Smartlink Payment Gateway

Merchant Integration Specification

Version 1.2

Hanoi 03-2008

Index

I. Overview

i. Document purpose

This document describe how to integrate new Internet merchant website to Smartlink payment gateway and transaction processing flow which provided by Smartlink gateway.

Based on this, merchant can do cost analysis, what type of transaction supported.

ii. System overview

Smartlink gateway (Smartlink Payment Gateway) solution is a multi-function gateway for card products. System is designed for requirement from customer that they want to do online payment with ATM debit card internet. Smartlink Payment Gateway will help to perform almost payment process when customer doing transaction like: receive payment order, card information authorization, routing transaction, view and report transaction.

Smartlink Payment Gateway designed and followed all international financial standards, provide monitor function to control transaction and user in system.

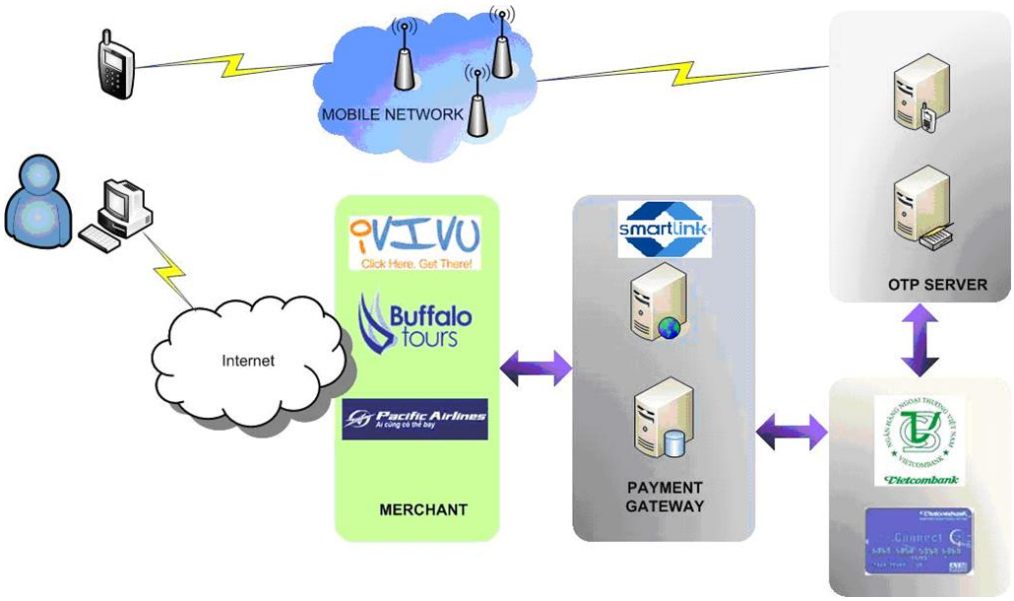
iii. System glossary

SNGlossary	Description
1Smartlink Payment Gateway	Payment Gateway solution provided by Smartlink
2Merchant shopping cart	Web site where customer can access to select, order product or service before going to do payment.
3Bank system	System which manage customer debit card account and support processing fund transfer amount from customer card account to merchant account
4SSL	Secure Socket layer, encryption protocol for web connection
5OTP	One time password generated by bank system and sent to customer mobile under SMS, customer will open SMS and get OTP code
6VCB	Joint Stock Foreign Trade Bank of Vietnam

II. Solution Feature

i. Connection model

With purpose to support receiving order payment from merchant website, processing transaction and return back result to initialize web site, system designed interface to communicate through form submit and URL redirect. This help to simply connect and integration in between with high secure feature.
Below is general connection graphic in between Service providers, bank system and Smartlink Payment Gateway.



