Anonymous Access to BPOINT Data Vault

Version 1.4

Contents

1. Overview

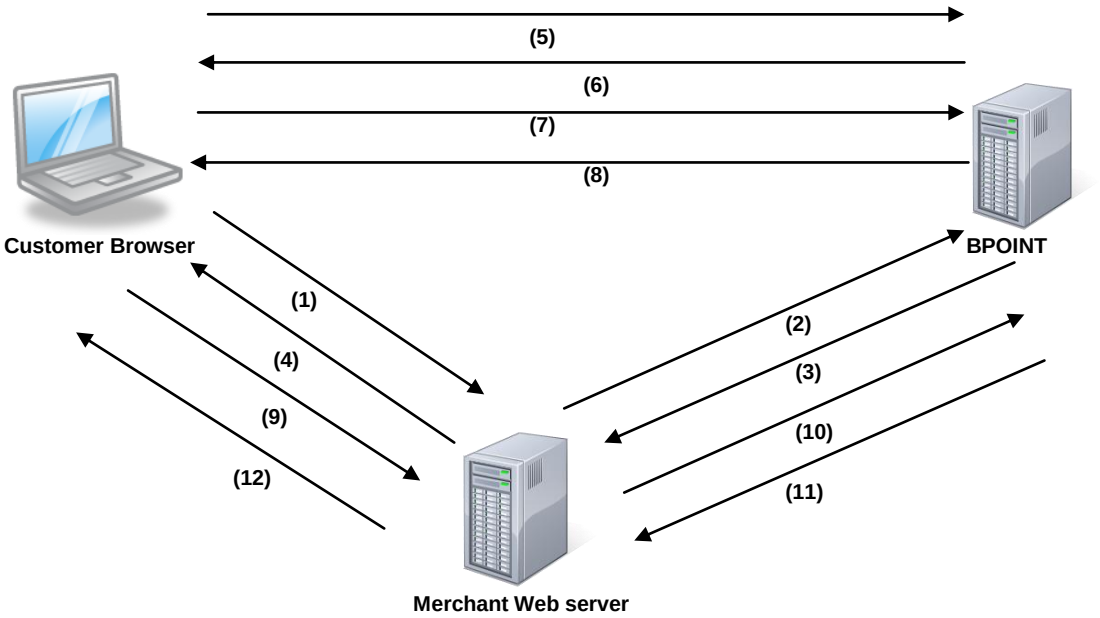
BPOINT Anonymous access to Data Vault offers a secure, PCI DSS compliant interface to the BPOINT platform to securely store credit card details. It is designed to make sure that no credit card information ever goes through the merchant's web server. The platform sends card details details directly from the customer's web browser to BPOINT over SSL connection. The result of storage is then either displayed on the screen or redirected back to merchant, depending upon the facility configuration.

Anonymous access to BPOINT Data Vault is available to all merchants and will be turned on only as requested.

Basic description of the anonymous access to data vault is as follows:

1. Customer visits merchant's web site.
2. Customer proceeds to add account / save credit card details page.
3. Merchant's site requests a once off security token from BPOINT API.
4. Merchant's web site redirects the customer to BPOINT data vault page with the security token in URL. No SSL certificate is required by the merchant. The data vault page is secured using BPOINT SSL certificate.
5. Customer types in credit card details on the BPOINT data vault page.
6. Data vault page sends card details directly to BPOINT.
7. BPOINT stores the card details and generates a data vault token number. The result is then displayed on the customer's browser in a BPOINT (merchant branded) receipt page.
8. If redirection is enabled then BPOINT redirects customer browser to merchant's receipt page, effectively relaying the result of the operation to merchant.
9. Merchant verifies that the data vault response has not been modified.

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



(1) Customer requests to add account / save credit card details on the merchant web page
(2) Merchant web server invokes “CreateSession” web service method of the BPOINT web service API
(3) BPOINT authenticates the merchant and returns back with security token
(4) Merchant web server redirects customer to BPOINT data vault page with security token in URL
(5) Redirection causes customer browser to request BPOINT data vault page
(6) BPOINT displays data vault (either add or update data vault) 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 validates the details and displays response in the customer browser.

The process ends at step 8 if redirection is not configured for the facility. Steps below happen only if redirection is enabled for the facility.

(8) BPOINT validates the details 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 invokes “GetAnonymousToken” web service method of the BPOINT web service API
(11) BPOINT authenticates the merchant and returns back with the verification response and token details
(12) Based on the verification response either receipt or error page is displayed to the customer

2. Add to Data Vault

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

1. Authentication (CreateSession request)
2. Redirection to BPOINT add token page

Steps below will only happen if redirection is enabled for the merchant facility.

