BPOINT Payment Page
Receipt Redirection

Version 1.4.2

Version history

Version	Changes	Author	Date
1.4.0	Original version	Premier Technologies (NP)	20 Oct 2011
1.4.1	Updates based on latest payment connector changes and IP address not compulsory changes	Premier Technologies (NP)	15 May 2012
1.4.2	Updates for Add and Update token methods	Premier Technologies (NP)	19 Oct 2012

Contents

1. Overview

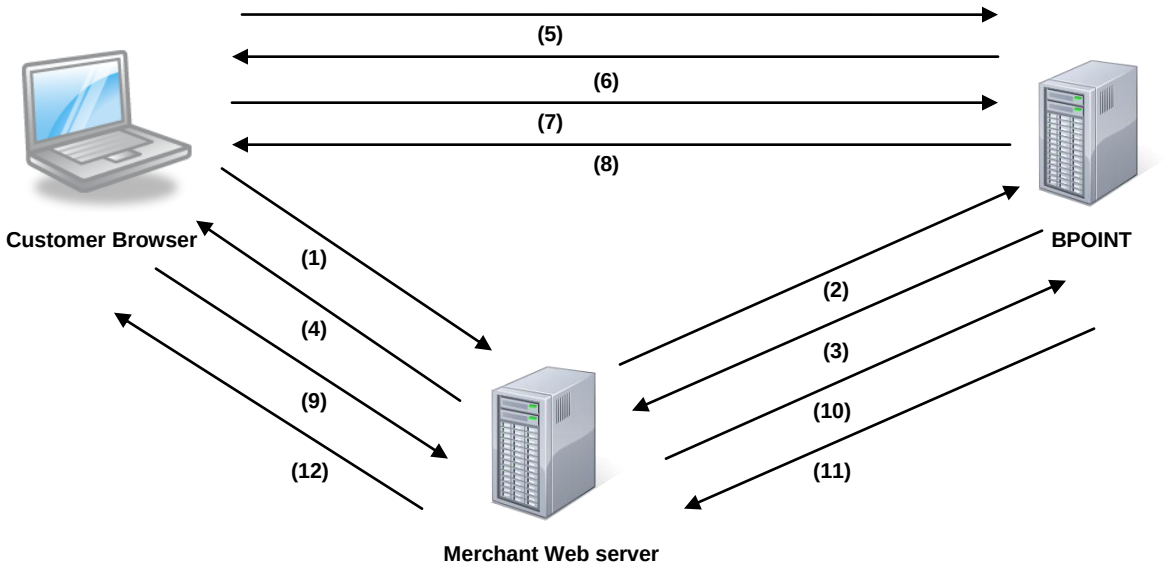
BPOINT Payment Page offers a secure, PCI DSS compliant interface to the BPOINT platform, enabling anonymous users to either make a payment or securely store their card details in BPOINT Data Vault. It's design makes sure that no credit card information ever goes through the merchant's web server. Payment Page sends the account details directly from the customer's web browser to BPOINT platform over SSL connection. The result is then either displayed on the screen or relayed back to merchant via browser redirection mechanism, depending upon the facility configuration.

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

Basic description of the process with Payment Page:

1. Customer visits merchant's web site.
2. Customer proceeds to payment or to add account / save credit card details page.
3. Merchant's site requests a once off session token from BPOINT Payment Connector.
4. Merchant's web site redirects the customer to BPOINT page with the session token in URL. No SSL certificate is required by the merchant. The BPOINT page is secured using BPOINT SSL certificate.
5. Customer types in credit card details on the BPOINT page, which sends the credit card information directly to BPOINT.
6. BPOINT processes the request and sends a response to customer's browser. The result is then displayed in the customer's browser on a BPOINT (merchant branded) receipt page.
7. If redirection is enabled then BPOINT redirects customer browser to merchant's receipt page, effectively relaying the result of the operation to merchant.
8. 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 or to save credit card details 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 session token
(4) Merchant web server redirects customer to BPOINT page with session token in URL
(5) Redirection causes customer browser to request the required BPOINT 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
(8) BPOINT processes the transaction 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.
- 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	apiuser	Username of the user set up with API level user permissions.
in_merchant_password	Alphanumeric Special characters Max 50 characters	Yes	SecurePas1	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	Yes	12345678	Customer reference 1

