

|  |
| --- |
| **合作商对接技术规范** |
| 杭州向上电子商务有限公司 |
|  |
| 本资料仅提供给经授权使用者。杭州向上电子商务有限公司拥有本资料所有内容的全部版权、专利权、商标权及其它知识产权。未经杭州向上电子商务有限公司的明确书面许可，任何人不得修改、复制、传播、转载本资料的任何内容或将本资料用于任何商业目的。且除了有限的使用权以外，杭州向上电子商务有限公司也未将任何知识产权授予任何授权使用者。接受本资料表示接受杭州向上电子商务有限公司的授权条款和保密条款。 |
|  |
| **杭州向上电子商务有限公司** |
| **2013/10/23** |
|  |

[1. 引言 2](#_Toc338942973)

[1.1. 目标 2](#_Toc338942974)

[1.2. 名词定义 2](#_Toc338942975)

[1.3. 参考文献 2](#_Toc338942976)

[2. 概述 2](#_Toc338942977)

[2.1. 概述 2](#_Toc338942978)

[2.2. 交易流程 2](#_Toc338942979)

[2.3. 相关约定 3](#_Toc338942980)

[2.4. RSA 签名 3](#_Toc338942981)

[2.5. 接口返回结果以XML表示 3](#_Toc338942982)

[2.6. 通用参数 4](#_Toc338942983)

[2.7. 接口返回结果 4](#_Toc338942984)

[3. 合作商要求 5](#_Toc338942985)

[4. 对接联调 5](#_Toc338942986)

[4.1. 联调环境 5](#_Toc338942987)

[4.2. 联调测试用例 5](#_Toc338942988)

[5. 技术接口 6](#_Toc338942989)

[5.1. 话费充值下单 6](#_Toc338942990)

[5.2. 游戏充值下单 7](#_Toc338942991)

[5.3. 订单查询 7](#_Toc338942992)

[5.4. 余额查询 8](#_Toc338942993)

[5.5. 对帐数据下载 9](#_Toc338942994)

[5.6. 订单结果通知 10](#_Toc338942995)

[6. 上线步骤 10](#_Toc338942996)

[7. 附录 11](#_Toc338942997)

[7.1. 请求错误码 11](#_Toc338942998)

[7.2. OPENSSL密钥对生成 11](#_Toc338942999)

[7.3. C#生成密钥对 12](#_Toc338943000)

# 

特别说明：

1. 由于网络、充值程序、数据库等各种原因，有可能出现订单发送后，出现订单查询不到的现象，为了避免不必要的损失，请延时5分钟在进行查询，或者重新发起充值请求，不可将该错误直接判定为充值失败。
2. 在查询过程中,出现除非明确返回订单失败 OrderFail ,否则不能判定订单失败

# 引言

## 目标

本文档的目的是为向上话费充值系统定义一个直连代理公共接口规范，对外部直连代理系统与向上话费充值系统开放平台协作中的交互模式、安全机制、外部系统接入与管理方式等制定统一的标准。同时也帮助直连代理技术人员接入向上话费充值系统，并快速掌握相关功能，便于尽快投入使用。

## 名词定义

ＲＳＡ签名：采用RSA（SHA1）进行数字签名

合作商系统：与向上话费充值系统对接，进行话费充值的系统。

订单结果通知：向上话费充值系统充值完成后，会议HTTP的方式通知合作商系统。

## 参考文献

1. RSA算法 <http://baike.baidu.com/view/7520.htm>

# 概述

## 概述

向上话费充值系统接口使用HTTPS传输数据，兼容POST/GET方式连接并发送信息。每个HTTP请求发送后，合作商系统在接收并处理请求时必须首先保证整个处理流程（至少是对请求信息的保存步骤）确保成功后，才能返回给发送端确认信息。当合作商系统接收到确认信息后，才认为整个请求被成功发送。

