VIETTEL GLOBAL JOIN STOC COMPANY JSC

CONNECT API DOCCUMENT
WITH MPS SYSTEM

Ha Noi, 08/2015

APPENDIX

TABLE CHECK NOTE CHANGE

*A – New, M – Edit, D – Delete

Change day	Location	A * M	Address	Old version	Change description	New version
11/06/2014	- 2.3.1 - 2.3.2	M		1.3		1.4

1   INTRODUCE

1.1   Document Main Step

All this document have:

- ❖ **Part I:** Introduce document overview, the concept language, the acronym or image was been using.
- ❖ **Part II:** Connection source detail description
- ❖ **Part III:** All document appendix: error Table, source translate table

1.2   Concept, acronym

Acronym	Description	Note
HTTP Redirect	It mean get information function between CP and Viettel	
RSA Private key	one key in double key encode of RSA	
RSA Public key	one key in double key encode of RSA	
AES Des key	Key encode AES	

Table 1: Decription and acronym

1.3   A l l   acronym was been using

Acronym	Note
CP	Provider
S1-S10	Step1 to step 10

Table 2: all acronym was been using

1.4   All document read more

Document name	The day apply	Source	Note

Table 3: Table document

2 OVERVIEW DESCRIPTION

2.1 Overview description
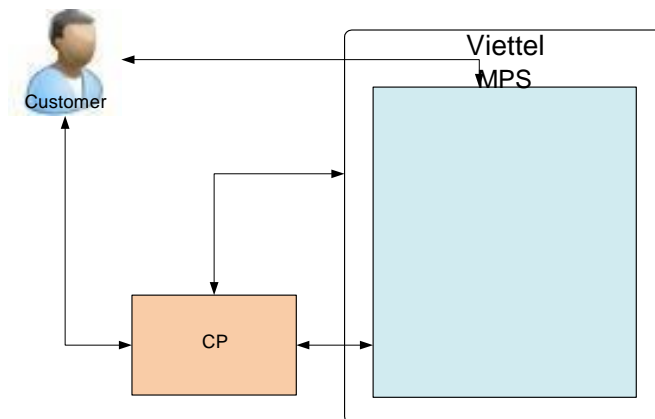
Technique connect detail document between CP and MPS System of Viettel

2.2 Fomat send data

Step encode description and send data between Viettel(A) and CP(B)

Encode key of Viettel and CP

- Viettel: PubVT, PriVT, PubCP

- CP: PubCP, PrivCP, PubVT

S1: Input data send from CP to VT follow format for example:

SUB=zzzCATE=game&ITEM=Mario&SUB_CP=AE&CONT=Good Game
&PRICE=10&REQ=12313060514 1022002&MOBILE=84986062758&SOU
RCE=CLIENT

S2: CP encode data and input follow AES-key algorithm on step by step transaction of CP for example:

value=xacxvcvcvfdfsdfs

S3: Format new data follow: input_encrypted + key AES for example:

value=ffsdfsdfreawrew&key=0dded43371cd3150953b256eb3ae4bc8

S4: CP encode by PubVT for example:

DATA=fsdfrgdfgd6547869870==-0=-0

S5: CP create data signature by PrivCP for example:

SIG=dfsdthgfyuytu6576579769645645645

S6: Send information data_encrypted and signature to VT follow http Redirect for example:

http://xxx.yyy.zzz.vvv/charge.html?PRO=Centech&CMD=DOWNLOAD&SER=

game&SUB=game10K&DATA=TtTu6wSg1TjKT0Hil5VvYVbY%2F77Z21IbYo

3fnN4jB&SIG=jYyBCMT8ufWBYKtMig8xJx1rSAXrdNNLlsz8

S7: (A) receive data on request and confirm true signature or no

S8: If verify = true , (A) decryption data by PrivVT

S9: Follow data_decrypted have input_incrypted and key AES

S10: Decryption data input_encrypted by key AES

2.3   Decription all connect function

2.3.1   Detail Table index in short message

All parameters send request to payment always have full function on table under, if the parameter have not value so take blank and over come