3. Receipt page redirection (to merchant's receipt page)
4. Redirect response verification (GetAnonymousToken request)

Authentication (CreateSession request)

NOTE: Before starting, the anonymous data vault facility has to be enabled by requesting the support desk. Support desk will supply a "Shared Secret" key that will be required to complete some of the requests below.
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 security token is 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 unique security token to allow merchant's customer to store card details.
- Security token prevents processing of duplicate payments. Security token becomes invalid as soon as a add data vault request is received with that token.

Authentication request URL

Authentication request is a web service call to "CreateSession" web method from https://www.bpoint.com.au/evolve/service.asmx URL.

Sending Authentication request

The Authentication request is completed by sending a SOAP request to "CreateSession" web method of the BPOINT web service API.
CreateSession Web Method has following signature

Request –

```
<CreateSession xmlns="urn:Eve">
   <username>string</username>
   <password>string</password>
   <merchantNumber>string</merchantNumber>
   <ipAddress>string</ipAddress>
```

```
   <sharedSecret>string</sharedSecret>
</CreateSession>
```

Response –

```
<CreateSessionResponse xmlns="urn:Eve">
   <CreateSessionResult>string</CreateSessionResult>
   <response>
     <ResponseCode>SUCCESS or ERROR</ResponseCode>
     <ResponseMessage>string</ResponseMessage>
   </response>
 </CreateSessionResponse>
```

Parameter Name	Data Type	Details
Input Parameters		
username	String	Username provided by BPOINT
password	String	Password provided by BPOINT
merchantNumber	String	Your BPOINT Merchant number
ipAddress	String	IP Address of the machine where the requet is coming from. If the request is initiated by browser then this field should be populated with the client (browser) IP Address
sharedSecret	String	This is a special password shared with merchants who has access to this facility (as supplied by the support desk)
Output Parameters		
response	ServiceResponse	Indicates whether the web service call was successful. ResponseMessage will contain details about the Error if ResponseCode is equal to Error
CreateSessionResult	String	If ResponseCode is equal to Success then this field will contain the Session ID

Redirection to BPOINT add token page

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

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

BPOINT add token URL

https://www.bpoint.com.au/payments/<shop>.sf?ViewAction=SF-ViewAddDataVaultToken

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

Parameter name	Optional / Required	Details
VaultSessionId	Required	This is the session Id that you will get back from the CreateSession web method. This is a compulsory parameter and without this the request will fail
Ref1	Optional	This is Customer Reference number 1. This is optional if you want your customers to populate it. Reference 1 is compulsory while registering the token but it is optional to be included in query string. If it is not populated using query string then the card registration will not be successful unless customer types something into the text field.
Ref2	Optional	This is Customer Reference number 2. This is optional if you want your customers to populate it
Ref3	Optional	This is Customer Reference number 3. This is optional if you want your customers to populate it
DispRef1	Optional	If 0 then Customer Reference number 1 will not be shown on the page. The default is 1. Make sure that if you are setting DispRef1 = 0 then populate Ref1 variable. Customer Reference number 1 [Ref1] is compulsory and DispRef1 = 0 will hide the field from the page. User will not be able to populate

		details and system will show error once the page is Submitted.
DispRef2	Optional	If 0 then Customer Reference number 2 will not be shown on the page. The default is 1.
DispRef3	Optional	If 0 then Customer Reference number 3 will not be shown on the page. The default is 1.
CRN1Name	Optional	If populated then the value passed in will be used to label the Customer Reference 1 field. Default is “Reference 1”
CRN2Name	Optional	If populated then the value passed in will be used to label the Customer Reference 2 field. Default is “Reference 2”
CRN3Name	Optional	If populated then the value passed in will be used to label the Customer Reference 3 field. Default is “Reference 3”

Sample add redirection URL

https://www.bpoint.com.au/payments/<shop>.sf?ViewAction=SF-ViewAddDataVaultToken&VaultSessionId=CC18E26E78A3383084E4901ACC97CF6D&Ref1=test1&Ref2=test2&Ref3=test3&DispRef1=0&DispRef2=0&DispRef3=0&CRN1Name=TestRef1&CRN2Name=TestRef2&CRN3Name=TestRef3

Error conditions

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

- VaultSessionId parameter is not present
- VaultSessionId parameter present but has populated with incorrect session id
- Session Id is 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 are populated with URL unsafe characters E.g. # and ?

Extra Notes

If redirection feature is not enabled then the customer experience ends at this step. Customer will see response 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)

NOTE: This step (and the next step) will only happen if redirection is enabled. Support desk can enable the redirection feature. A receipt page URL needs to be supplied to support desk in order to have this feature enabled.

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 preconfigured by the merchant with the BPOINT system. If a receipt page URL is not preconfigured then the redirection will not occur and the customer will see a BPOINT (merchant branded) receipt page.

