

藍新金流服務平台

批次約定信用卡付款授權

技術串接手冊

標準版

程式版本號：1.0

文件版本號：P_BATCHAGREEMENT_1.0.0

(文件為藍新科技股份有限公司版權所有)

版本異動

異動序號	文件版本號	修改內容	日期
1	P_BATCHAGREEMENT_1.0.0	初版	2021/08/19

目錄

一、串接目的.....	3
二、使用條件與資料交換方式.....	4
三、交易流程.....	5
四、批次約定信用卡授權參數設定.....	6
五、批次約定信用卡授權系統回應訊息.....	10
六、授權結果系統回傳參數說明.....	13
附件一：EncryptData_加解密方法.....	17
附件二、HashData 處理方式	21
附件三：API 發動系統回應代碼表	22
附件四：授權結果回應代碼表.....	23

一、串接目的

藍新金流提供批次約定信用卡付款授權機制，讓商店可以用「約定信用卡付款授權 Token」進行批次授權交易。

進行批次授權之前，商店需引導付款人綁定信用卡並取得藍新金流提供的該付款人之「約定信用卡付款授權 Token」(請參考藍新金流 NewwebPay_約定信用卡付款授權 API)。之後商店只需要使用「約定信用卡付款授權 Token」以幕後批次的方式，進行「已約定授權」交易即可。

