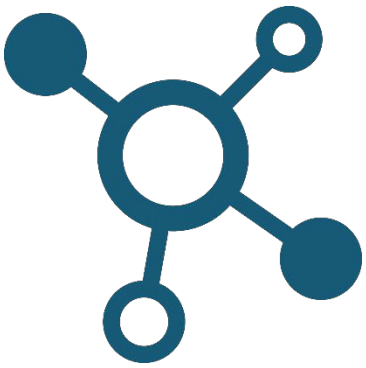

PAYA Gateway

PAYA Gateway Connect: Integrated Payments

Interface Specification – Back Office PayPage

PAYA Gateway Connect: Integrated Payments

Interface Specification – Back Office PayPage

Contents

Introduction

This document provides the technical details required to process MOTO (Customer Not Present) transactions through the PAYA Gateway Back Office PayPage. The document will define the PayPage Web Interface message format for transaction authorisation where the cardholder's details are directly entered into a secure web page and an authorisation is submitted to the relevant merchant Acquirer through the PAYA Gateway.

For compliance with PCI DSS version 3 the PAYA Gateway Back Office PayPage can only be able to be used on browsers which support TLS 1.2 and above.

When using the Card Alias function of the PAYA Gateway Back Office PayPage (see section 3.4), the PAYA Gateway conforms to the 2018 Visa & MasterCard Credential On File mandate. This states that scheme reference data will be retained from the first authorisation of the card and supplied to the relevant Merchant Acquirer (where supported) for every subsequent transaction.

1 PayPage Interface Options

The Back Office PayPage should be presented within an Iframe and be called using one of the following methods:

1. SOAP API Method
2. POST Method*

*requires the use of security hashing (see section 1.3 for further details).

1.1 The SOAP API Method

This is the most secure way of presenting a Back Office PayPage request to the PAYA Gateway system. Using this method, a PaypageRequest containing all required input parameters (explained further in section 3.2), is sent to the PAYA Gateway via a WCF service. Once received by PAYA Gateway, the input parameters will be saved in xml format and a unique token is generated and returned.

The Back Office PayPage is then called via the POST method (see section 1.2 below) to the Payment Gateway by providing the token number and SupplierID.

As the token is stored in our database, the Back Office PayPage can be called at any time so if required there can be a delay between generating the token (i.e. upon receipt of an order) and calling the Back Office PayPage to take payment (i.e. after invoicing).

1.1.1 Generating and using a PayPage Token

To generate a token, an objPaypageRequestResponse request is sent to the PAYA Gateway API containing all required PayPage input parameters. See section 3.1 information on parameters available and please refer to document *PAYA Gateway Connect - Back Office PayPage - SOAP API Request* for assistance in forming a request.

A GenerateTokenResponse is received containing the result of this request. If successful, the token will be passed back in this response.

Using the POST Method, the Supplier ID and Token is then submitted to the PAYA Gateway. Using the input parameters stored against that token the Paypage is generated for the cardholder.

1.2 The POST Method

Using the POST method, the Querystring containing all required PayPage request parameters (see section 3.1), is sent at the time the client's browser is redirected to the PAYA Gateway Back Office PayPage. This method is used in conjunction with the Hash Security method (see section 1.3 below).

1.3 Security Hash Requirements

Any POST request must be sent in to the PAYA Gateway using a hashing algorithm.

For each Supplier ID used to call the PayPage, three items of data are required:

1 - Hash Algorithm
2 - Key 1
3 - Key 2

For the Hash Algorithm, we support either **SHA256** or **HMAC**. For the **HMAC** Keys specifically, the values must be 64Bit Keys (8bytes), 16 hexadecimal characters long. Both **HMAC** and **SHA256** keys and opted Hash Algorithm are exchanged with PAYA Gateway during the implementation and testing phase of the PayPage project. Please see below how to calculate your Hash values.

SHA256
The SHA256 hash value is calculated by appending each PAYA Gateway defined parameter & value, in the order they appear in the POST request, to a querystring delimited with '&'; excluding the Hash field. The request should then be salted by appending either Key 1 or Key 2 to the end of the request. This is then hashed using SHA256 outputted to binary, and the binary result Base64 Encoded.

HMAC
The POST request is formed, using each PAYA Gateway defined parameter, and excluding the Hash parameter. Both the request and a binary version of Key 1 or Key 2 are to be processed through a HMAC SHA256 function. The generated value then is Base64 Encoded and the Base64 encoded result should then be encoded with URL Data encoding.

