中间业务平台接口规范

（机构版 v1.1）

版本号	日期	姓名	描述
v1.0	2010/12/01	周忠杰，张浩	基本通讯模式以及接口类型
v1.1	2011/11/05	陶晔	报文格式修订

目 录

1.机构接入方式

1.1. 异步长连接

上海德颐中间业务平台对外支持点对点的异步长连接接入。平台与接入机构间约定双方提供 TCP 服务的端口号，建立一对或多对单工 SOCKET 端口（互为客户 / 服务端），客户端作为发送数据端口，服务端作为接收数据端口。

异步长连接保持心跳包机制。

1.2. 同步短连接

部分交易应用并发量不大的情况下机构间也支持同步短连接方式接入。此时上海德颐对外提供统一接入端口

1.3. 格式符号说明

本格式符号定义如下：

符号	含义
M	必用数据元，如此域无内容，报文鉴别出错
C	可选数据元
C+	返回成功时必选
BINARY,B,b,Byte	2 进制数据
N,n	数字数据
A,a	字母表数据
ANS	数字与字典组合
LVAR, .	可变长（0－9）
LLVAR, ..	可变长（0－99）
LLLVAR, ...	可变长（0－999）
ASC	ASC 压缩
BCD	BCD 压缩

1.4. 报文结构说明

交易报文包含两个组成部分：报文长度和应用数据。其结构如下图所示：

报文长度（不含本身）| 报文包体数据（不定长）

报文长度占 4 个字节，是以 ASCII 码表示的十进制数，右靠左补 ASC ‘0’。

注：心跳包为 3 分钟未有交易则发送 ASCII 格式的 ‘0000’

2. 交易接口

2.1. 管理报文

2.1.1. 签到请求

位	域名定义	属性	格式	类型	请求	响应	备　　注
-	报文类型	n4		ASCII	0820	0830	
-	位元表	Bit64		BCD	M	M	
7	交易传输时间	n10	MMDDhhmmss	ASCII	C	C	
11	系统跟踪号	n6		ASCII	M	M	
12	本地交易时间	n6	HHMMSS	ASCII	M	M	
13	本地交易日期	n4	MMDD	ASCII	M	M	
33	交易机构	N..11	LLVAR	ASCII	M	M	
39	响应码	an2		ASCII		M	
48	签到交换数据	ans…512	LLLVAR	ASCII		C	当 39 域为 00 时必选

48 域用法说明：

ID	数据元名称	类型	说明
	长度	an	“040”
1	加密的 PIN 密钥	an	16 字节的 PIK
2	PIN 密钥的验证码	an	4 字节的 PIN CHECK VALUE
3	加密的 MAC 密钥	an	16 字节的 MAK
4	MAC 密钥的验证码	an	4 字节的 MAC CHECK VALUE

注：前 20 个字节为 PIN 的工作密钥的密文，后 20 个字节为 MAC 的工作密钥的密文。（其中，前 16 个字节是密文，后 4 个字节使 checkvalue；前 16 个字节解出明文后，对 8 个 0x00 做 des，取结果的前四位与 checkvalue 的值比较应该是一致的）。

2.2 交易报文

2.2.1. 信用卡还款

位	域名定义	属性	格式	类型	请求	响应	备　　注
	消息类型	N4		ASCII	M	M	0200|0210
	位图	B64		BCD	M	M	
2	交易卡号	N..19	LLVAR	ASCII	C	M	
3	处理码	N6		ASCII	M	M	200000
4	交易金额	N12		ASCII	M	M	
7	交易传输时间	N10	MMDDhhmmss	ASCII	M	M	
11	交易流水号	N6		ASCII	M	M	
12	本地交易时间	N6	hhmmss	ASCII	M	M	
13	本地交易日期	N4	MMDD	ASCII	M	M	
33	交易机构	N..11	LLVAR	ASCII	M	M	
34	第二交易帐号	Ans..99	LLVAR	ASCII	M	M	信用卡卡号
35	第二磁道数据	Ans..37	LLVAR	ASCII	M		
36	第三磁道数据	Ans...104	LLLVAR	ASCII	C		如果存在3磁道则出现
37	系统参考号	AN12		ASCII		C	
38	授权码	AN6		ASCII		C	
39	返回代码	AN2		ASCII		M	00表示成功
41	终端号	N8		ASCII	M	M	
42	商户号	N15		ASCII	M	M	
52	个人密码	B 64		BCD	C		有PIN输入时必选
64	MAC	B 64		BCD	M	C+	

