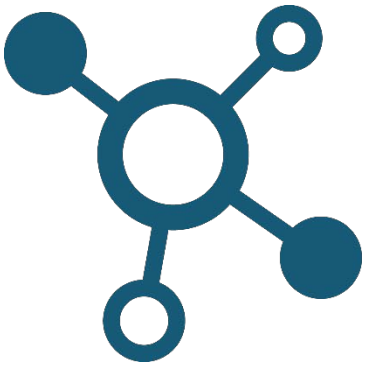

PAYA Gateway

PAYA Gateway Connect: Integrated Payments

Interface Specification – Ecommerce PayPage

PAYA Gateway Connect: Integrated Payments

Interface Specification – Ecommerce PayPage

Contents

PAYA Gateway Connect: Integrated Payments

Interface Specification – Ecommerce PayPage

Introduction

This document provides the technical details required to process Ecommerce transactions through the PAYA Gateway PayPage. The document will define the PayPage Web Interface message format for transaction authorisation where the cardholder enters their card details directly into a secure web page and an authorisation is submitted to the relevant merchant Acquirer through the ITS Payment Gateway.

The PAYA Gateway PayPage fully supports the EMV 3D Secure (3DS) Version 2 which includes Visa Secure, MasterCard Identity Check and American Express SafeKey MPI (Merchant Plug In) cardholder verification security standards. In addition to this, the PAYA Gateway PayPage also supports the use of digital wallets (through Google Pay™ and Apple Pay) as a way to provide payment information for a transaction.

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

When using the Card Alias function of the PAYA Gateway PayPage (see chapter 3.5), 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 PayPage should be presented within an Iframe and be called using one of the following methods:

a. SOAP API Method
b. POST Method

1.1 SOAP API Method

This is the most secure way of presenting a PayPage request to the PAYA Gateway system. Using this method, a PaypageRequest containing all required input parameters (explained further in section 3.1), is sent to PAYA Gateway Connect 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 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 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 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 - Ecommerce 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 Connect. Using the input parameters stored against that token, the PayPage is generated for the cardholder.

1.2 POST Method

Using the POST method, the query string containing all required PayPage request parameters (see section 3), is sent at the time the client's browser is redirected to the PAYA Gateway 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 on 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 query string 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 PayPage.

2.1 MPI & Authorisation

Display Mode
When used in its default form, the PayPage will be presented to the cardholder, where they will be prompted to enter in the relevant details (varying on the initial request sent into PAYA Gateway). The PAYA Gateway PayPage will then process an MPI call and if authentication is challenged, the cardholder will be required to complete 3DS authentication. Once completed the transaction will proceed to authorisation through the PAYA Gateway where the results will be sent back to the Merchant as part of the PostBack Result and the cardholder will be redirected appropriately.

Display Mode None
This option gives the ability to call the PayPage to perform both card holder authentication and an authorisation without showing the PAYA Gateway PayPage to the cardholder (the authentication process will still be presented to the cardholder however). Where the PAYA Gateway PayPage is not displayed to the user all cardholder data must be included in the initial PayPage request. (See section 3 for the required parameters).

2.2 MPI Only

This option gives the ability to call the PayPage and enable the card holder to complete 3DS authentication only (no authorisation will take place). Using this option will complete the PayPage session after the MPI call and return the results to the merchant via the PostBack message. The cardholder will also be redirected depending on the success of the authentication request. The MPI Only option has a further 2 sub options which are as follows:

Display Mode
This mode is used when the calling entity wishes the PAYA Gateway PayPage to capture the card details prior to 3DS authentication.
Display Mode None
This mode is used when the calling entity has already captured the cardholder details but just wants to use the PAYA Gateway PayPage to redirect to the MPI. In this scenario there will be no PAYA Gateway PayPage presented to the cardholder, instead they will be redirected to the card Issuer's site to complete authentication. The PostBack and redirect process is the same as for the Display Mode function.

2.3 Capture Only

The PayPage also allows merchants to capture card details so that the card can be charged later. Any Capture Only request will still go through 3DSecure authentication and if this fails then the card will not be stored. For further details on how to utilise the PayPage for Capture Only please see section 3.5.

3. PayPage Input Parameters

The following table sets represent the parameters 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 put 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
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
ThreeDSV2Return	Boolean	1	O	When set, this will enable the return of the additional 3DS V2 return details in the PostBack URL. This is also configurable by ITS as part of the Merchant set up
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 PostBack & Redirection Parameters

The merchant must specify the URLs where the results of the transaction should be posted to (PostBackURL) and where the card holder 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 URLs 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 cardholder to. A list of ITS 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 3D Secure Data Parameters

3.3.1 Card Holder Data

The following table describes the additional cardholder fields that are available to send as part of 3DS V2. Whilst none of this data is mandatory, to increase the chances of a frictionless experience for the cardholder, the fields detailed with an "R" are the fields we recommend you send at minimum. If the merchant system is unable to provide the information in this section, PAYA Gateway can provide a separate page for the cardholder to complete during the transaction with the display of this page controlled by the '3DSCardInfo' calling parameter (see section 3.2 above). The fields presented to the cardholder will vary depending on whether the PayPage is being used only to store card details or to process an authorisation.

