NEWEB

Merchant Pay Page (mPP)

4.0.2

Programmer's Guide and Reference

History of changes

Seq	Version	Release Date	Major Changes	Author
1.	1.1	2011/10/14	Initial release	Jasmine Lin
2.	1.2	2011/11/28	Update credit card numbers for test.	Jasmine Lin
3.	2.1	2012/1/19	Update the description of transmitted parameters.	Jasmine Lin
4	2.2	2012/8/15	Update credit card numbers for test.	Jasmine Lin
5	2.3	2012/11/5	Update credit card numbers for test.	Jasmine Lin
6	3.1	2013/5/30	Update the description of transmitted parameters.	Jasmine Lin
7	3.2	2013/11/16	Update credit card numbers for test.	Jasmine Lin
8	3.3	2013/12/3	Modify the default value for “DepositFlag”	Jasmine Lin

Table of Contents

HISTORY OF CHANGES 2

1 PAYMENT FLOWS AND DESCRIPTION 4

1.1 Normal case description 4
1.2 Abnormal cases and descriptions 5

2 USING MD5 FOR INTEGRITY CHECKSUM 7

3 NEWEB REQUESTED PARAMETERS 13

3.1 Parameters for general transactions 13
3.2 Parameters for installment transactions 14
3.3 Parameters for national travel card transaction 14
3.4 Parameters for redeemed transaction(Only for Shin Kong Acquiring Bank) 15

4 NEWEB RETURNED PARAMETERS 16

5 THE ID AND CREDIT CARD NUMBERS FOR TEST 21

6 GENERAL NOTICES 22

7 SAMPLE PAY PAGES FOR TEST 23

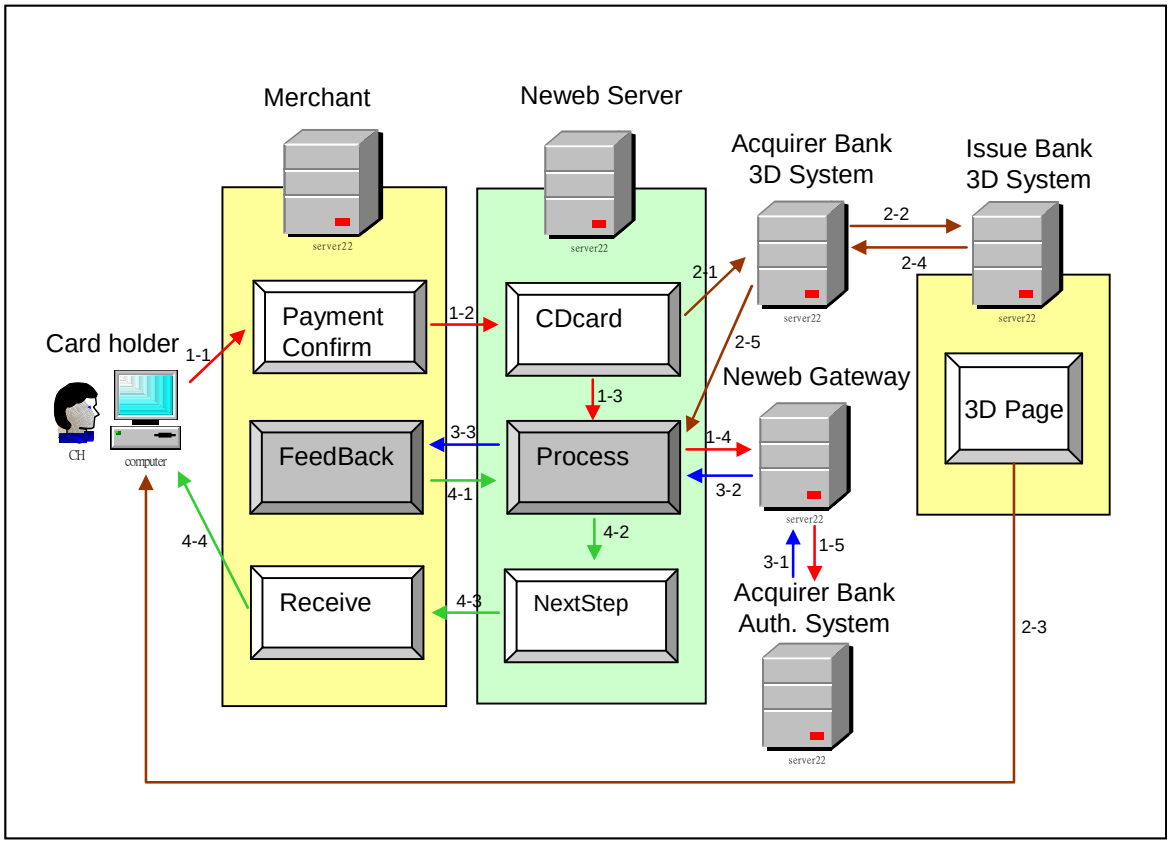
8 USEFUL TIPS BEFORE TEST 25

9 USEFUL TIPS BEFORE GOING PRODUCTION 26

APPENDIX I CREDIT CARD PAYMENT TERM DEFINITIONS 27

1 Payment Flows and Description

1.1 Normal case description



1. Sending an approval request

Step 1-1：Cardholders click a confirm button on merchant's shopping cart web page and "PaymentConfirm" program on merchant site receives all necessary information.

Step 1-2："PaymentConfirm" program redirects Cardholders' browser to a pay page(CDcard) on Neweb site and passes all necessary information to CDcard at the same time.

Step 1-3：Cardholders fill in Credit Card informations on this pay page and, in a non 3D case, CDCard submits these informations to "Process" reside in Neweb. This means that merchants do not take any responsibility for keeping credit card informations.

