和普通的O2O商户存在不同的地方。合作理财公司需要定期同步理财产品信息、理财收益信息到O2O服务器。 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | 级别：中  影响：  如果第三方合作商户被冒充，那么假冒的商户可能会发送不存在的订购信息到O2O服务器，那么钱包用户实际没有做线下操作，但是在荣耀钱包的“惠生活”记录里面会查到该信息，会对用户照成不必要的误解。用户本身的利益没有照成任何损失，但是被假冒的商户将在按比例结算时收到影响。  可能性：  目前传输通道采用HTTPS，并且对消息进行鉴权认证，攻击者只有发起成功的SSL攻击和破解摘要密码才能突破防线。 |
| 已有消减措施 | 1、传输通道加密  采用HTTPS进行数据加密传输  2、通过签名进行认证鉴权   * 签名算法   只有用商户标示channelCode和对应密码生成签名通过认证后才能够调用钱包O2O的接口。  其中参数签名=hmac-sha256(key, content)  Key为O2O服务器给商户分配的秘钥，而channelCode和channleName为商户从开发者联盟申请的。  Content=channelCode+channelName+operateTime；   * 认证步骤   商户根据华为确定的消息认证的方案，明确其生成的签名参数；  然后，在调用O2O服务器接口时， 携带签名参数和相应的接口字段到O2O；  O2O服务器同样生成对应的签名，核对是否与携带过来的是否一致；  3、对于合作O2O商户增加IP白名单限制 |
| 建议消减措施 | 无 |
| 产品落地计划 | 无 |
| 抵赖（R） | 风险（Risk） | 级别：低  影响：  如果合法的第三方合作商户恶意发送订购信息到O2O服务器，在用户的消费记录查询页面里会有信息而影响用户体验；同时，如果该订单涉及结算费用， 那么将会增加商户的损失。  可能性：  由于该操作对于第三方商户没有带来好处，反而可能会增加商户的结算费用（商户付钱给华为），因此该攻击可能性很低。 |
| 已有消减措施 | 1. 对于商户的接口提供日志信息 |
| 建议消减措施 | 1、增加审计功能，所有关键信息录入审计库  审计信息包含：合作商户信息、渠道码信息、操作时间、购买用户信息等关键字段。 |
| 产品落地计划 | 计划在9月份实施 |

### 钱包APP

|  |  |  |
| --- | --- | --- |
| 元素名称 | 钱包APP | |
| 元素概述 | 钱包APP为终端用户提供服务。 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | 级别：低  影响：  如果钱包APP被仿冒，即意味着身份认证系统失效，攻击者可以利用仿冒的身份查看、操作该用户所有业务数据会造成用户隐私数据泄露，利用被仿冒用户购买商品造成财产损失。  可能性：  用户能进入华为账户和UP系统窃取用户信息，或者破解SSL登陆过程获取明文信息。  恶意程序模拟用户通过客户端向服务器发送请求，类似CSRF跨站请求伪造。 |
| 已有消减措施 | 1、携带用户身份标识的请求，全部通过https方式传输请求和响应报文。  2、钱包服务器访问UP登陆鉴权接口对用户登陆状态进行鉴权，鉴权通过才能进行业务操作。获取缺省首页信息接口不需要对用户的登陆状态进行鉴权，而其它的接口必须对用户的登陆状态进行鉴权。钱包O2O服务器要求校验时保证userID和ST两个参数全部传入且不能为空，从而保证需要鉴权的接口不会绕过鉴权机制。  3、用户在客户端上的身份验证由UP保证，分析参考UP输出。 |
| 建议消减措施 | N/A |
| 产品落地计划 | N/A |
| 抵赖（R） | 风险（Risk） | 级别：低  影响：  合法的终端用户登录荣耀钱包进行的各项操作都是其自身完成的，不会对业务操作产生影响。  可能性：  手机被其他人员窃取使用。 |
| 已有消减措施 | 无 |
| 建议消减措施 | 1. 对于关键操作增加用户行为日志功能，保存一定时间内的用户操作信息。主要是用户的订单日志信息。 |
| 产品落地计划 | 计划在9月份落地。 |

### CDN服务

|  |  |  |
| --- | --- | --- |
| 元素名称 | CDN服务 | |
| 元素概述 | 访问O2O的静态资源服务器。 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | 级别：中  影响：  如果CDN服务被仿冒，将会从O2O服务器获取一些配置信息，这些数据是公开的，不会造成影响。比如运营活动的图片。  可能性：  静态资源本来公网就可以访问，只能获取不能修改。 |
| 已有消减措施 | 无 |
| 建议消减措施 | 1. 建议对资源服务器进行最小化权限配置，例如CDN网络如果只需要HTTP的Get请求，那么将限制CDN请求的类型，比如post、put等操作将被限制。 |
| 产品落地计划 | 计划在9月份落地。 |
| 抵赖（R） | 风险（Risk） | 不涉及。 |
| 已有消减措施 | 不涉及。 |
| 建议消减措施 | 不涉及。 |
| 产品落地计划 | 不涉及。 |

### 华为UP

|  |  |  |
| --- | --- | --- |
| 元素名称 | 华为UP系统 | |
| 元素概述 | O2O服务器对终端用户发起的请求进行认证的系统。 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | 级别：低  影响：  如果UP服务器被仿冒   1. 会导致用户个人数据被收集，从而导致个人用户的数据泄密。 2. 会导致用户登陆鉴权失效，无法识别用户的登陆状态。 3. 会导致用户与设备之间的绑定关系错误，导致会员系统无法识别用户终端等级，从而展示错误的权益数据给用户。   可能性：   1. hosts文件被修改，导致域名解析的IP地址指向仿冒的UP服务器 |
| 已有消减措施 | 1. 运维已确认，只有Root用户和业务用户具有修改hosts文件的权限，无其他策略 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 抵赖（R） | 风险（Risk） | 级别：低  影响：  UP只是做华为用户信息的认证授权，没有实质性的影响；  可能性：  UP服务器实际上是华为实现的系统的一部分，因此在消除了仿冒威胁的前提下，不存在向O2O服务器抵赖的问题。 |
| 已有消减措施 | 1、O2O服务器侧提供交互日志 |
| 建议消减措施 |  |
| 产品落地计划 |  |

### 支付服务器

|  |  |  |
| --- | --- | --- |
| 元素名称 | 支付服务器 | |
| 元素概述 | 对于华为自有商品，用户通过终端APP发起订购并完成支付后，支付服务器将把订单状态信息同步到O2O服务器，O2O服务器收到后会更新订单状态。 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | 级别：中  影响：  如果支付服务器被伪造，那么就会对于用户该买商品的交易造成实际的影响，比如实际没有支付成功也返回支付完成，从而造成财务损失。  可能性：  恶意用户绕过鉴权和SSL，理论上可能发生上述行为。 |
| 已有消减措施 | 1. 传输通道经过SSL加密  2. O2O服务器对于支付服务器进行用户名和密码的认证 |
| 建议消减措施 | N/A |
| 产品落地计划 |  |
| 抵赖（R） | 风险（Risk） | 级别：低  影响：如果支付服务器发送恶意信息，那么就会同步不存在的订单信息到O2O服务器数据库，华为钱包用户就会看到自己根本没有发生过的订购记录，但是由于这些记录不是真实发生的，所以不对用户利益造成重大损失。 |
| 已有消减措施 | 对于接口调用，已经记录了业务日志。 |
| 建议消减措施 |  |
| 产品落地计划 |  |