Upon submitting the hashed PayPage request, **SHA256** or **HMAC**, the hash value provided will be validated by the PAYA Gateway, by looping through the passed fields, excluding the hash field. The hash is then recalculated using a stored version of Key 1 or Key 2. Where matching, the PayPage will be presented.

2 PayPage Processing Modes

All functions below are supported by both POST and SOAP API methods of calling the Back Office PayPage.

2.1 Authorisation

Display mode
When used in its default form, the Back Office PayPage will be presented to the user, where they will be prompted to enter in the relevant details (varying on the initial request sent into PAYA Gateway). Once completed the transaction will proceed to authorisation through the PAYA Gateway where the results will be sent back as part of the Postback Result and the user will be redirected appropriately.

Display Mode None
This option gives the ability to call the Back Office PayPage to perform an authorisation without showing the PAYA Gateway Back Office PayPage to the user. Where the PAYA Gateway Back Office PayPage is not displayed to the user all cardholder data must be included in the initial PayPage request. (see section 3.1 for the core parameters).

2.2 Capture Only

The PayPage also allows merchants to capture card details so that the card can be charged later. Any Capture Only request will be subject to an account verification request and if this fails then the card will not be stored. For further details on how to utilise the Back Office PayPage for Capture Only please see section 3.4.

3 PayPage Input Parameters

The following table sets represent the values to be passed to the PayPage to process a transaction.

3.1 Core Transaction Parameters

Field name	Type	Data Length	Mandatory / Optional	Details
SupplierID	Alpha Numeric	50	M	Identifies the supplier to PAYA Gateway. PAYA Gateway will provide this to the merchant to pass in this field prior to live implementation
Reference	Alpha Numeric	50	M	Unique transaction reference
Amount	Numeric	19	M	This is the amount of the transaction to be authorised. It should be in the smallest currency unit (e.g. £12.34 = 1234) **Note:** This field is only mandatory for transactions where an authorisation is being processed. PayPage sessions that are for 'CaptureOnly' transactions do not require this field
RType	Numeric	1	M	States the type of transaction to be processed: • 0 = Standard Sale • 1 = Refund • 2 = Restricted Refund. This will refund against a transaction reference previously processed.
RtypeReference	Alpha Numeric	20	O	Mandatory when processing a restricted refund (RType = 2) This reference must match the reference used in the sale.
CurrencyCode	Alpha	3	M	3-letter alpha currency code form ISO standard 4217
CountryCode	Alpha	3	M	3-letter alpha country code form ISO standard 3166
CV2AVSControl	Alpha	3	M	This field determines which fields are to be inputted by the cardholder. A combination of the below can be

				used, however 'C' in this field is mandatory • C = CV2 **(mandatory)** • A = Address Numerics • P = Postcode Numerics
AddressNumerics	Numeric String	10	O	If the Address numerics are already known, then they may be specified in this field. If provided and the CV2AVSControl field contains an 'A' then the cardholder will not be prompted to enter these details
PostcodeNumerics	Numeric String	10	O	If the Postcode numerics are already known, then they may be specified in this field. If provided and the CV2AVSControl field contains a 'P' then the cardholder will not be prompted to enter these details
CV2AVSPolicy	Encoded String	28	O	This field specifies your acceptance policy. Any transaction that is not approved by the policy will be automatically reversed and rejected (acquirer dependant). See section 6 for more details on the construction of this field
Hash	Alpha Numeric	32	M	This is the parameter containing a hash of the query string (see section 1.3 for more detail) **NOTE:** The security HASH must be the last parameter in the calling string

3.2 Post Back & Redirection Parameters

The merchant must specify the URL's where the results of the transaction should be posted to (PostBackURL) and where the user should be re-directed to, dependant on the result of the transaction. These can either be specified in the request or can be pre-configured into the PAYA Gateway (if the URL's are static) so that they can be excluded from the PayPage call (recommended for POST Method).

All URLS must be HTTPS with the re-direct URLs being publicly accessible for PAYA Gateway to re-direct the user to. A list of PAYA Gateway IP addresses will be provided as part of the PayPage implementation.

Field name	Type	Data Length	Mandatory / Optional	Details
PostbackResultURL	URL	256	O	This is the URL of the merchant system that the results of the transaction will be posted back to
OnCompletionURL	URL	256	O	When the transaction has completed successfully, the cardholder browser will be re-directed to this URL

OnErrorURL	URL	256	O	If an error occurs, then the cardholder browser will be re-directed to this URL

3.3 Additional Optional & Reference Fields

The following optional fields are available in the standard PayPage interface.