Please Note: The Shipping details are only required if they differ from the billing address.

Field Name	Type	Data Length	Mandatory / Optional	Details
CHAddMatch	Boolean	1	O	Y/N - Does the Shipping Address match the Billing Address? If 'Y' Shipping details are not required
CHBillCity	Alpha Numeric	50	R	Account Billing Address – City
CHBillAddCountryCode	Alpha Numeric	3	R	Account Billing Address – Country Needs to be the 3-character alpha or numeric ISO-3166-1 value. Accepted values can be provided upon request.
CHBillAddress1	Alpha Numeric	50	R	Account Billing Address – Address Line 1
CHBillAddress2	Alpha Numeric	50	O	Account Billing Address – Address Line 2
CHBillAddress3	Alpha Numeric	50	O	Account Billing Address – Address Line 3
CHBillPostalCode	Alpha Numeric	16	R	Account Billing Address – Postal / Zip code
CHBillState	Alpha Numeric	3	O	Account Billing Address – State (US only)
CHEmailAddress	Alpha Numeric	254	R	Card Holder Email Address associated with the transaction or on file with the merchant
CHMobNumberCC	Numeric	3	R	Card Holder Mobile Country Calling Code. To be supplied in addition to the Mobile Number

CHMobNumber	Numeric	15	R	Card Holder Mobile Phone Number. To be supplied where unable to provide Landline Number details.
CHLandLineNumberCC	Numeric	3	O	Card Holder Landline Country Code. To be supplied in addition to the Landline Number.
CHLandLineNumber	Numeric	15	O	Card Holder Landline Phone Number. To be supplied where unable to provide Mobile Number details.
CHName	Alpha Numeric	2-45	O	Card Holder Name as it appears on the card. Mandatory if DisplayMode 'NONE' is used
CHShipToCity	Alpha Numeric	50	O	Shipping Address – City
CHShipToAddCountryCode	Alpha Numeric	3	O	Shipping Address – Country Needs to be the 3-character alpha or numeric ISO-3166-1 value. Accepted values can be provided upon request.
CHShipToAddress1	Alpha Numeric	50	O	Shipping Address – Line 1
CHShipToAddress2	Alpha Numeric	50	O	Shipping Address – Line 2
CHShipToAddress3	Alpha Numeric	50	O	Shipping Address – Line 3
CHShipToPostalCode	Alpha Numeric	16	O	Shipping Address – Post / ZIP code
CHShipToState	Alpha Numeric	3	O	Shipping Address – State (US only)

3.3.2 Card Holder Account Security – Merchant Systems

The following fields are designed to give the Card Issuer as much information on how the card holder interacts with the merchant so that they can identify potentially fraudulent activity on the card and request authentication on the transaction.

Field Name	Type	Data Length	Mandatory / Optional	Details
CHChallengeInd	Alpha Numeric	2	O	Indicates what the preference is of the merchant to challenge the cardholder via 3DS **01** = No Preference **02** = No Challenge Requested **03** = Challenge Requested **04** = Challenge Request Mandated (High Risk merchant types e.g., Gaming)

CHAuthenticationInd	Alpha Numeric	2	O	Indicates how the cardholder was authenticated by the merchant website prior to placing an order & paying **01** = No Authentication Occurred **02** = Login using Merchant Own Credentials **03** = Login using federated ID (Single login used across multiple companies) **04** = Login using Card Issuer Credentials **05** = Login using 3rd Party Authentication **06** = Login using FIDO (Fast ID Online) Open Authentication Authenticator
CHAccAge	Alpha Numeric	2	O	Indicates how long the cardholder has held the account on the merchant site **01** = Guest Checkout **02** = Account Created during this Transaction **03** = Account less than 30 days old **04** = Account 30 – 60 Days old **05** = Account more than 60 Days old
CHAccChange	Alpha Numeric	2	O	Indicates when the account was last changed, for example a change of address or user / password on the merchant system **01** = Changed during this transaction **02** = Changed less than 30 days ago **03** = Changed 30 - 60 days ago **04** = Changed more than 60 days ago
CHPassChange	Alpha Numeric	2	O	Indicates when the account holder last changed their account password on the merchant site **01** = No Change **02** = Changed during this Transaction **03** = Changed less than 3-0 Days ago **04** = Changed 30 - 60 days ago **05** = Changed more than 60 days ago
CHShipToInd	Alpha Numeric	2	O	Indicates when the shipping address was first used on this account **01** = This transaction only **02** = Less than 30 days **03** = 30 – 60 Days **04** = More than 60 Days
CHTransActivity24	Numeric	3	O	Number of transactions (successful and abandoned) for this cardholder account with that Merchant across all payment accounts, in the previous 24 hours
CHTransActivityYr	Numeric	3	O	Number of transactions (successful and abandoned) for this cardholder account