Step 1-4：The approval request will be sent to acquiring bank through Neweb Gateway.

Step 1-5：Acquiring bank will execute the transaction via its authorization system which has access to credit network and finally gets the approval result from issuing bank.

2. 3D Verification process

Step 2-1：In a 3D case, CDCard will direct the flow to acquirer's 3D system.

Step 2-2：Acquirer's 3D system will direct the flow to issuing bank's 3D system.

Step 2-3：A Cardholder will need to be verified by giving his 3D password which is assigned by cardholder himself while he applying his credit card for 3D function.
Step 2-4：Issuing bank's 3D system returns the verified result to acquirer's.
Step 2-5：Acquirer's 3D system returns the verified result to Neweb. Neweb process proceeds to send approval request only if the verified result indicates a successful verification,

3. Merchant get response to approval request
Step 3-1：Succeeding to step 1-5, acquirer responds to the approval request and returns its result to Neweb Gareway.
Step 3-2：Neweb Gateway send the approval result to Neweb Process.
Step 3-3：Neweb Process prepares all necessary parameters, which are made of PRC、SRC、Ordernumber and Amount, etc. ,for calling Merchant's FeedBack program. Merchant can save the received parameters to database. FeedBack is running as a background program on merchant's web site and cardholders should not be aware of any information processed by this program on their browser.

4. Cardholders see the result of transaction on merchant's web page
Step 4-1：After FeedBack program successfully processes the calling HTTP request, it should return a HTTPCode of value 200 to Neweb Process.
Step 4-2：The flow will be directed to Neweb NextStep program which is acting as a relay page between cardholders' browser and the Receive web page of merchant.
Step 4-3：NextStep relay page will automatically redirect all necessary parameters to Reveive on merchant site via cardholders' browser so that cardholders will see the final result of transaction on this web page prepared by merchant. If the cardholders' browser is restrained from redirecting action, cardholders could force the redirect action manually by clicking a button on this NextStep page.
Step 4-4：Here we suggest that merchant's Receive web page should compare and re-confirm the value of parameters with those gotten in Feedback program in order to present an accurate message to cardholders.

1.2 Abnormal cases and descriptions

According to the exceptions that might occur due to network or other system outages, here are some tips for merchant to deal with each situation.

1 "PaymentConfirm" program could not redirects Cardholders' browser to a pay page(CDcard) on Neweb site：

- Check the linkage in PaymentConfirm program if the CDcard url setting is correct.
- Check to see if merchant's DNS works properly.
- Call for Neweb customer center to see if Neweb site works properly.

2 Neweb Process program could not have a normal connection with Feedback program of merchant after getting a successful transaction from acquirer：

- If the case is that Neweb can not make the result send to merchant, Neweb Process will reverse the transaction and treat the transaction as a failure to prevent a mismatched perception of the transaction between the cardholder and merchant.

- If the case is that Neweb makes the result send to FeedBack program of merchant yet the Feedback do not respond the http request with HTTP code 200, Neweb Process will assume that merchant's Feedback program encounters an internal error. Neweb will reverse the transaction and treat the transaction as a failure as well. Merchant should monitor its system logs to see if there exists any internal errors and fixed the bugs.

3 Neweb NextStep could not normally redirect information to merchant Receive page：

- One of the common causes of this problem is network outages. Cardholders could just click the previous page button of browser and the NextStep will be execute again.
- If network is no problem, merchant might need to check whether Receive is working properly or settings of PaymentConfirm is correct. Neweb system will not reverse the transaction status at this stage and merchant should reconcile transaction status with the details of daily report provided by Neweb.

4 Cardholders' improper operations cause incomplete or duplicate orders：

- If cardholders interrupts the operation on CDcard(such as closing browser), that will make an incomplete order. Such orders do not need further process like cancellation or refund because they have not been sent to acquirer yet.
- If cardholders repeatedly click the previous page button of browser after seeing the merchant's Receive page, this may result in coming back to CDcard page and resending a duplicate order number. Neweb system will reject a duplicate order number immediately; therefore, a later duplicate order will not affect the transaction status of original order.