### 收货地址服务器

|  |  |  |
| --- | --- | --- |
| 元素名称 | 收货地址服务器 | |
| 元素概述 | 收货地址服务器用于存储云平台业务下所有用户的收货地址  对于华为自有商品，用户通过终端APP发起产品购买， 需要接入收货地址服务器来获取用户的收货地址。 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | 级别：低  影响：  如果收货地址平台服务器被仿冒，用户维护的收货地址信息（收货人姓名、电话号码、详细收货地址）被收集和利用，可能对用户日常生活造成困扰。  可能性：  hosts文件被修改，导致域名解析的IP地址指向仿冒的收货地址服务器。 |
| 已有消减措施 | 收货地址服务器已经进行用户名和密码的认证； |
| 建议消减措施 | N/A |
| 产品落地计划 | N/A |
| 抵赖（R） | 风险（Risk） | 级别：低  影响：  如果在获取用户收货地址的接口，收货地址服务器发送恶意信息，那么用户就会看到自己没有管理使用过的收货地址信息；由于用户在支付前有个修改订单的过程，因此会触发一个地址新增或者修改的接口。同时，修订后的订单信息也会记录正确的收货地址，所以不对用户利益造成重大损失。  可能性：  由于同属于华为内部系统并且有日志记录，基本上不存在抵赖的情况。 |
| 已有消减措施 | 对于接口调用，已经记录了系统业务日志。 |
| 建议消减措施 |  |
| 产品落地计划 |  |

### Push网关

|  |  |  |
| --- | --- | --- |
| 元素名称 | Push网关 | |
| 元素概述 | Push网关用于向用户上的终端推送消息。 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | 级别：低  影响：  如果push网关被伪造，那么就会把需要推送的消息发送到错误的服务器，由于推送的信息为用户反馈意见的处理结果，因此对于用户体验的友好性是有影响的。  可能性：  hosts文件被修改，导致域名解析的IP地址指向仿冒的积分平台服务器。 |
| 已有消减措施 | Push网关对于O2O服务器进行用户名和密码认证 |
| 建议消减措施 | N/A |
| 产品落地计划 | N/A |
| 抵赖（R） | 风险（Risk） | 级别：低  影响：  Push网关同属于华为内网部件，发生抵赖的可能性很低。  如果Push网关发生抵赖，将不能够对O2O服务器的消息下发到终端。 |
| 已有消减措施 | 对于接口调用，已经记录了系统业务日志。 |
| 建议消减措施 |  |
| 产品落地计划 |  |

## 数据流分析

### 与合作商户的数据流

|  |  |  |
| --- | --- | --- |
| 元素名称 | 与合作商户的数据流 | |
| 元素概述 | 合作商户同步订单消息到O2O业务服务器；  如果是理财公司，还将同步7日年化收益率、昨日收益等数据； | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | 级别：中  影响：  用户看到的订购数据与实际发生的订购数据不符，这个只是展示的问题，但不影响用户根本利益。  对于理财产品，用户看到的昨日收益和七日年化数据不正确，影响用户体验。  可能性：  传输过程不使用Session, 每次都是独立传输，除非破解HTTPS通道。 |
| 已有消减措施 | 1. 数据传输采用HTTPS  2. 对传输内容的数据做摘要算法确定数据的完整性；  传输的数据包括订单信息（订单号、华为用户ID、商户ID、产品ID、产品价格以及订单状态）；  关于理财传输的数据包括理财商户标示、理财产品ID和理财产品的七日年化收益率、我的理财的昨日收益等数据。 |
| 建议消减措施 | N/A |
| 产品落地计划 | 已经实施。 |
| 信息泄漏（I） | 风险（Risk） | 级别：中  影响：用户在合作商户购买记录被泄露，对客户隐私有影响，所泄露的商品数据涉及到敏感信息，比如我的理财的金额、购买商品的数量和价格等信息。  可能性：传输过程不使用Session, 每次都是独立传输，除非破解HTTPS通道。 |
| 已有消减措施 | 1. 数据传输采用HTTPS (在分发服务器上配置证书) |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 拒绝服务(D) | 风险（Risk） | 级别：中  影响：如果请求量很大，会对O2O服务所在机房的带宽资源、服务器CPU、数据库服务器存储产生较大的压力，造成O2O其他业务中断。  可能性：如果合法用户大量发送消息，或者恶意用户破解SSL/TLS传输秘钥，然后仿冒发送大量信息，上述可能性还是存在的。 |
| 已有消减措施 | 1. 对于传输报文的最大大小在Tomcat进行设置  当前默认设置为10K，可以灵活配置； |
| 建议消减措施 |  |
| 产品落地计划 |  |

### 与钱包APP的数据流

|  |  |  |
| --- | --- | --- |
| 元素名称 | 与钱包APP的数据流 | |
| 元素概述 | 荣耀钱包APP和O2O服务器存在大量的交互信息，主要业务包括：   * 华为自有商品管理（获取信息，列表信息，订购） * 获取商品信息和列表无认证，订购信息UP认证 * 获取惠生活首页信息 (无认证) * 获取理财信息 (UP认证) * 获取权益信息 (UP认证) * 获取消息通知 (UP认证) * 获取订购记录 (UP认证) * 进行意见反馈（无认证） | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | 级别：中  影响：如果数据在传输过程被篡改，用户的信息获取不正确，特别是理财相关的信息被窜改会有问题。  可能性：传输过程不使用Session, 每次都是独立传输，除非破解HTTPS通道。 |
| 已有消减措施 | 涉及隐私数据或敏感信息的统一使用https通道加密传输。已和运维确认，SSL和TLS的版本号和加密套件由F5组件控制。 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 信息泄漏（I） | 风险（Risk） | 级别：中  影响：如果数据在传输过程被泄露，用户相关的账户信息，特别是理财的财务信息会被泄露，给用户产品造成较大影响。  可能性：传输过程不使用Session, 每次都是独立传输，除非破解HTTPS通道。 |
| 已有消减措施 | 1. 传输通道使用HTTPS  (对于获取商品和获取商品列表使用http,这些都是非用户敏感信息) |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 拒绝服务(D) | 风险（Risk） | 级别：中  影响：如果请求量很大，会对O2O服务所在机房的带宽资源、服务器CPU、数据库服务器存储产生较大的压力，造成O2O其他业务中断。  可能性：这个可能性比较大，只要合法的华为钱包用户使用其账户，通过不断的发送合法的消息过来，就会造成服务器全面瘫痪。 |
| 已有消减措施 | 1. 对于常用的数据通过Redis缓存提供服务  2. 服务器通过集群方式分流现网压力 |
| 建议消减措施 |  |
| 产品落地计划 |  |