Output Parameters

Name:	Example:	Description:
Success	0	Result of add token request. 0 indicates that en error has occurred and the token was not created. 1 indicates that the token was created. In case of error check ErrMsg parameter for more information.
ErrMsg		Message describing the error, returned only if Success is 0.
Ref1		Customer reference number 1, as passed to the Anonymous Add Token page
Ref2		Customer reference number 2, as passed to the Anonymous Add Token page
Ref3		Customer reference number 3, as passed to the Anonymous Add Token page
Sig		Signature (used to sign all parameters to allow merchant to verify the parameters have not been tampered with) for enhanced security.

NOTE: The token number will not be passed as a parameter in the redirection URL as for security reasons it should not be exposed to the customer.

Redirect response verification (GetAnonymousToken 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, add token response data has not been tampered with. This check is required as add token response data is passed back via customer's browser in plain text and can be easily changed.

As a failsafe mechanism, in case of Receipt redirection or Response verification request failure, the 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.

Verification request URL

Verification request is a web service call to "GetAnonymousToken" web method from https://www.bpoint.com.au/evolve/service.asmx URL.

Sending Verification request

The Verification request is completed by sending a SOAP request to "GetAnonymousToken" web method of the BPOINT web service API.

GetAnonymousToken Web Method has following signature

Request –

```
<GetAnonymousToken xmlns="urn:Eve">
  <username>string</username>
  <password>string</password>
  <merchantNumber>string</merchantNumber>
  <success>string</success>
  <CRN1>string</CRN1>
  <CRN2>string</CRN2>
  <CRN3>string</CRN3>
  <signature>string</signature>
</GetAnonymousToken>
```

Response –

```
<GetAnonymousTokenResponse xmlns="urn:Eve">
  <GetAnonymousTokenResult>
    <VerificationResult>boolean</VerificationResult>
    <DVToken>
      <CardNumber>string</CardNumber>
      <ExpiryDate>string</ExpiryDate>
      <CRN1>string</CRN1>
      <CRN2>string</CRN2>
      <CRN3>string</CRN3>
      <Token>string</Token>
```

```
    <MaskedCardNumber>string</MaskedCardNumber>
    <CardType>string</CardType>
    <UpdatedUsername>string</UpdatedUsername>
    <UpdatedDate>dateTime</UpdatedDate>
    <CreatedUsername>string</CreatedUsername>
    <CreatedDate>dateTime</CreatedDate>
   </DVToken>
  </GetAnonymousTokenResult>
  <response>
   <ResponseCode>SUCCESS or ERROR</ResponseCode>
   <ResponseMessage>string</ResponseMessage>
  </response>
</GetAnonymousTokenResponse>
```

Parameter Name	Data Type	Details
Input Parameters		
username	String	Username provided by BPOINT
password	String	Password provided by BPOINT
merchantNumber	String	Your BPOINT Merchant number
success	String	Success parameter passed in redirection.
CRN1	String	Value of parameter Ref1 passed in redirection.
CRN2	String	Value of parameter Ref3 passed in redirection.
CRN3	String	Value of parameter Ref2 passed in redirection.
signature	String	Value of parameter Sig passed in redirection.
Output Parameters		
ResponseCode	SUCCESS or ERROR	SUCCESS indicates that the request was completed successfully and VerificationResult field should be checked to see if the parameters and signature were verified. ERROR indicates that there a system error has occurred and the operation could not be completed. In case of an ERROR response, element GetAnonymousTokenResult will not be populated.
ResponseMessage	String	In case of an ERROR this field will contain a description of the problem
VerificationResult	Boolean	True indicates that the parameters have not

		been tampered with. False indicates that the parameters have been tampered with. No token information will be returned if VerificationResult is false.
CardNumber	String	Credit card number for the relating token. For security reasons will always be null.
CardType	String	Eg. “MC” = mastercard “VC” = visacard
ExpiryDate	String	The expiry date of card
CRN1	String	Reference number 1 stored with the token
CRN2	String	Reference number 2 stored with the token
CRN3	String	Reference number 3 stored with the token
Token	String	The token number
MaskedCardNumber	String	The first 6 and last 3 digits of the credit card number
CreatedDate	DateTime	Date the token was created
CreatedUsername	String	Username who created the token
UpdatedDate	DateTime	Date the token was updated
UpdatedUserName	String	Username who last updated the token

3. Update Data Vault

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

1. Authentication (CreateSession request)
2. Redirection to BPOINT update token page

NOTE: The anonymous data vault update process currently does not support redirection back to merchant receipt page.

Authentication (CreateSession request)

NOTE: Before starting, the anonymous data vault facility has to be enabled by requesting the support desk. Support desk will supply a "Shared Secret" key that will be required to complete some of the requests below.