				with the 3DS Requestor across all payment accounts in the previous 12 months
CardAddCheck	Numeric	3	O	Number of attempts to add the card to the account in the last 24 hours
AccValuePurchase	Numeric	12	O	Value of purchases in the last 6 months in lowest currency denominator
AccSuspAccInd	Alpha Numeric	2	O	Suspicious Account Activity **01** = No Suspicious Activity **02** = Suspicious Activity
AccNameUsed	Alpha Numeric	2	O	The Account Name used as the 'Ship to' name **01** = Identical name used **02** = Different name used
AccPayAge	Alpha Numeric	8	O	This is the date that the account was created on the merchant system (YYYYMMDD)
AccPayAccInd	Alpha Numeric	2	O	Indicates the length of time that this card was enrolled in the cardholder's account with the merchant **01** = No Account Guest Check-out **02** = Account created during this transaction **03** = Account less than 30 days old **04** = Account 30-60 days old **05** = Account more than 60 days old
MercAccID	Alpha Numeric	30	O	The Account ID the cardholder uses to login on to the Merchant system
CHBrowserIP	Alpha Numeric	45	O	IP V4 or IP V6 Address of the cardholder's browser when performing the transaction

3.4 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
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 element is carried within the PostBack and re-direct messages and can be used to identify which transaction is returning data
AuthenticateFailResult	Boolean	1	O	**Y/N** to select the return of a different PayPage result code when authentication fails. If Yes and ResultCode = 8 (NotAuthorised) and 3D Secure authentication failed, return ResultCode 15 (AuthenticationFailed)
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
ProcessingMode	Alpha	7	O	If the PayPage is to be used for 3DS authentication only then enter MPIONLY. If this field is omitted standard function will be assumed (see section 2 for further details)
DisplayMode	Alpha	7	O	If the PayPage is to be hidden from the cardholder then enter NONE. If this field is omitted, then display function will be assumed (see section 2 for further details)

3.5 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 Card Holder will still be required to go through the 3DS authentication regardless of whether the PAYA Gateway PayPage is only used for card storage and no authorisation is taking place.

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)
CardStoreConsent	Boolean	1	O	**Y/N** field to signify if the cardholder should be asked to give consent to having their card details stored using a check box on the PayPage. The card details will always be stored under the requested Alias or generated Token for the purposes of refunds. The result of the check box will be in the results parameter 'CardStoreConsentResult'.(See section 4.1)

3.6 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 the 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 for a list of reason codes
ResultCode	Numeric	2	See section 5 for further details
ResultMessage	Alpha Numeric	21	See section 5 for further details
ResultDescription	Alpha Numeric	21	See section 5 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 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
CardHolderName	Alpha	45	The name entered in the Cardholder Name field
Amount	Numeric	19	Transaction amount
SAmount	Numeric	19	The sale amount
SAmount	Numeric	19	The sale amount
BrowserStatus	Numeric	1	Browser status on exit: = Page Loaded = Aborted = 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
CardStoreConsentResult	Numeric	1	Result of the Card holder consent question = Accepted = Declined by Card Holder
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
ATSD	Alpha Numeric	4	Additional Transaction Security Data
ECI	Alpha Numeric	2	Ecommerce Indicator
CAV	Alpha Numeric	28	Cardholder Authentication Value
XID	Alpha Numeric	28	Unique Transaction ID supplied to PAYA Gateway by our MPI provider
DeclinedForSCA	Alpha	5	True/False to inform if the transaction was declined because there is a need for card holder authentication to take place (SCA)
Capture	Alpha Numeric	4	This value will be used when submitting a Settlement Request ECER = Secure transaction with cardholder certificate, which is the most secure protocol of all three results and will be the default for all 3DS authenticated Transactions E3DS = Secure transaction with 3D secure merchant certificate (Merchant is enrolled – Card Holder may not be enrolled) i.e., 3DS authentication was attempted ECOM = Non-Authenticated transaction with no 3D Secure
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

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

4.2 3D Secure PostBack Data

The following table represents the additional information that is returned by the 3D Secure Version 2 authentication process. This data will be passed back in the PostBack URL data if requested in 3DSV2Return parameter in incoming request (see section 3.2).