In this diagram, we can see that Smartlink will be the middle to communicate with all merchant integrated, and there are some connections as list below:

- Customer-Merchant: customer access merchant website through web browser to initial product/service selection for order.
- **Merchant-Smartlink**: merchant web site after integrate will send payment request to Smartlink through URL redirect with parameters appended. This also includes redirect transaction result back from Smartlink to merchant web site and display for customer.
- Smartlink to Bank: this connection help Smartlink to communicate with Bank system for payment order processing
- Bank to OTP server: when customer required to enter OTP, this connection will help to request OTP server to generate OTP code for each customer when transact.
- OTP server to Mobile network: when OTP generated, this unique code will be transfer to customer hand phone through mobile network. Then customer can receive and enter to OTP authorization web page.

ii. Connection prototype

The current connection between merchant website and Smartlink web server gateway implement under URL redirection.
With this implementation, connection will not be depended on web page language (Asp, Php, Cfm, Jsp…) code and business model. To prepare for URL redirect connection, Smartlink gateway will public order URL for merchant web site with list of required parameters and checksum value (show the consistent of parameter values), merchant website also public URL for Smartlink gateway to return back result.

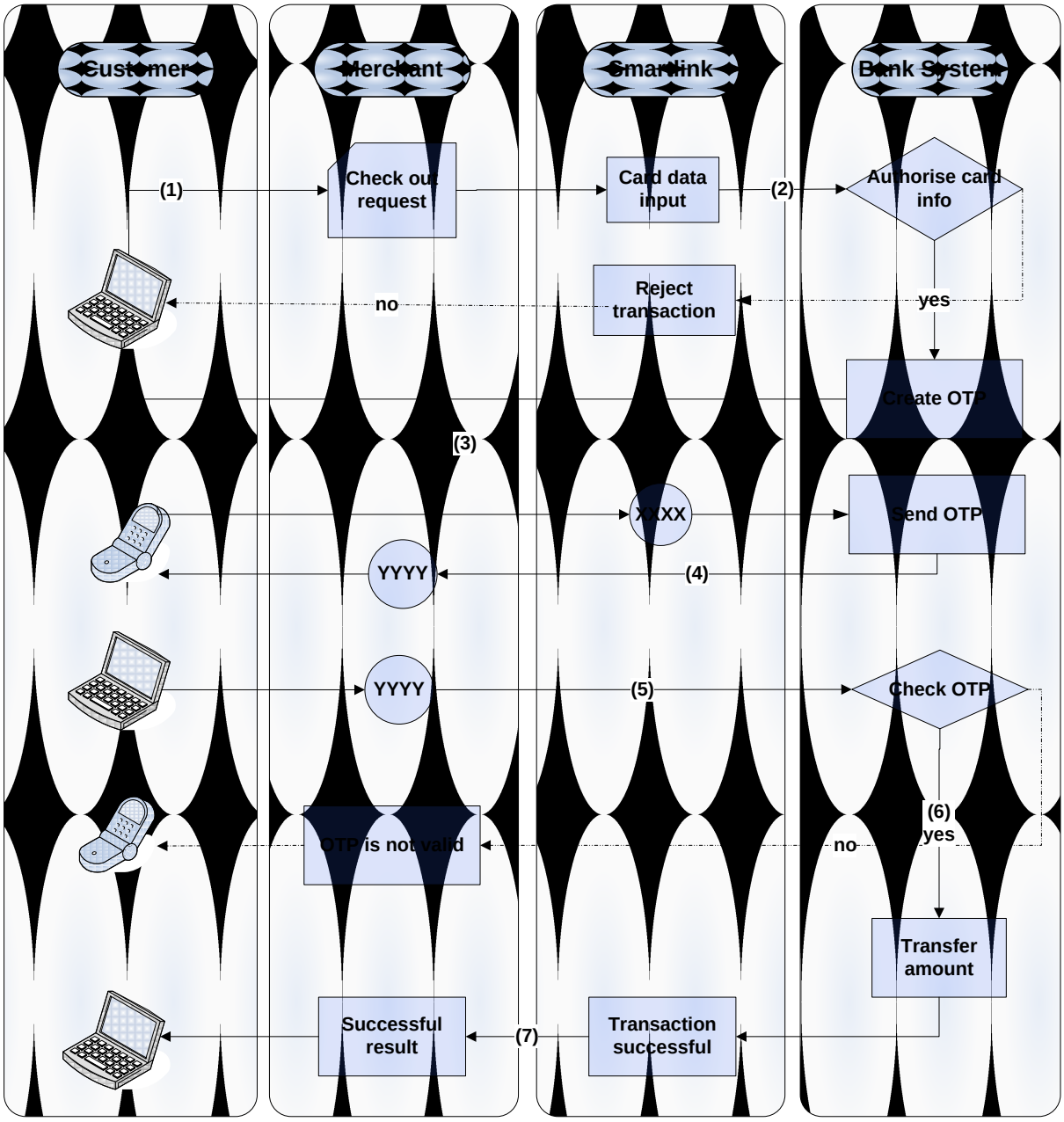
iii. Function support

With the purpose designing payment gateway solution, below are standard functions will be implement:

- Purchase function: This will perform order payment request from merchant website. This function will be performed online through merchant and Smartlink URL redirection.
- Refund function: this will help to refund partial amount of money based on purchase transaction. At the current, merchant staff need to access transaction management web site provided by Smartlink to do refund customer transaction.
- Transaction query: to check status of purchase transaction successful or not. At the current, merchant staff need to access transaction management web site provided by Smartlink to check status of their customer transaction. This operation will be included in **Merchant Transaction Management guide.doc**.
- Authorization: system did not support authorization function at the current.
- Capture: system did not support capture function at the current.

I. Transaction flow

i. Transaction flow



Step 1: Buying product on web

- Customer access to shopping cart of merchant on internet.

- Merchant check the validity of customer order then send payment request to Smartlink to process transaction.
- Webpage will be redirect to Smartlink card data entry webpage to support customer enter card information (Card no, card holder name, issue/expire date).

Step 2: Check customer information

- Smartlink will send card info to Bank host to check card and account in Bank system.
- Bank host will require customer double check payment amount, term and condition displayed on screen when do online payment to accept payment.

Step 3: Generate OTP code

- Bank host will check the valid of card account, balance, limit. If all condition are passed, prepaid host will ask customer send SMS with transaction authorization code display on web page (XXXX) to Bank SMS gateway (SMS format and gateway number also displayed on web page).

Step 4: Send OTP through SMS

- Customer can send a SMS with predefine format to Prepaid host SMS gateway to get OTP.

Step 5: Valid customer

- Once received OTP from bank, customer will enter OTP (YYYY) to web page of bank host to confirm transaction.
- Bank host will certify OTP. If valid, then Bank host will authorize transaction.

Step 6: Inform transaction result and settlement

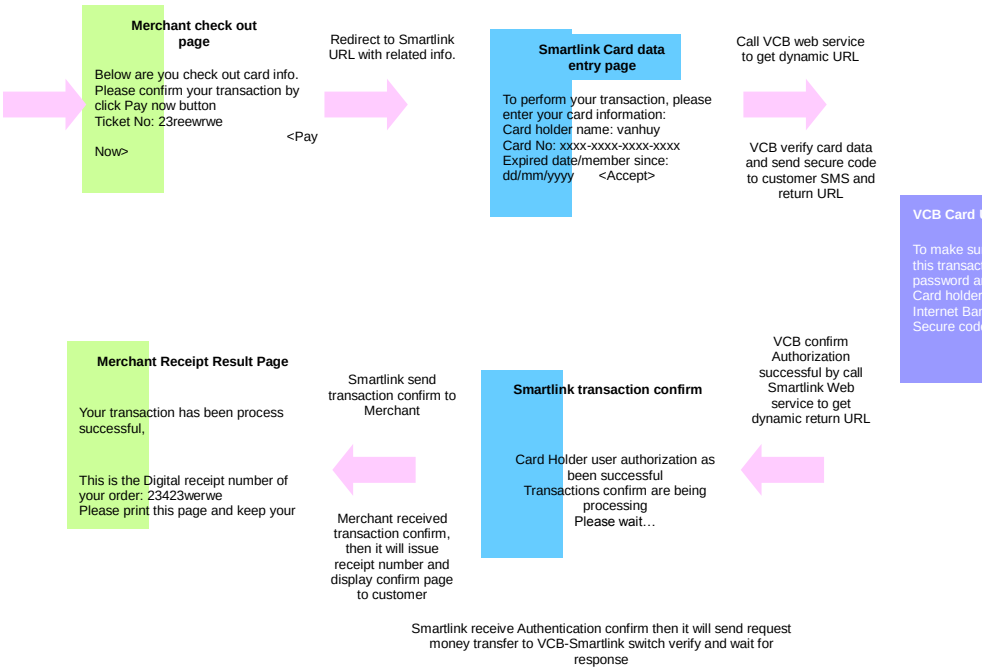
- Bank host send transaction result (Accept or reject) to Smartlink. Smartlink system will redirect result back to merchant website.
- If transaction authorized, Bank host will debit customer card account and credit merchant account after calculate fee.