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 security token is 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 unique security token to allow merchant's customer to update card details.
- Security token prevents processing of duplicate payments. Security token becomes invalid as soon as a add data vault request is received with that token.

Authentication request URL

Authentication request is a web service call to "CreateSession" web method from https://www.bpoint.com.au/evolve/service.asmx URL.

Sending Authentication request

The Authentication request is completed by sending a SOAP request to "CreateSession" web method of the BPOINT web service API.

CreateSession Web Method has following signature

Request –

```
<CreateSession xmlns="urn:Eve">
   <username>string</username>
   <password>string</password>
   <merchantNumber>string</merchantNumber>
   <ipAddress>string</ipAddress>
   <sharedSecret>string</sharedSecret>
</CreateSession>
```

Response –

```
<CreateSessionResponse xmlns="urn:Eve">
   <CreateSessionResult>string</CreateSessionResult>
   <response>
     <ResponseCode>SUCCESS or ERROR</ResponseCode>
     <ResponseMessage>string</ResponseMessage>
   </response>
 </CreateSessionResponse>
```

Parameter Name	Data Type	Details
Input Parameters		
username	String	Username provided by BPOINT
password	String	Password provided by BPOINT
merchantNumber	String	Your BPOINT Merchant number
ipAddress	String	IP Address of the machine where the requet is coming from. If the request is initiated by browser then this field should be populated with the client (browser) IP Address
sharedSecret	String	This is a special password shared with merchants who has access to this facility (as supplied by the support desk)
Output Parameters		
response	ServiceResponse	Indicates whether the web service call was successful. ResponseMessage will contain details about the Error if ResponseCode is equal to Error
CreateSessionResult	String	If ResponseCode is equal to Success then this field will contain the Session ID

Redirection to BPOINT update token page

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

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

BPOINT update token URL

https://www.bpoint.com.au/payments/<shop>.sf?ViewAction=SF-ViewUpdateDataVaultToken

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

Parameter name	Optional / Required	Details
VaultTokenId	Required	This is the data vault token Id generated by BPOINT system when the customer details are added to BPOINT Data Vault. This is the token number for which the details will be updated.
VaultSessionId	Required	This is the session Id that you will get back from the CreateSession web method. This is a compulsory parameter and without this the request will fail
Ref1	Optional	This is Customer Reference number 1. This is optional. If you want to change the existing customer details then you will need to populate it.
Ref2	Optional	This is Customer Reference number 2. This is optional. If you want to change the existing customer details then you will need to populate it.
Ref3	Optional	This is Customer Reference number 3. This is optional. If you want to change the existing customer details then you will need to populate it.
DispRef1	Optional	If 0 then Customer Reference number 1 will not be shown on the page. The default is 1.
DispRef2	Optional	If 0 then Customer Reference number 2 will not be shown on the page. The default is 1.
DispRef3	Optional	If 0 then Customer Reference number 3 will

		not be shown on the page. The default is 1.
CRN1Name	Optional	If populated then the value passed in will be used to label the Customer Reference 1 field. Default is “Reference 1”
CRN2Name	Optional	If populated then the value passed in will be used to label the Customer Reference 2 field. Default is “Reference 2”
CRN3Name	Optional	If populated then the value passed in will be used to label the Customer Reference 3 field. Default is “Reference 3”

Sample update redirection URL

https://www.bpoint.com.au/payments/<shop>.sf?ViewAction=SF-ViewUpdateDataVaultToken&VaultTokenId=5999991010324368&VaultSessionId=CC18E26E78A3383084E4901ACC97CF6D&Ref1=test1&Ref2=test2&Ref3=test3&DispRef1=0&DispRef2=0&DispRef3=0&CRN1Name=TestRef1&CRN2Name=TestRef2&CRN3Name=TestRef3

Error conditions

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

- VaultSessionId parameter is not present
- VaultSessionId parameter present but has populated with incorrect session id
- Session Id is 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]
- VaultTokenId parameter is not present
- VaultTokenId parameter present but has populated with incorrect token id
- The query string variables are populated with non URL safe characters E.g. # and ?

Extra Notes

If Ref1, Ref2 and Ref3 query string variables are not populated then the page will retrieve the existing (Ref1, Ref2 and Ref3) customer details associated with VaultTokenId and will prompt to enter new Credit card details. On “Submit” the new details will be updated with BPOINT system.

If Ref1, Ref2 or Ref3 query string variables are populated then on “Submit” new card details along with new customer details (Ref1, Ref2 and Ref3) will be updated with BPOINT system.

Customer will see response 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.

4. Appendix

- All customer reference numbers should be less than or equal to 50 characters and should not contain one of these characters: & ? , \n \t \r
- Credit card numbers are validated using Luhn check algorithm
- Expiry dates are validated to be in future