2 Using MD5 for Integrity Checksum

MD5 is a defacto algorithm of hash function. Given any two texts with tiny difference will lead to apparent different in hash value. It's theoretically impossible to drive the original text from its hash value.

```
'Build the integrity checksum for payment information(PaymentConfirm2.asp)
//** md5編碼時所需使用的Code，藍新科技提供，請妥善保存
//** 使用md5編碼過後的值，才能往藍新科技送

        r_MerchantNumber = request("MerchantNumber")
        r_OrderNumber = request("OrderNumber")
        r_Amount = request("Amount")
        r_OrgOrderNumber = request("OrgOrderNumber")
        r_ApproveFlag = request("ApproveFlag")
        r_DepositFlag = request("DepositFlag")
        r_Englishmode = request("Englishmode")
        r_Period = request("Period")
        r_Code = "abcd1234"

        encryptstr = lcase(md5(r_MerchantNumber & r_OrderNumber & r_Code & r_Amount))


'Inspect the checksum of payment result for integrity(feedback2.asp)
//** md5編碼時所需使用的Code，藍新科技提供，請妥善保存
//** 比對藍新回傳之CheckSum與使用md5編碼的chkstr值是否相同

        Code = "abcd1234"
        CheckSum = request("CheckSum")
        PRC = request("PRC")
        SRC = request("SRC")
        ApprovalCode = request("ApprovalCode")
        BankResponseCode = request("BankResponseCode")
        MerchantNumber = request("MerchantNumber")
        OrderNumber = request("OrderNumber")
        Amount = request("Amount")
        BatchNumber = request("BatchNumber")

      chkstr = MerchantNumber & OrderNumber & PRC & SRC & Code & Amount
   chkstr = lcase(md5(chkstr))

if PRC="0" and SRC="0" then
      '回傳成功，但結果有可能遭竄改，因此需和編碼內容比較
      if chkstr=CheckSum then
         response.write "<br>交易成功"
         response.write "<br>訂單編號    ：" & OrderNumber
         response.write "<br>交易金額    ：" & Amount
         response.write "<br>授權碼       ：" & ApprovalCode
         response.write "<br>銀行回傳碼：" & BankResponseCode
         response.write "<br>批次號碼  ：" & BatchNumber
      else
         '資料遭竄改
```

```
        response.write "交易結果有誤，請與我們聯絡!"
    end if
elseif PRC="34" and SRC="171" then
    BankResponseCode = request("BankResponseCode")

    response.write "<br>交易失敗(金融失敗)"
    response.write "<br>訂單編號　：" & OrderNumber
    response.write "<br>交易金額　：" & Amount
    response.write "<br>銀行回傳碼：" & BankResponseCode
elseif PRC="8" and SRC="204" then
    response.write "<br>訂單編號重複!"
elseif PRC="52" and SRC="554" then
    response.write "<br>使用者帳號密碼錯誤!"
else
    response.write "<br>交易失敗(系統錯誤)"
    response.write "<br>訂單編號　：" & OrderNumber
    response.write "<br>交易金額　：" & Amount
end if
```

```
' Build the integrity checksum for payment information(PaymentConfirm2.aspx)
//** md5編碼時所需使用的Code，藍新科技提供，請妥善保存
//** 使用md5編碼過後的值，才能往藍新科技送

    Dim r_MerchantNumber = request("MerchantNumber")
    Dim r_OrderNumber = request("OrderNumber")
    Dim r_Amount      = request("Amount")
    Dim r_OrgOrderNumber = request("OrgOrderNumber")
    Dim r_ApproveFlag = request("ApproveFlag")
    Dim r_DepositFlag = request("DepositFlag")
    Dim r_Englishmode = request("Englishmode")
    Dim r_Period = request("Period")
    Dim r_Code = "abcd1234"
    Dim encryptstr =
    lcase(FormsAuthentication.HashPasswordForStoringInConfigFile(r_MerchantNumber &
    r_OrderNumber & r_Code & r_Amount,"md5"))

'Inspect the checksum of payment result for integrity(feedback2.aspx)
//** md5編碼時所需使用的Code，藍新科技提供，請妥善保存
//** 比對藍新回傳之CheckSum與使用md5編碼的chkstr值是否相同

    Dim Code = "abcd1234"
    Dim CheckSum = request("CheckSum")
    Dim PRC = request("PRC")
    Dim SRC = request("SRC")
    Dim ApprovalCode = request("ApprovalCode")
    Dim BankResponseCode = request("BankResponseCode")
    Dim MerchantNumber = request("MerchantNumber")
    Dim OrderNumber = request("OrderNumber")
    Dim Amount = request("Amount")
    Dim BatchNumber = request("BatchNumber")

    Dim chkstr = MerchantNumber & OrderNumber & PRC & SRC & Code & Amount
    chkstr = lcase(FormsAuthentication.HashPasswordForStoringInConfigFile (chkstr,"md5"))
```

```
if PRC="0" and SRC="0" then
    '回傳成功，但結果有可能遭竄改，因此需和編碼內容比較
    if chkstr=CheckSum then
        response.write("<br>交易成功")
        response.write("<br>訂單編號    ：" & OrderNumber)
        response.write("<br>交易金額    ：" & Amount)
        response.write("<br>授權碼       ：" & ApprovalCode)
        response.write("<br>銀行回傳碼：" & BankResponseCode)
        response.write("<br>批次號碼  ：" & BatchNumber)
    else
        '資料遭竄改
        response.write("交易結果有誤，請與我們聯絡!")
    end if
elseif PRC="34" and SRC="171" then
    response.write("<br>交易失敗(金融失敗)")
    response.write("<br>訂單編號    ：" & OrderNumber)
    response.write("<br>交易金額    ：" & Amount)
    response.write("<br>銀行回傳碼：" & BankResponseCode)
elseif PRC="8" and SRC="204" then
    response.write("<br>訂單編號重複!")
elseif PRC="52" and SRC="554" then
    response.write("<br>使用者帳號密碼錯誤!")
else
    response.write("<br>交易失敗(系統錯誤)")
    response.write("<br>訂單編號    ：" & OrderNumber)
    response.write("<br>交易金額    ：" & Amount)
end if
```

' Build the integrity checksum for payment information(PaymentConfirm2.jsp)

```
//** md5編碼時所需使用的Code，藍新科技提供，請妥善保存
//** 使用md5編碼過後的值，才能往藍新科技送

        String r_MerchantNumber = request.getParameter("MerchantNumber");
        String r_OrderNumber = request.getParameter("OrderNumber");
        String r_Amount = request.getParameter("Amount");
        String r_OrgOrderNumber = request.getParameter("OrgOrderNumber");
        String r_ApproveFlag = request.getParameter("ApproveFlag");
        String r_DepositFlag = request.getParameter("DepositFlag");
        String r_Englishmode = request.getParameter("Englishmode");
        String r_Period = request.getParameter("Period");
        String r_Code = "abcd1234";

        String encryptstr = DigestUtils.md5Hex(r_MerchantNumber + r_OrderNumber + r_Code +
        r_Amount);
```

