BPOINT®

Receivables Solution

BPOINT Payment Page Receipt Redirection

Version 1.4

Contents

1. Overview

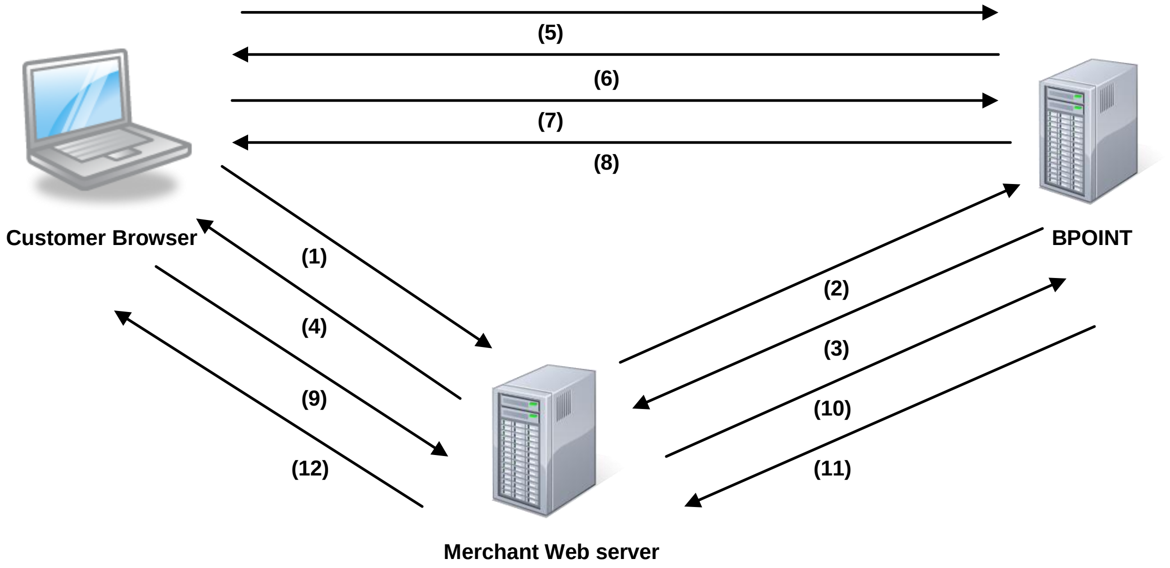
BPOINT Payment Page offers a secure, PCI DSS compliant interface to the BPOINT payment platform with minimal programming effort. It's design makes sure that no credit card information ever goes through the merchant's web server. Payment Page sends the payment details directly from the customer's web browser to BPOINT payment platform over SSL connection. Payment result is then relayed to the merchant via receipt page redirection mechanism.

BPOINT Payment Page is available to all merchants and maybe customized to meet particular merchant's requirements.

Basic description of the payment process with Payment Page:

1. Customer visits merchant's web site.
2. Customer proceeds to payment.
3. Merchant's site requests a once off security token from BPOINT Payment Connector.
4. Merchant's web site redirects the customer to BPOINT payment page. No SSL certificate is required by the merchant. The payment page is secured using BPOINT SSL certificate.
5. Customer types in credit card details on the BPOINT page.
6. Payment page sends payment information directly to BPOINT.
7. BPOINT processes a payment and sends a response to customer's browser.
8. Response redirects customer's browser to merchant's receipt page, effectively relaying transaction result to the merchant.
9. Merchant verifies that the payment response has not been modified.