在某些要求务必送达的请求中，上述通知-确认流程必须由接收端确保，如果合作商系统不能接收到正确响应将会按照一定的逻辑重复发送请求。

目前的协议中，订单结果通知是必须送达合作商系统的信息。

## 交易流程

合作商系统按文档要求将充值请求的相关信息如被充值号码、充值金额等参数发送到向上话费充值系统接口，向上话费充值系统接口生成订单并扣除合作商的钱款。

向上话费充值系统内部处理完成后会异步通知直连代理人支付结果，合作商系统在接收到订单处理结果之后，可以对数据库进行相应更新，并在显示给用户的页面中做出相应提示,由于网络故障或其它原因导致合作商系统没有正确接收支付结果时，合作商系统可以调用“4.3订单查询”接口查询订单的状态。

## 相关约定

1. 通讯通道采用HTTPS安全通道，兼容POST或GET方法进行数据传输，接口中数据采用UTF-8进行编码
2. 向上话费充值系统收到合作商请求后，结果以ＸＭＬ的方式返回，合作商应对返回数据进行ＸＭＬ方式解析
3. 向上话费充值系统在订单处理完结后，会以HTTP POST的方式通知合作商系统，通知超时时间为5秒，超时后延时1分钟重试，重试15次，之后不会在通知
4. 本接口采用RSA单向加密算法进行签名验证，签名数据采用UTF-8编码，消息摘要采用SHA1
5. 接口所有参数的参数名一律采用小写
6. 向上话费充值系统具有幂等性，在下单时出现网络错误、系统错误等情况时，务必使用原先的订单号重新下单
7. 在订单查询时，向上话费充值系统除非返回明确的失败状态，不可视订单失败
8. 向上充值系统的公钥会定期进行更换，以保证时效性。合作商系统应具备能力，快速更换公钥而不至于充值业务受影响。

## RSA 签名

根据参数名称将所有请求参数按照字母先后顺序排序:key + value .... key + value。例如：将foo=1,bar=2,baz=3 排序为bar=2,baz=3,foo=1，参数名和参数值链接后，得到拼装字符串bar2baz3foo1，将拼装后的字符串 bar2baz3foo1 转换成 byte[] 字节流，然后采用RSA私钥进行签名,使用公钥进行签名验证，签名时使用SHA1摘要算法。

签名样例：

## 接口返回结果以XML表示

## 通用参数

以下表格中的参数，在每个接口请求中都需要传送

|  |  |  |
| --- | --- | --- |
| **参数** | **说明** | **举例** |
| time | 时间标签，1970-1-1到当前时间的秒数，该时间标签与本系统的时间相差不能超过5分钟 |  |
| macid | 代理商编号，由系统配置 |  |
| sign | Rsa签名结果,采用Base64编码，ＨＴＴＰ发送时，需要进行URL编码 |  |

## 接口返回结果

<result>

<id>2012081011275351200435 </id>

<OrderId>GYSID</OrderId>

<Deno>100</Deno>

<SuccessDeno>100</SuccessDeno>

<ErrCode>OrderSuccess</ErrCode>

<ErrInfo>成功</ErrInfo>

<Sign>ABAFSFewrjwrjlwqr=</Sign>

</result>

字段说明:

|  |  |  |
| --- | --- | --- |
| **参数** | **说明** | **举例** |
| id | 订单号 | 13958168215 |
| oderid | 合作商订单号，用于对帐和订单查询。长度不超过20位 | 2012080800000001 |
| deno | 充值面额，整数 | 50 |
| SuccessDeno | 充值成功面额 |  |
| ErrCode | 错误代码，状态代码 |  |
| Errinfo | 错误信息 |  |
| Sign | 消息签名 |  |

签名验证算法：将字段说明中的各个字段，值提取出来，字段名转换小写，按照字母顺序升序排序，然后使用向上话费充值系统的公钥进行签名验证。计算方式RSA签名算法。

# 合作商要求

1. 保留合作商系统与向上话费充值系统的交互日志，至少保留7天，用作系统异常时的问题跟踪
2. 合作商系统采纳订单异步订单通知状态前，验证通知来源IP、数字签名
3. 合作商系统在下单核订单查询过程中，务必使用向上话费充值系统的公钥验证返回结果的合法性
4. 合作商系统必须在指定时间下载对帐数据进行对帐，若对帐异常，请务必告知杭州向上电子商务有限公司相关人员
5. 合作商必须在次日检查前一日的扣款情况，如果出现扣款异常，请务必告知杭州向上电子商务有限公司相关人员