### 与CDN的数据流

|  |  |  |
| --- | --- | --- |
| 元素名称 | 与CDN的数据流 | |
| 元素概述 | O2O的分发服务器作为CDN的数据源为终端用户获取静态资源服务，当前主要是图片信息。 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | 级别：中  影响： 如果数据被篡改，到时用户获取的图片资源等信息被恶意破坏，最后到达钱包客户端的消息会被破坏。  可能性：目前这些资源都是HTTP的GET方式获取，在通道是完全可以被修改的。 |
| 已有消减措施 | 通过HTTPS接口来确保传输的放篡改 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 信息泄漏（I） | 风险（Risk） | 不涉及 |
| 已有消减措施 | 不涉及 |
| 建议消减措施 | 不涉及 |
| 产品落地计划 | 不涉及 |
| 拒绝服务(D) | 风险（Risk） | 级别：中  影响：如果请求量很大，会对O2O分发服务器的带宽资源、服务器CPU、数据库服务器存储产生较大的压力，造成O2O资源服务宕机。  可能性：目前图片等资源通过CDN分发网络减少对分发服务器的访问，但是如果恶意用户直接访问O2O分发服务器也是有可能的，这种攻击存在的可能性很大。 |
| 已有消减措施 | 1、分发服务器内部有缓存策略  2、与O2O分发服务器的接口为https |
| 建议消减措施 | 1. 后期对于请求需要做流量控制 |
| 产品落地计划 | 计划9月份启动 |

### 与支付服务器的数据流

|  |  |  |
| --- | --- | --- |
| 元素名称 | 与支付服务器的数据流 | |
| 元素概述 | 一方面O2O服务器会和支付服务器发起支付请求，另一方面支付服务器会将用户付费的状态同步给O2O服务器 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | 级别：低  影响：如果支付数据在传输过程被篡改，尤其是支付的金额被修改， 将造成用户财产损失。  可能性：内部除非内部人员恶意破坏，跨机房除非破解VPN隧道。 |
| 已有消减措施 | 1. O2O服务器与支付服务器部署在同一个局域网，使用内网地址进行访问。与运维人员确认，若部署在不同的机房则通过IPSEC VPN通道进行交互. |
| 建议消减措施 |  |
| 产品落地计划 | 已经落地。 |
| 信息泄漏（I） | 风险（Risk） | 级别：低  影响：如果数据在传输过程信息泄露，计费和用户鉴权信息会被恶意用户获取，造成重大影响。  可能性：内部除非内部人员恶意破坏，跨机房除非破解VPN隧道。 |
| 已有消减措施 | 1. O2O服务器与支付服务器部署在同一个局域网，使用内网地址进行访问。与运维人员确认，若部署在不同的机房则通过IPSEC VPN通道进行交互. |
| 建议消减措施 |  |
| 产品落地计划 | 已经落地。 |
| 拒绝服务(D) | 风险（Risk） | 级别：低  影响：如果请求量很大，会对O2O服务所在机房的带宽资源、服务器CPU、数据库服务器存储产生较大的压力，造成O2O其他业务中断。  可能性：内网服务器间交互，可能性低。 |
| 已有消减措施 |  |
| 建议消减措施 |  |
| 产品落地计划 |  |

### 与UP的数据流

|  |  |  |
| --- | --- | --- |
| 元素名称 | 与UP的数据流 | |
| 元素概述 | O2O服务器会发请求消息到UP对用户进行鉴权 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | 级别：低  影响：如果数据在传输过程被篡改，鉴权信息会有问题，将会导致用户业务不可用。  可能性：内部除非内部人员恶意破坏，跨机房除非破解VPN隧道。 |
| 已有消减措施 | 1. O2O服务器与UP服务器部署在同一个局域网，使用内网地址进行访问。与运维人员确认，若部署在不同的机房则通过VPN（SSL）通道进行交互. |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 信息泄漏（I） | 风险（Risk） | 级别：低  影响：如果数据在传输过程信息泄露，用户鉴权信息会被恶意用户获取，将可能会导致ST和UserID被第三方获取。 同时，由于ST和UserID都只是在华为系统才有效的数据，因此影响的程度有限。  可能性：内部除非内部人员恶意破坏，跨机房除非破解VPN隧道。 |
| 已有消减措施 | 1. O2O服务器与UP服务器部署在同一个局域网，使用内网地址进行访问。与运维人员确认，若部署在不同的机房则通过VPN（SSL）通道进行交互. |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 拒绝服务(D) | 风险（Risk） | 级别：低  影响：如果请求量很大，会对O2O服务所在机房的带宽资源、服务器CPU、数据库服务器存储产生较大的压力，造成O2O其他业务中断。  可能性：内网服务器间交互，可能性低。 |
| 已有消减措施 |  |
| 建议消减措施 |  |
| 产品落地计划 |  |

### 与收货地址服务器的数据流

|  |  |  |
| --- | --- | --- |
| 元素名称 | 与收货地址服务器的数据流 | |
| 元素概述 | 收货地址服务器与O2O服务器之间的管理数据 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | 级别：低  影响：如果收货数据在传输过程信息被篡改，导致终端用户不能够收到该买的商品，从而造成损失。 例如收货地址的省市区信息， 联系方式。  可能性：内部除非内部人员恶意破坏，跨机房除非破解VPN隧道。 |
| 已有消减措施 | 1、收货地址服务器与O2O服务器部署在同一个局域网，通过内网地址进行访问。 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 信息泄漏（I） | 风险（Risk） | 级别：低  影响：如果数据在传输过程信息泄露，用户收货信息会泄露，收货数据可能被利用。  可能性：   1. 用户敏感数据迁移 2. 敏感数据明文传输 3. 中间人攻击 |
| 已有消减措施 | 1、对请求参数按照字典升序排列拼接后再拼上分配给业务的密钥进行签名来验证请求参数的完整性。  2、收货地址服务器与O2O服务器在同一个局域网，使用内网地址进行访问。与运维人员确认，收货地址服务器和O2O服务器分别部署在不同的机房则通过VPN（SSL）通道进行交互。  3、敏感信息加密， 比如手机号 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 拒绝服务(D) | 风险（Risk） | 级别：低  影响：如果请求量很大，会对收货地址服务器带宽资源、服务器CPU产生较大的压力，造成O2O部分业务不可用。  可能性：  短时间内请求峰值超过收货地址服务器的性能指标；  内网服务器间交互，拒绝服务的可能性低。 |
| 已有消减措施 |  |
| 建议消减措施 | 无 |
| 产品落地计划 | 无 |

### 与PUSH网关的数据流

|  |  |  |
| --- | --- | --- |
| 元素名称 | 与Push网关的数据流 | |
| 元素概述 | 发送PUSH消息 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | 级别：低  影响：如果与Push推送消息在传输过程信息被篡改，导致用户反馈的信息不能够送达到终端上，影响用户体验。  可能性：内部除非内部人员恶意破坏，跨机房除非破解VPN隧道。 |
| 已有消减措施 | 1、Push网关与O2O服务器部署在同一个局域网，通过内网地址进行访问。 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 信息泄漏（I） | 风险（Risk） | 级别：低  影响：如果数据在传输过程信息泄露，可能导致用户敏感信息被泄露而可能被利用。  可能性：   1. 用户敏感数据迁移 2. 敏感数据明文传输 |
| 已有消减措施 | 1、对请求参数按照字典升序排列拼接后再拼上分配给业务的密钥进行签名来验证请求参数的完整性。  2、Push网关与O2O服务器在同一个局域网，使用内网地址进行访问。与运维人员确认，收货地址服务器和O2O服务器分别部署在不同的机房则通过VPN（SSL）通道进行交互。  3、敏感信息加密， 比如手机号和邮件地址。 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 拒绝服务(D) | 风险（Risk） | 级别：低  影响：如果请求量很大，会对Push网关带宽资源、服务器CPU产生较大的压力，造成部分消息不能够送达。  可能性：  短时间内请求峰值超过Push网关推送的性能指标；  内网服务器间交互，拒绝服务的可能性低。 |
| 已有消减措施 |  |
| 建议消减措施 |  |
| 产品落地计划 |  |