	Max 50 characters			
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

Content-Type: application/x-www-form-urlencoded

Host: www.bpoint.com.au

Content-Length: 172

in_merchant_number=5353000000000000&in_merchant_username=apiuser&in_merchant_password=SecurePas1&in_ip_address=127.0.0.1&in_amount=1000&in_billercode=10009&in_crn1=12345678

Sample response

HTTP/1.1 200 OK

Cache-Control: private

Content-Type: text/html; charset=utf-8

p3p: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"

Set-Cookie: ASP.NET_SessionId=p2bfca55nihwqs55p0z4xb45; path=/; secure; HttpOnly

Server: Apache2

Date: Mon, 29 Oct 2012 23:32:49 GMT

out_request_resp_code=0

out_token=01ad0370-583b-4c0b-b757-555545e0e3ad

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 → THEMES 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. Default is “0”

Sample request

https://www.bpoint.com.au/payments/<shop>?in_pay_token=01ad0370-583b-4c0b-b757-555545e0e3ad&IsFixed=0

Error conditions

An error page will be displayed if any of the following is true while accessing BPOINT payment page

- in_pay_token parameter present in the URL but has populated with incorrect session token
- Session token passed in as in_pay_token has expired [On the test system there is currently no expiry on the session id. But the production / live system expires the session after 20 minutes]
- The query string variables values contain URL unsafe characters E.g. # and ?

Extra Notes

If neither “in_receipt_page_url” is populated in authentication nor the merchant facility is configured with receipt page URL then the customer experience ends at this step. Customer will see result in a BPOINT (merchant branded) receipt page. Periodic calls can be made to “SearchTransactions” Web service API method to retrieve token information and sync it with merchant’s database. Please refer to BPOINT Web Service API document for more information on “SearchTransactions” method call.

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	apiuser	Username of the user set up with payment connector permissions.
in_merchant_password	Alphanumeric Special characters Max 50 characters	Yes	SecurePas1	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=9898009&in_response_code=0&in_bank_response_code=00&in_auth_result=Approved&in_txn_number=12345&in_receipt_number=51234567890&in_settlement_date=20101230&in_expiry_date=1212&in_account_number=512345...346&in_payment_date=20101230123500&in_verify_token=McZUhzbSmP9ihEBP7vLEeFQv88UUbFY63AfOf7Uj4GDXlI3kQQi60w==

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. Adding Record to DataVault

Add to data vault process can be broken up into steps as below:

1. Authentication (AuthV2 request)
2. Redirection to BPOINT add token page
3. Receipt page redirection (to merchant's receipt page)
4. Redirect response lookup (Lookup request)

Authentication (AuthV2 request)

Before merchant's web site can redirect to BPOINT add data vault page, it has to complete an Authentication request. The Authentication request serves following functions:

- Authenticates the merchant by merchant number, username and password. If these details are not correct, session token will not be generated. Since the authentication request is initiated from merchant's server directly to BPOINT platform, merchant's credentials are never exposed to any 3rd party.
- Creates a session and stores all parameters passed to the request. A unique session token generated for that session is returned to the merchant to allow a merchant's customer to add a DataVault record.
- Prevents multiple additions of a DataVault record. Session token becomes invalid as soon as an Add data vault request is received for that token.
- Security token is valid only for a predefined period of time (20 minutes). If the Add data vault request is not attempted during that time then a new security token will need to be generated again by making another authentication request.

Authentication request URL

https://www.bpoint.com.au/payconnect/authv2.aspx

Sending Authentication request

The authentication request is completed by a simple HTTP POST request initiated from the merchant's web server to authentication 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 input 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	apiuser	Username of the user set up with API level user permissions.
in_merchant_password	Alphanumeric Special characters Max 50 characters	Yes	SecurePas1	Password
in_ip_address	Numeric, full stop allowed Max 15 characters	No	127.0.0.1	Customer's IP address.
in_receipt_page_url	URL	No		If provided it will overwrite receipt page URL configured in the system for the merchant facility.
in_billercode	Numeric Max 50 digits	No	10009	Biller code. Passing in Biller code will trigger the preconfigured, biller accepted card type validation.
in_crn1	Alphanumeric Max 50 characters	No	12345678	Customer reference 1. If value is passed in then the textbox on the page will be read only.
in_crn2	Alphanumeric Max 50 characters	No		Customer reference 2. If value is passed in then the textbox on the page will be read only.
in_crn3	Alphanumeric Max 50	No		Customer reference 3. If value is passed in then the textbox on the