# 对接联调

## 联调环境

联调地址：http:// 42.120.5.186:82/shop/buyunit

联调账号：admin

对接联系QQ：2214925592

向上话费充值系统公钥：

|  |  |
| --- | --- |
| OpenSSL公钥 | C# 公钥 |
|  |  |

联调帐号密钥对：

|  |  |
| --- | --- |
| OpenSSL密钥对 | C# 密钥对 |
|  |  |

## 联调测试用例

一下表格为联调关键步骤，请合作商技术人员务必仔细逐个测试

|  |  |  |  |
| --- | --- | --- | --- |
| **阶段** | **联调项目** | **步骤说明** | **预期结果** |
| 下单阶段 |  |  |  |
|  |  |  |
| 订单查询 |  |  |  |
|  |  |  |
| 余额查询 |  |  |  |
| 对帐下载 |  |  |  |
| 异步通知 |  |  |  |
| 关键环节 | 查询时授权错误 |  |  |
| 查询时网络错误 |  |  |
| 订单不存在处理 |  |  |

# 技术接口

## 话费充值下单

合作商系统向向上话费充值系统发起充值请求，向上话费充值系统将检查请求有效性， 而后扣款，扣款成功后将订单装入列队，最后返回下单结果。合作商系统在发送下单请求后，需要确认返回结果的合法性、有效性，如出现向上话费充值系统没有返回数据、没有出现网络错误、服务超时、服务器内部错误等情况，需延时重新发送，直至有明确的结果返回。

注意：为了避免定单号重复现象，商户需在订单前加上向上提供的合作商唯一编码。

### 业务参数

|  |  |  |
| --- | --- | --- |
| **参数** | **说明** | **举例** |
| phone | 充值号码，11位数字 | 13958168215 |
| deno | 充值面额，整数 | 50 |
| orderid | 合作商订单号，用于对帐和订单查询。长度不超过20位 | 2012080800000001 |

### 请求样例

请求地址：/orderpay.do

请求样例:

deno=10&macid=test&orderid=2012081313511811302422&phone=13958168215&sign=KgMholUY9mWHgfcjktLZ6ssbb2OHLvpbvpbt1p1PKcEl26QdID0fIfZaBgf%2bzV11kmDcBOyGiisWmVTyBttCrzvxmzl1oTO7z%2fxb8oZnfYT8%2foSsBB2F4%2f7r1fH7iD8xO%2bOyTqnMSeMcwCtbhnqSBt%2fVvO8y1pPY%2b9dBq3abvgU%3d&time=1344865878

返回结果:

<result><id>2012081313511813800005</id><orderid>2012081313511811302422</orderid><deno>10</deno><successdeno>10</successdeno><errcode>OrderSended</errcode><errinfo>处理中</errinfo><sign>cM2VyBjnnrmDuZsqPRuwNNTvvc2poEb1qdrv4EiyNLMtp3Bn5WrADxbd/ZPdU4opdB2NzOMRvH9Tw/x2cTDkbHm6FswdWNvf9ecNk37yoNo1vxHDa699PeAC9eiCS6BCkL54ZR9u3Foo+8gdW0YDMlP3fsJyhSLG//0SLityo+M=</sign></result>

## 游戏充值下单

合作商系统向向上话费充值系统发起充值请求，向上话费充值系统将检查请求有效性， 而后扣款，扣款成功后将订单装入列队，最后返回下单结果。合作商系统在发送下单请求后，需要确认返回结果的合法性、有效性，如出现向上话费充值系统没有返回数据、没有出现网络错误、服务超时、服务器内部错误等情况，需延时重新发送，直至有明确的结果返回。