Please refer to the diagram below for a detailed call flow:



(1) Customer requests to make a payment on the merchant web page

(2) Merchant web server initiates HTTP POST request to BPOINT for authentication

(3) BPOINT authenticates the merchant and returns back with security token

(4) Merchant web server redirects customer to BPOINT payment page with security token in URL

(5) Redirection causes customer browser to request BPOINT payment page

(6) BPOINT displays payment page to customer

(7) Customer types in the card details and click on “Submit” button. This initiates HTTP POST directly to BPOINT for payment

(8) BPOINT processes the payment and redirects the response to merchant configured receipt URL

(9) The page before rendering makes a HTTP GET request to merchant web server

(10)Merchant web server sends a HTTP POST request to BPOINT to verify the payment response

(11)BPOINT authenticates the merchant and returns back with the verification response

(12) Based on the verification response either receipt or error page is displayed to the customer

2. Payment Process

Payment process can be broken up into 4 major stages:

1. Pre-payment authentication (Auth request)
2. Redirection to BPOINT payment page
3. Receipt page redirection (to merchant's receipt page)
4. Redirect response verification (Verify request)

Pre-payment authentication (Auth request)

Before merchant's web site can redirect to BPOINT payment page, it has to complete an Auth request. The Auth request serves following functions:

- Authenticates the merchant by merchant number, username and password. If these details are not correct security token is not be generated. Since the Auth request is initiated from merchant's server directly to BPOINT platform merchant's credentials are never exposed to any 3rd party.
- Creates a unique security token to allow merchant's customer to process a payment. Customer's IP address is tied to the security token and the payment request will only be accepted from that IP.
- Security token prevents processing of duplicate payments. Security token becomes invalid as soon as a payment request is received with that token.
- Signs data that will be passed with the payment request (such as amount, customer reference numbers etc). If the payment details are tampered with the payment request will be rejected.
- Security token is valid only for a predefined period of time (20 minutes). If the payment request is not attempted during that time then new security token will need to be generated.

Auth request URL

https://www.bpoint.com.au/payconnect/auth.aspx

Sending Auth request

The Auth request is completed by a simple HTTP POST request initiated from the merchant's web server to Auth request URL. Input parameters are passed inside the body of the POST request. The response parameters are returned in the name=value pairs, separated by new line characters.

IMPORTANT NOTE:

1. Make sure that the input parameter values are URL encoded.
2. Only pass in number of CRNs to Auth request as accepted by the BPOINT payment page. Failure to do so will result in an error. E.g. If your BPOINT payment page accepts only CRN1 then passing in CRN2 or CRN3 to the Auth request will result in error.

Input Parameters

Name	Value	Mandatory	Example	Description
in_merchant_number	Numeric 16 digits	Yes	5353000000000000	Merchant facility number.
in_merchant_username	Alphanumeric Max 50 characters	Yes	connectoruser	Username of the user set up with payment connector permissions.
in_merchant_password	Alphanumeric Special characters Max 50 characters	Yes	SecurePassword0	Password
in_ip_address	Numeric, full stop allowed Max 15 characters	No	127.0.0.1	Customer's IP address.
in_receipt_page_url	Receipt page URL	No		Receipt page URL. If provided it will overwrite receipt page URL stored in the system.
in_amount	Numeric Max 9 digits	Yes	1000	Payment amount, in cents Eg: $10.12 must be passed in as 1012
in_billercode	Numeric Max 50 digits	Yes	10009	Biller code

in_crn1	Alphanumeric Max 50 characters	Yes	Accnum123	Customer reference 1
in_crn2	Alphanumeric Max 50 characters	No		Customer reference 2
in_crn3	Alphanumeric Max 50 characters	No		Customer reference 3

Output Parameters

Name	**Example**	**Description**
out_request_resp_code	0	Result of the auth request. 0 indicates success, nonzero value indicate that error has occurred. Please refer to appendix for error code descriptions
out_errortext		Message describing the error, returned only if out_request_resp_code is not 0.
out_pay_token		Security token to be used with pay request, returned only when out_request_resp_code is 0.