Field name	Type	Data Length	Mandatory / Optional	Details
CardInfoRequired	Alpha	1	O	This field specifies the card details that will be sent in the postback. If omitted, then Masked is assumed The options are: • F = FULL **(For fully PCI compliant Service Providers only)** • M = MASKED • A = ALIASNAME
RequiredCardType	Alpha Numeric	8	O	This may be used to restrict the card type that is entered on the PayPage. Options: • PCARD = Card entered must be a Purchasing Card • NOTPCARD = Card entered must not be a Purchasing Card
AutomaticLevel1Settlement	Boolean	1	O	Y/N field indicating that the transaction should be settled automatically once authorisation has been approved
CardholderMessage	Alpha Numeric	20	O	Displayed below the Transaction Reference for additional cardholder information relating to this transaction
UserReference	Alpha Numeric	20	O	Optional user reference that can be provided. This field need not be unique as it is not checked by the ITS system
ContextData	Alpha Numeric	100	O	This is an element that is carried within the postback and re-direct messages and can be used to identify which transaction is returning data
UseCardNumber (<=19N) UseExpiryDate (MMYY), UseStartDate (MMYY) UseIssueNumber (NN)	Alpha Numeric	29	O	These should be specified (scheme dependent) when the PayPage is not used to capture the card details The card holder will not be prompted to enter the details if they are provided in the request
CV2Code	Numeric String	3/4	O	The CV2/4DBC code may be specified here when the PayPage is not used to capture the card details. If provided, and the CV2AVSControl field contains

				a ‘C’ then the cardholder will not be prompted
DisplayMode	Alpha	7	O	If the PayPage is to be hidden from the user then enter NONE. If this field is omitted, then display function will be assumed (see section 2 for further details)

3.4 Card Storage

The PAYA Gateway PayPage enables a merchant to store and re-use card details in the PAYA Gateway system using either a merchant allocated alias name or by generating a tokenised alias name, using a pre-defined token pattern stored in the PAYA Gateway system.

The following fields may be used to either capture card details for future use or to specify an alias to be used by the PayPage.

Field name	Type	Data Length	Mandatory / Optional	Details
ProcessControl	Alpha	11	O	If the PayPage is to be used only for card storage only then CAPTUREONLY should be present in this field (see section 2 for further details)
UseAlias	Alpha Numeric	32	O	Specifies the alias or token name to be used in the transaction
AliasToStoreAs	Alpha Numeric	32	O	Specifies the unique reference the card details should be stored under in the ITS Payment Gateway. Will be ignored if GetTok parameter is present
GetTok	Alpha	4	O	True/Yes to indicate if a token alias should be automatically generated for the card details entered on the PayPage. A token will always be generated except if the card fails 3DS authentication. The Token will be returned in the PostBack parameters under the ‘AliasName’ Tag. (see section 4.1)

3.5 International Client Custom Fields

The following fields enable enhanced custom options in the PayPage for international merchants.

Field name	Type	Data Length	Mandatory / Optional	Details
MarketControl	Boolean	1	O	Y/N specifying whether the Market & Engagement number fields are to be displayed to the cardholder
MarkNum	Alpha Numeric	25	O	French Purchasing card Market Number. If Market Control=Y this field is mandatory
EngageNum	Alpha Numeric	25	O	French Purchasing card Engagement number. If Market Control=Y this field is mandatory
PageLanguage	Alpha	2	O	Language designator code which specifies the language to be used when the PayPage is displayed • EN = English (Default) • DE = German • NL = Dutch • FR = French • ES = Spanish • IT = Italian
PageLocale	Alpha	2	O	Country designator specifies the country specific version of the language • EN = UK (Default) • DE = Germany • AT = Austria • FR = France • ES = Spain • IT = Italy

4 Return Parameters

4.1 PayPage Transactional Responses

These fields are passed to the PostbackURL, OnCompletionURL and ErrorURL with some being populated only if the corresponding input parameter was submitted.