## 处理过程分析

### 业务服务器

|  |  |  |
| --- | --- | --- |
| 元素名称 | 业务服务器 | |
| 元素概述 | 业务服务器提供与第三方商户和内部望远的接口以及业务逻辑的处理。 | |
| 威胁 | STRIDE | |
| 仿冒（S） | 风险（Risk） | 级别：中  影响：O2O业务服务器被仿冒，首先用户的敏感信息（比如订单信息、理财收益数据等）将被收集和使用；并且无法完成正常的业务流程而影响用户在客户端的体验。  仿冒的部件也可能访问UP，但是不会返回多余的敏感信息。  可能性：  1、客户端与服务器之间没有使用CA证书认证机制  2、CA认证证书已失效  3、证书更新机制不完善被攻击者替换证书 |
| 已有消减措施 | 1、客户端与服务器之间在传输用户数据时全部使用HTTPS通道  2、已与运维人员确认，依赖现网运维人员控制CA证书有效期  3、已与运维人员确认，依赖现网运维人员控制CA证书的安全保护措施 |
| 建议消减措施 | 建议数字签名（SHA256(RSA2048)）平台地址，软件包上传到support网站上，升级之前校验签名，然后执行升级操作；  针对重要文件（如重要业务脚本）进行签名，运行过程中进行校验； |
| 产品落地计划 |  |
| 篡改（T） | 风险（Risk） | 级别：中  影响：O2O业务服务器被篡改，可以获取业务数据库的信息，造成信息泄露，并且恶意的操作可能导致数据库服务器承受很大压力甚至瘫痪。  可能性：  1. 客户端请求参数包含恶意代码则消息接入部件没有进行校验或者校验方法不当造成注入攻击；  2、系统升级软件和固件未做安全验证，升级过程未记录操作日志。 |
| 已有消减措施 | 1、业务升级时研发人员将升级包压缩、加密（密码为运维约定的规则）上传至SVN指定目录，而操作系统升级时运维人员会进行完整性验证，操作系统的history记录运维人员操作过程 |
| 建议消减措施 | 无 |
| 产品落地计划 | 业务操作的主要流程都会有相关操作日志。 |
| 抵赖（R） | 风险（Risk） | 级别：低  影响：O2O业务服务器为服务提供方，并且服务端有相关的日志操作信息。  可能性：  有日志信息，抵赖可能性很低。 |
| 已有消减措施 | 业务操作的主要流程都会有相关操作日志。 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 信息泄漏（I） | 风险（Risk） | 级别：中  影响：如果O2O业务服务器信息泄露，那么会造成  1. 用户的隐私数据户泄露（华为账户和ServiceToken）。  2. 数据库和Redis等访问的用户名、密码泄露  可能性：  1. 不当的代码导致恶意代码注入。  2. 秘钥、密码没有加密存储 |
| 已有消减措施 | 1. 对于秘钥和密码加密存储在文件系统;  2. 日志信息中，对于隐私数据加密或者匿名 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 拒绝服务(D) | 风险（Risk） | 级别：中  影响：业务无法使用。  可能性：大量发送消息导致资源服务器瘫痪。 |
| 已有消减措施 | 1. 集群部署，横向可扩展，分担业务流量  2. 鉴权接口，对于不可信任的消息直接丢弃 |
| 建议消减措施 | 1. 增加流量控制功能 |
| 产品落地计划 | 计划9月份版本落地 |
| 特权提升（E） | 风险（Risk） | 级别：中  影响：获取数据库的高权限，接口可以直接访问，获取其他用户的信息。  可能性：如果分发服务器没有关闭这些操作，并且对于NFS资源有写权限。 |
| 已有消减措施 | 1. 访问数据库的用户提供最小化权限（只访问业务数据库）  2. REDIS访问增加用户名密码机制，并且其密码有强度要求：至少长度为10位，而且取值范围为大小写字母、数字和特殊字符；  3. 部署在内网，不提供外网直接访问的通道 |
| 建议消减措施 |  |
| 产品落地计划 |  |

### 分发服务器

|  |  |  |
| --- | --- | --- |
| 元素名称 | 分发服务器 | |
| 元素概述 | 分发服务器接收外部网络数据并基于规则路由到业务服务器，同时提供HTML静态资源的访问。 | |
| 威胁 | STRIDE | |
| 仿冒（S） | 风险（Risk） | 级别：中  影响：如果O2O业务分发服务器被仿冒，所有数据经过业务接口服务器的时候还是会去认证，不会对业务正确性造成影响，此外外部所有https认证都是失败。  可能性：如果仿冒的服务器获取了现网分发服务器机器的证书，现网CA证书失效或者证书更新机制不完善被攻击者更换了证书。 |
| 已有消减措施 | 1. 客户端与服务器之间在传输用户数据时全部使用HTTPS通道传输交互参数。 2. 已与运维人员确认，依赖现网运维人员控制CA证书有效期。 3. 已与运维人员确认，依赖现网运维人员控制CA证书的安全保护措施。 |
| 建议消减措施 |  |
| 产品落地计划 |  |
|  | 2风险（Risk） | 级别：中  影响：如果O2O业务分发服务器处理过程被窜改，会导致业务数据流无法正确导入到后台业务处理服务器。  可能性：现网分发服务器的分发策略文件和LUA脚本被修改。 |
| 已有消减措施 | 1. 分发服务器所有可执行文件为单一的一个组件，不依赖外部的动态库。  2. 分发服务器的配置文件只有ROOT权限才能修改 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 抵赖（R） | 风险（Risk） | 级别：低  影响：只要O2O分发服务器发送消息到业务服务器，就会对其记录日志，但是这个影响对整个业务处理影响不大。  可能性：默认现网接口日志没有打开，并且审计日志还没有完善，这方面是存在可能性。 |
| 已有消减措施 | 1. 接口日志 |
| 建议消减措施 | 1. 增加审计日志 |
| 产品落地计划 | 计划在9月份版本落地 |
| 信息泄漏（I） | 风险（Risk） | 级别：低  影响：分发服务器不处理实际业务，所以不涉及用户数据的泄露，但是有可能泄露分发服务器的版本号被外部利用既有漏洞进行攻击。  可能性：用户发送特定异常信息导致回复分发服务器错误处理页面其中会暴漏分发服务器的版本信息。 |
| 已有消减措施 |  |
| 建议消减措施 | 1. 分发服务器处理异常信息定制化，不使用默认的错误页面  2. 对于分发服务器进行安全加固 |
| 产品落地计划 | 计划在9月份落地 |
| 拒绝服务(D) | 风险（Risk） | 级别：中  影响：分发服务器为核心处理单元，如果该服务器发生DOS那么后台业务将无法处理外部请求。  可能性：外部发送大量消息到接口服务器。 |
| 已有消减措施 | 1. 目前部署分发服务器集群分担外部流量 |
| 建议消减措施 | 1. 进行分层级的流控   1. 控制NGXIN处理报文的大小和HTTP请求类型   3. 现网运维工具加强对于分发服务器的健康监控和告警 |
| 产品落地计划 | 计划在9月份落地 |
| 特权提升（E） | 风险（Risk） | 低：  【影响】  无效或者非法的请求被缓存到消息队列中，占用消息队列内存，同时业务服务器会处理该无效请求造成资源浪费。  【可能性】  MQ组件的鉴权密码在配置文件中明文配置。 |
| 已有消减措施 | MQ使用口令方式对每次操作请求进行鉴权，口令长度为随机64为字符串支持可配置。  由于鉴权密码为明文,所以需要严格控制redis.conf配置文件的控制权限，安装指南中明确要求运维对配置文件的访问权限控制为640。安装MQ组件时创建用户组和用户，只能使用业务用户权限才可以更新MQ配置文件内容。 |
| 建议消减措施 | 无 |
| 产品落地计划 | 无 |

