Direct API

takepayments gateway

V1.1 – 16th December 2019

takepayments
we make it easy

takepayments
we make it easy

Contents

Introduction

Intended Audience

This document is technical in nature and should be used by your company's developers to integrate your systems into the payment gateway. It assumes that the reader has knowledge and understanding of basic HTML concepts such as form post.

Simplifying the Integration Process

There are many complexities when dealing with card transactions. If you try and tackle them all at once the task of integrating will seem complicated. The best way to do the integration is to follow a simple step by step approach and break the process down into manageable sections, each adding functionality as you go along.

To assist you example code is available in the resource section in most of the common programming languages. Where possible please use these well documented examples as a starting point.

Adhering to good coding practices will also greatly simplify your task.

IMPORTANT INFORMATION: PLEASE READ CAREFULLY

Important Notes

Gateway URLs

The full URL to use in your posts to the gateway is https://gw1.tponlinepayments2.com or https://gw2.tponlinepayments2.com or https://gw3.tponlinepayments2.com/

Gateway Messages

The gateway accepts data in the form of SOAP (v1.1) XML messages over HTTPS. Port 4430 needs to be open for outbound communication.

If IP whitelisting is required, the IP addresses used are: 37.200.119.135, 91.185.171.231, 91.185.171.234 or 37.200.119.138

Notation Explained

The message variables are primarily described using a hierarchical table – the hierarchy information is implied by the indentation amount of the first column. You can see the XML schema diagrams and example messages in the appendices. The table has 5 Columns:

1. **Tag/Attribute Name** – this contains the name of the tag (or the name of the attribute of a tag)
2. **Data Type** – this gives the valid data type that a tag or attribute can contain
3. **Max Length** – this gives the maximum length for the contents of a tag or attribute. If a "-" is in this column, then the tag or attribute has no max length, or it is a special type (like a Boolean for example)
4. **Mandatory or Always present** – for input messages, this is whether the tag or attribute is required for a valid message & for output messages this is whether the tag or attribute will always be present in the message
5. **Comment** – this gives a brief description of the function of the tag or attribute along with anything else worth noting in relation to that tag or attribute

Rows in orange are tags that do not have any content (i.e. they can have attributes, but they don't have any content apart from child tags).

Rows in white are either tags that have content or are attributes (marked so) of the containing tag.

Notation Explained

The communication between the merchant's system/customer's browser, to the gateway PaymentForm are POST via HTML form variables. The below table or similar format is used throughout this document to help explain the requirements for passing/receiving variables to/from the gateway.

Tag/Attribute Name	Data Type	Max Length	Mandatory or Always Present	Comments
RootTag (no attributes or content, only child tags)				
ChildTag (has no content)				
AnAttribute (attribute)				
AnotherChildTag (has content)				

NOTE: The Mandatory/Always Present fields take into account their scope in the XML hierarchy – if a tag is labelled as Mandatory, then it is mandatory if its parent tag is present. The same applies to a tag's presence in the response message.

This simple table would represent the simple XML message (not including the SOAP envelope or body):

```
<RootTag>
   <ChildTag AnAttribute="SomeValue">
      <AnotherChildTag>SomeValue</AnotherChildTag>
   </ChildTag>
</RootTag>
```

Data Types:

Data Type	Description
N	Numeric – only numbers allowed
A	Alpha – any printable character is allowed
DT	Date Time stamps
B	Boolean – only TRUE or FALSE are allowed – these are passed as strings for the hash and form (i.e. "true" instead of 1)
-	Special types – these variables only allow a specific set of values. Details of the allowed value are in the comments section.

CardDetailsTransaction

Introduction

The CardDetailsTransaction message is the mainstay of the gateway. It is the one message that merchants must implement in order to process card payments (along with the ThreeDSecureAuthentication message if they wish to be able to take payments that are validated by the 3D Secure scheme)

CardDetailsTransaction – Request

Below are the details for the request message to initiate a transaction where the card details are submitted.

Tag/Attribute Name	Data Type	Max Length	Mandatory	Comments
PaymentMessage			**Yes**	
MerchantAuthentication			**Yes**	
MerchantID (attribute)	A	15	Yes	The gateway account merchant ID issued (not to be confused with the MMS username)
Password (attribute)	A	15	Yes	The gateway account password
TransactionDetails			**Yes**	
Amount (attribute)	N	15	Yes	The transaction amount in minor currency – e.g. for £10.00, it must be submitted as 1000.
CurrencyCode (attribute)	N	3	Yes	ISO 4217 e.g. GBP: 826
OrderID	-	50	Yes	A merchant side ID for the order – primarily used to for determining duplicate transactions
OrderDescription	A	256	No (N/A)	A description for the order
AuthCode	A	-	No (See comment)	This provides an auth code for the transaction is one was obtained manually
ThreeDSecurePassthroughData			**No**	
EnrolmentStatus (attribute)	A	1	Yes	The status value from the VeRes (CH.enrolled) – can be either Y, N or U
AuthenticationStatus (attribute)	A	1	No	The status value from the PaRes (TX. Status) – can be either Y, N, U or A

Tag/Attribute Name		Data Type	Max Length	Mandatory	Comments
	ECI (attribute)	A	2	No	The 2 digital electronic commerce indicators from the PaRes (TX.eci). Must be present if AuthenticationStatus is either Y or A
	AuthenticationValue	N	28	No	The authentication value from the PaRes. For Verified By Visa, this is known as CAVV (Cardholder Authentication Verification Value), for MasterCard SecureCode, it is known as UCAF (Universal Cardholder Authentication Field). It must be present if AuthenticationStatus is either Y or A
	TransactionIdentifier	A	28	No	The transaction identifier (xid) for the transaction
MessageDetails				**Yes**	
	TransactionType (attribute)	-	-	Yes	Must be either SALE, REFUND or PREAUTH
ThreeDSecureBrowserDetails				**No**	
	DeviceCategory (attribute)	N	-	No	Determines the category for the customer's browser – 0 for computer grade browser, 1 for a mobile device
	AcceptHeaders	A		No	The headers that the device's browser accepts
	UserAgent	A		No	The user agent string for the device's browser
TransactionControl				**No**	
	EchoCardType	B	-	No (False)	Instructs the gateway to include the card type of the transaction in the message response
	EchoAVSCheckResult	B	-	No (False)	Instructs the gateway to include the AVS results for the transaction in the message response
	EchoCV2CheckResult	B	-	No (False)	Instructs the gateway to include the CV2 results for the transaction in the message response