Field name	Type	Length	Details
SupplierID	Alpha Numeric	50	Supplier ID used for the transaction
UserReference	Alpha Numeric	20	The User Reference passed in the input parameter
TransactionID	Numeric		PAYA Gateway System generated Unique Transaction ID associated with authorisation stage of this transaction

EndTransaction	Alpha Numeric	5	True / False. Confirms if the PayPage session has been completed end to end
TransUniNbr	Numeric	50	PAYA Gateway System generated Unique Transaction ID associated with this transaction
AuthdateTime	Alpha Numeric	14	Date / Time of the authorisation local to ITS in the format YYYYMMDDHHMMSS
ReasonCode	Numeric	4	See section 5.3 for a list of reason codes
ResultCode	Numeric	2	See section 5.1 for further details
ResultMessage	Alpha Numeric	21	See section 5.1 for further details
ResultDescription	Alpha Numeric	21	See section 5.1 for further details
PCard	Boolean	1	Y/N = Indicates if the card used for the transaction is a Purchasing Card
SchemeName	Alpha	17	The card scheme used for the transaction
AuthResultCode	Numeric	4	The result code of the authorisation
AuthReasonCode	Numeric	4	Same as Reason Code. See section 5.3 for further details
AuthReasonDescription	Alpha Numeric	36	The 'raw' text from the Payment gateway
HostResponseMessage	Alpha Numeric	100	Response message received from the acquirer authorisation host
Reference	Alpha Numeric	50	The transaction reference
AuthCode	Alpha Numeric	6	The authorisation code
AddendumType	Alpha	9	The type of addendum data required when this transaction is settled
MerchantID	Alpha Numeric	15	The Acquirer MerchantID
TerminalID	Numeric	8	The Acquirer TerminalID used for this transaction
CardNumber	Alpha Numeric	19	The card number as controlled by the 'CardInfoRequired' parameter
ExpiryDate	Numeric	6	The expiry date of the card used
StartDate	Numeric	6	The start date of the card used
IssueNumber	Numeric	2	The issue number of the card used
ContextData	Alpha Numeric	100	Details provided in the input parameter
eMsg	String	38	Combined Result code and message in a string
Amount	Numeric	19	Transaction amount
SAmount	Numeric	19	The sale amount
BrowserStatus	Numeric	1	Browser status on exit: 0 = Page Loaded 1 = Aborted 2 = Successful
SettlementResultCode	Alpha Numeric	2	Only populated if the 'Auto Level 1 Settlement' feature is enabled
SettlementResultDescription	Alpha Numeric	2	Only populated if the 'Auto Level 1 Settlement' feature is enabled
SchemeID	Alpha Numeric	0	Not currently in use
QueryString	Alpha Numeric	0	Not currently in use

CardType	Alpha Numeric	0	Not currently in use
VoiceReferalNumber	Alpha Numeric	0	Not currently in use
CV2AVSResults	Numeric	6	Numerical code as returned by the Acquiring host with the results of the CV2, AVS and Post Code validation
CV2Result	Alpha Numeric	1	Result of the CV2 validation
AVSAddressResult	Alpha Numeric	1	Result of the Address Numerics validation
AVSPostCodeResult	Alpha Numeric	1	Result of the Post Code Numerics validation
PageLanguage	Alpha Numeric	2	The language that was used for the page if specified in the input parameter
PageLocale	Alpha Numeric	2	The Locale that was used for the page if specified in the input parameter
MarketNumber	Alpha Numeric	25	French Market Number as entered on the Page by the cardholder
EngagementNumber	Alpha Numeric	25	French Engagement Number as entered on the Page by the Cardholder
CAResult	Alpha Numeric	26	If the PayPage has been used to store card details, the result will be passed in this parameter • OK:ADDED • OK:UPDATED • NOK:Unable to store Alias
CAReturnCode	Numeric	1	This is the corresponding return code for the CAResult parameter • 1 = Added • 2 = Updated • 3 = Used • 4 = Error
CAReturnDescription	Alpha Numeric	46	Description of the card alias result
AliasName	Alpha Numeric	32	Name of the Alias (Token) generated by the GetTok request

5 Result Codes

5.1 Transaction Result Codes

Code	Field	Details
0	NONE	Not defined
1	CompletedOK	The transaction was authorised
2	BadParams	The request was invalid due to invalid parameters in the request
3	SystemError	ITS Internal Error
4	InvalidUseAlias	The UseAlias does not exist
5	InvalidCardDetails	The card number (either in the specified alias or within the card number parameter) is not valid

6	WrongCardType	A PCard was presented when NOTPCARD is specified, or vice versa
7	UserAborted	The CardHolder chose to abort the transaction
8	NotAuthorised	The transaction was not authorised. The ResultMessage will contain information from the authorisation reason codes table
9	PostbackError	The postback attempt was received by the merchant system but another error occurred
10	PostbackFailed	The postback failed to be delivered to the specified URL
11	CV2Declined	The transaction was rejected due to the CV2AVCPolicy requirements
12	SettlementError	There was a settlement error when attempting to automatically settle the transaction
13	OriginalReferenceNotFound	Reference specified in 'RTypeReference' parameter for original sale transaction does not exist
14	AmountGreaterThanAuthedAmount	The amount specified in the refund transaction was greater than the original sale amount.
16	AlreadyAuthorised	Duplicate transaction reference & amount used
17	DuplicateReference	Duplicate transaction reference used

5.2 Authorisation Result Codes

The following values appear in response to authorisation.