### Portal服务器

|  |  |  |
| --- | --- | --- |
| 元素名称 | O2O管理Portal | |
| 元素概述 | 对分析的元素进行描述 | |
| 威胁 | STRIDE | |
| 仿冒（S） | 风险（Risk） | 级别：中  影响：如果管理Portal被仿冒，那么运营人员可能登陆类似钓鱼的网站，泄露口令。恶意攻击者利用获得的口令登陆真正的Portal破坏业务的可用性。  可能性：   1. 口令认证不安全 2. 合法会话被劫持 3. 凭证泄露(VPN) |
| 已有消减措施 | 1. 口令复杂度已按照安全要求进行限制、默认口令首次登陆时必须重新修改密码、口令使用SHA256(userName+pawd)加密存储、密码验证操作数据库时使用了预编译防止SQL注入、密码过期失效、修改密码时需要口令确认。 2. 系统不存在特殊方式直接访问系统，用户必须登录。密码连续输入失败次数达到阀值则锁定账号，失效时间为2分钟。。 3. 输入口令使用“.”代替明文、口令输入域不允许拷贝、不支持记住密码功能、日志中未打印明文口令。   与运维人员确认，管理Portal部署在内网环境不会提供公网访问地址，运营人员必须通过VPN（VPN是SSL）通道才能访问管理Portal。产品已规划会员服务将会引用百度、腾讯等合作商户的权益，在管理员页面需要浏览权益的图片，所以需要能够访问公网权限。 |
| 建议消减措施 |  |
| 产品落地计划 | 9月份版本 |
| 篡改（T） | 风险（Risk） | 级别：中  影响：如果管理Portal被篡改，将无法提供首页配置、理财频道配置等基本活动，钱包终端APP将无法使用。  可能性：  VPN密码泄露或者VPN网络被破解后进行：  1. 恶意代码注入  2. 利用既有的操作系统或者Tomcat WEB服务器漏洞进行攻击。 |
| 已有消减措施 | 1、 管理页面上所有输入数据都会在JS侧和JAVA侧使用正则表达式进行校验来保证用户输入合法性，避免注入;  2、 业务没有使用动态链接库; |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 抵赖（R） | 风险（Risk） | 级别：低  影响：对于恶意操作被抵赖会造成业务无法使用，并且也很难查到操作人员的信息  可能性：  1. VPN密码泄露或者VPN网络被破解，并成功破解登陆Portal密码。  2. 如果合法的管理员进行恶意操作  以上可能性较低 |
| 已有消减措施 | 1. 增加审计日志  2. 定期强制变更密码 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 信息泄漏（I） | 风险（Risk） | 优先级： 低  影响：管理员账户/密码泄露，攻击者利用该信息可以修改钱包首页配置，发送PUSH消息给终端用户，造成恶劣影响。  可能性：  1. VPN网络环境被攻破  2. 获取Portal管理员用户名、密码 |
| 已有消减措施 | 1. 使用VPN进行通道加密  2. 处理过程中，运营人员的账号会被明文打印，但是登陆密码不会明文输出到日志文件且不存在开关控制，内部操作数据库或者其他部件异常时会将异常进行捕获将异常信息处理后返回给调用方来防止系统信息泄露。  3. 管理员页面上所有输入数据都会在JS侧和JAVA侧使用正则表达式进行校验来保证用户输入合法性，避免注入  4. 代码中未硬编码密钥信息，且数据库连接字符串的用户名和密码使用AES加密（AES128+CBC+安全随机函数生成16位随机字节）存储在配置文件中 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 拒绝服务(D) | 风险（Risk） | 优先级： 低  影响：钱包首页将无法控制，钱包业务无法正常配置。  可能性：  1. VPN网络环境被攻破 |
| 已有消减措施 | 1. 网络环境隔离，Portal不直接开放到公网环境，外部无法直接访问  2. 交互时发起大量的资源请求，Tomcat的server.xml中增加配置限制请求体、请求头、url中的最大数据量。 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 特权提升（E） | 风险（Risk） | 级别：低  影响：  仿冒的合法的用户访问系统，使用被仿冒用户的高级权限对系统进行操作。  可能性：  目前Portal的用户管理还没有提供权限控制，即运营管理人员都存在相同的权限。 |
| 已有消减措施 | 1、口令复杂度已按照安全要求进行限制、默认口令首次登陆时必须重新修改密码、口令使用SHA256(userName+pawd)加密存储、密码验证操作数据库时使用了预编译防止SQL注入、密码过期失效、修改密码时需要口令确认。  2、系统不存在特殊方式直接访问系统，用户必须登录。密码连续输入失败次数达到阀值则锁定账号。 |
| 建议消减措施 | 提供权限控制模块，对于不同角色的用户提供不同的权限。 |
| 产品落地计划 |  |

## 数据存储分析

### 业务配置数据与日志

|  |  |  |
| --- | --- | --- |
| 元素名称 | 业务配置数据与日志 | |
| 元素概述 | 业务配置为服务器运行的配置，日志为服务器运行过程中记录的所有日志信息 | |
| 威胁 | TI[R]D | |
| 篡改（T） | 风险（Risk） | 级别： 高  影响：  1. 如果日志配置被篡改，导致日志打印过于频繁或者无日志，不便于问题定位.  2. 如果数据库、REDIS等访问的用户名密码和IP等信息被篡改，会导致重启后业务不可用，但不影响已经上线运行的系统。  4. 其他配置第三方信息的配置文件，例如：PUSH网关、Gate Way、业务配置信息等，会造成操作业务不可用。  5、运营人员的登录口令泄露后，将导致攻击者仿冒和利用账号对应的权限对系统内的数据进行操作，可以篡改订单的收货地址、数量等信息，从而造成财产损失。  可能性：  1. 不恰当的WEB服务器访问控制  2. 恶意代码注入、SQL注入 |
| 已有消减措施 | 1. 做好WEB服务器的控制，防止攻击者能通过WEB服务器的漏洞进行PUT、POST操作，进而修改配置信息。  2. 系统中配置的密钥等敏感信息全部使用AES加密（AES128+CBC+安全随机函数生成16位随机字节）后保存在数据库和配置文件中，而运营人员的登陆口令使用Sha256进行了不可逆算法加密后存储。配置文件的访问权限依赖运维创建业务用户的权限。 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 信息泄漏（I） | 风险（Risk） | 优先级： 高  影响：  1. 如果日志配置被泄露，无重大影响.  2. 如果数据库、REDIS等访问的用户名密码和IP等信息被泄露，会导致内部重要信息被黑客利用，照成重大威胁。  3. 其他配置第三方信息的配置文件，例如：PUSH网关、Gate Way、业务配置信息等被泄露，不会造成重大影响。  可能性：  1. 不恰当的WEB服务器访问控制  2. 对外抛出内部异常堆栈 |
| 已有消减措施 | 1. 数据存储中所有敏感信息均经过加密存储。  2. 设置应用用户的访问权限，当前只有运维能访问配置服务器的配置文件。  3. 加固WEB 服务器防止被恶意攻击者发起目录遍历攻击。  4. 对于业务服务器不直接对外部网络开放。，不同机房之间使用VPN技术加密访问通道。 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 抵赖（R） | 风险（Risk） | 优先级： 低  影响：  恶意人员修改了配置文件后会造成实时生效的业务不可用，其他业务重启后会失效。  可能性：  1. 目前对于文件的修改无审计日志，操作是完全可以抵赖的 |
| 已有消减措施 | 1. 内部系统不直接对外网开放， |
| 建议消减措施 | 1. 对于文件系统的配置，增加日志记录的功能 |
| 产品落地计划 |  |
| 拒绝服务(D) | 风险（Risk） | 业务配置是文件系统中的文件，不涉及DDOS攻击。 |
| 已有消减措施 | N/A |
| 建议消减措施 | N/A |
| 产品落地计划 | N/A |