Tag/Attribute Name	Data Type	Max Length	Mandatory	Comments
EchoAmountReceived	B	-	No (False)	Instructs the gateway to include the amount that was passed to it in the message response
DuplicateDelay	N	3	No (60)	Sets the amount of time (in seconds) that any orders to the same gateway account with the same OrderID and CardNumber should be rejected
AVSOverridePolicy	-	-	No (As set in MMS)	Sets an override AVS checking policy for this transaction. (See Appendix 3 for details)
CV2OverridePolicy	-	-	No (As set in MMS)	Sets an override CV2 checking policy for this transaction. (See Appendix 3 for details)
ThreeDSecureOverridePolicy	B	-	No (As set in MMS)	Instructs the gateway to enable/disable 3D Secure checking for this transaction (where possible)
CardDetails			**Yes**	
CardName	A	100	Yes	The name on the customer's card
CardNumber	N	20	Yes	The customer's card number
ExpiryDate			**Yes**	
Month (attribute)	N	2	Yes	The month of the expiry date in 2-digit numeric format - e.g. for July, must be submitted as 07
Year (attribute)	N	2	Yes	The year of the expiry date in 2-digit numeric format - e.g. for 2019, must be submitted as 19
StartDate			**Yes**	
Month (attribute)	N	2	Yes	The month of the expiry date in 2-digit numeric format - e.g. for July, must be submitted as 07
Year (attribute)	N	2	Yes	The year of the expiry date in 2-digit numeric format - e.g. for 2019, must be submitted as 19

Tag/Attribute Name	Data Type	Max Length	Mandatory	Comments
CV2	N	4	No	The security number (also called CVV or CVV2) printed on the customer's card - usually the last 3 or 4 digits printed on the signature strip
IssueNumber	N	2	No	The issue number printed on the customer's card
CustomerDetails			**No**	
BillingAddress			**No**	
Address1	A	100	No	Customer's billing address line 1
Address2	A	50	No	Customer's billing address line 2
Address3	A	50	No	Customer's billing address line 3
Address4	A	50	No	Customer's billing address line 4
City	A	50	No	Customer's billing address city
State	A	50	No	Customer's billing address state
PostCode	A	50	No	Customer's billing address post code
CountryCode	N	3	No	ISO 3166-1 e.g. United Kingdom: 826
EmailAddress	E	100	No	The email address of the customer - NOTE: anything passed in here is validated as an email address, so anything passed in must be a valid email address
PhoneNumber	A	30	No	The customer's phone number
CustomerIPAddress	I	15	No	The IP address of the customer (NOT the IP address of the merchant's website). This is used to determine the customer's country of origin. The format is xxx.xxx.xxx.xxx
DateOfBirth	**D**	**10**	**No**	**The date of birth of the customer. Must be in the format YYYY-MM-DD**

takepayments
we make it easy

CardDetailsTransaction – example SOAP request

```
<CardDetailsTransaction xmlns='https://www.thepaymentgateway.net/'>
   <PaymentMessage>
      <MerchantAuthentication Password='**PASSWORD**' MerchantID='**MERCHANTID**'/>
      <TransactionDetails Amount='2968' CurrencyCode='826'>
         <MessageDetails TransactionType='SALE'/>
         <TransactionControl>
<ThreeDSecureOverridePolicy>true</ThreeDSecureOverridePolicy>
            <DuplicateDelay>60</DuplicateDelay>
            <EchoCardType>true</EchoCardType>
            <EchoAVSCheckResult>true</EchoAVSCheckResult>
            <EchoCV2CheckResult>true</EchoCV2CheckResult>

<EchoThreeDSecureAuthenticationCheckResult>true</EchoThreeDSecureAuthenticationCheck
Result>
            <EchoAmountReceived>false</EchoAmountReceived>
         </TransactionControl>
         <ThreeDSecureBrowserDetails>
            <AcceptHeaders>*/*</AcceptHeaders>
            <UserAgent></UserAgent>
         </ThreeDSecureBrowserDetails>
         <OrderID>Order-928</OrderID>
         <OrderDescription>Order description </OrderDescription>
      </TransactionDetails>
      <CardDetails>
         <CardName>Geoff Wayne</CardName>
         <CV2>341</CV2>
         <CardNumber>4976350000006891</CardNumber>
         <ExpiryDate Month='01' Year='25'/>
         <StartDate Month='' Year=''/>
      </CardDetails>
      <CustomerDetails>
         <BillingAddress>
            <Address1>113 Broad Street West</Address1>
            <Address2></Address2>
            <Address3></Address3>
            <Address4></Address4>
            <City>Oldpine</City>
            <State>Strongbarrow</State>
            <PostCode>SB42 1SX</PostCode>
         </BillingAddress>
      </CustomerDetails>
   </PaymentMessage>
</CardDetailsTransaction>
```

CardDetailsTransactionResponse

Below are the details for the response that will be received after sending a CardDetailsTransaction request.