2.2.2. 手机充值

位	域名定义	属性	格式	类型	请求	响应	备　　注
	消息类型	N4		ASCII	M	M	0200
	位图	B64		BCD	M	M	
2	交易卡号	N..19	LLVAR	ASCII	C	C	
3	处理码	N6		ASCII	M	M	300000
4	交易金额	N12		ASCII	M	M	
7	交易传输时间	N10	MMDDhhmmss	ASCII	M	M	
11	交易流水号	N6		ASCII	M	M	
12	本地交易时间	N6	hhmmss	ASCII	M	M	
13	本地交易日期	N4	MMDD	ASCII	M	M	
33	交易机构	N..11	LLVAR	ASCII	M	M	
34	第二交易帐号	Ans..99	LLVAR	ASCII	M	M	充值手机号

35	第二磁道数据	Ans..37	LLVAR	ASCII	M		
36	第三磁道数据	Ans...104	LLLVAR	ASCII	C		如果存在3磁道则出现
37	系统参考号	AN12		ASCII	C	C	
39	返回代码	AN2		ASCII		M	00表示成功
41	终端号	N8		ASCII	M	M	
42	商户号	N15		ASCII	M	M	
64	MAC	B 64		BCD	M	C+	

注：不同交易对应的交易代码是不同的，具体待业务确认后确定。

2.2.3. 手机充值（无支付版本）

位	域名定义	属性	格式	类型	请求	响应	备　　注
	消息类型	N4		ASCII	M	M	0200||0210
	位图	B64		BCD	M	M	
2	交易卡号	N..19	LLVAR	ASCII	C	C	付款帐号
3	处理码	N6		ASCII	M	M	300000
4	交易金额	N12		ASCII	M	M	
7	交易传输时间	N10	MMDDhhmmss	ASCII	M	M	
11	交易流水号	N6		ASCII	M	M	
12	本地交易时间	N6	hhmmss	ASCII	M	M	
13	本地交易日期	N4	MMDD	ASCII	M	M	
33	交易机构	N..11	LLVAR	ASCII	M	M	
34	第二交易帐号	Ans..99	LLVAR	ASCII	M	M	充值手机号
37	系统参考号	AN12		ASCII	C	C	
39	返回代码	AN2		ASCII		M	00表示成功
41	终端号	N8		ASCII	M	M	
42	商户号	N15		ASCII	M	M	