### 业务参数

|  |  |  |  |
| --- | --- | --- | --- |
| **参数** | **说明** | | **举例** |
| account | 充值的游戏账号 | |  |
| deno | 充值面额，整数 | | 50 |
| orderid | 合作商订单号，用于对帐和订单查询。长度不超过20位 | | 2012080800000001 |
| arsid | 游戏运营商编号 | 游戏相关参数,请参考游戏对接详细说明 | 文档请向商务索要 |
| areacode | 游戏归属地 |
| extparam | 游戏相关参数 |

### 请求样例

请求地址：/orderpayforgame.do

请求样例:

返回结果:

## 订单查询

订单查询仅作为订单结果通知的辅助功能，在通知失败时，使用订单查询获取订单结果。

本系统具有订单处理结果通知的功能，通知功能具有通知失败重新尝试通知的功能，建议订单30分钟查询一次。

在订单查询过程结果，前查询动作成功的前提下，才能进行订单状态的判断。

注意：系统中订单和资金变动明细只保存最近10天的数据。

### 业务参数

|  |  |  |
| --- | --- | --- |
| **参数** | **说明** | **举例** |
| oderid | 合作商订单号，用于对帐和订单查询。长度不超过20位 | 2012080800000001 |

### 请求样例

请求地址：/query.do

请求样例:

macid=test&orderid=2012081312534895000459&sign=kK9crCH7HWaIjHjz%2b5jP4KIuwTG5ZYmMlPW4mVJf%2bwLTzi88godrGRQ81UH0pdtcxolhye%2fbE8IAs8H7Rspvi4BTPJl11qomguFLlONKD9vpgCCqHQGRgiGAo5V6iw3W6V7GJh4l7wcKrmnTu8TgJ6wD7mQ6CCVIunrK5IvgFY8%3d&time=1344862799

查询结果样例:

<result><id>2012081307270423800361</id><orderid>2012081307270420601083</orderid><deno>10</deno><successdeno>10</successdeno><errcode>OrderFail</errcode><errinfo>失败</errinfo><sign>X39kW64GW7z/NPK1AE7Fvk3DXf+2f1+Lil0LmK3CiBuxGWGt91nw02HBw9Eizn+XQZ4daQgOsQ+zNbzWFck+Qyk44RBlGsBvRA85cx69GV7tHCgEqQSCvkJWnFVYXRKgEBstw1hOmeEsozGBE5caNkBRjeuHeQ74cOwUg9VYv1c=</sign></result>

### 注意要点

1. 查询过程,签名失败,不能将订单处理成失败
2. 订单查询不存在的处理

## 余额查询

余额查询结果仅供参考,余额数据,依据扣款日志、订单实际扣款计算得出。

### 返回结果

<result><balance>100.00</balance></result>

### 请求样例

地址：/balance.do

请求样例:

macid=test&sign=kK9crCH7HWaIjHjz%2b5jP4KIuwTG5ZYmMlPW4mVJf%2bwLTzi88godrGRQ81UH0pdtcxolhye%2fbE8IAs8H7Rspvi4BTPJl11qomguFLlONKD9vpgCCqHQGRgiGAo5V6iw3W6V7GJh4l7wcKrmnTu8TgJ6wD7mQ6CCVIunrK5IvgFY8%3d&time=1344862799

## 对帐数据下载

注意：本系统将在3点-9点间导出前一天的订单数据，请安排好相应的下载时间

对帐文件以TXT文件的方式保存

### 业务参数

|  |  |  |
| --- | --- | --- |
| **参数** | **说明** | **举例** |
| date | 对帐数据日期 | 2012-08-08 |

### 返回结果

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 向上订单号 | 代理订单号 | 充值号码 | 充值面额 | 充值状态 | 充值时间 |
| 111111 | 121212 | 1333333333 | 10 | SUCCESS | 2012-09-01 18:00:00 |
| 222222 | 232323 | 1888888888 | 20 | REFUND\_SUCCESS | 2012-09-01 20:00:00 |