Tag/Attribute Name	Data Type	Max Length	Always Present	Comments
CardDetailsTransactionResponse			**Yes**	
CardDetailsTransactionResult			**Yes**	
AuthorisationAttempted (attribute)	B	-	Yes	This indicates whether the transaction was sent to the acquirer for authorisation, or whether it failed before authorisation
StatusCode	N		Yes	This indicates the status of the transaction
Message	A		Yes	This gives a more detailed description of the status of the transaction
ErrorMessages			**No**	
MessageDetail			**Yes**	
Detail (multiple)	A	256	Yes	If there were multiple error messages (e.g. multiple input variable validation errors, then they will be detailed here)
PreviousTransactionResult			**No**	
StatusCode	N		Yes	If the transaction was deemed to be a duplicate transaction, this indicates the status of the previous transaction
Message	A		Yes	If the transaction was deemed to be a duplicate transaction, this gives a more detailed description of the status of the previous transaction
TransactionOutputData			**No**	

Tag/Attribute Name	Data Type	Max Length	Always Present	Comments
CrossReference (attribute)	A	25	Yes	This is the unique cross reference for this transaction. If the card has been determined as requiring 3D Secure authentication this must be used as the merchant reference. If the transaction required 3D Secure authentication, then this must be passed to the ACS as 'MD'. If the transaction was rejected as a duplicate transaction; this value will hold the cross reference of the previous transaction
AuthCode	A	15	No	If the transaction was successful, then the auth code is passed out here
AddressNumericCheckResult	-	-	No	If requested in the CardDetailsTransaction request message, this gives the results of the address numeric check - will be PASSED, FAILED, PARTIAL, NOT_CHECKED or UNKNOWN
PostCodeCheckResult	-	-	No	If requested in the CardDetailsTransaction request message, this gives the results of the post code check - will be PASSED, FAILED, PARTIAL, NOT_CHECKED or UNKNOWN
CV2CheckResult	-	-	No	If requested in the CardDetailsTransaction request message, this gives the results of the CV2check - will be PASSED, FAILED, NOT_CHECKED or UNKNOWN
CardTypeData			**No**	
CardType	A	-	Yes	If requested in the CardDetailsTransaction request message, this gives the card type for the transaction. (See Appendix 4 for details)
Issuer	A	100	No	The card issuer (if known)

Tag/Attribute Name	Data Type	Max Length	Always Present	Comments
AmountReceived	N	15	No	If requested in the CardDetailsTransaction request message, this gives the amount that was passed to the gateway via the request message
ThreeDSecureOutputData			**No**	
PaREQ	A	-	Yes	If the card has been determined as requiring 3D Secure authentication, this gives the base64 encoded payment request that must be passed to the ACS for authentication. This must be sent to the ACS as 'PaReq'
ACSURL	A	-	Yes	If the card has been determined as requiring 3D
				Secure authentication, this gives the URL of the ACS server that the PaREQ must be sent to
GatewayEntryPoints			**Yes**	
GatewayEntryPoint (multiple)			**Yes**	
EntryPointURL (attribute)	A	256	Yes	The URL of the active gateway entry point
Metric (attribute)	N	5	Yes	A metric value giving an indication of whether transactions should be sent to this gateway entry point

Things to Note

- If requested, the AmountReceived will always echo the amount passed to the gateway in the CardDetailsTransaction message, regardless of the outcome of the transaction (apart from if the message could not be validated due to content errors)
- If the CV2 is not submitted in the CardDetailsTransaction message, then the CV2CheckResult returned in the CardDetailsTransactionResponse will be deemed as UNKNOWN, rather than FAILED
- If the address or the post code information is not submitted in the CardDetailsTransaction message, then the AddressNumericCheckResult and/or the PostCodeCheckResult returned in the CardDetailsTransactionResponse will be deemed as UNKNOWN rather than FAILED
- If the transaction requires 3D Secure validation, then the CrossReference will be used as the variable "MD" which needs to be posted to the Access Control Server (ACSURL) along with the PaREQ

CardDetailsTransactionResponse – example SOAP response

If not 3d secure is requested, or not required, the CardDetailsTransactionResponse will be returned, if 3d secure is required see the next section for sending the 3D Secure request.

```
<CardDetailsTransactionResponse xmlns="https://www.thepaymentgateway.net/">
   <CardDetailsTransactionResult AuthorisationAttempted="True">
      <StatusCode>0</StatusCode>
      <Message>AuthCode: 093608</Message>
   </CardDetailsTransactionResult>
   <TransactionOutputData CrossReference="191108090553085601602273">
      <AuthCode>093608</AuthCode>
      <AddressNumericCheckResult>PASSED</AddressNumericCheckResult>
      <PostCodeCheckResult>PASSED</PostCodeCheckResult>
      <CV2CheckResult>PASSED</CV2CheckResult>
      <CardTypeData>
         <CardType>VISA</CardType>
         <CardClass>PERSONAL</CardClass>
         <Issuer ISOCode="250">CREDIT INDUSTRIEL ET COMMERCIA</Issuer>
      </CardTypeData>
      <AmountReceived>7304</AmountReceived>
      <GatewayEntryPoints>
         <GatewayEntryPoint EntryPointURL="https://gw1.tponlinepayments2.com:4430/"
Metric="100" />
         <GatewayEntryPoint EntryPointURL="https://gw2.tponlinepayments2.com:4430/"
Metric="200" />
      </GatewayEntryPoints>
   </TransactionOutputData>
</CardDetailsTransactionResponse>
```

CardDetailsTransactionResponse – example SOAP response – 3D Secure Required

3D Secure has been request, the ACS URL provides the endpoint to submit the information to.

```
<CardDetailsTransactionResponse xmlns="https://www.thepaymentgateway.net/">
   <CardDetailsTransactionResult AuthorisationAttempted="False">
      <StatusCode>3</StatusCode>
      <Message>Issuer authentication required</Message>
   </CardDetailsTransactionResult>
   <TransactionOutputData CrossReference="191108085848137801526378">
      <CardTypeData>
         <CardType>VISA</CardType>
         <CardClass>PERSONAL</CardClass>
         <Issuer ISOCode="250">CREDIT INDUSTRIEL ET COMMERCIA</Issuer>
      </CardTypeData>
      <ThreeDSecureOutputData>
<PaREQ>eJxVUstuwjAQvFfqP0S5F8fOownaGNGiqqhKQG04cHQdC4LIAycpj6+vHRJoJR92Zj3r3Vn
D5JTvjR8h66wsQhOPLNMQBS/TrNiE5ip5e/LNCX18gGQrhZh9Cd5KQSESdc02wsjS0FxOP8Uh8LEde
Lbn2iaFjqHQV6Wq6IgAGqASS75lRUOB8cPLPKaY2I7rPfuAegJyIeezGx8AuhJQsFzQJTtfyklYqw9AH
QG8bItGnqlPPEADgFbu6bZpqjFC1VXS5t+S8RKQTgG6N7JsdVSrUqcspdFuc4mTlbOYrY/xbkqi3fq4S
DiJkygEpG9AyhpBiYUDjC3fsPyx648dNUDHA8t1D5QEI08PdUVQ6UemQ0pn/jKgnJXK+mGKAYE4Va
p1rQF0iyEVNacLmQpp6FBmVaPMNVQHOgHoPtHruzaaN8o/z3XUwWpNlva643T9TNlFXAt3D2gASK
tQv0jUr1tF/77BL/rGu9c=</PaREQ>
<ACSURL>https://gw1.tponlinepayments2.com:4430/ACS/Default.aspx</ACSURL>
      </ThreeDSecureOutputData>
      <GatewayEntryPoints>
         <GatewayEntryPoint EntryPointURL="https://gw1.tponlinepayments2.com:4430/"
Metric="100" />
         <GatewayEntryPoint EntryPointURL="https://gw2.tponlinepayments2.com:4430/"
Metric="200" />
      </GatewayEntryPoints>
   </TransactionOutputData>
</CardDetailsTransactionResponse>
```