二、使用條件與資料交換方式

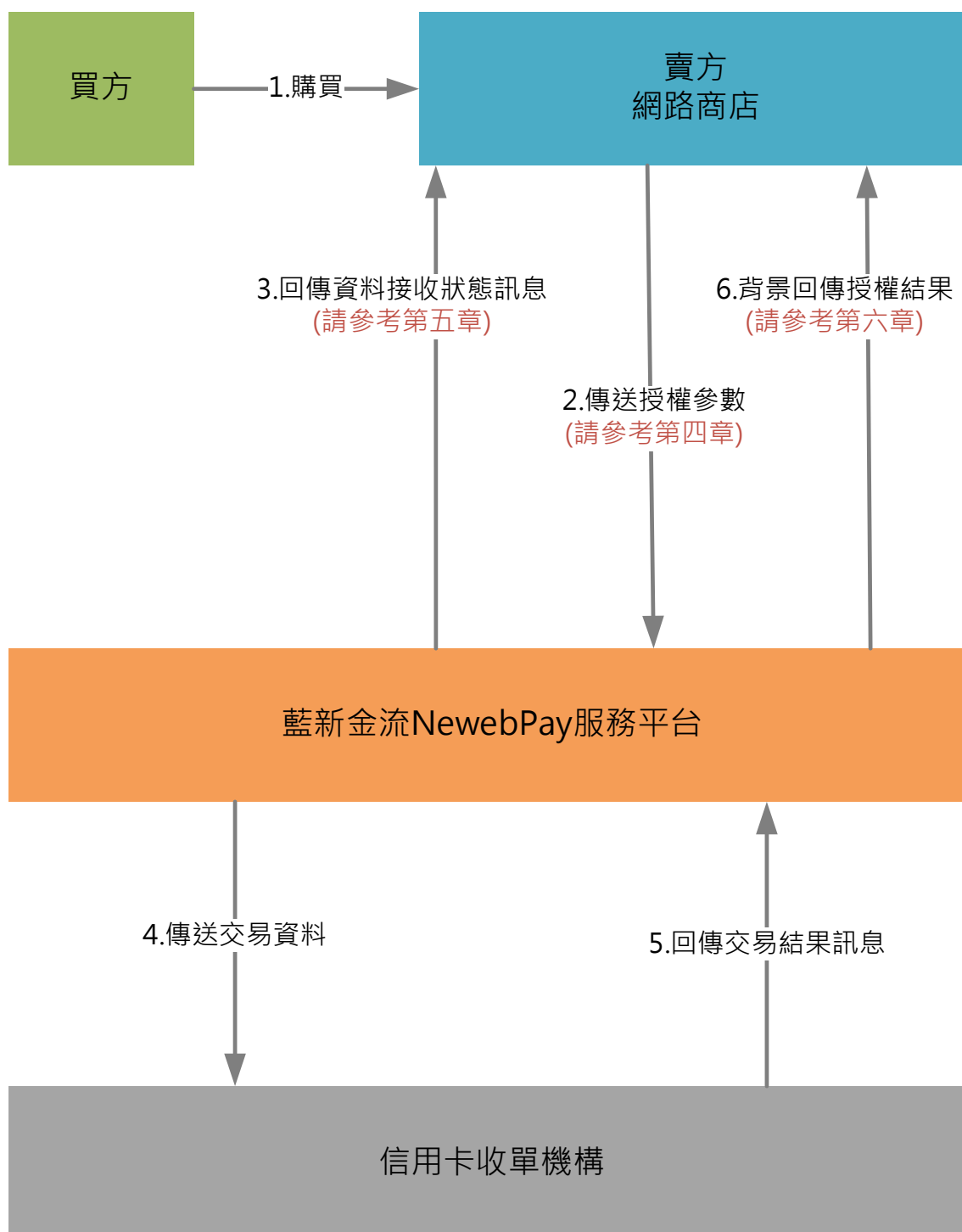
(一) 批次約定信用卡付款授權工具使用條件

1. 以單一商店為主體發動。
2. 商店需向藍新金流申請並約定 IP (適用約定信用卡 API 串接 IP，如商店已申請相關 IP 可直接使用本 API)。
3. 商店需有能接收藍新金流服務平台接收授權結果用之網址。
4. 每批可接受最高筆數為 30,000 筆。

(二) 資料交換方式

1. 商店以「HTTP POST」方式傳送參數至藍新金流平台進行查詢。
2. 傳送方式須以後端 Post 進行。
3. 藍新金流將以 Web Service 方式回應批次資料接收結果。
4. 授權結果將以幕後方式 (Notify) 傳送至商店指定網址。
5. 編碼格式為 UTF-8。

三、交易流程



四、批次約定信用卡授權參數設定

(一)串接網址：

(1) 測試串接網址：

<https://ccore.newwebpay.com/API/CreditCardBatch/create>

(2) 正式串接網址：

<https://core.newwebpay.com/API/CreditCardBatch/create>

(二)Post 參數說明：

參數名稱	參數中文名稱	必填	型態	備註
UID_	商店代號	V	Varchar(15)	商店代號。
Version_	串接程式版本	V	Varchar(5)	請帶 1.0。
EncryptData_	壓縮加密資料	V	Text	1.資料需先壓縮後再加密。 2.相關加密及資料壓縮方法請參考 “ 附件一 ”。
RespondType_	格式	V	Varchar(15)	固定為 JSON
HashData_	雜湊資料	V	Text	相關方法請參考 “ 附件二 ”。
Encoding_	壓縮類型	V	Varchar(10)	1.固定為 gzip 2.資料壓縮時需使用 gzip 壓縮格式

* 【備註】參數後方均有底線“_”符號。

(三) 『EncryptData_』 內含欄位：

參數名稱	參數中文名稱	必填	型態	備註
NotifyURL	授權結果通知網址	V	Varchar(50)	1.以幕後方式回傳給商店相關支付結果資料；請參考 章節五、授權結果系統回傳參數說明。 2. 只接受 80 與 443 Port。
TimeStamp	時間戳記	V	Varchar(50)	自從Unix 紀元 (格林威治時間1970 年1月1 日00:00:00) 到當前時間的秒數，若以php程式語言為例，即為呼叫time()函式所回傳的值。 例：2014-05-15 15:00:00這個時間的時間戳記為1400137200。
TotalCount	總筆數	V	Int(5)	純數字，最高筆數為30000筆。
TotalAmt	總金額	V	Int(15)	純數字，授權總金額加總。
BatchNo	批號	V	Date	本批號碼。同商店不得有批號不得重複。 為時間格式yyyymmddHIS 如：20210715163620
Detail	授權詳細資料	V	txt	1.本批授權的詳細資料，以陣列格式將每筆資料存放於此。 2.每筆資料所需欄位請參考下方說明。