注：不同交易对应的交易代码是不同的，具体待业务确认后确定。

3. 附录

MAC 算法

参与报文校验码（MAC）的数据由三部分产生：初始数据，原始数据，补位数据。

MAC 算法如下：

1）算法定义：采用 DES CBC 算法。

2）初始数据：0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00。

3）原始数据：

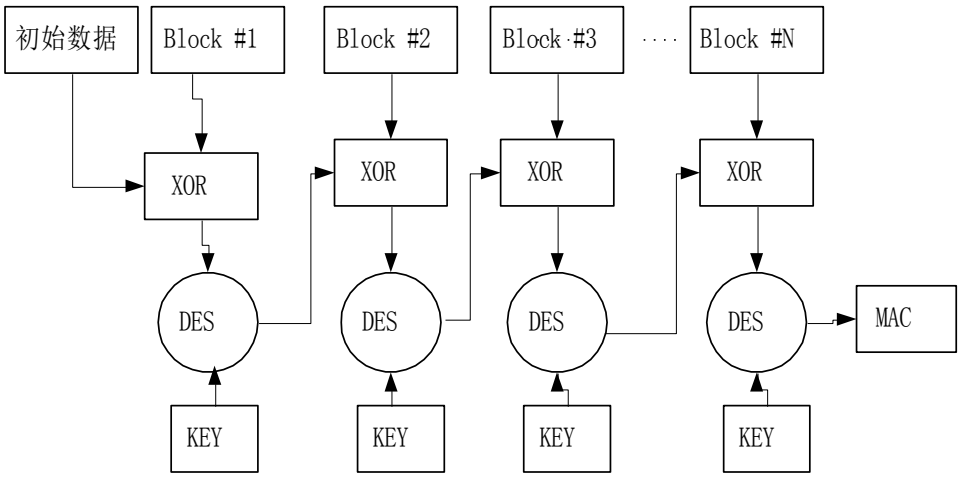
4）补位数据：若原始数据不是 8 的倍数，则右补齐 0x00。若原

始数据为 8 的整数倍，则不用补齐 0x00。

5）密　　钥：MAC 密钥。

MAC 的产生由以下方式完成：(最后一组数据长度若不足 8 的倍数，则右补齐 0x00；若数据长度为 8 的整数倍，则无需补充 0x00)。

MAC 签名计算流程图：



参与计算 MAC 的域如下：

0(报文类型),2,3,4,7,11,18,20,21,25,28,32,33,38,39,41,42,48

MAC域的构成将根据bitmap中上述域是否出现在报文中来确定。上述域只要出现在报文中，应截下送入MAC计算域。

对所选择的MAC报文域，应进一步作字符处理。除去一些冗余信息，以提高MAC的质量。处理方法如下：

(1) 带长度值的域在计算MAC时应包含其长度值信息；

(2) 在域和域之间插入一个空格；

(3) 所有的小写字母转换成大写字母；

(4) 除了字母(A-Z)，数字(0-9)，空格，逗号(，)，点号(.)以外的字符都删去；

(5) 删去所有域的打头空格和结尾空格；

(6) 多于一个的连续空格，由一个空格代替。

电话支付终端终端采用ECB的加密方式，简述如下：

a) 将欲发送到电话支付中心的数据，从报文类型到有效数据域之间的部分构成MAC ELEMEMENT BLOCK （MAB）。

b) 对MAB，按每8个字节做异或（不管信息中的字符格式），如果最后不满8个字节，则添加“0X00”。

示例：

MAB = M1 M2 M3 M4

其中：

M1 = MS11 MS12 MS13 MS14 MS15 MS16 MS17 MS18

M2 = MS21 MS22 MS23 MS24 MS25 MS26 MS27 MS28

M3 = MS31 MS32 MS33 MS34 MS35 MS36 MS37 MS38

M4 = MS41 MS42 MS43 MS44 MS45 MS46 MS47 MS48

按如下规则进行异或运算：

```
                MS11 MS12 MS13 MS14 MS15 MS16 MS17 MS18
XOR)            MS21 MS22 MS23 MS24 MS25 MS26 MS27 MS28
-----------------------------------------------------
TEMP BLOCK1 =  TM11 TM12 TM13 TM14 TM15 TM16 TM17 TM18
```

然后，进行下一步的运算：

```
               TM11 TM12 TM13 TM14 TM15 TM16 TM17 TM18
XOR)            MS31 MS32 MS33 MS34 MS35 MS36 MS37 MS38
-----------------------------------------------------
TEMP BLOCK2 =  TM21 TM22 TM23 TM24 TM25 TM26 TM27 TM28
```

再进行下一步的运算：

```
              TM21 TM22 TM23 TM24 TM25 TM26 TM27 TM28
XOR)           MS41 MS42 MS43 MS44 MS45 MS46 MS47 MS48
-----------------------------------------------------
RESULT BLOCK = TM31 TM32 TM33 TM34 TM35 TM36 TM37 TM38
```

c) 将异或运算后的最后8个字节（RESULT BLOCK）转换成16 个HEXDECIMAL：

```
RESULT BLOCK = TM31 TM32 TM33 TM34 TM35 TM36 TM37 TM38
             = TM311 TM312 TM321 TM322 TM331 TM332 TM341 TM342 ||
               TM351 TM352 TM361 TM362 TM371 TM372 TM381 TM382
```

d) 取前8 个字节用MAK加密：

```
ENC BLOCK1 = eMAK (TM311 TM312 TM321 TM322 TM331 TM332 TM341 TM342)
           = EN11 EN12 EN13 EN14 EN15 EN16 EN17 EN18
```

e) 将加密后的结果与后8 个字节异或：

```
            EN11  EN12  EN13  EN14  EN15  EN16  EN17  EN18
XOR)        TM351 TM352 TM361 TM362 TM371 TM372 TM381 TM382
-------------------------------------------------------------
TEMP BLOCK= TE11  TE12  TE13  TE14  TE15  TE16  TE17  TE18
```

f) 用异或的结果TEMP BLOCK 再进行一次双倍长密钥算法运算。

```
ENC BLOCK2 = eMAK (TE11 TE12 TE13 TE14 TE15 TE16 TE17 TE18)
           = EN21 EN22 EN23 EN24 EN25 EN26 EN27 EN28
```

g) 将运算后的结果（ENC BLOCK2）转换成16 个HEXDECIMAL：

```
ENC BLOCK2 = EN21 EN22 EN23 EN24 EN25 EN26 EN27 EN28
           = EM211 EM212 EM221 EM222 EM231 EM232 EM241 EM242 ||
             EM251 EM252 EM261 EM262 EM271 EM272 EM281 EM282
```

示例：

```
ENC RESULT= %H84, %H56, %HB1, %HCD, %H5A, %H3F, %H84, %H84
```

转换成16 个HEXDECIMAL:

“8456B1CD5A3F8484”

h) 取前8个字节作为MAC值。

取”8456B1CD”为MAC值。

PIN 算法

密码明文＝2 位密码长度＋密码明文（若不足 8 位补’F’）

帐户密码密文=DES(密码明文，PIN 密钥)

若个人密码是“123456”，则帐户密码明文为“06123456”

密文为：DES(0x060x12/0x34/0x56/0xFF/0xFF/0xFF/0xFF, PINKEY)

注：需要对主帐号做异或处理

11 des 还是 3des

’00’ -- plain text

’11’ -- DES

’13’ -- 3DES

’21’ -- MD5

’22’ -- base64