ThreeDSecureAuthentication

Introduction

The 3D Secure authentication request is used when the initial transaction has been returned as requiring the customer to validate their card details with their card issuer. This validation interrupts the payment process & effectively causes a single transaction to be handled in 2 distinct messages – the first message is the initial CardDetailsTransaction message, which completes with a "3D Secure validation required" result & the second message, which contains the 3D Secure validation response from the customer's card issuer (collected by the customer themselves). The ThreeDSecureAuthentication is the second of the two messages described above.

Request

Below are the details for the request message to initiate a 3D Secure authentication transaction

Tag/Attribute Name	Data Type	Max Length	Mandatory	Comments
ThreeDSecureMessage			**Yes**	
MerchantAuthentication			**Yes**	
MerchantID	A	15	Yes	The gateway account merchant ID issued (not to be confused with the MMS username)
Password	A	15	Yes	The gateway account password
ThreeDSecureInputData			**Yes**	
CrossReference (attribute)	A	25	Yes	The cross reference returned by the previous response that included the ThreeDSecureOutputData
PaRES	A	-	Yes	The base64 encoded PaRES string returned by the interaction with the ACS server

3D Secure Required – example request form

Using the information in the CardDetailsTransactionResponse -> ThreeDSecureOutputData section complete and submit a 3d secure request form. This is typically submitted to an iframe so that the card issuers 3D secure authentication can be completed without fully redirecting the customer.

```
<form method="POST" action="https://gw1.tponlinepayments2.com:4430/ACS/Default.aspx"
target="ACSFrame">
    <input type="hidden" name="PaReq"
value="eJxVUstuwjAQvFfqP0S5F8fOownaGNGiqqhKQG04cHQdC4LIAycpj6+vHRJoJR92Zj3r3VnD5JT
vjR8h66wsQhOPLNMQBS/TrNiE5ip5e/LNCX18gGQrhZh9Cd5KQSESdc02wsjS0FxOP8Uh8LEdeLbn2ia
FjqHQV6Wq6IgAGqASS75lRUOB8cPLPKaY2I7rPfuAegJyleezGx8AuhJQsFzQJTtfykIYqw9AHQG8bItGn
qlPPEADgFbu6bZpqjFC1VXS5t+S8RKQTgG6N7JsdVSrUqcspdFuc4mTlbOYrY/xbkqi3fq4SDiJkygEpG9
AyhpBiYUDjC3fsPyx648dNUDHA8t1D5QEI08PdUVQ6UemQ0pn/jKgnJXK+mGKAYE4Vap1rQF0iyEVNa
cLmQpp6FBmVaPMNVQHOgHoPtHruzaaN8o/z3XUwWpNlva643T9TNlFXAt3D2gASKtQv0jUr1tF/77B
L/rGu9c=">
    <input type="hidden" name="MD" value="19110808584813780152637 8">
    <input type="hidden" name="TermUrl" value="http://gateway.test/process.php">
</form>
```

3D Secure Required – example POST response

Once completed the card issues with respond with the MD (CrossReference) and PaRes (outcome) variables.

```
PaRes:
eJxlkm1PwjAQx9+b+B2WvZeue2IjRwlkkvBiSHSo+K7pmjFlD2wdTj69bUXA2KTp9de76/+uhUlf7IwDb
9q8KscmHlimwUtWpXmZjc11Mr8LzAm5vYFk23AePXHWNZxAzNuWZtzl07G5mj7yvW8FTuCHruubBB
Rp9VkQ7qw0xMJLJT7dQuQlAxvQ71Yma9iWloIAZfvZYkmw7biePwwAnQAUvFlEZx4C+gGALrGrTlmtF
NfnKVkm62N8ZE58vHfid9Yvo+zzIfqQMxsDUh6QUsGJbeEQYyswsDVyvZHnAdIcapVuWlSdzI19W+q9Ji
Db0Mg+fZHA9gGdd8D7uiq59JABZxvQRVxNS+KGQ9/xLD38IMQyt6SQvBIQefFflKxXc2gFFV1LNoBOFjB
6OJC3Yl7zl9ClzqygxbNae2qLblPGsljtApzlxJLVqVVHTXdZ1eRiWyipfwEgJQXpZ9Q91o+t8PUn+AZTHr
aw
MD: 191108104555745301504071
```

ThreeDSecureAuthentication – example SOAP request

Using the variables sent from the card issuer, complete another SOAP request to the payment gateway to process the transaction.

```
<ThreeDSecureAuthentication xmlns='https://www.thepaymentgateway.net/'>
   <ThreeDSecureMessage>
      <ThreeDSecureInputData CrossReference='191108104555745301504071'>
<PaRES>eJxlkm1PwjAQx9+b+B2WvZeue2IjRwlkkvBiSHSo+K7pmjFlD2wdTj69bUXA2KTp9de76/+uh
Ulf7IwDb9q8KscmHlimwUtWpXmZjc11Mr8LzAm5vYFk23AePXHWNZxAzNuWZtzI07G5mj7yvW8FTu
CHruubBBRp9VkQ7qw0xMJLJT7dQuQlAxvQ71Yma9iWloIAZfvZYkmw7biePwwAnQAUvFlEZx4C+gGA
LrGrTlmtFNfnKVkm62N8ZE58vHfid9Yvo+zzIfqQMxsDUh6QUsGJbeEQYyswsDVyvZHnAdIcapVuWlSdz
I19W+q9JiDb0Mg+fZHA9gGdd8D7uiq59JABZxvQRVxNS+KGQ9/xLD38lMQyt6SQvBlQefFflKxXc2gFFV
1LNoBOFjB6OJC3Yl7zl9ClzqygxbNae2qLblPGsljtApzlxJLVqVVHTXdZ1eRiWyipfwEgJQXpZ9Q91o+t8
PUn+AZTHraw</PaRES>
      </ThreeDSecureInputData>
      <MerchantAuthentication Password="**PASSWORD**" MerchantID="**MERCHANTID**"/>
   </ThreeDSecureMessage>
</ThreeDSecureAuthentication>
```