Sample request

```
POST https://www.bpoint.com.au/payconnect/auth.aspx HTTP/1.1
Host: www.bpoint.com.au
Content-Type: application/x-www-form-urlencoded
Content-Length: 171

in_merchant_number=5353000000000000&in_merchant_username=connectoruser&in_merchant_password=SecurePassword0&in_amount=1000&in_merchant_reference=Invoice123&in_crn1=Accnum123&in_ip_address=127.0.0.1
```

Sample response

```
HTTP/1.1 200 OK
Cache-Control: private
Pragma: no-cache
Content-Length: 74
Content-Type: text/html; charset=utf-8
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Server: Apache2
Date: Wed, 29 Dec 2010 02:35:36 GMT

out_request_resp_code=0
out_pay_token=O/+/k2x/LBHGD/4zLemoo8ftd4+Y/IlmKO+TT6LWBdHPF/om/eCtDg==
```

Redirection to BPOINT payment page

The Biller code, customer reference numbers and amount parameters passed in to the Auth request will be used to display the BPOINT payment page to the customer.

Parameters displayed the BPOINT payment page will be read-only so that they cannot be modified by customer.

The BPOINT payment page submits the payment directly to the BPOINT system.

BPOINT payment page URL

https://www.bpoint.com.au/payments/<shop>

Where <shop> is the short merchant name allocated to the merchant by the bank. This URL can be obtained by logging on to Biller Back Office and then navigating to INTERNET section.

Input Parameters

Name	Value	Mandatory	Example	Description
in_pay_token	Alphanumeric Special characters	Yes		Security token received as out_pay_token response parameter from the auth request
IsFixed	1 or 0	No	1	Pass this in if you do not want to display the “Edit” button on the payment confirm screen

Receipt page redirection

Once the payment is processed, the response will be redirected to the merchant's receipt page URL. The receipt page URL can be preconfigured by the merchant with the BPOINT system or it can be passed in the Auth request. If receipt page URL is not present the redirection will not occur and the customer will see a BPOINT (merchant branded) receipt page.

Output Parameters

Name:	Example:	Description:
out_request_resp_code	0	Result of the pay request. 0 indicates success, nonzero value indicate that error has occurred. **Note: 0 does not indicate that payment was approved. Check out_response_code parameter to determine the result of the transaction.**
out_errortext		Message describing the error, returned only if out_request_resp_code is not 0.
out_amount		Amount
out_billercode		Biller code
out_crn1		Customer reference 1
out_crn2		Customer reference 2
out_crn3		Customer reference 3
out_response_code		Transaction summary response code. See Transaction Response Code document
out_bank_response_code		Bank response code See Transaction Response Code document
out_auth_result		Response text
out_txn_number		Transaction number, required for refunds via API
out_receipt_number		Receipt number
out_settlement_date		Settlement date in yyyyMMdd format
out_expiry_date		Card expiry date, in MM/yy format
out_account_number		Truncated credit card number

out_payment_date		Transaction date and time, in dd/MM/yyyy hh:mm:ss tt format
out_verify_token		Security token to be used with the Verify request, to verify that response parameters have not been changed during the redirection.

Redirect response verification (Verify request)

Before merchant’s web site renders the receipt page to the customer, it is recommended that the verify request is used to make sure the payment response data has not been tampered with. This check is required as the payment response data is passed back via customer’s browser in plain text and can be easily changed.

Security token for the Verify request is valid only for a predefined period of time (20 minutes). If the verify request is not attempted during that time then the merchant should use the BPOINT API to verify that the transaction occurred.

Security token for the Verify request can only be used once. Once a request is performed the token becomes invalid. This is an additional security feature to stop potential duplicate redirections to merchant’s receipt page.

As a failsafe mechanism, in case of Pay redirection or Verify request failure, the merchant should implement a call to the BPOINT API and invoke “SearchTransactions” method to regularly reconcile their system against the BPOINT database. Please refer to “BPOINT Web Service API” guide for more information on “SearchTransactions” method.

Verify request URL

https://www.bpoint.com.au/payconnect/verify.aspx

Sending Verify request

The Verify request is completed by a simple HTTP POST request initiated from the merchant’s web server to Verify request URL. Input parameters are passed inside the body of the POST request. The response parameters are returned in the name=value pairs, separated by new line characters. **NOTE**: Make sure that the parameter values are URL encoded.