Value	Details
1000	Previously Authorised
1001	Offline validated
1002	Offline approved
1003	Unable to contact acquirer
1004	Online approved
1005	Online referred
1006	Online declined
1007	Offline declined

PAYA Gateway recommend that the merchant treats codes 1003 and 1005 as declines as there is no option within the PayPage to enter a manual authorisation code.

5.3 Authorisation Reason Codes

Some of these errors will be displayed on screen to the cardholder or, if Display Mode None is used, these will be passed as part of the Postback response.

Value	Auth Result Description
	MESSAGE FORMAT VALIDATION ERRORS
2001	Invalid transaction type
2002	Invalid date / time
2003	Invalid currency code
2004	Invalid country code
2005	Invalid reference
2006	Invalid amount
	CARD DATA ERRORS
2101	Invalid card number
2102	Invalid expiry date
2103	Invalid start date
2104	Invalid issue number
2105	Invalid CV2 / 4DBC
2106	Invalid card usage (service codes, etc)
	TRANSACTION VALIDATION ERRORS
2201	Card not taken
2202	Transaction type not allowed
2203	Ceiling limit exceeded
2204	Reference required
2205	Supplier ID required
2206	Card code 10 (hotcard check failed)
2207	Duplicated Transaction Reference
2208	Service Not Allowed
2209	Key Entry Not Allowed
	CV2 / AVS Policy VALIDATION ERRORS
3000	CV2 / AVS Criteria not met
	SYSTEM ERRORS
	Contact ITS with this information
9501	System Error: ISO Validation
9502	System Error: Card Validation
9503	System Error: Authorisation
9504	System Error: Configuration

6 Appendix

6.1 CV2 AVS Policy Information & Responses

The PAYA Gateway PayPage allows the merchant to control if a transaction should be successful following the verification of the address and CV2 code using the CV2AVSPolicy parameter (see section 3.2). When a policy is set, and a transaction does not meet the required criteria, the transaction will be automatically cancelled by the PAYA Gateway.

Please note this is acquirer dependant as some acquirers do not pass back the CV2AVS information in their authorisation response to determine if a transaction passes the required policy or not.

The Control Policy configuration requires an initial setting of which there are two options:

A = Accept all with the exception of…….
D = Decline all with the exception of……

The table below provides the response information in relation to the configuration item.

Configuration Item	CV2/4DBC	Postcode Numeric	Address Numeric	Numerical Response
@	OK	OK	OK	2,2,2
A	OK	OK	No Match	2,2,4
B	OK	OK	Not Checked	2,2,1
C	OK	No Match	OK	2,4,2
D	OK	No Match	No Match	2,4,4
E	OK	No Match	Not Checked	2,4,1
F	OK	Not Checked	OK	2,1,2
G	OK	Not Checked	No Match	2,1,4
H	OK	Not Checked	Not Checked	2,1,1
I	No Match	OK	OK	4,2,2
J	No Match	OK	No Match	4,2,4
K	No Match	OK	Not Checked	4,2,1
L	No Match	No Match	OK	4,4,2
M	No Match	No Match	No Match	4,4,4
N	No Match	No Match	Not Checked	4,4,1
O	No Match	Not Checked	OK	4,1,2
P	No Match	Not Checked	No Match	4,1,4
Q	No Match	Not Checked	Not Checked	4,1,1
R	Not Checked	OK	OK	1,2,2
S	Not Checked	OK	No Match	1,2,4
T	Not Checked	OK	Not Checked	1,2,1
U	Not Checked	No Match	OK	1,4,2
V	Not Checked	No Match	No Match	1,4,4

W	Not Checked	No Match	Not Checked	1,4,1
X	Not Checked	Not Checked	OK	1,1,2
Y	Not Checked	Not Checked	No Match	1,1,4
Z	Not Checked	Not Checked	Not Checked	1,1,1

Example Policies

- D@AB
  The merchant requires the CV2 and Postcode to always be correct.
- D@ABCF
  The merchant requires the CV2 and either the Address or Postcode numeric to always be correct.
- D@CF
  The merchant requires the CV2 and Address to always be correct.
- D@ABCDEFGH
  The merchant only requires the CV2 to always be correct.