Response

Below are the details for the response that will be received after sending a ThreeDSecureAuthentication request.

Tag/Attribute Name	Data Type	Max Length	Always Present	Comments
ThreeDSecureAuthenticationResponse			**Yes**	
ThreeDSecureAuthenticationResult			**Yes**	
AuthorisationAttempted (attribute)	B	-	Yes	This indicates whether the transaction was actually sent to the acquirer for authorisation, or whether it failed before authorisation
StatusCode	N	-	Yes	This indicates the status of the transaction
Message	A	-	Yes	This gives a more detailed description of the status of the transaction
ErrorMessages			**No**	
MessageDetail			**Yes**	
Detail (multiple)	A	256	Yes	If there were multiple error messages (e.g. multiple input variable validation errors, then they will be detailed here)
PreviousTransactionResult			**No**	
StatusCode	N		Yes	If the transaction was deemed to be a duplicate transaction, this indicates the status of the previous transaction
Message	A		Yes	If the transaction was deemed to be a duplicate transaction, this gives a more detailed description of the status of the previous transaction
TransactionOutputData			**No**	
CrossReference (attribute)	A	25	Yes	This is the unique cross reference for this transaction. If the transaction was rejected as a duplicate transaction, this value will hold the cross reference of the previous transaction

Tag/Attribute Name	Data Type	Max Length	Always Present	Comments
AuthCode	A	15	No	If the transaction was successful, then the auth code is passed out here
AddressNumericCheckResult	-	-	No	If requested in the initial CardDetailsTransaction or CrossReferenceTransaction request message, this gives the results of the address numeric check - will be PASSED, FAILED, NOT_CHECKED or UNKNOWN
PostCodeCheckResult	-	-	No	If requested in the initial CardDetailsTransaction or CrossReferenceTransaction request message, this gives the results of the post code check - will be PASSED, FAILED, NOT_CHECKED or UNKNOWN
CV2CheckResult	-	-	No	If requested in the initial CardDetailsTransaction or CrossReferenceTransaction request message, this gives the results of the CV2check - will be PASSED, FAILED, NOT_CHECKED or UNKNOWN
ThreeDSecureAuthenticationCheckResult	-	-	No	This gives the results of the 3D Secure authentication check - will be PASSED, FAILED or UNKNOWN
CardTypeData			**No**	
CardType	A	-	Yes	If requested in the initial CardDetailsTransaction or CrossReferenceTransaction request message, this gives the card type for the transaction. (See Appendix 4 for details)
Issuer	A	100	No	The card issuer (if known)
AmountReceived	N	15	No	If requested in the initial CardDetailsTransaction or CrossReferenceTransaction request message, this gives the amount that was passed to the gateway via the request message
GatewayEntryPoints			**Yes**	

Tag/Attribute Name		Data Type	Max Length	Always Present	Comments
	EntryPointURL (attribute)	A	256	Yes	The URL of the active gateway entry point
	Metric (attribute)	N	5	Yes	A metric value giving an indication of whether transactions should be sent to this gateway entry point

Things to Note

- The contents of the variable "MD" used in the 3D Secure validation process should be passed in as the CrossReference of the ThreeDSecureAuthentication message
- The value of the ThreeDSecureAuthentication results will give the results of the 3D Secure authentication – it will be either PASSED, FAILED or UNKNOWN. It is worth noting that in some cases, even if the authentication is UNKNOWN or FAILED, then the transaction can still be processed (albeit without the liability shift that happens with 3D Secure authentication

ThreeDSecureAuthenticationResponse – example SOAP response

```
<ThreeDSecureAuthenticationResponse xmlns="https://www.thepaymentgateway.net/">
   <ThreeDSecureAuthenticationResult AuthorisationAttempted="True">
      <StatusCode>0</StatusCode>
      <Message>AuthCode: 471947</Message>
   </ThreeDSecureAuthenticationResult>
   <TransactionOutputData CrossReference="191108104601438401677264">
      <AuthCode>471947</AuthCode>
      <AddressNumericCheckResult>PASSED</AddressNumericCheckResult>
      <PostCodeCheckResult>PASSED</PostCodeCheckResult>
<ThreeDSecureAuthenticationCheckResult>PASSED</ThreeDSecureAuthenticationCheckResult>
      <CV2CheckResult>PASSED</CV2CheckResult>
      <CardTypeData>
         <CardType>VISA</CardType>
         <CardClass>PERSONAL</CardClass>
         <Issuer ISOCode="250">CREDIT INDUSTRIEL ET COMMERCIA</Issuer>
      </CardTypeData>
      <GatewayEntryPoints>
         <GatewayEntryPoint EntryPointURL="https://gw1.tponlinepayments2.com:4430/"
Metric="100" />
         <GatewayEntryPoint EntryPointURL="https://gw2.tponlinepayments2.com:4430/"
Metric="200" />
      </GatewayEntryPoints>
   </TransactionOutputData>
</ThreeDSecureAuthenticationResponse>
```

CrossReferenceTransaction

Introduction

Cross reference transactions are primarily used so that the merchant can run subsequent transactions against previous transactions without having to store the credit card details from the original transaction. These transactions may be subsequent sales (used for recurring billing), full or partial collection of funds (if the initial transaction was a pre-authorisation), or full or partial refunds (if the initial transaction was a sale or a collection)

Request

Below are the details for the request message to initiate a cross reference transaction.