‘Inspect the checksum of payment result for integrity(feedback2.jsp)

```
//** md5編碼時所需使用的Code，藍新科技提供，請妥善保存
//** 比對藍新回傳之CheckSum與使用md5編碼的chkstr值是否相同

        String Code = "abcd1234";
        String CheckSum = request.getParameter("CheckSum");
```

```
        String PRC = request.getParameter("PRC");
        String SRC = request.getParameter("SRC");
        String ApprovalCode = request.getParameter("ApprovalCode");
        String BankResponseCode = request.getParameter("BankResponseCode");
        String MerchantNumber = request.getParameter("MerchantNumber");
        String OrderNumber = request.getParameter("OrderNumber");
        String Amount = request.getParameter("Amount");
        String BatchNumber = request.getParameter("BatchNumber");

        String NowTime = new SimpleDateFormat("yyyy-MM-dd HH:mm:ss").format(new Date());

try{
    String chkstr = MerchantNumber+OrderNumber+PRC+SRC+Code+Amount;
    chkstr = DigestUtils.md5Hex(chkstr);
    if(PRC.equals("0") && SRC.equals("0")){
        //-- 回傳成功，但結果有可能遭竄改，因此需和編碼內容比較
        if(chkstr.equals(CheckSum)){
            out.println("<br>交易成功"                    );
            out.println("<br>訂單編號    ：" + OrderNumber     );
            out.println("<br>交易金額    ：" + Amount          );
            out.println("<br>授權碼      ：" + ApprovalCode    );
            out.println("<br>銀行回傳碼：" + BankResponseCode );
            out.println("<br>批次號碼  ：" + BatchNumber );
        }else{
            //-- 資料遭竄改
            out.println("交易結果有誤，請與我們聯絡!");
        }
    }else if(PRC.equals("34") && SRC.equals("171")){
        BankResponseCode = initPara(request.getParameter("BankResponseCode"));

        out.println("<br>交易失敗(金融失敗)"            );
        out.println("<br>訂單編號    ：" + OrderNumber     );
        out.println("<br>交易金額    ：" + Amount          );
        out.println("<br>銀行回傳碼：" + BankResponseCode );
    }else if(PRC.equals("8") && SRC.equals("204")){
        out.println("<br>訂單編號重複!");
    }else if(PRC.equals("52") && SRC.equals("554")){
        out.println("<br>使用者帳號密碼錯誤!");
    }else{
        out.println("<br>交易失敗(系統錯誤)"        );
        out.println("<br>訂單編號    ：" + OrderNumber );
        out.println("<br>交易金額    ：" + Amount      );
    }
}catch(Exception ex){
    System.err.println("Feedback failed!==>");
    ex.printStackTrace(System.err);
}
```

```
' Build the integrity checksum for payment information(PaymentConfirm2.php)

//** md5編碼時所需使用的Code，藍新科技提供，請妥善保存
//** 使用md5編碼過後的值，才能往藍新科技送
```

```
  <input type=hidden name="MerchantNumber" value="<?php print $MerchantNumber ?>">
  <input type=hidden name="OrderNumber"    value="<?php print $OrderNumber ?>">
 <input type=hidden name="Amount"         value="<?php print $Amount ?>">
 <input type=hidden name="OrgOrderNumber" value="<?php print $OrgOrderNumber ?>">
 <input type=hidden name="ApproveFlag"    value="<?php print $ApproveFlag ?>">
 <input type=hidden name="DepositFlag"    value="<?php print $DepositFlag ?>">
 <input type=hidden name="Englishmode"    value="<?php print $Englishmode ?>">
 <input type=hidden name="Period"         value="<?php print $Period ?>">
  <input type=hidden name="OrderURL"       value="http://xxx.xxx.xxx/feedback2.php">
 <input type=hidden name="ReturnURL"      value="http://xxx.xxx.xxx/receive.php">
 <input type=hidden name="checksum"       value="<?php print
md5($MerchantNumber.$OrderNumber."abcd1234".$Amount) ?>">
 <input type=hidden name="op"             value="AcceptPayment">
```

'Inspect the checksum of payment result for integrity(feedback2.php)

```
//** md5編碼時所需使用的Code，藍新科技提供，請妥善保存
//** 比對藍新回傳之CheckSum與使用md5編碼的chkstr值是否相同

<?php
   $Code = "abcd1234";
   $chkstr = $MerchantNumber.$OrderNumber.$PRC.$SRC.$Code.$Amount;
   $chkstr = md5($chkstr);
   if($PRC=="0" && $SRC=="0"){
      //-- 回傳成功，但結果有可能遭竄改，因此需和編碼內容比較
      if($chkstr==$CheckSum){
?>
         <br><?php print $chkstr ?>
         <br><?php print $CheckSum ?>
         <br>交易成功
         <br>訂單編號    ：<?php print $OrderNumber ?>
         <br>交易金額    ：<?php print $Amount ?>
         <br>授權碼      ：<?php print $ApprovalCode ?>
         <br>銀行回傳碼：<?php print $BankResponseCode ?>
         <br>批次號碼  ：<?php print $BatchNumber ?>
<?php
      }else{
?>
         //-- 資料遭竄改
         交易結果有誤，請與我們聯絡!
<?php
      }
   }else if($PRC=="34" && $SRC=="171"){
?>
      <br>交易失敗(金融失敗)
      <br>訂單編號    ：<?php print $OrderNumber ?>
      <br>交易金額    ：<?php print $Amount ?>
      <br>銀行回傳碼：<?php print $BankResponseCode ?>

<?php
   }else if($PRC=="8" && $SRC=="204"){
?>
      <br>訂單編號重複!
<?php
```

```
   }else if($PRC=="52" && $SRC=="554"){
?>
      <br>使用者帳號密碼錯誤!
<?php
   }else{
?>
      <br>交易失敗(系統錯誤)";
      <br>訂單編號    ：<?php print $OrderNumber ?>
      <br>交易金額    ：<?php print $Amount ?>
<?php
   }
?>
```

The purpose of using MD5 as integrity check is to protect asynchronous transmitted information between neweb and merchant from tampering. There are 3 times to adopt MD5 checksum during a whole transaction.