Parameters	Descriptions	Values	Size	Acronym
signature	Signature confirm	String	2048	SIG
mobile	The number needed payment. If subscriber using 3G so system doesn't check and charging online, apply for all CPs online payment.	String	15	MOBILE
data	Data was be encode	String	4000	DATA
service_id	Payment service		20	SER
sub_service_id	Description subscriber service	String	20	SUB
category_name	List produce needed payment	String	30	CATE
item_name	Produce needed payment	String	25	ITEM
sub_cp_name	Subscriber provider name	String	30	SUB_CP
contents	More description	String	100	CONT
response_code	Result error code	String	Bảng mã lỗi bên dưới	RES
price	Money need pay	String	10	PRICE
cmd	Function payment: - REGISTER: register subscriber service - CANCEL: cancel subscriber - DOWNLOAD, CHARGE,	String	20	CMD

Parameter	Description	Values	Độ dài dữ liệu	Ký hiệu
	MO,…: payment not problem with subscriber.			
provider_id	Id of CP on MPS system	String	20	PRO
key	Key AES follow transaction	String	32	KEY
cp_request_id	Id transaction on CP	String	18	REQ
charge_type	Payment function: mobile, card,… (MOBILE, CARD, …)	String	10	TYPE
source_type	Payment source (client,wap/web) - *if SOURCE=WAP and have url return so return redirect url enif put http response*	String	5	SOURCE
imei	Imei of mobile device - *if SOURCE=CLIENT so keep IMEI must have, not follow every function*	String	50	IMEI
session_id	Session id of customer when connect to CP page.	String	100	SESS
otp	Code payment otp, Timeout for transaction OTP from receive result to submit may be default 120s	String	20	OTP
otp_type	Request payment otp: 0 – request send OTP code 1 – request payment by OTP input, cp_request_id send when submit OTP need same with cp_request_id of transaction send OTP 2- request send OTP by FLASH	String	1	OTP_TYPE
user_name	Phone number register service of customers	String	15	USER
password	Pasword of customers	String	10	PASS

2.3.2 *Payment*

Viettel build this function provide command for CP payment to buy number content

Reason: Because function **HTTP_REFERER** of **HTTP REQUEST** can be change when disabled form client browser, when Customer confirm CP to payment error. So that when send request always need cpCode.

Change: Update more parameter of mobile and source, and all parameter need values

Request: **http://xxx.yyy.zzz/charge.html**?PRO=xxx &SER=yyy&SUB=zzz&CMD=vvv&DATA='.urlencode($data_encrypted).'&SIG='.$signature;

Purpose: Payment when customer buy number content CP

a. Parameter needed encode (in parmeter DATA index b)

No.	Parameters	Descriptions	values
1.	SUB	Description about charges package of service	String
2.	CATE	List service need payment	String
3.	ITEM	Produce need payment	String
4.	SUB_CP	Provider	String
5.	CONT	More description	String
6.	PRICE	Price	String
7.	REQ	Transaction code of CP	String
8.	MOBILE	The number needed payment. If subscriber using 3G so system doesn't check and charging online, apply for all CPs online payment.	String
9.	SOURCE	Payment source (WAP/CLIENT), if don't send data so default is wap. If application send so print values, don't redirect link url	String

No.	Parameter	Description	Values
10.	TYPE	Payment flow, if don't have this parameter so default is Mobile payment. Beside that system support: card, banking, vas,…	String

b. Parameter send to HTTP request (on GET url request)

No.	Parameter	Description	values
1.	PRO	Indentification of CP on MPS system	String
2.	SER	Payment service	String
3.	SUB	Description charges package of service	String
4.	CMD	Function payment: DOWNLOAD, REGISTER, CANCEL, RESTORE,… RESTORE: follow this command, system will payment repeat with subscriber with inactive status	String
5.	DATA	Data after encode	String
6.	SIG	Signature encode for data	String

c. **Result**: Return request after decryption

No.	Parameter	Description	Values
1.	REQ	Transaction code on CP system	String
2.	RES	Error code	String
3.	MOBILE	Phone number need payment(if payment by basic account)	String