Tag/Attribute Name	Data Type	Max Length	Mandatory (Default)	Comments
PaymentMessage			**Yes**	
MerchantAuthentication			**Yes**	
MerchantID	A	15	Yes	The gateway account merchant ID issued (not to be confused with the MMS username)
Password	A	15	Yes	The gateway account password
TransactionDetails			**Yes**	
Amount (attribute)	N	15	No (False)	The transaction amount in minor currency - e.g. for £10.00, it must be submitted as 1000. Mandatory for all TransactionTypes except VOID
CurrencyCode (attribute)	N	3	No (False)	ISO 4217 e.g. GBP: 826. Mandatory for all TransactionTypes except VOID
OrderID	A	50	Yes	A merchant side ID for the order - primarily used to for determining duplicate transactions. Pulled forward from the previous transaction if not set & NewTransaction is false
OrderDescription	A	256	No (See comment)	A description for the order. Pulled forward from the previous transaction if not set & NewTransaction is false
MessageDetails				

Tag/Attribute Name	Data Type	Max Length	Mandatory (Default)	Comments
TransactionType (attribute)	-	-	Yes	Must be either COLLECTION, REFUND, PREAUTH, SALE, VOID or RETRY
NewTransaction (attribute)	B	-	No (True)	Instructs the gateway to treat this transaction as a new transaction
CrossReference (attribute)	A	25	Yes	The cross reference for the previous transaction
TransactionControl			**No**	
EchoCardType	B	-	No (False)	Instructs the gateway to include the card type of the transaction in the message response
EchoAVSCheckResult	B	-	No (False)	Instructs the gateway to include the AVS results for the transaction in the message response
EchoCV2CheckResult	B	-	No (False)	Instructs the gateway to include the CV2 results for the transaction in the message response
EchoAmountReceived	B	-	No (False)	Instructs the gateway to include the amount that was passed to it in the message response
DuplicateDelay	N	3	No (60)	Sets the amount of time (in seconds) that any orders to the same gateway account with the same OrderID and CardNumber should be rejected
AVSOverridePolicy	-	4	No (As set in MMS)	Sets an override AVS checking policy for this transaction. (See Appendix 3 for details)
CV2OverridePolicy	-	2	No (As set in MMS)	Sets an override CV2 checking policy for this transaction. (See Appendix 3 for details)
ThreeDSecureOverridePolicy	B	-	No (False)	Instructs the gateway to enable/disable 3D Secure checking for this transaction (where possible)
OverrideCardDetails			**No**	

Tag/Attribute Name	Data Type	Max Length	Mandatory (Default)	Comments
CardName	A	100	No (See comment)	The name on the customer's card. Only submit to override the value for the previous transaction (submit "blank" to not use the value from the previous transaction)
CardNumber	N	20	No (See comment)	The customer's card number. Only submit to override the value for the previous transaction
ExpiryDate			**No**	
Month	N	2	No (See comment)	The month of the expiry date in 2-digit numeric format - e.g. for July, must be submitted as 07. Only submit to override the value for the previous transaction (submit -1 to not use the value from the previous transaction)
Year	N	2	No (See comment)	The year of the expiry date in 2-digit numeric format - e.g. for 2007, must be submitted as 07. Only submit to override the value for the previous transaction (submit -1 to not use the value from the previous transaction)
CV2	N	4	No (See comment)	The security number (also called CVV or CVV2) printed on the customer's card - usually the last 3 or 4 digits printed on the signature strip. Only submit to override the value for the previous transaction (submit -1 to not use the value from the previous transaction)
IssueNumber	N	2	No (See comment)	The issue number printed on the customer's card. Only submit to override the value for the previous transaction (submit -1 to not use the value from the previous transaction)
CustomerDetails			**No**	
BillingAddress			**No**	

Tag/Attribute Name	Data Type	Max Length	Mandatory (Default)	Comments
Address1	A	100	No (See comment)	Customer's billing address line 1. Only pulled forward from previous transaction if NONE of the address fields have been set
Address2	A	50	No (See comment)	Customer's billing address line 2. Only pulled forward from previous transaction if NONE of the address fields have been set
Address3	A	50	No (See comment)	Customer's billing address line 3. Only pulled forward from previous transaction if NONE of the address fields have been set
Address4	A	50	No (See comment)	Customer's billing address line 4. Only pulled forward from previous transaction if NONE of the address fields have been set
City	A	50	No (See comment)	Customer's billing address city. Only pulled forward from previous transaction if NONE of the address fields have been set
State	A	50	No (See comment)	Customer's billing address state. Only pulled forward from previous transaction if NONE of the address fields have been set
PostCode	A	50	No (See comment)	Customer's billing address post code. Only pulled forward from previous transaction if NONE of the address fields have been set
CountryCode	N	3	No (See comment)	ISO 3166-1 e.g. United Kingdom: 826. Only pulled forward from previous transaction if NONE of the address fields have been set
EmailAddress	E	100	No (See comment)	The email address of the customer - NOTE: anything passed in here is validated as an email address, so anything passed in must be a valid email address. Pulled forward from previous transaction if not set

Tag/Attribute Name	Data Type	Max Length	Mandatory (Default)	Comments
PhoneNumber	A	30	No (See comment)	The customer's phone number. Pulled forward from previous transaction if not set
CustomerIPAddress	I	15	No	The IP address of the customer (NOT the IP address of the merchant's website). This is used to determine the customer's country of origin. The format is xxx.xxx.xxx.xxx
DateOfBirth	D	10	No	The date of birth of the customer. Must be in the format YYYY-MM-DD
PrimaryAccountDetails			**No**	
Name	A	100	No	The name of the primary account holder (used for MCC 6012 accounts only)
AccountNumber	A	50	No	The account number of the primary account holder (used for MCC 6012 accounts only)
DateOfBirth	D	10	No	The date of birth of the primary account holder (used for MCC 6012 accounts only)
AddressDetails			**No**	
PostCode	A	50	No	The post code of the primary account holder (used for MCC 6012 accounts only)