The first adoption is from merchant PaymentConfirm to neweb CDcard. Neweb should do the integrity check and the source text format is：

Value_of_MerchantNumber&Value_of_OrderNumber&Value_of_Code&Value_of_Amount

The second adoption is from Neweb Process to merchant FeedBack. Merchant should do the integrity check and the source text format is：

Value_of_MerchantNumber&Value_of_OrderNumber&Value_of_PRC&Value_of_SRC&Value_of_Code&Value_of_Amount

The third adoption is from Neweb NextStep redirect to merchant's Receive page. Merchant should do the integrity check and the source text format is：

Value_of_MerchantNumber&Value_of_OrderNumber&Value_of_FinalResult&Value_of_PRC&Value_of_Code&Value_of_SRC&Value_of_Amount

Notice：

※The '&' in text format just means a contact operator, do not place '&' in source text.

※The value of **Code** is given by Neweb, merchant must keep the Code safe as a secret.

※Be sure to compare any two CheckSums in the same measure of uppercase or lowercase.

3 Neweb Requested Parameters

3.1 Parameters for general transactions

Neweb CDcard requires the following parameters for a general transaction(non installment)：

Parameter Name	Caption	Data Type & Format	Parameter Description
MerchantNumber	商店編號	6 digits	Required, assigned by Neweb
OrderNumber	藍新訂單編號	Numeric(15), unique to each MerchantNumber	Required, no special characters
Amount	訂單金額	9(9)v9(2), can not be 0 ex：100.00	Required, a minimum of 50
OrgOrderNumber	商家訂單編號	Alphanumeric(20)	
ApproveFlag	授權指標	0 or 1	Default is 1
DepositFlag	請款指標	0 or 1 (see Note1)	Default is 1
Englishmode	中英文版本指標	0：Chinese mode 1：English mode	Default is 0
iphonepage	手機刷卡頁版本指標	0：PC/NB pay page 1：iPhone pay page	Default is 0
OrderURL	訂單回傳網址	A complete URL mapping to Feedback program of merchant. (Connection port is restricted to 80 or 443 only)	Required
ReturnURL	交易回傳網址	A complete URL mapping to Receive page of merchant.	Required
checksum	編碼值	MD5 hashed value (see Note2)	Required, uppercase or lowercase makes no difference
op	交易模式	Constant：AcceptPayment	Required

Note1： It is suggested that merchant keep the default value. It depends on acquirer whether deposit can be operated separately.

Note2： The source text of checksum is Value_of_MerchantNumber&Value_of_OrderNumber&Value_of_Code&Value_of_Amount **code is given by Neweb when merchants apply for service.**

3.2 Parameters for installment transactions

Neweb CDcard requires the additional parameters for a installment transaction：

Parameter Name	Caption	Data Type & Format	Parameter Description
Period	分期期數	Integer(see Note3)	Required only for installment transaction, do not use it in other type of transaction. Specify 6 or 12 as period in the test environment.

Note3：Installment transaction requires a special application to acquirer for installment MID. All acquirers only accept intra-bank cards for installment transaction. The rules of verifying period and ID vary from acquirer to acquirer, as follows：

Acquirers / Functions	**Union Bank**	**Citibank**	**Chinatrust Bank**	**Cathay United Bank**	**Shin Kong Bank**
ID/ Passport Number	required	optional	optional	optional	optional
Online Refund	N/A	full amount	full amount	full amount	full amount
3D support	N/A	N/A	available	N/A	N/A
Periods of Installment	Generally accepted periods are 3、6、12、18、24. Actually accepted periods are specified by the contract of merchant and acquirer.				

3.3 Parameters for national travel card transaction

Neweb CDcard requires the additional parameters for a national travel card transaction：

Parameter Name	Caption	Data Type & Format	Parameter Description
ctravel_startdate	行程起日	yyyyMMdd	Required only for national travel card transaction, do not use it in other type of transaction
ctravel_enddate	行程迄日	yyyyMMdd	Required only for national travel card transaction, do not use it in other type of transaction
ctravel_zipcode	郵遞區號	Numeric(3)	Required only for national travel card transaction, do not use it in other type of transaction

3.4 Parameters for redeemed transaction(Only for Shin Kong Acquiring Bank)

Neweb CDcard requires the additional parameters for a redeemed transaction：

Parameter Name	Caption	Data Type & Format	Parameter Description
redemption	紅利折抵指標	Constant：1	Required only for redeemed transaction, do not use it in other type of transaction

4 Neweb Returned Parameters

Section 4.1 through 4.6 explain a variety of parameters that Neweb will send to merchant's FeedBack program depending on type of transaction and its particular condition.

4.1 List of general parameters sent to FeedBack(OrderURL)

Parameter Name	Parameter Description
CheckSum	Value of MD5 hash
PRC	Primary Return Code
SRC	Secondary Return Code
ApprovalCode	Bank approval code, Alphanumeric(6)
BankResponseCode	Bank Response Code, Alphanumeric(8)
MerchantNumber	Merchant number
OrderNumber	Order number
Amount	Transaction amount
BatchNumber	Batch number

4.2 Sample message format sent to FeedBack while completing an authorization from acquirer：

CheckSum=xxx&PRC=xxx&SRC=xxx&ApprovalCode=xxxxxx&BankResponseCode=x/xx&MerchantNumber=xxxxxx&OrderNumber=xxx&Amount=xxx&BatchNumber=xxx

It is suggested that merchant should do the integrity check by regenerating a new MD5 hashed value as below and comparing it with the received.