	characters			page will be read only.
in_crn1_name	Alphanumeric. Max 50 characters	No	Reference Number	The label to be displayed for in_crn1 field after redirection. Default is: “Customer Reference 1”.
in_crn2_name	Alphanumeric. Max 50 characters	No	Your Name	The label to be displayed for in_crn2 field after redirection. Default is: “Customer Reference 2”.
in_crn3_name	Alphanumeric. Max 50 characters	No	Postcode	The label to be displayed for in_crn3 field after redirection. Default is: “Customer Reference 3”.
in_show_crn1	0 or 1	No	0	Value “1” will show in_crn1 field on the page after redirection. “0” will hide it. Default is “1”.
in_show_crn2	0 or 1	No	0	Value “1” will show in_crn2 field on the page after redirection. “0” will hide it. Default is “1”.
in_show_crn3	0 or 1	No	0	Value “1” will show in_crn3 field on the page after redirection. “0” will hide it. Default is “1”.
in_show_customer_fields	0 or 1	No	0	Value “1” will show in_email field on the page after redirection. “0” will hide it. Default is “0”.
in_email	Valid Email address. Max 250 characters	No	a@b.com	

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. In case of error either check “out_errortext” parameter for more information or refer to appendix for error code descriptions.
out_errortext		Message describing the error, returned only if out_request_resp_code is not 0.
out_token		Session token, returned only when out_request_resp_code is 0. To be used with Add request.

Sample request

POST https://www.bpoint.com.au/payconnect/authv2.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: www.bpoint.com.au
Content-Length: 152

in_merchant_number=5353000000000000&in_merchant_username=apiuser&in_merchant_password=SecurePas1&in_crn1=12345678&in_ip_address=127.0.0.1&in_show_crn1=1

Sample response

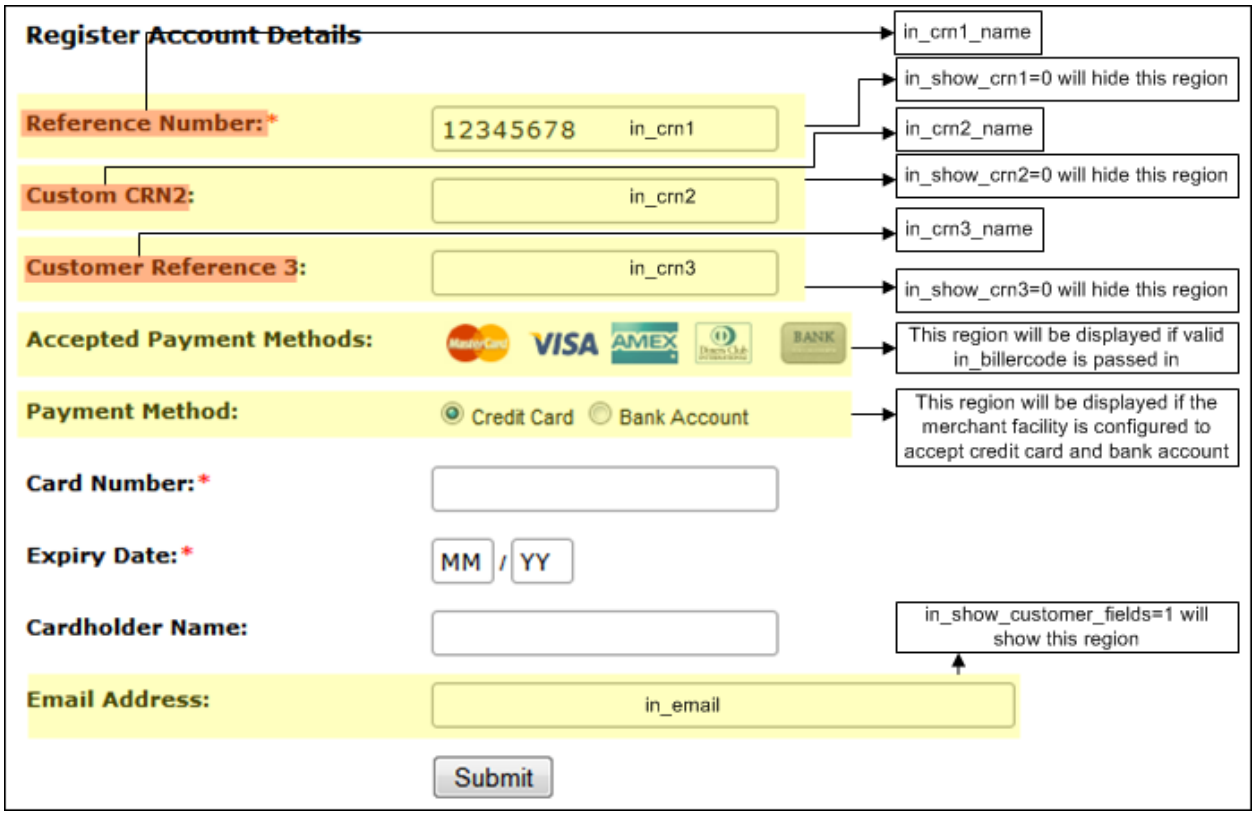
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
p3p: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Set-Cookie: ASP.NET_SessionId=p2bfca55nihwqs55p0z4xb45; path=/; secure; HttpOnly
Server: Apache2
Date: Mon, 29 Oct 2012 23:32:49 GMT