No.	Parameter	Description	Values
4.	CMD	Function payment	String
5.	PRICE	Money was be charging	String
6.	SOURCE	Payment source (WAP/CLIENT)	

2.3.3 Login when confirmed subscriber (header enrichment)

Viettel build this function support user automatic Login into system to using service of CP

Description: When user connect to wap of CP, CP automatic call to url to get subscriber of Viettel. Viettel indentified and check information of subscriber used service of CP yet

Result: Result information will be return follow List Error in Apendix 3.1

Request: **http://xxx.yyy.zzz/MPS/mobile.html**?PRO=xxx &SER=yyy&SUB=zzz&DATA='.urlencode($data_encrypted).'&SIG='.$signature;

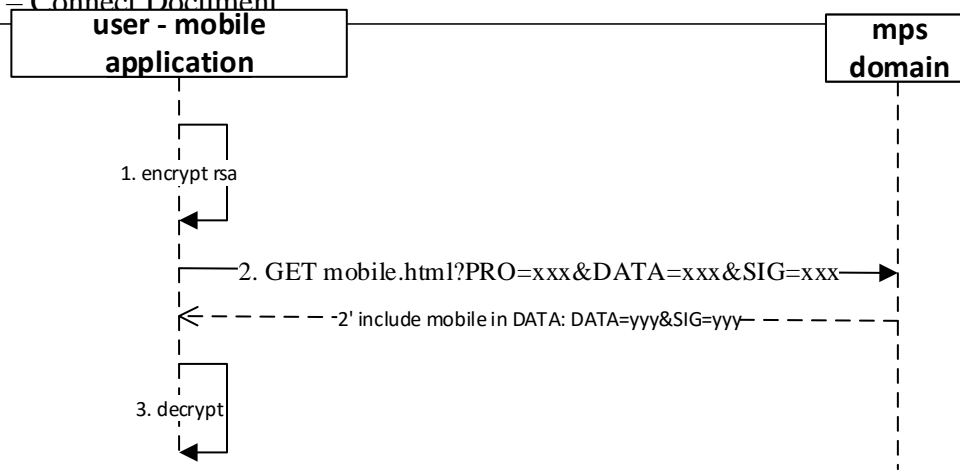**Purpose**: Login for indentification mobile follow wap.