(四) 『Detail』 內含欄位 (JSON 格式)：

參數名稱	參數中文名稱	必填	型態	備註
MerchantOrderNo	商店訂單編號	V	Varchar(30)	1.商店自訂訂單編號，限英、數字、“_” 格式。 例：201406010001。 2.長度限制為 30 字。 3.同一商店中此編號不可重覆。
Amt	訂單金額	V	int(10)	1.純數字不含符號，例：1000。 2.幣別：新台幣。
ProdDesc	商品資訊	V	Varchar(50)	1.限制長度為 50 字。 2.編碼為Utf-8格式。
PayerEmail	付款人電子信箱	V	Varchar(50)	於交易完成或付款完成時，通知付款人使用。

Type	授權類型	V	int(2)	固定帶2
TokenTerm	約定信用卡付款之 付款人綁定資料	V	Varchar(20)	1.可對應付款人之資料，用於綁定付款人與信用卡卡號時使用，例：會員編號、Email。 2.限英、數字，「.」、「_」、「@」、「-」格式。
TokenValue	約定信用卡付款授權Token	V	Varchar(70)	為首次約定授權成功時，回傳的TokenValue 參數值。

傳送範例：

EncryptData 壓縮前範例：

```
{
  "NotifyURL": "https://cwww.newwebpay.com/test.php",
  "TimeStamp": 1627894455,
  "TotalCount": 2,
  "TotalAmt": 31,
  "BatchNo": "20210805165415",
  "Detail": [
    {
      "MerchantOrderNo": "1627894455_2",
      "Amt": 16,
      "ProdDesc": "Newweb test Product",
      "PayerEmail": "test@newweb.com",
      "Type": 2,
      "TokenTerm": "test@newweb.com",
      "TokenValue": "0785a73c76d6fe5678cf3989c66c78cd11ac33c7bcd564c137e9b18b0b363a1667"
    },
    {
      "MerchantOrderNo": "1627894455_2",
      "Amt": 16,
      "ProdDesc": "Newweb test Product",
      "PayerEmail": "test@newweb.com",
      "Type": 2,
      "TokenTerm": "test@newweb.com",
      "TokenValue": "03a5a73c76d6fe18cf3989c66c78cd11ac33c7bcd564c137e9b18b0b363a1667"
    }
  ]
}
```

EncryptData 壓縮加密後結果 (URL Encode→壓縮為 gzip 格式→AES 256 加密)：

key = 12345678901234567890123456789012

iv = 0000000000000000

```
AAf08838f5285f782ac2ef68bee6f7d91f28abedf1b2e3ce2f9144ddc03587a53a5b5d72d194655fe652177
ebe9c0ad5f1be485029969f6ae09b1a2f6733b63f5b929092df5313895c88f99fa68d51e99f3d5616dbd89c
c7fb5e17666505f8bcb8dae45b029b985ee4e6fe71e937453b326e2dcdcf772c96771c58475597c66147c2
51f93a77fbd6d4d2688ee448c36fc8f39879611b79bedca2fe6b04bc54b6110041e4396d7c28d399875a7c
a2363c2666d4950723e1d19bc22fd362820da11f32681d774447ce29e9dab035e397d65e1c2f8cb241acb
2936565f59be2daf2b025f23eda8737c253a3ab3806894a5e6570755f563de62f5048f1af96541b7a6e0241
7297d26875c0164aaa52c3b10f28b418cc2788e3297cac4af0bd82d14ec6a9a43bb8f27d42f28fdb534b93
74548efef7c8c5cb3c1bafda2320432b72ce4c359a4fddbd6196c08bf541c9f8e509db538149f34a25daef2
544add668be9c64987681893308c415a48c2ac192c896e37b0d29ef5205abd917e3cff365c383bfe1dc744
bf3aefa2fd3f3742875ee579888a7a955bf28fa01514dae3c2d121075e454907583c721cda2e2dcd8be1c28
bf02b29d2f6a4e10f4244588a74bc1e22e1e584132c555412b251f399254023fcae943601ef62fd479ad867
b0802b98e13718d5509d90ea20f88513f61ba027ed5d19b8f73164c1011f46bd02d1cb76e54b04c9e550f
7b68990c4766b35e1b162bfa774384030cb2cfbd475f29ca8eacff12d879035208faa78e9aed9fda4cdb794
```

```
a785a4e99a605d52168e5a33d363d26a5f5b5e65c8fa55d58d501394a30ec0290b08791b1912adec03964
77facbf5ae0d19d5fdb51ca0791e20bf949358eed0490c8db8d747757390306944af81ca0bfb1e0550f5f2d
d3feea082072f304430f89b2fa181dd37e99c221c4d23db6be313b96e5d5cd62e90bbe70a91b0d7443e90
fae189757bf8fe2eed1926072ce5e14fbf4e9dd41e02a87a44351aa4533be2ee00c39436c82e380703fc8e0
ddf37b48fd7a3e6e838b01d225e41f95e6461061ce6919ae5d84a22583862d65f8e9a07ec81a9a30fa79b6
6fb6351a81ce9d5734baa0d8907fadb8c59cd87a07bed5cb167b9aed181df00d45fff79f94dd99503f457c9
4c08315621d23912a11283df88
```