out_request_resp_code=0
out_token=c90792b9-5202-41c9-b2b1-a50db3116155

Redirection to BPOINT add token page

Once a valid session token is received, the customer browser then need to redirect to BPOINT add token page.

The Biller code, customer reference numbers and other parameters passed in to the authentication request will be used to display the BPOINT add token page to the customer. Please refer to the screenshot below for information on how the parameters passed to the authentication request will be used on BPOINT add token page.



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

The BPOINT add token page submits card details directly to the BPOINT system.

BPOINT add token page URL

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

Where **<shop>** is the short merchant name allocated to the merchant by the bank. The payment page URL (https://www.bpoint.com.au/payments/**<shop>**) for your merchant facility can be obtained by logging on to Biller Back Office and then navigating to INTERNET → THEMES section. Suffix the payment page URL with ".adddv" for BPOINT add token page.

Input Parameters

Name	Value	Mandatory	Example	Description
in_sessionid	Alphanumeric, Special characters	Yes		Session token received as out_token response parameter from the authentication request

Sample request

https://www.bpoint.com.au/payments/<shop>.adddv?in_sessionid=c90792b9-5202-41c9-b2b1-a50db3116155

Error conditions

An error page will be displayed if any of the following is true while accessing BPOINT add token page

- in_sessionid parameter is not present in the URL
- in_sessionid parameter present in the URL but has populated with incorrect session token
- Session token has expired [On the test system there is currently no expiry on the session id. But the production / live system expires the session after 20 minutes]
- The query string variables values contain URL unsafe characters E.g. # and ?

Extra Notes

If neither "in_receipt_page_url" is populated in authentication nor the merchant facility is configured with receipt page URL then the customer experience ends at this step. Customer will see result in a BPOINT (merchant branded) receipt page. Periodic calls can be made to "SearchTokens" Web service API method to retrieve token information and sync it with merchant's database. Please refer to BPOINT Web Service API document for more information on "SearchTokens" method call.

Receipt page redirection (to merchant's receipt page)

Once the add data vault request is successful, the response will be redirected to the merchant's receipt page URL. The receipt page URL has to be either passed in using "in_receipt_page_url" parameter in Authentication request or preconfigured with the BPOINT system for the merchant facility. If neither of two is true then 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 add token request. 0 indicates success, nonzero value indicate that error has occurred. In case of error either check "out_errortext" parameter for more information or refer to appendix for error code descriptions
out_errortext		Message describing the error, returned only if out_request_resp_code is not 0.
out_lookup_sessionid		Session token, returned only when out_request_resp_code is 0. To be used with following lookup request to get the details about the data vault token record that was created.

Extra Notes

- The token number will not be passed back as a parameter in the redirection URL. For security reasons it should not be exposed to the customer under any circumstances. The following Response Lookup call has to be made in order to get the data vault token number and sync it with merchant's system.
- As a failsafe mechanism, in case of Receipt redirection failure, merchant should implement a call to the BPOINT Web Service API and invoke "SearchTokens" method to sync token details with their system. Please refer to "BPOINT Web Service API" guide for more information on "SearchTokens" method.

Redirect response lookup (Lookup request)

Lookup request provides a way to retrieve response data directly to the merchant without passing it in as a parameter in redirection to merchant's receipt page.