Step 7: Deliver service/product

- When received redirect result on successful transaction from Smartlink, merchant will display result on web page and start service deliver process to customer.

ii. Screen flow

This will describe screen by screen what customer can see when they do transaction and do payment by bank card



II. Transferred Data Definition

Through URL redirect, there are certain data append to help Smartlink gateway receive and conform payment request to bank, and vice versa, Smartlink gateway can transfer transaction result back to merchant web site.

There are two directions which URL redirect initializes:

- Redirect from Merchant website to Smartlink gateway web site
- Redirect from Smartlink web site back to merchant website with transaction result.

i. Redirect Request from Merchant to Smartlink

To request payment transaction from merchant web site to Smartlink gateway website, redirect process will happen along with transaction data.

At merchant web site, after select product or service and click check out button to start payment process, merchant website will get customer transaction information and redirect to Smartlink gateway URL address with data as below:

- http://smartlink.vn/onecomm-pay/vpc.op? + parameter string
- Parameter string format: [parameter name]=[parameter value]&[parameter name]=[parameter value]&[parameter name]=[parameter value]&…
- The order of parameter can be exchanged, because we trace by parameter name.

Parameters definition:

Parameter	Requited Optional	Field type	Length	Example Value
vpc_Version	The version of the Virtual Payment Client being used. The current version is 1.			
	Required	Alphanumeric	1,8	1
virtualPaymentClientURL	http address of payment gateway	alphabet	1..45	
vpc_Command	Indicates the transaction type. This must be equal to **pay**			
	Required	Alphanumeric	1,16	pay
vpc_AccessCode	The access code authenticates you on the Payment Server so that a merchant cannot access another merchant's MerchantId. The access code is provided to you when you registered your merchant profile with your Payment Provider.			
	Required	Alphanumeric	8	d03due3
vpc_MerchTxnRef	A unique value created by the merchant to identify the DO. It is used to track the progess of a transaction and allows it to be identified on the Payment Server should a communication's failure occur and the DR is not received. It may be in part an order number or invoice number, but it should also reflect the transaction attempt. For example, if a cardholder has insufficient funds on their card and you allow them to repeat the transaction with another credit card. The value may be test1234/1 on the first attempt, test1234/2 on the second attempt and test1234/3 on the third attempt. It can use text made up of any of the base US ASCII characters in the range, hexadecimal20 to 126.			

	Required	Alphanumeric	1,40	Test1234/1
vpc_Merchant	The unique merchant Id assigned to you by your Payment Provider.			
	Required	Alphanumeric	1,16	TESTMERCHANT01
vpc_OrderInfo	Your own identifier used to identify the transaction with the cardholder. For example, a shopping cart number, an order number, or an invoice number.			
	Optional	Alphanumeric	1,34	Test1234
vpc_Amount	The amount of the transaction in the smallest currency unit expressed as an integer. For example, if the transaction amount is VND 599.54 then the amount is 59954.			
	Required	Alphanumeric	1,10	59954
vpc_ReturnURL	The URL that is displayed to the cardholder's browser when the Payment Server sends the DR.It must be a complete URL. The Return URL must start with either http:// or https:// and may be up to 255 characters. If the return URL is not supplied, your default vpc_ReturnURL that you nominated when you registered your merchant profile with your Payment Provider is used.			
	Required	Alphanumeric	1,255	http://returnurl/Receipt.asp
vpc_Locale	Used in SSL type transactions for specifying the language that is used on the Payment Server pages that are displayed to the cardholder. If the locale is not supplied the Payment Server defined default of 'vn' is used.			
	Required	Alphanumeric	2,5	vn
vpc_Currency	The currency of the amount. The currency is VND			
	Required	Alphanumeric	1,3	VND
vpc_TicketNo	Ticket No is IP address of the computer of the cardholder.			
	Required	Alphanumeric	1,45	210.245.0.1

				1

Note: Parameter name can be changed following merchant advice during integration.