五、批次約定信用卡授權系統回應訊息

(一) 回應訊息會以「Web Service」方式回應端末設備。

(二) 如資料接收失敗，系統將不會對本批資料作任何處理，也不會發送Notify通知。

(三) 回傳格式：JSON。

(四) 回傳參數說明：

參數名稱	參數中文名稱	型態	備註
Status	回傳狀態	Varchar(10)	1.若資料接收成功，則回傳1000。 2.若資料接收失敗，則回傳錯誤代碼。 相關代碼表請參考“附件四”。
Message	回傳訊息	Varchar(30)	文字，敘述此次交易狀態。
EncryptData	加密資料	Text	相關解密及資料解壓縮方法請參考“附件一”。
HashData	雜湊資料	Text	相關方法請參考“附件二”。
UID	商店代號	Varchar(15)	商店代號
Version	串接程式版本	Varchar(5)	固定為1.0。
Encoding	壓縮類型	Varchar(10)	1.此為保留欄位，固定為空值 2.本回傳資料無壓縮。

(五) 『EncryptData』內含欄位 (JSON格式)：

參數名稱	參數中文名稱	型態	備註
BatchNo	批號	Date	本批號碼。為時間格式yyyymmddHHIS。 如：20210715163620
ErrorList	錯誤列表	txt	以陣列形式呈現。列出授權資料中，因資料格式錯誤導致無法授權的相對應內容。

(六) 『ErrorList』 內含欄位 (陣列格式) :

參數名稱	參數中文名稱	型態	備註
Index	資料索引位置	int(5)	索引位置。如：33表示該筆資料位於該批第33筆
MerchantOrderNo	商店訂單編號	Varchar (30)	商店自訂訂單編號
ErrorMsg	錯誤訊息	txt	顯示錯誤原因。如：金額格式錯誤

範例：

原始接收資料：

```
{
  "Status": "1000",
  "Message": "批次授權作業 - 成功",
  "EncryptData": "876b9f8884589339030472cb3c98b28e7f01bf941fb95bfa09edc45154f350
0f22b598ba52b3e2de93dca4d8c1705a1fdafa204faf983ccde2c5eb0fca4312bd",
  "HashData": "A8FF6BC5F4CE2D66E8420114EF8BA9DBA008C90D8D6D821F6E87775742A
7B685",
  "UID": "HHH122255555",
  "Version": "1.0",
  "Encoding": ""
}
```

EncryptData AES 解密 (String) :

```
{
  "BatchNo": "20210730171311",
  "ErrorList": []
}
```

交易失敗範例:

```
{
  "Status": "1106",
  "Message": "明細資料錯誤",
  "EncryptData": "43bcbf077b5d2b6a395485604f4a098e17169e67abe0a4f8e88be3313d77dcc2bb
b203fac12c0f741c1194ff7068d9bc6cbdc9a116792632e6790e5c92b2500c0fffb7d4934a2b559ef18b9
414b455b909a3abbac26ad873f3d739c3b168c379ac8ed5f9bee9a5e38c3641d84a1b91f0bd0762a25
8cc5173f9701499d127c27e",
  "HashData": "F9D878BA4C59D14C5C763EB29210A738A3D8C07D4C43B000A428002F64F3CC12",
  "UID": "MS14961955",
  "Version": "1.0",
  "Encoding": ""
}
```