### MYSQL数据存储

|  |  |  |
| --- | --- | --- |
| 元素名称 | MYSQL数据存储 | |
| 元素概述 | MYSQL数据存储 | |
| 威胁 | TI[R]D | |
| 篡改（T） | 风险（Risk） | 级别：中  影响：如果MySQL数据库被篡改，用户数据被遭到破坏，业务将无法正常工作。  可能性：  1. 不恰当的业务代码，造成SQL注入  2. 数据库中的业务数据和操作日志数据存储没有做完整性校验。  3. 数据库访问权限分配时控制不当，没有做到最小范围控制。 |
| 已有消减措施 | 1. 已与运维确认访问数据库的权限控制到业务用户，同一个账号不能同时访问多个业务的数据库实例。  2. 已与运维确认数据库访问权限只会授权给部署业务服务的IP，并且对建表、建索引等操作范围进行赋权  3. 已与运维确认数据库的存储空间使用情况已有工具监控和告警。 |
| 建议消减措施 | N/A |
| 产品落地计划 | N/A |
| 信息泄漏（I） | 风险（Risk） | 级别：中  影响：如果MySQL数据库被泄露，用户隐私数据会被恶意攻击者利用。  可能性：  1. 数据库访问权限分配时控制不当，没有做到最小范围控制。 |
| 已有消减措施 | 1. 已与运维确认访问数据库的权限控制到业务用户，同一个账号不能同时访问多个业务的数据库实例。  2. 已与运维确认数据库访问权限只会授权给部署业务服务的IP，并且对建表、建索引等操作范围进行赋权  3. 数据库的用户名和密码加密存储 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 拒绝服务(D) | 风险（Risk） | 级别：中  影响：如果MYSQL服务器被攻击，停止对外服务，  可能性：  1. 数据库访问权限分配时控制不当，没有做到最小范围控制。 |
| 已有消减措施 | 1. 使用REDIS缓存，对于读多写少数据直接从REDIS获取减少对于数据库的访问操作。  2. 做好现网的数据库关键指标告警提示  3. 数据库不直接对外网开放，杜绝直接向数据库发起攻击的可能性 |
| 建议消减措施 | 1. 业务数据（用户级）分库分表  2. 数据库读写表、库分离 |
| 产品落地计划 | 计划在9月和10月份的计划落地 |

### NFS共享文件存储

|  |  |  |
| --- | --- | --- |
| 元素名称 | NFS共享文件存储 | |
| 元素概述 | NFS共享文件存储 | |
| 威胁 | TI[R]D | |
| 篡改（T） | 风险（Risk） | 级别：中  影响：如果共享存储被篡改，对于钱包APP终端的展示信息会造成重大影响，有的业务（例如：合作公司推广广告业务）无法使用。  可能性：  1. 不恰当的分发服务器配置，造成恶意攻击者可以通过分发服务器的漏洞直接修改NFS的文件  2. 门户PORTAL漏洞造成，恶意攻击者可以修改NFS服务器的原始文件。 |
| 已有消减措施 | 1. 加固分发服务器，防止目录遍历攻击  2. 修改NFS文件对于分发服务器为只读，杜绝修改操作的可能性  3. 门户PORTAL不直接对外网开放，通过VPN加密通道。 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 信息泄漏（I） | 风险（Risk） | 级别：低  影响：如果分发服务器信息泄露会造成攻击者利用特定版本分发服务器的漏洞发起攻击，但是文件是只读的，而且这些文件信息本来就是公开的不涉及隐私。  可能性：  1. 不恰当的分发服务器配置，造成分发服务器版本泄露 |
| 已有消减措施 |  |
| 建议消减措施 | 1. 加固分发服务器防止版本泄露，特别是异常访问场景 |
| 产品落地计划 | 计划在9月份 |
| 拒绝服务(D) | 风险（Risk） | 级别：中  影响：导致现网的数据将无法正常下载，钱包APP无法正常使用。  可能性：  1. 向分发服务器发送大量请求，造成服务器瘫痪 |
| 已有消减措施 | 1. 手机终端部直接访问NGXIN，而是通过CDN分发网络获取，减少服务器的访问 |
| 建议消减措施 | 1. 对于分发服务器的访问提供流量控制，因为NGXIN还是直接可以在外网访问得到。 |
| 产品落地计划 |  |

### REDIS缓存

|  |  |  |
| --- | --- | --- |
| 元素名称 | REDIS缓存 | |
| 元素概述 | 对分析的元素进行描述 | |
| 威胁 | TI[R]D | |
| 篡改（T） | 风险（Risk） | 级别：中  影响：导致现网荣耀钱包APP获取错误信息，业务无法使用。  可能性：  1. 业务提供了供外部修改REDIS缓存的漏洞 |
| 已有消减措施 | 1. REDIS不直接对外部开放，杜绝直接被攻击的可能性  2. 增加REDIS访问的密码，不提供无鉴权的数据控制 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 信息泄漏（I） | 风险（Risk） | 级别：低  影响：目前REDIS缓存的都是需要对外开放的信息，无敏感信息，基本无影响。  可能性：  不涉及 |
| 已有消减措施 | 不涉及 |
| 建议消减措施 |  |
| 产品落地计划 |  |
| 拒绝服务(D) | 风险（Risk） | 级别：中  影响：导致现网的数据将无法正常下载，钱包APP无法正常使用。  可能性：  1. 业务服务器发送大量请求，造成服务器瘫痪 |
| 已有消减措施 |  |
| 建议消减措施 | 1. 做业务层面的流量控制机制  2. 现网部署重要指标健康，进行及时告警 |
| 产品落地计划 |  |

## 隐私设计规范Checklist自检

*根据《消费者BG隐私设计规范V1.0》中的规则和要求，整理出各子系统/模块中所涉及的个人数据（定义见规范中描述），对照规范中的每一条规则和建议，确认对个人数据和隐私空间的处理是否满足规范要求，并填写《消费者BG隐私设计规范Checklist-V1.0》表格中”消费者BG隐私设计规范Checklist”页的E和F列，以及” 个人数据清单”页。针对不满足的规则项，需要纳入产品的安全需求，并进行整改。*