MD5(Value_of_MerchantNumber&Value_of_OrderNumber&Value_of_PRC&Value_of_SRC&Value_of_Code&Value_of_Amount)

Be sure to compare the two CheckSums in the same uppercase or lowercase.

4.3 Sample message format with extra parameters sent to FeedBack. These extra parameters need a separate setting by request：

CheckSum=xxx&PRC=xxx&SRC=xxx&ApprovalCode=xxxxxx&BankResponseCode=x/xx&MerchantNumber=xxxxxx&OrderNumber=xxx&Amount=xxx&BatchNumber=xxx&cardnumber=xxxx&issuebank=&EngName=

If a cardholder fills in the issuer and cardholder's name with Chinese characters, the value of the two parameters will be in Chinese characters. To avoid errors while parsing the value of Chinese characters, it is suggested that setting big5 to encoding.

4.4 List of extra parameters ：

Parameter Name	Parameter Description
Cardnumber	Credit card number(front 6 and last 4)
Issuebank	Issuing bank
EngName	Cardholder's English Name

4.5 Sample message format for redeemed transaction sent to FeedBack：

PRC=xxx&SRC=xxx&BANKRESPONSECODE=x/xx&STATUS=1&XID=&APPROVALCODE=xxxxxx&REDEMPTION_POINT=xxx&REDEMPTION_AMOUNT=xxx&REDEMPTION_REMAIN=xxxxxx&REDEMPTION_PAYAMOUNT=xxxxx

4.6 List of parameters for redeemed transaction：

Parameter Name	Parameter Description
REDEMPTION_POINT	Redeemed point
REDEMPTION_AMOUNT	Deducted amount
REDEMPTION_REMAIN	Unredeemed point
REDEMPTION_PAYAMOUNT	Actually paid amount

Section 4.7 through 4.8 explain a variety of parameters that Neweb will send to merchant's Receive page depending on type of transaction and its particular condition.

4.7 General Parameters redirected to Receive(ReturnURL) after getting a response from FeedBack(OrderURL)：

Parameter Name	Parameter Description
final_result	The final result of transaction
P_MerchantNumber	Merchant number

P_OrderNumber	Order number
P_Amount	Transaction amount
P_CheckSum	MD5 hashed value
final_return_PRC	Primary Return Code
final_return_SRC	Secondary Return Code
final_return_ApproveCode	Bank approval code, Alphanumeric(6)
final_return_BankRC	Bank Response Code, Alphanumeric(8)
final_return_BatchNumber	Batch number

※ The number and position of parameters sending to Feedback and Receive are not fixed. Be sure to parse all parameters by their name instead of position in message text.

4.8 Additional Parameters redirected to Receive(ReturnURL) if it's a redeemed transaction：

Parameter Name	Parameter Description
final_redemption_point	Redeemed point
final_redemption_amount	Deducted amount
final_redemption_remain	Unredeemed point
final_redemption_payamount	Actually paid amount

The usage of parameters in Receive：

1. final_result－The purpose of this parameter is to determine whether a transaction is finally successful or not. 1：success，0：failure

2. final_return_PRC、final_return_SRC、final_return_ApproveCode、final_return_BankRC. The values of this 4 parameters should be consistent with those of PRC, SRC, BankResponseCode and ApprovalCode in FeedBack.
3. P_CheckSum is a MD5 hashed value as below：
   MD5(Value_of_MerchantNumber&Value_of_OrderNumber&Value_of_final_result&Value_of_PRC&Value_of_Code&Value_of_SRC&Value_of_Amount)

4. According to best practice, all parameters in FeedBack should comply with final_result in Receive. Following table illustrates the different actions for merchants that apply to each condition in the matrix.

FeedBack / Receive	PRC,SRC=0	PRC,SRC≠0	Not be called (W/O logging)
final_result=1	Successful transaction is confirmed.		Successful transaction is confirmed. Merchant should update DB by the value of parameters in Receive. Merchant may need to check server if any unexpected errors occur at FeedBack.
final_result=0	Transaction failed. Merchant should revise DB by the value of parameters in Receive if FeedBack has ever updated DB. The transaction will be treated as void in Neweb system. Merchant may need to check if any network issues occur at FeedBack. Contact Neweb customer service for further details.	Transaction failed. According to PRC/SRC, Receive page should show the cardholder a corresponding message.	Transaction failed.
Not be called (W/O logging)	An ambiguous transaction. Merchant may need to check if any network issues occur at Receive. Merchant may refer to Neweb admin web site or daily report to verify the final status of each transaction.	Transaction failed.	An incomplete transaction. The case usually occurs when cardholders give up halfway at CDcard page or 3D verification page. Merchant may refer to Neweb admin web site or daily report to verify the final status of each transaction.

- As long as final _result=1 in Receive is sustained, merchant can consider the transaction successful and the other parameters will be as final_return_PRC=0、final_return_SRC=0、final_return_BankRC=0/00、final_return_ApproveCode=xxxxxx.
- If a transaction is failed, then final_return_PRC and final_return_SRC must not be a value of 0. Here are some very common pairs of PRC/SRC：
  - PRC=34,SRC=171,BankRC=x/xx：Issuing banks reject the transaction due to a problem relative to the credit card itself, and which can be pointed to a more explicit reason by BankRC. Please refer to document「銀行回覆碼代碼表.pdf」for detailed BankRC description.
  - PRC=15,SRC=1018：Acquirer's system can not process (request not to Issuer yet) the transaction normally due to the reason that bank hosts busy or networks break transiently.