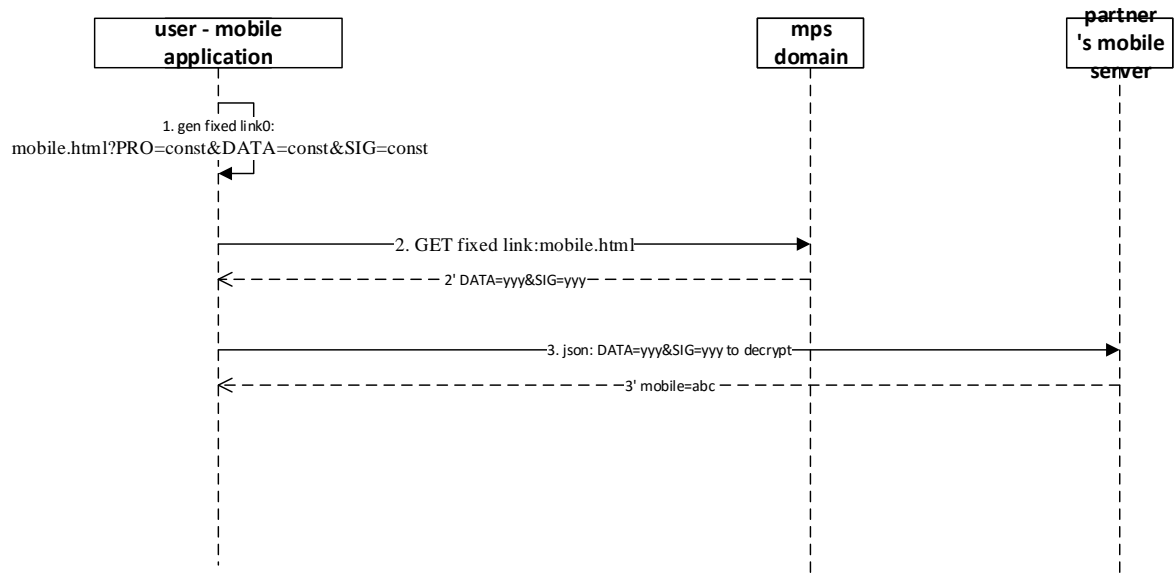1. partner in view – wap (user use 3g,4g,5g go to website)
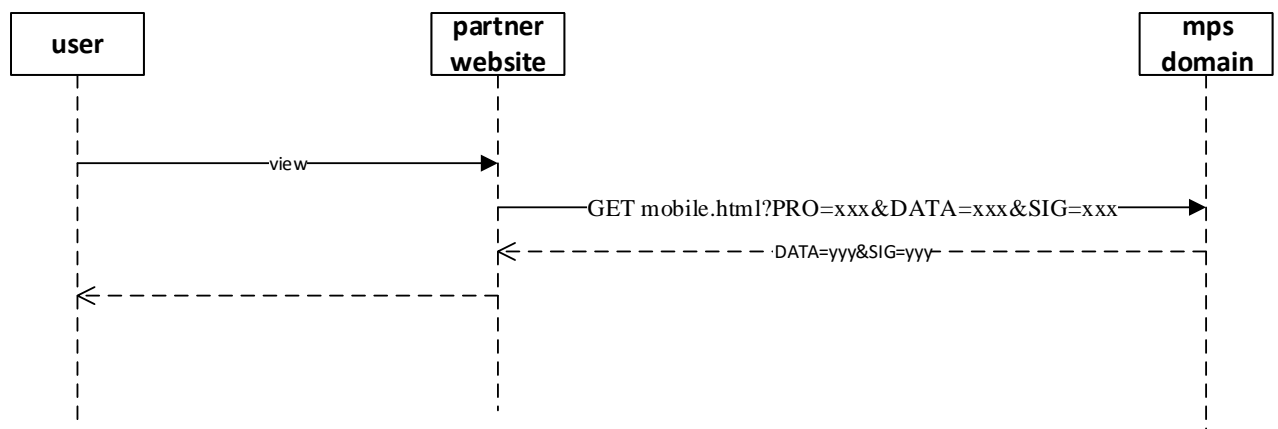
2. partner in view – mobile application (user use 3g,4g,5g)
– way 1
Wit mobile application, partner can choose way 1 or way 2
to detect msisdn.
- with way 1: rsa keys stored in mobile application. Not
secure by way 2 (rsa keys on server)

3. partner in view – mobile application (user use 3g,4g,5g)
– way 2

a. Parameter need encode (in parmeter DATA index b)

No.	Parameter	Description	Values
1.	SUB	Description for service charges Package	String
2.	REQ	Config code for transaction of CP	String
3.	SOURCE	Payment source (WAP/CLIENT), If don't send data to system, it put default is wap	String
4.	SESS	Session id of customer when connect to site of CP	String

b. Parameter send to HTTP Request (on GET url request)

No.	Parameter	Description	Values
1.	PRO	Config of CP on MPS system	String
2.	SER	Payment service	String
3.	SUB	Description for service charges Package	String
4.	DATA	Data after encode	String

No.	Parameter	Description	Values
5.	SIG	Signature of Data was be encode	String

c. **Return Result:** Return request when finish encode

No.	Parameter	Description	Values
1.	REQ	Config code for transaction of CP	String
2.	RES	List Error transaction	String
3.	MOBILE	MSISDN need chaging for service (If chaging by basic account)	String
4.	CMD	Form payment	String
5.	PRICE	Money need charging	String
6.	SOURCE	Payment source (WAP/CLIENT)	

2.3.4 *Login when don't confirm subscriber*

Viettel build this function to support user login to system using service of CP follow login form of Viettel

Description: When Viettel system don't confirm subscriber, it provide for CP one function login by show login form to confirm Username(mobile) and password

Result: Result information will be return follow List Error in Apendix 3.1

Request: **http://xxx.yyy.zzz/MPS /login.html**?PRO=xxx &SER=yyy&SUB=zzz&DATA='.urlencode($data_encrypted).'&SIG='.$signature;