Lookup request URL

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

Sending Lookup request

The Lookup request is completed by a simple HTTP POST request initiated from the merchant's web server to Lookup 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	apiuser	Username of the user set up with API level user permissions.
in_merchant_password	Alphanumeric, Special characters Max 50 characters	Yes	SecurePas1	Password
in_token	Alphanumeric, special characters	Yes		"out_lookup_sessionid" parameter received from "Receipt Page Redirection" URL query string

Output Parameters

Name	Example	Description
out_request_resp_code	0	Result of the lookup request. 0 indicates success, nonzero value indicate that error has occurred. In case of error either check "out_errortext" parameter for more information or refer to appendix for error code descriptions
out_errortext		Message describing the error, returned only if out_request_resp_code is not 0.
out_dvtoken	5999991183131863	The data vault token number.
out_account_number	444433…111	Truncated card number. For card numbers: First 6 digits … last 3 digits, e.g.: 444433…111 For bank account details: 6 digit BSB number ### last 3 digits of the account number, e.g.: 063123###123
out_expiry_date	0513	Credit card expiry date in MMYY format. This field will be blank for bank account records
out_crn1	12345678	Customer reference 1 stored with the data vault token record
out_crn2		Customer reference 2 stored with the data vault token record
out_crn3		Customer reference 3 stored with the data vault token record
out_card_type	MC	Abbreviated value indicating the card type that is stored with data vault token record. VC – Visa credit card MC – MasterCard credit card AX – American Express credit card DC – Diners Club credit card JC – JCB credit card

		BA – Bank account
out_email_address	a@b.com	Customer email address if stored with data vault token record
out_account_name		Cardholder or bank account name if stored with data vault token record

Sample request

POST https://www.bpoint.com.au/payconnect/lookup.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: www.bpoint.com.au
Content-Length: 142

in_merchant_number=5353000000000000&in_merchant_username=apiuser&in_merchant_password=SecurePas1&in_token=9d725cfc-dd4d-4bcf-8b78-af7616eb8636

Sample response

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
p3p: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Set-Cookie: ASP.NET_SessionId=p2bfca55nihwqs55p0z4xb45; path=/; secure; HttpOnly
Server: Apache2
Date: Mon, 29 Oct 2012 23:32:49 GMT

out_request_resp_code=0
out_dvtoken=5999991183131863
out_account_number=444433…111
out_expiry_date=0513
out_crn1=12345678
out_crn2=
out_crn3=
out_card_type=VC
out_email_address=
out_account_name=test

4. Updating DataVault Record

Updating data vault record process can be broken up into steps as below:

1. Authentication (AuthV2 request)
2. Redirection to BPOINT update token page
3. Receipt page redirection (to merchant's receipt page)
4. Redirect response lookup (Lookup request)

Authentication (AuthV2 request)

Before merchant's web site can redirect to BPOINT update data vault page, it has to complete an Authentication request. The Authentication request serves following functions:

- Authenticates the merchant by merchant number, username and password. If these details are not correct, session token will not be generated. Since the authentication request is initiated from merchant's server directly to BPOINT platform, merchant's credentials are never exposed to any 3rd party.
- Creates a session and stores all parameters passed to the request. A unique session token generated for that session is returned to the merchant to allow a merchant's customer to update an existing DataVault record.
- Prevents multiple submissions for a DataVault record. Session token becomes invalid as soon as an update data vault request is received for that token.
- Security token is valid only for a predefined period of time (20 minutes). If the update data vault request is not attempted during that time then a new security token will need to be generated again by making another authentication request.

Authentication request URL

https://www.bpoint.com.au/payconnect/authv2.aspx

Sending Authentication request

The authentication request is completed by a simple HTTP POST request initiated from the merchant's web server to authentication 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 input 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	apiuser	Username of the user set up with API level user permissions.
in_merchant_password	Alphanumeric Special characters Max 50 characters	Yes	SecurePas1	Password
in_ip_address	Numeric, full stop allowed Max 15 characters	No	127.0.0.1	Customer's IP address.
in_receipt_page_url	URL	No		If provided it will overwrite receipt page URL configured in the system for the merchant facility.
in_dvtoken	Numeric 16 characters	Yes	5999991183131863	Validated only after redirected to BPOINT Update token page
in_billercode	Numeric Max 50 digits	No	10009	Biller code. Passing in Biller code will trigger the preconfigured, biller accepted card type validation.
in_crn1	Alphanumeric Max 50 characters	No	12345678	Customer reference 1. If value is passed in then it will overwrite the stored value for the data vault record. This field will always be read only on the BPOINT update token page.
in_crn2	Alphanumeric	No		Customer reference 2. If value is