Once Smartlink receive URL redirect process from merchant website, gateway will parsing parameter and calculate checksum (refer to check sum value calculation) value based on those. If both check sum values are match, then gateway web server will continue to get data from URL then form a payment order, encrypt and send to bank system.

To get those data and redirect to Smartlink web server gateway, merchant web site should have ability to create and get value from product selection process of customer then convert to according value of each parameter. Those will be store into merchant transaction database for cross-check later, customer support, and customer order processing later.

For detail of field values in certain case, just refer to below Field values description.

ii. Redirect Response from Smartlink to Merchant

To response transaction result back to merchant web site, Smartlink web server will redirect transaction data back to predefine URL (attached in request redirect from merchant to Smartlink or from merchant profile in Smartlink gateway database).

At Smartlink web site, after sending payment request to Bank web server, this system will ask customer to enter OTP value before going to authorize transaction. Authorize transaction process is limit, velocity, card, account status checking before transferring amount of money from customer card account to merchant account with fee included. Once authorize process complete, Smartlink gateway will receive response and redirect back to merchant URL with attached parameter string:

- http://merchant-shoping.vn/response.asp? + parameter string
- Parameter string format: [parameter name]=[parameter value]&[parameter name]=[parameter value]&[parameter name]=[parameter value]&…
- The order of parameter can be exchanged, because we trace by parameter name.

Parameters definition:

Parameter	Requited Optional	Field type	Length	Example Value
vpc_Version	The version of the Virtual Payment Client being used. The current version is 1.			
	Required	Alphanumeric	1,8	1
vpc_Command	The value of the vpc_Comand DO input field that is			

	returned in the DR			
	Required	Alphanumeric	1,16	Pay
vpc_TransactionNo	Payment server transaction id			
vpc_AccessCode	The access code authenticates you on the Payment Server so that a merchant cannot access another merchant's MerchantId. The access code is provided to you when you registered your merchant profile with your Payment Provider.			
	Required	Alphanumeric	8	d03due3
vpc_MerchTxnRef	A unique value created by the merchant to identify the DO. It is used to track the progess of a transaction and allows it to be identified on the Payment Server should a communication's failure occur and the DR is not received. It may be in part an order number or invoice number, but it should also reflect the transaction attempt. For example, if a cardholder has insufficient funds on their card and you allow them to repeat the transaction with another credit card. The value may be test1234/1 on the first attempt, test1234/2 on the second attempt and test1234/3 on the third attempt. It can use text made up of any of the base US ASCII characters in the range, hexadecimal20 to 126.			
	Required	Alphanumeric	1,40	Test1234/1
vpc_Merchant	The unique merchant Id assigned to you by your Payment Provider.			
	Required	Alphanumeric	1,16	TESTMERCHANT01
vpc_OrderInfo	Your own identifier used to identify the transaction with the cardholder. For example, a shopping cart number, an order number, or an invoice number.			
	Optional	Alphanumeric	1,34	Test1234
vpc_Amount	The amount of the transaction in the smallest currency unit expressed as an integer. For example, if the transaction amount is VND 599.54 then the amount is 59954.			
	Required	Alphanumeric	1,10	59954
vpc_ReturnURL	The URL that is displayed to the cardholder's browser			

	when the Payment Server sends the DR.It must be a complete URL. The Return URL must start with either http:// or https:// and may be up to 255 characters. If the return URL is not supplied, your default vpc_ReturnURL that you nominated when you registered your merchant profile with your Payment Provider is used.			
	Required	Alphanumeric	1,255	http://returnurl/Receipt.asp
vpc_Locale	Used in SSL type transactions for specifying the language that is used on the Payment Server pages that are displayed to the cardholder. If the locale is not supplied the Payment Server defined default of 'vn' is used.			
	Required	Alphanumeric	2,5	vn
vpc_Currency	The currency of the amount. The currency is VND			
	Required	Alphanumeric	1,3	VND
vpc_TicketNo	Ticket No is IP address of the computer of the cardholder.			
	Required	Alphanumeric	1,45	210.245.0.11
vpc_AdditionData	Additional Data			
	Optional	Alphanumeric	1,255	