Purpose: Login by wifi/client when don't confirm mobile

b. Parameter need encode (in parmeter DATA)

No.	Parameter	Description	Values
1.	SUB	Payment service	String
2.	REQ	Config code for transaction of CP	String
3.	SOURCE	Payment source (WAP/CLIENT), If don't send data to system, it put default is wap	String

| 4. | SESS | Session id of customer | String |

b. Parameter send to HTTP Request (on GET url request)

No.	Parameter	Description	Values
1.	PRO	Config of CP on MPS system	String
2.	SER	Payment system	String
3.	SUB	Description for service charges Package	String
4.	DATA	Data after encode	String
5.	SIG	Signature of Data was be encoding	String

c. **Return Result:** Return request when finish encode

No.	Parameter	Description	Values
1.	REQ	Config code for transaction of CP	String
2.	RES	List Error	String
3.	MOBILE	Subscriber (if customer want to payment by basic account)	String
4.	CMD	Function payment	String
5.	PRICE	Money was be charging	String
6.	SOURCE	Payment source (WAP/CLIENT)	

2.3.5 Login follow client

Viettel build this function support for user login CP system to user follow client of CP provider

Description: When client of CP build want login to MPS system, it must send username(mobile) and password, device imei follow http request link to MPS.

Result: Result information will be return follow List Error in Apendix 3.1

Request: **http://xxx.yyy.zzz/MPS /login.html**?PRO=xxx &SER=yyy&SUB=zzz&USER=ttt&PASS=yyy&DATA='.urlencode(

$data_encrypted).'&SIG='.$signature;

Purpose: Provide for customer login with CP client

a. Parameter need encode (in parmeter DATA)

No.	Parameter	Description	Values
1.	SUB	Charges package of service need payment	String
2.	REQ	Config code for transaction of CP	String
3.	IMEI	Imei number of device, must have when source_type = CLIENT	String
4.	SOURCE	Payment source (WAP/CLIENT), If don't send data to system, it put default is wap	String
5.	SESS	Session id of customer when login by client of CP	String

b. Parameter send to HTTP Request (on GET url request)

No.	Parameter	Description	values
1.	PRO	Config of CP on MPS system	String
2.	SER	Payment system	String
3.	SUB	Description for service charges Package	String
4.	USER	Phone number of customer, it can be user for connect by wifi or client	
5.	PASS	Password of customer, it can be user for connect by wifi or client	
6.	DATA	Data after encode	String
7.	SIG	Signature of data after encode	String

c. **Return Result:** Return request when finish encode

No.	Parameter	Description	Values
1.	REQ	Config code for transaction of CP	String

No.	Parameter	Description	Values
2.	RES	Transaction Error	String
3.	MOBILE	Subscriber (if customer want to payment by basic account)	String
4.	CMD	Function payment	String
5.	PRICE	Money was be charging	String
6.	SOURCE	Payment source(WAP/CLIENT)	String

2.3.6 Check transaction status

Viettel build this function support CP check again all transaction from Viettel send to payment before

Reason: Because data send public tranship 2G/3G maybe drop transaction information, so conflict data between CP and Viettel.

Request: **http://xxx.yyy.zzz/MPS /check .html**?PRO=xxx &SER=yyy&SUB=zzz&CMD=vvv&DATA='.urlencode($data_encrypted).'&SIG='.$signature;

Purpose: Check transaction status, default timeout transaction is 120s from CP send payment request to send request check transaction

Note: In response message return follow data online not url return

a. Data need encode (in parmeter DATA)

No.	Parameter	Description	Values
1.	SUB	Description for service charges Package	String
2.	CATE	List service need payment	String
3.	ITEM	Produce need payment	String
4.	SUB_CP	Provider	String
5.	CONT	More description	String
6.	PRICE	Price must pay (market denominations)	String
7.	REQ	Transaction code of CP want to check	String
8.	MOBILE	Phone number need payment. If user using 3G so charge follow this parameter	String
9.	SOURCE	Payment source (client, wap/web, app),	String