Field Name	Type	Length	Details
3DSVersion	Alpha Numeric	3	Version number of the 3DS process used in the Authentication
DirectoryServerTransactionID	Alpha Numeric	36	Unique ID generated by the 3DS Directory Server
ACSTransactionID	Alpha Numeric	36	Unique ID created by the Issuer Authentication gateway for this transaction and can be used as proof of authentication
AuthenticationStatus	Alpha	1	Indicates the authentication status of the transaction Y = Authentication Successful N = Not Authenticated – Transaction Denied U = Authentication could not be performed. If the merchant wishes for an unauthenticated transaction to continue to authorisation this is configurable on the ITS Payment Gateway. A = Attempts Processing Performed. Not Authenticated/Verified, but a proof of attempted authentication/verification is provided. Authorisation can proceed. R = Authentication rejected
TransactionStatus	Alpha Numeric	2	Transaction Status Reason code 01 = Card Authentication Failed 02 = Unknown Device 03 = Unsupported Device 04 = Exceeds Authentication Frequency Limit 05 = Expired Card 06 = Invalid Card Number 07 = Invalid Transaction 08 = No Card Record 09 = Security Failure 10 = Stolen Card 11 = Suspected Fraud 12 = Transaction not permitted to cardholder 13 = Cardholder not enrolled in service 14 = Transaction timed out at the ACS 15 = Low confidence 16 = Medium confidence

			17 = High confidence 18 = Very High confidence 19 = Exceeds ACS maximum challenges 20 = Non-Payment transaction not supported 21 = 3RI transaction not supported 22 = ACS technical issue 23 = Decoupled Authentication required by ACS but not requested by 3DS Requestor 24 = 3DS Requestor Decoupled. Max Expiry Time exceeded 25 = Decoupled Authentication. Insufficient time to authenticate cardholder. ACS will not make attempt 26 = Authentication attempted but not performed by the cardholder
AuthenticationMethod	Alpha Numeric	2	The method with which the cardholder was authenticated 01 = Static Passcode 02 = SMS OTP (One Time Passcode) 03 = Key Fob or EMV Card Reader OTP 04 = APP OTP 05 = OTP Other 06 = KBA (Knowledge Based Authentication) 07 = OOB (Out of Bounds) Biometrics 08 = OOB Login 09 = OOB Other 10 = Other
AuthenticationType	Alpha Numeric	2	The type of authentication which took place 01 = Static-using static data / passwords 02 = Dynamic-using biometric dynamic data 03 = OOB-Other Out of bounds Data 04 = Decoupled-uses a separate process to the transaction e.g., mobile banking app authentication

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	PAYA Gateway 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	Not Currently in Use	Not Currently in Use
14	Not Currently in Use	Not Currently in Use
15	AuthenticationFailed	Transaction not authorised due to 3D Secure Authentication failure
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	Details
	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 except for…
D = Decline all except for…

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

6.2 Enabling Digital Wallets

To allow cardholders to process transactions through either Google Pay or Apple Pay, the function must be enabled on your Supplier set up. This will be managed with your PAYA Gateway testing contact during onboarding.

Any transaction processed through Google Pay or Apple Pay using a non-tokenised credential will always be subject to 3D Secure authentication in the same way a transaction processed outside of a digital wallet would be (i.e. a transaction processed outside of Google Pay or Apple Pay using a card number entered directly onto the PayPage) with the user likely being asked to authenticate themselves via 3DS.

Please also note that by enabling support for Google Pay the merchant agrees to adhere to the Google Pay APIs Acceptable Use Policy and accepts the terms defined in the Google Pay API Terms of Service.

6.2.1 Google and Apple Pay Inside An iframe

In order to be able to use Google and Apple Pay from within an iframe, under certain circumstances i.e. the Chrome browser on Android, there is a small change that needs to be done to the way the iframe is defined. Specifically a new attribute needs to be added to the iframe tag "*allow='payment'*" as an example:

```
<iframe src="https://ecommerce.its-connect.net/Paypage/?..." allow="payment">
</iframe>
```

As described here, if the iframe will be navigated across multiple origins that support the Payment Request API, then one can set allow to "payment *".

Please note that Apple Pay does not work from inside an iframe unless *Safari 17* or above is used.
In older versions of Safari, the Apple Pay button will only be visible if the user is redirected to the PayPage directly, as these versions of Safari don't support calls to the Payment Request API from inside a cross-origin iframe.

6.2.2 Apple Pay Certificates

To support Apple Pay, you will need to place a certificate file onto your webserver. This certificate is provided by Apple through a registration process involving your URL. This process is handled by PAYA Gateway, all we will need from you is the URL that you will be accessing the PayPage from.

Should you have multiple environments i.e. a production and a development environment, multiple certificates are able to be created to support testing before you move to the Production environment.