### 请求样例

地址：/billdownload.do

请求样例:

date=2012-08-24&macid=test&sign=kK9crCH7HWaIjHjz%2b5jP4KIuwTG5ZYmMlPW4mVJf%2bwLTzi88godrGRQ81UH0pdtcxolhye%2fbE8IAs8H7Rspvi4BTPJl11qomguFLlONKD9vpgCCqHQGRgiGAo5V6iw3W6V7GJh4l7wcKrmnTu8TgJ6wD7mQ6CCVIunrK5IvgFY8%3d&time=1344862799

## 订单结果通知

向上话费充值系统在订单处理完结后，会立即发送订单通知。通知已HTTP GET的方式发送。向上话费充值系统设置通知超时时间5s,通知失败后会延时1分钟重试，重试15次后终止。

若合作商系统长时间不能正确接收订单结果通知，向上话费充值系统会自动关闭通知功能，请合作商及时修正问题，并通知向上商务重新开启订单通知。

合作商系统收到通知并确认通知状态请务必返回 “true” 字符串，表示已经收到通知，向上话费充值系统将在收到确认消息后停止该订单的通知。

### 业务参数

|  |  |  |
| --- | --- | --- |
| **参数** | **说明** | **举例** |
| Id | 系统订单号 |  |
| OrderId | 合作商订单号 |  |
| Deno | 订单面额 |  |
| SuccessDeno | 成功面额 |  |
| Errcode | 错误代码 |  |
| Errinfo | 错误信息 |  |

### 请求样例

deno=10&errcode=OrderFail&errinfo=%e5%a4%b1%e8%b4%a5&id=2012090314522704800002&orderid=2012081313511811302422&sign=KLrtYMxwi%2fsHzLVybI%2b3QeJYhQtlTIrpq7ZGeX2Mqa0ILDE6fSt0rRQIsFxziNwSSxOolizumS0zCP%2fT9bslzFQiyHswpccJmC39l%2fpSPlfGF2SYUhrDMgKKDZQTXAdz3EdImhyUnnedLVtXoRgJdfEIIJ7cAIpaM%2fSwEP9aIu0%3d&successdeno=10

### 注意要点

1. 合作商系统收到通知时，需要确认通知的来源IP地址，验证签名
2. 向上话费充值系统会对一个订单尝试多次发起通知消息，合作商系统必须能够处理多次通知
3. 合作商在收到并确认消息时，务必返回”true” ，表示消息已经收到、并确认

# 上线步骤

1. 生成RSA密钥对，保留私钥，公钥提交到向上
2. 下单服务器ＩＰ地址表
3. 订单结果通知地址

# 附录

## 请求错误码

|  |  |  |
| --- | --- | --- |
| **状态码** | **说明** | **可采取后续处理** |
| OrderSuccess | 订单充值成功。 订单充值成功，可能是部分成功，请参考消息中订单面额和成功面额 | 订单处理成功 |
| OrderExists | 代理商订单号重复 | 订单提交失败 |
| OrderFail | 订单处理失败 | 订单处理失败 |
| OrderSended | 系统已经正确接收订单，并正在进行充值 | 等待通知 |
|  |  |  |
| ConfigError | 配置性错误，具体错误查看错误信息 | 调整账号配置 |
|  |  |  |
| NumberError | 号码错误 | 订单失败 |
| AccountClosed | 充值账号已经关闭，请联系商务 | 订单失败 |
| AccountBalance | 账号余额不足 | 订单失败 |
| ProductClosed | 充值产品暂不可用，稍后再试 | 订单失败 |
| ProductError | 产品错误，请联系商务 | 订单失败 |
| OrderNotExists | 订单查询失败，请延时5分钟再查，若还是查询不到，务必重新下单请求 | 延时重试 |

## OPENSSL密钥对生成

1. 下载OPENSSL
2. 首先生成私钥：openssl genrsa -out mykey.pem 1024
3. 然后生成相应的公钥openssl rsa -in mykey.pem -pubout > mykey.pub

对于java系统, 需要将PEM 格式 公钥,转换成DER 格式

## C#生成密钥对

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

//公钥

string pubKey = rsa.ToXmlString(false);

//私钥

string priKey = rsa.ToXmlString(true);

生成后,保存公钥和私钥,将公钥发给向上