takepayments
we make it easy

CrossReferenceTransaction – example SOAP request

```
<CrossReferenceTransaction xmlns="https://www.thepaymentgateway.net/">
   <PaymentMessage>
      <TransactionDetails Amount="1224" CurrencyCode="826">
         <MessageDetails TransactionType="SALE" CrossReference="191107134633228401845699"
NewTransaction="true" />
         <TransactionControl>
<ThreeDSecureOverridePolicy>false</ThreeDSecureOverridePolicy>
            <DuplicateDelay>60</DuplicateDelay>
            <EchoCardType>true</EchoCardType>
            <EchoAVSCheckResult>true</EchoAVSCheckResult>
            <EchoCV2CheckResult>true</EchoCV2CheckResult>
            <EchoAmountReceived>true</EchoAmountReceived>
         </TransactionControl>
         <OrderID>123</OrderID>
         <OrderDescription>Exam</OrderDescription>
      </TransactionDetails>
      <OverrideCardDetails>
         <CV2>341</CV2>
      </OverrideCardDetails>
      <MerchantAuthentication MerchantID="**MERCHANTID**" Password="**PASSWORD**" />
   </PaymentMessage>
</CrossReferenceTransaction>
```

Response

Below are the details for the response that will be received after sending a CrossReferenceTransaction request.

Tag/Attribute Name	Data Type	Max Length	Always Present	Comments
CrossReferenceTransactionResponse			**Yes**	
CrossReferenceTransactionResult			**Yes**	
AuthorisationAttempted (attribute)	B	-	Yes	This indicates whether the transaction was sent to the acquirer for authorisation, or whether it failed before authorisation
StatusCode	N	-	Yes	This indicates the status of the transaction
Message	A	-	Yes	This gives a more detailed description of the status of the transaction
ErrorMessages			**No**	
MessageDetail			**Yes**	
Detail (multiple)	A	256	Yes	If there were multiple error messages (e.g. multiple input variable validation errors, then they will be detailed here)
PreviousTransactionResult			**No**	
StatusCode	N		Yes	If the transaction was deemed to be a duplicate transaction, this indicates the status of the previous transaction
Message	A		Yes	If the transaction was deemed to be a duplicate transaction, this gives a more detailed description of the status of the previous transaction
TransactionOutputData			**No**	

Tag/Attribute Name	Data Type	Max Length	Always Present	Comments
CrossReference (attribute)	A	25	Yes	This is the unique cross reference for this transaction. If the card has been determined as requiring 3D Secure authentication this must be used as the merchant reference. If the transaction was rejected as a duplicate transaction, this value will hold the cross reference of the previous transaction
AuthCode	A	15	No	If the transaction was successful, then the auth code is passed out here
AddressNumericCheckResult	-	-	No	If requested in the CrossReferenceTransaction request message, this gives the results of the address numeric check - will be PASSED, FAILED, PARTIAL, NOT_CHECKED or UNKNOWN
PostCodeCheckResult	-	-	No	If requested in the CrossReferenceTransaction request message, this gives the results of the post code check - will be PASSED, FAILED, PARTIAL, NOT_CHECKED or UNKNOWN
CV2CheckResult	-	-	No	If requested in the CrossReferenceTransaction request message, this gives the results of the CV2check - will be PASSED, FAILED, NOT_CHECKED or UNKNOWN
CardTypeData				
CardType	A	-	Yes	If requested in the CrossReferenceTransaction request message, this gives the card type for the transaction. (See Appendix 4 for details)
Issuer	A	100	No	The card issuer (if known)

Tag/Attribute Name	Data Type	Max Length	Always Present	Comments
AmountReceived	N	15	No	If requested in the CrossReferenceTransaction request message, this gives the amount that was passed to the gateway via the request message
ThreeDSecureOutputData			**No**	
PaREQ	A	-	Yes	If the card has been determined as requiring 3D Secure authentication, this gives the base64 encoded payment request that must be passed to the ACS for authentication. This must be sent to the ACS as 'PaReq'
ACSURL	A	-	Yes	If the card has been determined as requiring 3D Secure authentication, this gives the URL of the ACS server that the PaREQ must be sent to
GatewayEntryPoints			**Yes**	
GatewayEntryPoint (multiple)			**Yes**	
EntryPointURL (attribute)	A	256	Yes	The URL of the active gateway entry point
Metric (attribute)	N	5	Yes	A metric value giving an indication of whether transactions should be sent to this gateway entry point

Things to Note

- We do not store the CV2 values of any transactions, so they are not available to be pulled forwards from the previous transaction. This means that the unless the CV2 is supplied as part of the OverrideCardDetails in the CrossReferenceTransaction message then the results returned will always be UNKNOWN
- If requested, the AmountReceived will always echo the amount passed to the gateway regardless of the outcome of the transaction (apart from if the message could not be validated due to content errors)
- If the address or the post code information is not submitted in the CrossReferenceTransaction message then the AddressNumericCheckResult and the PostCodeCheckResult will be deemed to be UNKNOWN rather than FAILED
- If this transaction is marked as not a new transaction in the CrossReferenceTransaction message, then the OrderID and OrderDescription will be pulled forward from the previous transaction unless they are present in this message

- If this transaction is marked as a new transaction in the CrossReferenceTransaction message, then the OrderID and OrderDescription will not be pulled forward from the previous transaction.

CrossReferenceTransactionResponse – example SOAP response

```
<CrossReferenceTransactionResponse xmlns="https://www.thepaymentgateway.net/">
  <CrossReferenceTransactionResult AuthorisationAttempted="True">
    <StatusCode>0</StatusCode>
    <Message>AuthCode: 733706</Message>
  </CrossReferenceTransactionResult>
  <TransactionOutputData CrossReference="191107135553912001652758">
    <AuthCode>733706</AuthCode>
    <AddressNumericCheckResult>PASSED</AddressNumericCheckResult>
    <PostCodeCheckResult>PASSED</PostCodeCheckResult>
    <CV2CheckResult>PASSED</CV2CheckResult>
    <CardTypeData>
      <CardType>VISA</CardType>
      <CardClass>PERSONAL</CardClass>
      <Issuer ISOCode="250">CREDIT INDUSTRIEL ET COMMERCIA</Issuer>
    </CardTypeData>
    <AmountReceived>1224</AmountReceived>
    <GatewayEntryPoints>
      <GatewayEntryPoint EntryPointURL="https://gw1.tponlinepayments2.com:4430/"
Metric="100" />
      <GatewayEntryPoint EntryPointURL="https://gw2.tponlinepayments2.com:4430/"
Metric="200" />
    </GatewayEntryPoints>
  </TransactionOutputData>
</CrossReferenceTransactionResponse>
```

Appendix

Appendix 1: Gateway Response StatusCodes

Below are the status codes likely to be received when integrating with the gateway.