Note: Parameter name can be changed following merchant advice during integration.

iii. Field values description

List of value for vpc_ResponseCode field

vpc_ResponseCode meaning	Value
Transaction successful	0
Bank system reject (card closed, account closed)	1
Card expired	3

Limit exceeded (Wrong OTP, amount / time per day)	4
No reply from Bank	5
Bank Communication failure	6
Insufficient fund	7
Check sum invalid	8
Transaction type not support	9

iv. Checksum Calculation

To check the integrity of data transferring through URL redirect, there are required below items:

- Method to calculate checksum data: can using 3DES or MD5 hashing function, most merchant using MD5 Hashing.
- Input data for 3DES or hashing function include string which concatenate all parameter and checksum key provided by Smartlink for each merchant profile.
- If using 3DES function, input data string will be separated every 8 characters and run through 3DES by 32 length hexa check sum key.
- If using MD5 function to make check sum value, just concatenate input data string plus 32 length check sum key provided by Smartlink.
- The length of check sum value is the first 32 character after running above function.
- Check sum key should be secure store by merchant website locally.

Before merchant website redirect data to Smartlink gateway server, it will calculate checksum data and plus to URL string. Smartlink web server, once, received URL string will parsing all data field and re calculate checksum value again, the matching process will be perform to check the integrity of data in URL redirection. If any unmatched result, the payment request will be rejected.

The checksum calculation and checking will be applied same process when Smartlink web server redirects back response to merchant website.

All data field list in URL string will be calculated checksum exclusive checksum field.

I. Data Security

i. Security channel

All redirect URL will begin with https://, this mean that data transfer in SSL channel, so whole data string under encryption or in secure channel.

Only merchant registered and having right checksum key can pass request to Smartlink gateway.

Checksum value will do merchant authorization and integrity of data transferred.

ii. One time Password authorization

With customer, to make more security and reduce lost and fraud, system support One time Password verification. When purchase or do online shopping, mobile phone or other devices (token…) to get unique code to enter and confirm transaction.

iii. Transaction rules

Each customer using bank card for online payment will be bank system monitored limit with certain rules like;

- number of transaction per day
- total transaction amount per day
- number time of enter wrong OTP

Those rules can help to reduce risk incase card lost or stolen.

I. Integrate and Implementation

i. Preparation

Before going to do system integration, Smartlink team will work with merchant to do system review to make sure it compatible or qualityable for integration with Smartlink payment gateway like:

- Merchant have shopping cart web
- Product delivery term and condition are list on web for customer clearly

ii. Integration

Smartlink will spend 01 engineer to support to merchant technical team during integration.

During integration, merchant_id and key will be provided for testing purpose only.

Estimated time for integration last around 5 day working.

iii. System Integration Test

After system integration complete, merchant will be provided testing account, card, and using merchant tester mobile to receive OTP. At this step, Merchant still in testing mode and transaction amount is not applicable to convert to actual cash.

The Testing will help system run smoothly before going to user acceptance test phase.

iv. User Acceptance Test

To make sure system running well and can cover both good and exceptional case, Smartlink will provide test script (preferred if merchant can add more case).

The UAT time for run through take around 1 week. After that merchant need to sign to UAT minute and confirm that they accept working flow and confirm to move to production later.

During UAT, merchant will be provided user and password to access to Merchant Transaction Monitoring web site to check transaction.

v. Production Mode

Before moving merchant to production mode, Smartlink need to receive official letter from merchant writing to request on production mode activate.

At this point if time, new merchant_id and checksum key will be generate and send to merchant in two separated packages.

In production mode, merchant will be provided web interface to control their customer transaction. Fraud report will be sent every hour if any.

During production mode, if any charge back or support request, it will be followed by appendix in contract.