EncryptData AES 解密範例：

```
{
  "BatchNo": "",
  "ErrorList": [
    {
      "Index": 0, "MerchantOrderNo": "1627637075_1",
      "ErrorMsg": "金額格式錯誤"
    }
  ]
}
```

六、授權結果系統回傳參數說明

(一)回應訊息會以「Notify」幕後資料傳方式，在批次結果處理完成後，將授權處理結果以背景方式傳送至商店指定網址。

(二)授權處理所需時間視資料筆數及網路速度決定，但如商店指定網址超過2小時仍未收到回傳資料，建議串接『單筆交易查詢API』來重新取得批次授權結果。

(三)回傳格式：JSON。

(四)回傳參數說明：

參數名稱	參數中文名稱	型態	備註
UID	商店代號	Varchar(15)	商店代號。
EncryptData	壓縮加密資料	Text	1.資料為經過壓縮後再加密。 2.相關解密及資料解壓縮方法請參考“附件一”。
HashData	雜湊資料	Text	相關方法請參考“附件二”。
Version	串接程式版本	Varchar(5)	固定為1.0。
Encoding	壓縮類型	Varchar(10)	固定為gzip

(五)『EncryptData』內含欄位（內為JSON格式）：

參數名稱	參數中文名稱	型態	備註
TimeStamp	時間戳記	Varchar(50)	純數字，如：1627638569。
O_TotalCount	原始資料總筆數	Int(5)	純數字
O_TotalAmt	原始資料總金額	Int(15)	純數字
S_TotalCount	授權成功總筆數	Int(5)	純數字
S_TotalAmt	授權成功總金額	Int(15)	純數字
BatchNo	批號	Date	本批號碼。為時間格式yyyymmddHIS 如：20210715163620
Detail	詳細資料	txt	1.本批授權的詳細資料，以JSON格式將每筆資料存放於此。

2.每筆資料所需欄位請參考下方說明。

(六) 『Detail』 內含欄位 (內為 JSON 格式) :

參數名稱	參數中文名稱	型態	備註
Status	回傳狀態	Varchar(10)	1.若資料授權成功，則回傳『SUCCESS』。 2.若資料授權失敗，則回傳錯誤代碼。 相關代碼表請參考“附件四”。
Messages	回傳訊息	Varchar(30)	文字，敘述此次交易狀態。
Amt	交易金額	Int(15)	本次交易授權金額。
TradeNo	藍新金流交易序號	Varchar(20)	由藍新金流平台產生的系統交易序號。
MerchantOrderNo	商店訂單編號	Varchar(30)	商店自訂的訂單編號。
RespondCode	金融機構回應碼	Varchar(10)	1.由收單機構所回應的回應碼。 2.若交易送至收單機構授權時已是失敗狀態，則本欄位的值會以空值回傳。
Auth	授權碼	Varchar(6)	1.由收單機構所回應的授權碼。 2.若交易送至收單機構授權時已是失敗狀態，則本欄位的值會以空值回傳。
AuthDate	授權日期	Varchar(8)	1.格式為 yyyymmdd，例：20140304。 2.若交易送至收單機構授權時已是失敗狀態，則本欄位的值會以空值回傳。
AuthTime	授權時間	Varchar(6)	1.格式為 hhmmss，例：164828。 2.若交易送至收單機構授權時已是失敗狀態，則本欄位的值會以空值回傳。
Card6No	卡號前六碼	Varchar(6)	1.信用卡卡號前六碼。 2.若交易送至收單機構授權時已是失敗狀態，則本欄位的值會以空值回傳。
Card4No	卡號後四碼	Varchar(4)	1.信用卡卡號後四碼。 2.若交易送至收單機構授權時已是失敗狀態，則本欄位的值會以空值回傳。
TokenLife	約定信用卡付款授權之有效日期	Date	1.為約定信用卡付款授權之有效日期，格式為 yyyy-mm-dd，例 2019-12-31。 2.當超過此約定信用卡付款之有效日期時，則無法再以“約定信用卡付款授權Token”進行“已約定授權”交易。