- PRC=52,SRC=554：Neweb reject the transaction due to the wrong account and password in connection.
- PRC=8,SRC=204：Neweb reject the transaction due to detecting a duplicate order number within a merchant number.
- Some other pairs of PRC/SRC may occur because of incorrect value of parameters in transaction request. Please refer to document「付款管理頁面回覆碼(PRC,SRC).pdf」for detailed PRC/SRC description or contact Neweb customer service for help.

5 The ID and Credit Card Numbers for Test

- **ID for test：**

  System accept any Identification number if it is compliant with R.O.C. ID coding rules.(An alphabetic character following 9 digits)

- **Credit card number for test：**

Test Case	VISA	MASTER	JCB
One time payment	4344-1173-3945-1014	5143-6137-7253-7541	3560-7212-3456-0032
Installment payment－Citiback	4563-1300-1000-2000	5148-9412-3456-0032	3565-6612-3456-0027
Installment payment－Union Bank	4344-1173-3945-1014	5242-6412-3456-0017	3565-9912-3456-0002
Installment payment－Cathay United Bank	4023-1011-2356-7894	5148-6912-3456-0041	3560-8512-3456-0003
Installment payment－Chinatrust Bank	4029-8012-3456-0092	5404-0012-3456-0026	3563-7512-3456-0036
Installment payment－Shin Kong Bank	4695-8500-1234-5674	5176-6612-3456-0106	3565-8412-3456-0090
Installment payment－Taishin Bank	4377-5200-0000-1234	5442-2800-0009-1234	3560-5800-0003-1234
Installment payment－E.SUN Bank	4907-0500-0007-1234	5588-9300-0003-1234	3560-9700-0006-1234
Redeemed payment－Shin Kong Bank	4695-8500-1234-5674	5176-6612-3456-0106	3565-8412-3456-0090
Expire Card	4329-4819-2212-5347	5430-4502-0000-2000	3560-6122-3456-0009
Fail Card	4563-1773-6837-4572	5430-4503-0000-2009	3560-5100-1234-5678
Amount Fail	4029-0078-0109-9296	5430-4504-0000-2008	3560-6100-0000-0002

Use the same expiry date and CVC2/CVV2 for test.
Expiry date：Dec, 2020
CVC2/CVV2：000.

6 General Notices

1. The correct retrieval of data depends on session operation while framing in web pages will interfere with operation of session; therefore, we suggest that merchant do not embed the Neweb's payment page and merchant's Receive page in a framed web page. The better way is using a pop up window (or independent web page).

2. The value of code given by Neweb plays a key role in securing connection between Neweb and merchants, we suggest that the value of code should be decrypted from configurations and assigned to a variable instead of being a constant directly defined in source program.

3. If merchants change the IP address of host domain name in FeedBack url, Neweb system may take a while to get the new IP address from the upper layer DNS and some of request to FeedBack will fail consequently. To bypass the problem, merchant could adopt the new IP instead of host domain name as a temporary url of FeedBack.

4. Neweb's merchant pay page supports revealing individual Logo of merchant at the top of web page as long as merchant providing a Logo picture complied with following requirements.