*隐私设计规范和自检表请从以下路径获取最新版本：*

[http://wss.huawei.com/sites/huaweidevice/tcso/4/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fhuaweidevice%2Ftcso%2F4%2F4%2E02%E5%AE%89%E5%85%A8%E8%A7%84%E8%8C%83%2F%E9%9A%90%E7%A7%81%E8%AE%BE%E8%AE%A1%E8%A7%84%E8%8C%83&FolderCTID=0x012000CD726E0699495C4A9F05C17D2C5C7AC0&View={6F458B1B-276A-4E11-85F5-9072BA83A8F4}](http://wss.huawei.com/sites/huaweidevice/tcso/4/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fhuaweidevice%2Ftcso%2F4%2F4%2E02%E5%AE%89%E5%85%A8%E8%A7%84%E8%8C%83%2F%E9%9A%90%E7%A7%81%E8%AE%BE%E8%AE%A1%E8%A7%84%E8%8C%83&FolderCTID=0x012000CD726E0699495C4A9F05C17D2C5C7AC0&View=%7b6F458B1B-276A-4E11-85F5-9072BA83A8F4%7d)

## 缺陷特性汇总

本章节将以上分析出的缺陷及消减措施汇总，便于跟踪落实。



# 安全需求设计

针对以上缺陷列表中产品接纳的部分，作为安全需求，本章节进行安全设计。

## 2015年8月安全需求设计

### 签名字段算法要求从sha1增强到sha256

* 级别：中
* 方案

涉及范围：

与钱包客户端的接口，计算运费uploadDeliveryAddress.do和创建订单createOrder.do两个接口

与支付服务器的接口，通知订单的支付结果NotifyHwPayResultAction 一个接口

关于实现方案：

与钱包客户端， 客户端在请求消息增加可选字段version，当version=2时，服务端返回的sign采用sha256加密；不携带version字段则为老接口，还是sha1。

与支付服务器，支付服务器在请求中增加signType字段，然后O2O服务器判断是老接口还是sha256。

### Coverity扫描结果高、中风险项的清理

* 级别：中

codeCC中coverity扫描及H、M的清零，L待定；误报的不管，

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | 当前扫描结果如下 | coverity |  | | New(H/M/L) | Dismissed | Fixed | | |  |  |  | | --- | --- | --- | |  | klocwork |  | | New(H/M/L) | Dismissed | Fixed | | fortify | Action | Links |
| [400012760](http://10.62.230.137:8080/queue-web/QueryCIJobList.do?jobId=400012760) | /cloud\_win32 | |  | | --- | | 768 | | cloud\_win32 | l00169780 | |  | | --- | | 55 (9/46/0) | |

## 2015年9月安全需求设计

### 物理组网不能有单节点故障求

* 级别：中
* 方案

如下图所示，当前管理Portal为单机部署，要求不能存在单节点故障。

02.

需要把Portal服务器修改为双机部署。

### Mysql数据库、Redis、Portal用户名和密码强度要求

* 级别：中
* 方案

当前计算速度(CPU 2G,每秒运算20亿次)

口令随机范围(当前95^10)

如果口令位8位， 那么暴力破解时间= 95^8/(2\*10^10\*60\*60\*24)=约为4天；

如果口令位10位， 那么暴力破解时间= 95^10/(2\*10^10\*60\*60\*24/365)=约为95年；

因此，要求mysql数据库密码强度为至少10位，建议16位。取值范围为大小写字母、数字和特殊字符；同时大小写、数字和特殊字符至少要3种。

Portal门户用户密码有效期可配；

对于用户名，要求6~32个字符长度；

### 用户敏感数据加密存储&日志匿名化

* 级别：中
* 方案

用户敏感信息不能明文出现在日志文件、数据库存储和异常信息中，需要加密保存。

而根据敏感数据处理措施要求：

A、 需要反向查找的敏感字段，此时字段采用SHA256加密。密文不可解密，但同一明文密文一致，便于业务反向查找。  
B、 无需反向查找的敏感字段，此时字段采用AES-CBC-随机向量加密。密文可解密，但同一明文多次加密密文不同，可供业务获取敏感字段明文信息。  
C、 既需求反向查找又需要解密的敏感字段，此时只能通过给表增加两个字段实现，SHA256加密字段用于查找，AES-CBC-随机向量加密字段用于解密获取明文。

系统当前在我的权益、订单等场景都使用了用户终端标示deviceId。同样，pushToken、deviceToken和serviceToken都需要加密保存。

同时，在打印日志时，需要做匿名化处理；隐藏部分要超过30%，采用\*号来部分代替。或者采用sha256加密打印。

加密方案要求采用：AES-CBC-随机向量加密，需要随机向量。

### 敏感信息加密算法的整改

* 级别：中
* 方案

当前敏感信息的加密算法采用框架的AES-128，要求统一修改为AES256–CBC-+IV使用安全随机数

同时，AES的密钥分散保存可以参考一下会员的代码。

### 软件版本的一致性，涉及升级完整性保护

* 级别：中

对外发布的软件包（含补丁包），必须提供完整性保护机制，并随软件包一起发布。

在公司自动化版本签名部署以前，以下两种方式都可以：

1、使用HASH工具获取SHA256校验和，HASH工具使用指导（请参考下述链接附件）：http://3ms.huawei.com/hi/index.php?app=Group&mod=Wiki&act=detail&id=2868533&gid=4355

2. VMP版本管理库若已部署自动签名的，则属于已满足该条红线， 否则请使用第1条进行HASH校验方式；

O2O服务器采用VMP来签名的方式实现。

### 日志打印&日志保存策略管理

* 级别：中
* 方案

当前O2O服务器提供4个级别的日志管理，分别为error，warn，info和debug；

其中，当前只是默认打印error和warn的日志。

error和warn日志：要求保存6个月,6个月前的自动删除；

info日志，需要打印关键的业务日志和操作日志，用于防抵赖。比如订单同步信息、创建订单信息等。数据库的增加、修改和删除操作。日志的有效期为3个月；

debug日志：记录全量的日志信息，默认不打开；

### 新增订单接口采用sha256签名

* 级别：中
* 方案

为了满足葡萄、去哪儿和携程等的要求，在9月份新增订单接口，要求采用HMAC-sha256签名；

### 限制CDN访问NGIN的权限

* 级别：中

建议对资源服务器进行最小化权限配置，例如CDN网络如果只需要HTTP的Get请求，那么将限制CDN请求的类型，比如post、put等操作将被限制。

### 意见反馈页面没有任何接入认证

* 级别：中
* 方案

对于新版本，钱包客户端直接跳转到统一采用手机服务的意见反馈页面；

对于钱包的老接口，服务端侧有两种方案：

1. 接收到老应用客户端的请求后，返回错误码；
2. 维持版本现状

## 遗留问题（待明确或暂不接纳）

### 与Vmall的接口存在sha1的签名

* 级别：中
* 问题描述

当前与vamll的<http://apidev.vmall.com/rest.php>地址的接口，huawei.trade.mgt.marketingAdjust设计的业务的签名还是sha1的。