	Max 50 characters			passed in then it will overwrite the stored value for the data vault record. This field will always be read only on the BPOINT update token page.
in_crn3	Alphanumeric Max 50 characters	No		Customer reference 3. If value is passed in then it will overwrite the stored value for the data vault record. This field will always be read only on the BPOINT update token page.
in_crn1_name	Alphanumeric. Max 50 characters	No	Reference Number	The label to be displayed for in_crn1 field after redirection. Default is: “Customer Reference 1”.
in_crn2_name	Alphanumeric. Max 50 characters	No	Your Name	The label to be displayed for in_crn2 field after redirection. Default is: “Customer Reference 2”.
in_crn3_name	Alphanumeric. Max 50 characters	No	Postcode	The label to be displayed for in_crn3 field after redirection. Default is: “Customer Reference 3”.
in_show_crn1	0 or 1	No	0	Value “1” will show in_crn1 field on the page after redirection. “0” will hide it. Default is “1”.
in_show_crn2	0 or 1	No	0	Value “1” will show in_crn2 field on the page after redirection. “0” will hide it. Default is “1”.
in_show_crn3	0 or 1	No	0	Value “1” will show in_crn3 field on the page after redirection. “0” will hide it. Default is “1”.
in_show_customer_fields	0 or 1	No	0	Value “1” will show in_email field

				on the page after redirection. “0” will hide it. Default is “0”.
in_email	Valid Email address. Max 250 characters	No	a@b.com	

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. In case of error either check “out_errortext” parameter for more information or refer to appendix for error code descriptions
out_errortext		Message describing the error, returned only if out_request_resp_code is not 0.
out_token		Session token, returned only when out_request_resp_code is 0. To be used with Add request.

Sample request

POST https://www.bpoint.com.au/payconnect/authv2.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: www.bpoint.com.au
Content-Length: 180

in_merchant_number=5353000000000000&in_merchant_username=apiuser&in_merchant_password=SecurePas1&in_dvtoken=5999991183131863&in_crn1=12345678&in_ip_address=127.0.0.1&in_show_crn1=1

Sample response

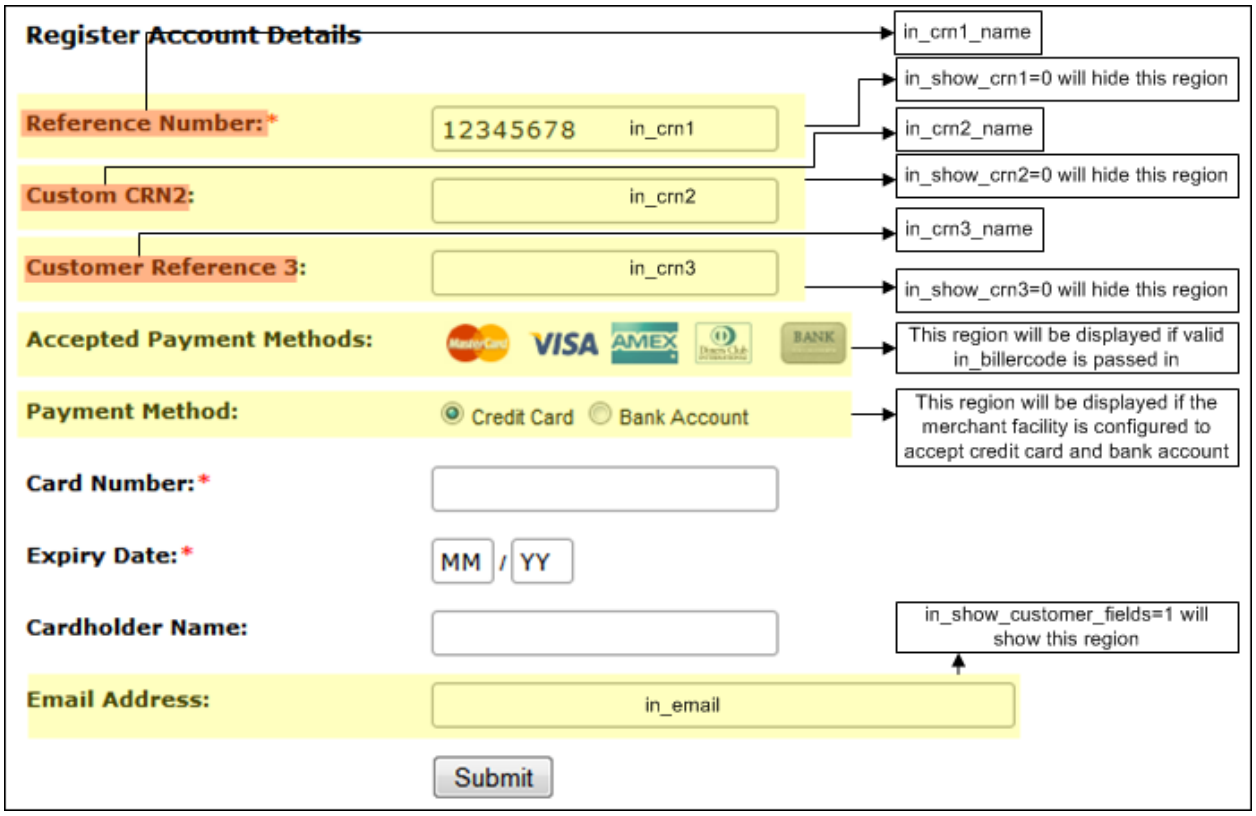
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
p3p: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Set-Cookie: ASP.NET_SessionId=p2bfca55nihwqs55p0z4xb45; path=/; secure; HttpOnly
Server: Apache2
Date: Mon, 29 Oct 2012 23:32:49 GMT