Input Parameters

Name	Value	Mandatory	Example	Description
in_merchant_number	Numeric 16 digits	Yes	5353000000000000	Merchant facility number.
in_merchant_username	Alphanumeric Max 50 characters	Yes	connectoruser	Username of the user set up with payment connector permissions.
in_merchant_password	Alphanumeric Special characters Max 50 characters	Yes	SecurePassword0	Password
in_amount	Numeric Max 9 digits	Yes	1000	out_amount parameter in payment response.
in_billercode	Numeric Max 50 digits	No	10009	out_billercode parameter in payment response.
in_crn1	Alphanumeric Max 50 characters	Yes	Accnum123	out_crn1 parameter in payment response.
in_crn2	Alphanumeric Max 50 characters	No		out_crn2 parameter in payment response.
in_crn3	Alphanumeric Max 50 characters	No		out_crn3 parameter in payment response.
in_response_code		Yes		out_response_code parameter in payment response.
in_bank_response_code		Yes		out_bank_response_code parameter in payment response.
in_auth_result		Yes		out_auth_result parameter

				in payment response.
in_txn_number		Yes		out_txn_number parameter in payment response
in_receipt_number		Yes		out_Receipt_number r parameter in payment response
in_settlement_date		Yes		out_settlement_date parameter in payment response
in_expiry_date		Yes		out_expiry_date parameter in payment response
in_account_number		Yes		out_account_number parameter in payment response
in_payment_date		Yes		out_payment_date parameter in payment response
in_verify_token		Yes		out_verify_token parameter in payment response

Output Parameters

Name:	**Example:**	**Description:**
out_request_resp_code	0	Result of the verify request. 0 indicates successful verification, nonzero value indicate that error has occurred
out_errortext		Message describing the error, returned only if out_request_resp_code is not 0.

Sample request

```
POST https://www.bpoint.com.au/payconnect/verify.aspx HTTP/1.1
Host: www.bpoint.com.au
Content-Type: application/x-www-form-urlencoded
Content-Length: 401

in_merchant_number=5353000000000000&in_amount=1000&in_merchant_reference=1234&in_crn1=98
98009&in_response_code=0&in_bank_response_code=00&in_auth_result=Approved&in_txn_number=1
2345&in_receipt_number=51234567890&in_settlement_date=20101230&in_expiry_date=1212&in_accou
nt_number=512345...346&in_payment_date=20101230123500&in_signature=McZUhzbSmP9ihEBP7vLE
eFQv88UUbFY63AfOf7Uj4GDXlI3kQQi60w==
```

Sample response

```
HTTP/1.1 200 OK
Cache-Control: private
Pragma: no-cache
Content-Length: 74
Content-Type: text/html; charset=utf-8
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Server: Apache2
Date: Wed, 29 Dec 2010 02:36:36 GMT

out_request_resp_code=0
```

3. Response Codes

Response Code	Error
1	Invalid parameter in_merchant_number
2	Invalid parameter in_merchant_username
3	Invalid parameter in_merchant_password
4	Invalid parameter in_ip_address
5	Invalid parameter in_amount
6	Amount cannot be zero or less than zero
8	Invalid parameter in_crn1
9	Invalid parameter in_crn2
10	Invalid parameter in_crn3
11	Invalid parameter in_credit_card
12	Invalid parameter in_expiry_month
13	Invalid parameter in_expiry_year
14	Invalid parameter in_cvv
15	Invalid parameter in_receipt_page_url
16	Invalid parameter in_response_code
17	Invalid parameter in_bank_response_code
18	Invalid parameter in_auth_result
19	Invalid parameter in_txn_number

20	Invalid parameter in_receipt_number
21	Invalid parameter in_settlement_date
22	Invalid parameter in_expiry_date
23	Invalid parameter in_account_number
24	Invalid parameter in_payment_date
25	Invalid parameter in_pay_token
26	Invalid parameter in_verify_token
27	The merchant number supplied is not present in the system
28	The biller code supplied is not present in the system
29	Invalid login details supplied
30	Signature verification failed (Invalid signature / data supplied)
31	Invalid session request (The session details not found in the system)
100	System error