* 方案

需要统一协调后修改为sha256

### 口令输入支持键盘安全控件。

* 级别：低

### 对于管理员分角色并赋予不同的管理权限，最小化权限原则.

* 级别：低

### 业务系统放DDos攻击

* 级别：低
* 方案

在分发服务器提供接口级的流量控制，有云平台统一提供；

暂不涉及应用级和用户级别的流量控制。

### 登陆成功未提示上次的异常登陆信息

* 级别：低
* 方案

O2O管理员Portal部署在内网，必须通过VPN通道才可以访问；  
所有的用户的登陆操作都已经记录了日志

### 与应用客户端的认证鉴权

* 级别：中
* 方案

当前与客户端的数据交互，采用https接口协议；同时对于登录后的页面通过UP提供userID和ST的认证鉴权；但是没有做接入时的用户名和密码鉴权。

因此，存在应用客户端假冒的风险。需要提供基于账号和密码的认证鉴权；

## 安全红线

### 安全红线要求

管理通道控制，不涉及研发由运维确认。

协议防攻击，对系统进行畸形报文攻击时应返回“系统忙”或者“参数不合法”这种模糊的错误码，且不能导致系统异常。

禁止未公开接口，系统业务不存在可绕过系统安全机制（认证、权限控制、日志记录）对系统或数据进行访问的功能，操作系统部分需要运维进行确认和维护。

软件完整性保护，研发编码、测试完成发布前首先使用赛门铁克软件对研发源码进行扫描保证不存在病毒，然后使用Sha256方式进行签名通过安全方式通知运维，将软件包上传至SVN并通知运维，运维获取软件包后同样进行Sha256方式签名然后比较鉴权字，防止软件升级包被篡改。**暂时未对重要的文件完整性进行保护。**

敏感数据保护，系统中不存在私有的加密算法，加密的密钥采用分层方式进行管理。口令、鉴权字和用户的敏感信息都经过加密存储在数据库中，在日志中打印时全部进行匿名化操作。

个人数据（隐私）保护，会员服务部署在廊坊机房为华为自研产品，所以不存在跨用户机房网络获取用户数据的情况。用户的数据使用AES/CBC/安全随机IV进行加密存储在数据库中，在日志文件中出现用户数据时使用匿名化处理。当前未提供管理Portal对用户数据进行统计和操作，普通用户可以查看自己的数据，运维人员可以直接访问数据库的方式解除到用户的加密数据。用户自己填写的详情信息、收货地址等可以通过客户端手动删除。但是**用户在积分乐园购买商品的订单（包含用户的收货地址）和客户端上报的pushToken与IMEI的对应关系用户无法手动删除，产品SE确认长期保留没有设置清除机制。**

口令安全，系统须提供检测口令复杂度的功能，若设置的口令不符合复杂度要求，必须给出合理的提示。初始化的管理员账号必须修改密码后才能进行业务操作，口令输入框中不直接显示明文且不支持拷贝。用户在修改密码时必须输入旧密码进行验证。

日志审计，用户的登陆、登出、锁定、解锁、角色权限变更、新增删除用户和用户属性变更、上传文件等都记录相关日志到数据库。管理员在管理页面上进行业务的增、删、改操作全部记录日志到数据库包括操作人、操作时间、操作内容、操作结果。**当前系统未提供业务供运维进行系统的启动、停止等命令操作，也未提供日志管理功能，只能有运维人员直接访问日志文件和数据库数据解除到审计日志。**

组网安全，客户端通过公网访问服务器，经过了非信任域。服务器提供给用户的接口全部使用HTTPS通道，且业务逻辑中使用到的客户端参数必须校验类型和长度，当问数据库时进行预编译防止注入攻击。在内网中访问MySql、Redis时使用口令方式验证，与UP、PUSH、会员交互时按照各个部件的接口规范进行交互。

## 应用安全

### 应用安全要求

* 用户认证模块采用防暴力破解机制，连续鉴权失败N次会锁定账号。 = 已经实现
* 用户所有请求通过一个servlet进行处理不做鉴权处理，但是所有的业务页面都会根据用户权限进行鉴权，所以不存在URL越权。
* 服务采用angular JS以防止执行恶意代码、跨站脚本攻击。
* 对用户身份鉴权、创建会话、维持会话、消亡会话严格按照“会话管理安全设计规范”规范进行完善。
* 系统在使用用户输入参数进行业务逻辑处理时，必须对参数进行类型、长度进行校验，访问数据库时需要使用预编译防止注入攻击。
* 排查系统内的各个目录，发布前不允许出现多余的目录或者文件资源。
* 用户身份验证通过后必须更换sessionid，防止session固化攻击。会话超时，修改密码成功后当前会话必须失效，用户重新进行身份认证。
* 会话标识sessionid、鉴权标识token、校验码checkCode等必须在服务器侧使用安全随机数进行生成。
* 管理员通过Portal进行业务增、删、改操作时必须记录审计日志，满足操作人、操作时间、操作内容、操作结果。
* WEB部件编码结束后使用AppScan进行扫描需达到无高风险级别漏洞、无涉及敏感信息的中级别漏洞，系统无异常。

# 各模块的分配需求

本章节从模块的角度罗列各个模块上的分配需求。

例如，分配在CC这个模块的系统需求如下：

（1）VPDN用户认证时，同一般PPP用户一样，认证信息送AAA认证处理；当收到AAA的认证响应时，直接返回给PPP模块处理；

（2）接受L2TP模块会话CID的申请、释放处理；通知L2TP会话拆除；

（3）在CIB表项中互存CID以及所在槽位信息以关联VPDN用户的PPP会话和L2TP会话；

（4）在L2TP通知会话连接建立时，维护L2TP会话CIB表，并下发到SPUE业务板；在L2TP通知会话连接拆除时，清除L2TP会话CIB表，同时通知用户对应的PPP会话拆除连接；在由AAA通知会话拆除时，则同时通知用户对应的PPP会话和L2TP会话连接拆除；

（5）在PPP上报连接UP时，通过CA模块下发PPP CIB表项到用户侧接口板LPUI(SPU)，同时向AAA发送启动计费通知； 而PPP上报连接DOWN时，向AAA发送停止计费通知，并在AAA通知清除表项时，清除PPP CIB表项，并同步清除对应接口板上表项。

# 各模块的接口描述

本章节从模块的角度罗列各个模块的接口。

建议采用以下形式描述：

1. 样表：XX功能接口表

|  |  |  |  |
| --- | --- | --- | --- |
| 接口名称 | 接口类型 | 涉及的模块 | 描述 |
| LRCI | 点对点消息通信 | OMA调用CLRC | 此接口完成XXX功能，。。。 |
|  |  |  |  |

# 备注和附录

本章节描述需要说明的附加内容。如果使用了DFD方法，则可能需要下面的“数据流图”和“数据字典”的章节。

## 数据字典

### 数据字典列表

罗列用到的数据名称和定义。

参考资料清单：

请罗列本文档所参考的有关参考文献和相关文档，格式如下：

作者＋书名（或杂志、文献、文档）＋出版社（或期号、卷号、公司文档编号）＋出版日期+起止页码

例如：

1. D. B. Leeson, “A Simple Model of Feedback Oscillator Noise Spectrum,” Proc. IEEE, pp329-330, February 1966
2. D. Wolaver, Phase-Locked Loop Circuit Design, Prentice Hall, New Jersey,1991