out_request_resp_code=0
out_token=2668a6cf-ecd7-4159-91cc-531da4a476fe

Redirection to BPOINT update token page

Once a valid session token is received, the customer browser then need to redirect to BPOINT update token page.

The Biller code, customer reference numbers and other parameters passed in to the authentication request will be used to display the BPOINT update token page to the customer. Please refer to the screenshot below for information on how the parameters passed to the authentication request will be used on BPOINT update token page.



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

The BPOINT update token page submits card details directly to the BPOINT system.

BPOINT update token page URL

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

Where **<shop>** is the short merchant name allocated to the merchant by the bank. The payment page URL (https://www.bpoint.com.au/payments/**<shop>**) for your merchant facility can be obtained by logging on to Biller Back Office and then navigating to INTERNET → THEMES section. Suffix the payment page URL with ".updatedv" for BPOINT update token page.

Input Parameters

Name	Value	Mandatory	Example	Description
in_sessionid	Alphanumeric, Special characters	Yes		Session token received as out_token response parameter from the authentication request

Sample request

https://www.bpoint.com.au/payments/<shop>.updatedv?in_sessionid=2668a6cf-ecd7-4159-91cc-531da4a476fe

Error conditions

An error page will be displayed if any of the following is true while accessing BPOINT update token page

- in_sessionid parameter is not present in the URL
- in_sessionid parameter present in the URL but has populated with incorrect session token
- Session token has expired [On the test system there is currently no expiry on the session id. But the production / live system expires the session after 20 minutes]
- The query string variables values contain URL unsafe characters E.g. # and ?

Extra Notes

If neither "in_receipt_page_url" is populated in authentication nor the merchant facility is configured with receipt page URL then the customer experience ends at this step. Customer will see result in a BPOINT (merchant branded) receipt page. Periodic calls can be made to "SearchTokens" Web service API method to retrieve token information and sync it with merchant's database. Please refer to BPOINT Web Service API document for more information on "SearchTokens" method call.

Receipt page redirection (to merchant's receipt page)

Once the update data vault request is successful, the response will be redirected to the merchant's receipt page URL. The receipt page URL has to be either passed in using "in_receipt_page_url" parameter in Authentication request or preconfigured with the BPOINT system for the merchant facility. If neither of two is true then 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 update token request. 0 indicates success, nonzero value indicate that error has occurred. In case of error either check "out_errortext" parameter for more information or refer to appendix for error code descriptions
out_errortext		Message describing the error, returned only if out_request_resp_code is not 0.
out_lookup_sessionid		Session token, returned only when out_request_resp_code is 0. To be used with following lookup request to get the details about the data vault token record that was created.

Extra Notes

- The token number will not be passed back as a parameter in the redirection URL. For security reasons it should not be exposed to the customer under any circumstances. The following Response Lookup call has to be made in order to get the data vault token number and sync it with merchant's system.
- As a failsafe mechanism, in case of Receipt redirection failure, merchant should implement a call to the BPOINT Web Service API and invoke "SearchTokens" method to sync token details with their system. Please refer to "BPOINT Web Service API" guide for more information on "SearchTokens" method.