範例：

原始接收資料：

```
{
  "UID":"MS14961955",
  "EncryptData":"9844db76d74feb3a0f6643a4ba5c9e886595ae8c5962ceb09f8e7206656c94b6b5
981d564e932a6d7ffad33bac5dfe553713b6ff53aac6e4a290ad75d24bd830ad698138096e4e7e5d999
08bd0a3b6a532ccb444c6b29cb8c4a280d734931d7a0ab973bec9686a2ad8f814e20f154661bca3238
b2b2737c7547db223f65a1e2e675d45a0ac5dca465c4e4db9090bc18e78871708495693edfe9bb258
b7df9e9af312d479db643255566bc6f08c9fa19f9bf9e4c8a68d3569bda04f1901b2d16235ee0d6f03f1
ba1604399f99ff74e949effb7831eaf7cb986c31050c949d5e3e",
  "Version":"1.0",
  "HashData":"578A034619A486822127E6674214F5754714B3EE658A3F61075139FED644F803",
  "Encoding":"gzip"
}
```


EncryptData 範例：

```
{
  "TimeStamp":1627638569,
  "O_TotalCount":1,
  "O_TotalAmt":0,
  "S_TotalCount":1,
  "S_TotalAmt":0,
  "BatchNo":"20210730172417",
  "Detail":[
    {
      "Status":"TRA10076",
      "Messages":"查無此 Token",
      "Amt":"",
      "TradeNo":"",
      "MerchantOrderNo":"",
      "RespondCode":"",
      "Auth":"",
      "AuthDate":"",
      "AuthTime":"",
      "Card6No":"",
      "Card4No":"",
      "TokenLife":""
    }
  ]
}
```

附件一：EncryptData_加解密方法

1. EncryptData_加密方法(以 PHP 為例)：

將屬於交易資料的欄位採用 JSON 格式進行編碼後再加密

2. 使用商店 HashKey 及 Hash IV 進行加密。

以下提供 PHP 版本程式語言加密範例以供參考

```
function nwp_encrypt($key = "", $iv = "0000000000000000", $str = "")
{
    $str = trim(bin2hex(openssl_encrypt(addpadding($str), 'aes-256-cbc', $key,
    OPENSSL_RAW_DATA|OPENSSL_ZERO_PADDING, $iv)));
    return $str;
}

function addpadding($string, $blocksize = 32)
{
    $len = strlen($string);
    $pad = $blocksize - ($len % $blocksize);
    $string .= str_repeat(chr($pad), $pad);
    return $string;
}

echo '原始字串:'.
echo '加密 key=' . $key = '12345678901234567890123456789012'. PHP_EOL;
echo '加密 iv=' . $iv = '0000000000000000'. PHP_EOL;
echo '加密前字串=' . $str = '{"aaa":"bbb"}'. PHP_EOL;
$str = gzencode($str); // 進行 gz 壓縮
echo '加密後字串:'. PHP_EOL;
echo nwp_encrypt($key, $iv, $str);
```

若非使用 PHP 程式語言編寫 Aes 加密機制，可參考下列測試資料與加密後結果：

加密 key=12345678901234567890123456789012

加密 iv=0000000000000000

加密前字串={"aaa":"bbb"}

加密後字串：

d8d9e3f2c8402404eef0b9db1fda24939e333992d10a9173e6c379e4ff294dd936dd5f194
20dd2eb8a10c0cf9a1e8dc7bc90cd29bbe9ba8b7e0da7f1d516b626