No.	Parameter	Description	Values
		if don't send data so system default wap. If application send request so system not return redirect url link	

b. HTTP request (on GET url request)

No.	Parameter	Description	Values
1.	PRO	Config of CP on MPS system	String
2.	CMD	Values CMD=CHECK	String
3.	SER	Payment service	String
4.	SUB	Description for service charges Package	String
5.	DATA	Data after encode	String
6.	SIG	Signature of data after encode	String

c. **Return Result: Return request when finish encode**

No.	Parameter	Description	Values
1.	REQ	Config code for transaction of CP	String
2.	RES	Transaction error	String
3.	MOBILE	MSISDN need chaging for service (If chaging by basic account)	String
4.	CMD	Function payment	String
5.	PRICE	Money need payment	String
6.	SOURCE	Payment source (WAP/CLIENT)	

2.3.7 OTP Payment

Viettel build this function support CP payment charges telecomunications by OTP function

Request: **http://xxx.yyy.zzz/MPS/otp.html**?PRO=xxx &SER=yyy&SUB=zzz&CMD=vvv&DATA='.urlencode($data_encrypted).'&SIG='.$signature;

Purpose: CP can payment by OTP
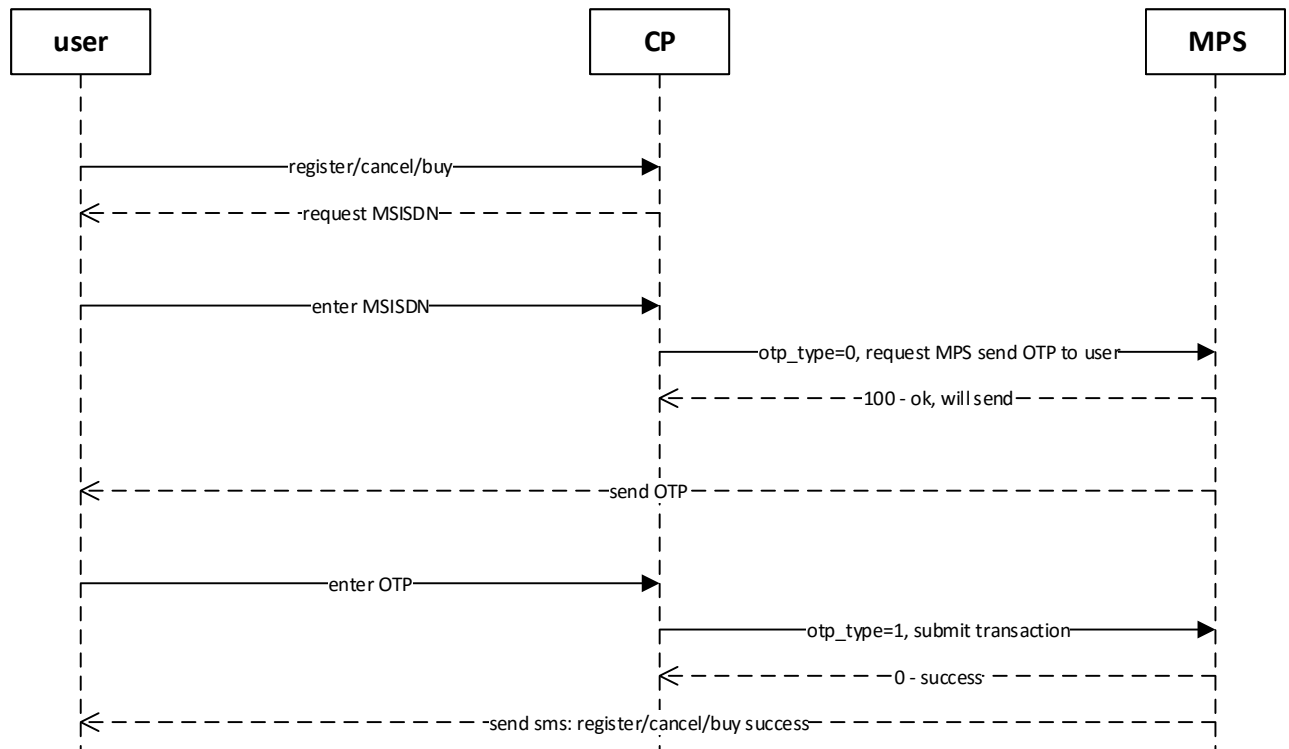
a. Data need encode