Redirect response lookup (Lookup request)

Lookup request provides a way to retrieve response data directly to the merchant without passing it in as a parameter in redirection to merchant's receipt page.

Lookup request URL

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

Sending Lookup request

The Lookup request is completed by a simple HTTP POST request initiated from the merchant's web server to Lookup 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	apiuser	Username of the user set up with API level user permissions.
in_merchant_password	Alphanumeric, Special characters Max 50 characters	Yes	SecurePas1	Password
in_token	Alphanumeric, special characters	Yes		"out_lookup_sessionid" parameter received from "Receipt Page Redirection" URL query string

Output Parameters

Name	Example	Description
out_request_resp_code	0	Result of the lookup request. 0 indicates success, nonzero value indicate that error has occurred. In case of error either check "out_errortext" parameter for more information or refer to appendix for error code descriptions
out_errortext		Message describing the error, returned only if out_request_resp_code is not 0.
out_dvtoken	5999991183131863	The data vault token number.
out_account_number	444433…111	Truncated card number. For card numbers: First 6 digits … last 3 digits, e.g.: 444433…111 For bank account details: 6 digit BSB number ### last 3 digits of the account number, e.g.: 063123###123
out_expiry_date	0513	Credit card expiry date in MMYY format. This field will be blank for bank account records
out_crn1	12345678	Customer reference 1 stored with the data vault token record
out_crn2		Customer reference 2 stored with the data vault token record
out_crn3		Customer reference 3 stored with the data vault token record
out_card_type	MC	Abbreviated value indicating the card type that is stored with data vault token record. VC – Visa credit card MC – MasterCard credit card AX – American Express credit card DC – Diners Club credit card JC – JCB credit card

		BA – Bank account
out_email_address	a@b.com	Customer email address if stored with data vault token record
out_account_name		Cardholder or bank account name if stored with data vault token record

Sample request

POST https://www.bpoint.com.au/payconnect/lookup.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: www.bpoint.com.au
Content-Length: 142

in_merchant_number=5353000000000000&in_merchant_username=apiuser&in_merchant_password=SecurePas1&in_token=9d725cfc-dd4d-4bcf-8b78-af7616eb8636

Sample response

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
p3p: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Set-Cookie: ASP.NET_SessionId=p2bfca55nihwqs55p0z4xb45; path=/; secure; HttpOnly
Server: Apache2
Date: Mon, 29 Oct 2012 23:32:49 GMT

out_request_resp_code=0
out_dvtoken=5999991183131863
out_account_number=444433…111
out_expiry_date=0513
out_crn1=12345678
out_crn2=
out_crn3=
out_card_type=VC
out_email_address=
out_account_name=test

5. Frequently Asked Questions

I am receiving invalid crn1, crn2 or crn3 error, why?

All customer reference numbers should be less than or equal to 50 characters and should not contain one of these characters: & ? , \n \t \r

How do I setup user with API permissions?

1. Log in to merchant backoffice either as an Administrator or Manager (T1)
2. Navigate to ADMIN → User Management
3. Proceed to create a new user
4. Provide the user name, email address (**NOTE:** The password will be emailed to this address) and from the "User Permissions" drop down box select "API"
5. Once you have received the password, the user account is ready. **NOTE:** User setup with API permissions can only login via API interfaces. This user is not allowed to log in via the merchant backoffice.

What are corresponding test system URLs?

Production (Live) system URL	**Corresponding Test system URL**
https://www.bpoint.com.au/payconnect/auth.aspx	https://bpoint-uat.premier.com.au/payconnect-uat/auth.aspx
https://www.bpoint.com.au/payments/**<shop>**	https://bpoint-uat.premier.com.au/payments-uat/**<shop>**
https://www.bpoint.com.au/payconnect/verify.aspx	https://bpoint-uat.premier.com.au/payconnect-uat/verify.aspx
https://www.bpoint.com.au/payconnect/authv2.aspx	https://bpoint-uat.premier.com.au/payconnect-uat/authv2.aspx
https://www.bpoint.com.au/payments/**<shop>**.adddv	https://bpoint-uat.premier.com.au/payments-uat/**<shop>**.adddv
https://www.bpoint.com.au/payconnect/lookup.aspx	https://bpoint-uat.premier.com.au/payconnect-uat/lookup.aspx
https://www.bpoint.com.au/payments/**<shop>**.updatedv	https://bpoint-uat.premier.com.au/payments-uat/**<shop>**.updatedv

6. 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)
38	User declined terms and conditions
100	System error