以下提供 PHP 版本程式語言解密範例以供參考

```
function create_aes_decrypt($parameter = "", $key = "", $iv = "") {
    return strippadding(openssl_decrypt(hex2bin($parameter), 'AES-256-CBC', $key,
    OPENSSL_RAW_DATA|OPENSSL_ZERO_PADDING, $iv));
}
function strippadding($string) {
    $slast = ord(substr($string, -1));
    $slastc = chr($slast);
    $pcheck = substr($string, -$slast);
    if (preg_match("/$slastc{" . $slast . "}/", $string)) {
        $string = substr($string, 0, strlen($string) - $slast);
        return $string;
    } else {
        return false;
    }
}
}
echo '加密後字串: ';
echo $encrypt_str =
'd8d9e3f2c8402404eef0b9db1fda24939e333992d10a9173e6c379e4ff294dd936dd5f194
20dd2eb8a10c0cf9a1e8dc7bc90cd29bbe9ba8b7e0da7f1d516b626';

echo PHP_EOL;
echo '加密 key=' . $key = '12345678901234567890123456789012'.PHP_EOL;
echo '加密 iv=' . $iv = '0000000000000000'.PHP_EOL;
$str = create_aes_decrypt($encrypt_str, $key, $iv); //解密
$str = gzdecode($str); // 進行 gz 解壓縮
echo '加密前字串=' . $str;
```

若非使用 PHP 程式語言編寫 Aes 解密機制，可參考下列測試資料與解密後結果：

加密 key=12345678901234567890123456789012

加密 iv=0000000000000000

加密後字串：

d8d9e3f2c8402404eef0b9db1fda24939e333992d10a9173e6c379e4ff294dd936dd5f194

20dd2eb8a10c0cf9a1e8dc7bc90cd29bbe9ba8b7e0da7f1d516b626

解密後字串={"aaa":"bbb"}

附件二、HashData 處理方式

1. 將 AES 加密字串前加上商店專屬加密 HashKey 及 HashIV。
2. 將串聯後的字串用 SHA256 壓碼後轉大寫。

範例程式：

1. EncryptData 交易資料 AES 加密後字串

AAAABBBBCCCCDDDD

2. 前面加上商店專屬的 HashKey，最後加上商店專屬的 HashIV

HashKey=12345678901234567890123456789012&AAAABBBBCCCCDDDD&HashIV=12345678

3. 使用 SHA256 壓碼過後並轉大寫

```
strtoupper(hash("sha256",  
"HashKey=12345678901234567890123456789012&AAAABBBBCCCCDDDD&HashIV  
=12345678"));
```

壓碼結果為：

5C6C504A2F2B2E3EB5CA80998F626307ACD327AC6DCE4FF84F86B021988B2576

附件三：API 發動系統回應代碼表

發動 API 時，可能遭遇下列狀況，其代碼與說明如下表所示：

錯誤代碼	錯誤原因	備註
1000	批次授權作業 - 成功	系統成功接收到資料
1101	新增訂單失敗	
1102	該單號執行中，請勿重覆執行	
1101	單號重覆	
1101	新增失敗	
1103	筆數不符	
1104	總額不符	
1105	IP 不允許	目前 IP 不在申請清單中
1106	明細資料錯誤	
1107	批次單號已存在	
1108	筆數超過上限	最高為 30,000 筆

附件四：授權結果回應代碼表

系統處理授權要求時，可能遭遇下列狀況，其代碼與說明如下表所示：

錯誤代碼	錯誤原因	備註
TRA10001	商店代號錯誤	
TRA10003	金額格式錯誤	
TRA10009	商店代號空白	
TRA10012	商店代號停用	
TRA10013	信用卡資格停用	
TRA10016	信用卡授權失敗	
TRA10037	商家訂單編號錯誤，只允許英數與底線	
TRA10052	商店不允許國外卡交易	
TRA10053	此商店目前無法使用信用卡交易 信用卡授權額度已滿	
TRA10061	特約商店信用卡收單行設定錯誤	
TRA10061_g	信用卡收單行設定錯誤	
TRA10075	新增交易訂單失敗	提示訂單編號重複或其他失敗原因
TRA10076	查無此 Token	
TRA10078	信用卡背面末三碼檢查錯誤	
TRA10079	卡片到期日檢查錯誤	
TRA10100E	玉山系統維護中	
TRA10100T	台新系統維護中	
TRA10681	信用卡交易序號編號錯誤	
TRA20001	交易資料新增失敗	
TRA20011	此商店不支援此信用卡交易	