No.	Parameter	Description	Values
1.	SUB	Description for service charges Package	String
2.	CATE	List service need payment	String
3.	ITEM	Produce need payment	String
4.	SUB_CP	Provider	String
5.	CONT	More Description	String
6.	PRICE	Price	String
7.	REQ	Config code for transaction of CP	String
8.	MOBILE	Phone number need payment follow OTP	String
9.	SOURCE	Payment source (client, wap/web, app), if don't send data so system default wap. If application send request so system not return redirect url link	String
10.	OTP	OTP code. Config timeout for transaction from OTP receive result to return default 120s	String
11.	OTP_TYPE	Payment request by OTP: 0 – request send OTP 1 – request payment with OTP , cp_request_id send before submit OTP must same with cp_request_id of transaction send from OTP	String

b. Data send to HTTP request

No.	Parameter	Description	Values
1.	PRO	Indentification CP on MPS system	String
2.	CMD	Which payment: DOWNLOAD, REGISTER, CANCEL,…	String
3.	SER	Payment service	String
4.	SUB	Description charges package service	String
5.	DATA	Data was been encoding	String
6.	SIG	Signature of data encode	String

c. Return Result: Return request after encode.

No.	Parameter	Description	values
1.	REQ	Transaction code of CP system	String
2.	RES	Transaction error code	String
3.	MOBILE	Subscriber (if customer want to payment by basic account)	String
4.	CMD	Function payment	String
5.	PRICE	Money was been charging	String
6.	SOURCE	Payment source (WAP/CLIENT)	

3   Apendix

3.1   List error transaction

Parameter	Description
0	Transaction success
1	Not find phone number
4	IP Client not into IP Pool
11	Parameter lack
13	Amount lack
14	cp request id lack
15	Value lack
16	aes key lack
17	name item lack
18	category item lack
22	CP code not true/do not active
23	Payment not true
24	No transaction confirm before
25	CP Request Id not true
503	MPS system error
101	error cover system
102	Error when register service
103	Error when payment by mobile account
104	Error when cancel service
201	Signature not true
202	Error payment
207	Register same charges package
401	Account have not money
402	Subscriber have not register payment
403	Subscriber empty
404	Phone number not true
405	Change own phone number
406	Error not find mobile to payment
407	CP redirect error: parameter SUB, SER, CMD not true or have not register
408	Subscriber using service

Parameter	Description
409	Subscriber lock
410	Phone number don't have in Viettel system
411	Subscriber was been cancel service
412	Subscriber have not use this service
413	Error get true money to payment: paramater SUB, SER, CMD, CATEGORY (with function payment CHARGE/DOWNLOAD) not true/not yet put full function
414	Subscriber cancel service but it have in list charging
415	Error : OTP code not true/not yet input OTP code
416	Error: OTP code empty/ timeout transaction
417	Error USSD time out
440	System error
501	Phone number not register
202	Error password on account MPS system
203	Error account MPS empty(msisdn/password not true)
204	Error: have account MPS but not user CP account
205	Error: have account MPS and user CP account

3.2   Fix time-out error

In transaction action, overcome client waiting more time. If overcome timeout transaction so MPS system have not finish for CP. CP need config timeout same or more timeout of MPS system.

3.3   Security and cheat

- All partner want to connect to Viettel must clear RSA key from Viettel provide. Partner must keep information very security for Viettel.

- Partner need register IP of them first to connect MPS system. If Partner didn't register so system not provide service.

- System config transaction is cpRequestId, all transaction send again or same will be cancel

3.4   cpRequestId config

cpRequestId is araylist confirm only one transaction from partner. transId follow form:
pppyyMMddHHmmss**XXX**

detail:

- yyMMddHHmmss is transaction time

- ppp is cpCode of Viettel provide for partner (0->999)

- XXX is default number 000 – 999