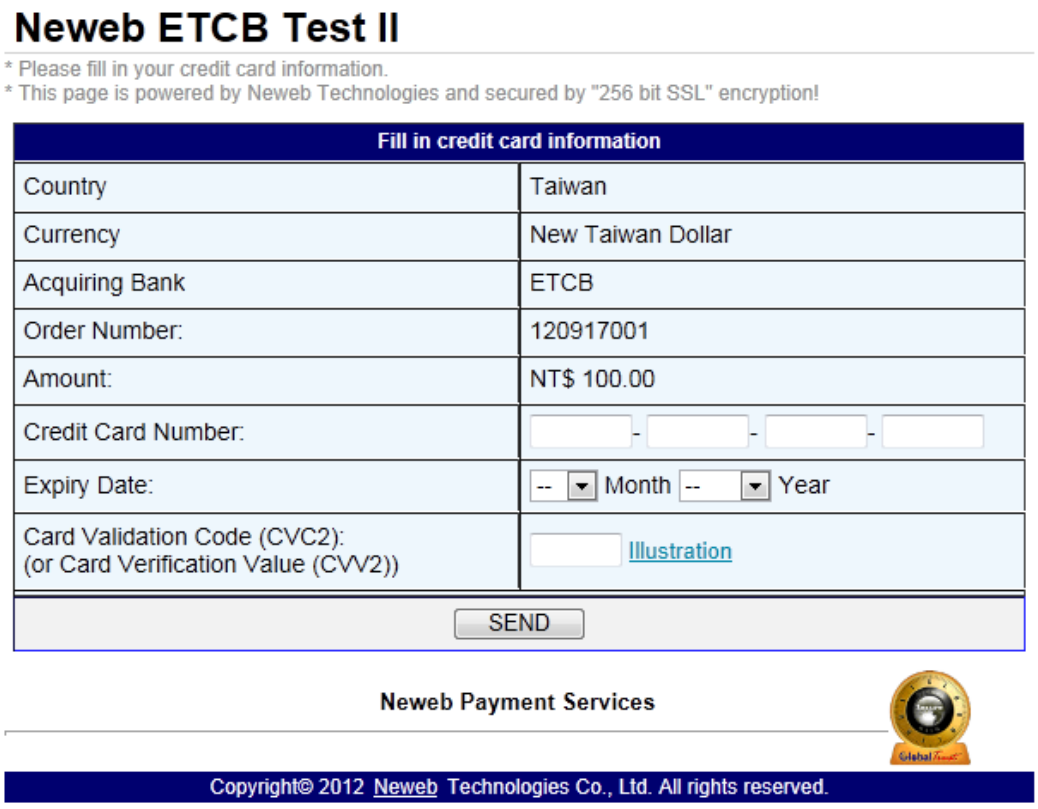
   Logo specification and sample：

   Pixel：(W)600 pix * (H)85 pix Size : Within 10K

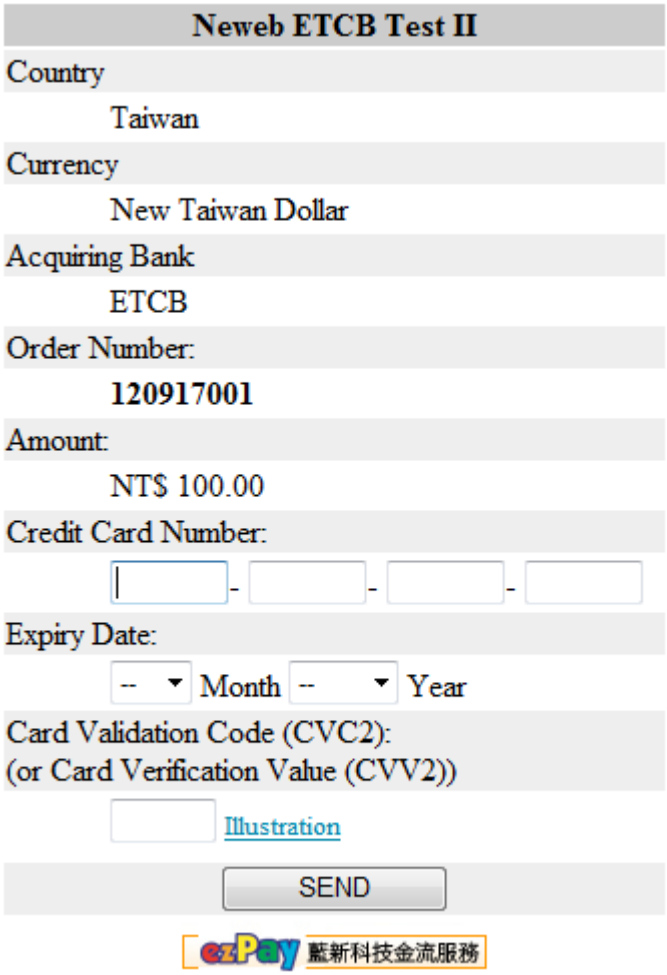
7 Sample Pay Pages for Test

Using the indicator of pay page (iphonepage), merchants are empowered to switch between two modes of pay page, which are PC/NB and iPhone modes：

- PC/NB pay page - iphonepage=0



- iPhone pay page - iphonepage=1



8 Useful Tips before Test

The followings takes ASP programs provided by Neweb for examples：

- Revise the OrderURL(http://xxxxx/feedback2.asp) and the ReturnURL(http://xxxxx/receive.asp) in PaymentConfirm2.asp and confirm that they are working properly.
- Make sure that the value of Code (abcd1234) used in MD5 is set as for test in PaymentConfirm2.asp.
- Make sure that the value of Code (abcd1234) used in MD5 is set as for test in feedback2.asp.
- Make sure that the value of Code (abcd1234) used in MD5 is set as for test in receive.asp.

9 Useful Tips before Going Production

The followings takes ASP programs provided by Neweb for examples：

- Revise the Neweb transaction url：replace the host for test with the host for production.
  Neweb transaction url for test：https://maple2.neweb.com.tw/NewebmPP/cdcard.jsp
  Neweb transaction url for production：https:// **[*hostname*]**/NewebmPP/cdcard.jsp where the **[*hostname*]** is included in attached of going production email notification.

- Revise the OrderURL(http://xxxxx/feedback2.asp) and the ReturnURL(http://xxxxx/receive.asp) in PaymentConfirm2.asp and confirm that they are working properly.

- Make sure that the value of Code (included in attached of going production email notification) used in MD5 is set as given in PaymentConfirm2.asp.

- Make sure that the value of Code (included in attached of going production email notification) used in MD5 is set as given in feedback2.asp.

- Make sure that the value of Code (included in attached of going production email notification) used in MD5 is set as given in receive.asp.

Appendix I Credit Card Payment Term Definitions

Merchant should be aware of these payment terms

1. Approval/Authorization

   Issuing bank check and determine if a specified credit card number is in good conditions. Such as:
   - Card number is not registered as a lost card.
   - Accumulated unsettle amount does not surpass credit limit.
   - Status is not lock due to cardholder's request or bank's risk control.

   If the answer is positive, issuer will reply the transaction by giving an approved code for merchant use in the following process.

2. Deposit/Capture

   It means that merchant has delivered his goods or services to customer and intends to capture money from its acquiring bank. Merchant should present approve code to its acquiring bank as evidence that the transaction is approved by issuer. Deposit action also links the transaction to a batch for proceeding settlement.

3. Settlement/Close batch

   The purpose of settlement is to fix the amount of a batch which contains multiple transactions so that the clearing operation between banks can be processed efficiently base on a batch instead of individual transaction. Accordingly, acquiring bank disburse funds to its merchants by settled batches periodically.

4. Credit/Refund

   Refund is used to return monies to the cardholders by adding a negative amount into the new opened batch which will reverse the positive amount occurred in the previously closed batch. The cardholders will see a positive amount and a corresponding negative amount on their bills (might be on the same month or different months), therefore, will not feel any loss.

Notice:

According to the settle operation rules set by acquiring bank, merchant should complete settlement within 21 days after payment transaction is approved. If there exists any transaction that exceeds the limitation, bank's system will not accept the settlement. Merchant should manually fill in an application form of collecting process and fax to acquiring bank directly. The funds of collecting process will be remitted to merchant in 130 days.