Status Code	Transaction Result	Description
0	Successful	**Transaction Authorised:** The transaction was successful, and you will be given an Authorisation Code as part of the message returned by the gateway.
3	Incomplete	**Transaction Awaiting 3D Secure Authentication:** Transaction is now awaiting 3D Secure Authentication from the customer. This status has a 2-hour expiry time set by the card scheme, at which point, the transaction will fail (Issuer Authentication Expired).
4	Referred	**Transaction Referred:** The card issuer has parked the transaction awaiting contact with the customer before proceeding to authorise or decline the transaction.
5	Declined	**Transaction Failed:** The transaction was declined by the card issuer or acquiring bank. In the event of the Address or CV2 verification failure, this will also be noted on the message from the gateway (Example, "Card declined: AVS policy + CV2 policy"). If the message given by the gateway only says "Card declined" with no other information, then no other information was given to us from the card issuer or acquiring bank as to the underlying reason why. The only person who can find out why the transaction was declined is the customer by contacting their bank directly.
20	Duplicate Transaction	The transaction which was processed was a duplicate. If this is the case, then the original transaction information is also passed back from the gateway so you can determine the result of the original transaction. Please refer to your respective integration method documentation form more information.
30	Failed (Error(s) Occurred)	**Transaction Failed:** This is usually an indicator that the integration to the gateway is incomplete and/or not working correctly. There will also be additional error information feedback from the gateway for merchants to determine what the error is specifically. Please refer to your respective integration methods documentation for more information.

Appendix 2: Transaction Data Flow

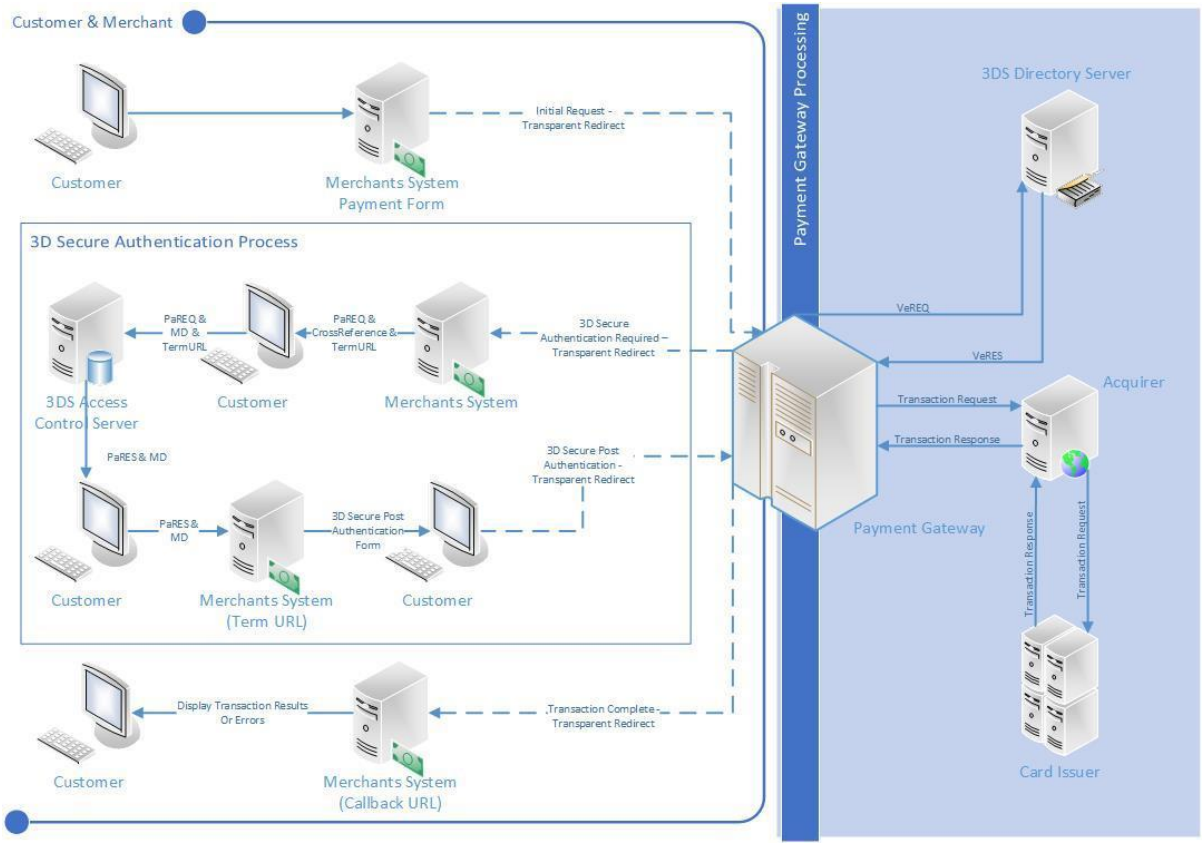
Listed below are the steps that a Transparent Redirect transaction will take. There are also 3 diagrams to show the transaction data flow in different scenarios.

1. The cardholder navigates to the merchant's website and supplies their card details into the merchant's payment form. The payment form is hosted directly on the merchant's system.
2. The Merchant and transactional data, optionally along with Customer information are passed to the payment gateway (Transparent Redirect URL), as part of a transparent redirect. The customer is unaware of this redirection as nothing changes on screen whilst processing takes place. The data passed to the payment gateway will be checked for errors at this point.
    a. If errors occur (for example; Variable Tampering), the payment gateway doesn't allow the transaction to go any further and the error details are passed back to the Merchant's system (CallbackURL) and moves to step 11.
    b. If no errors occurred, the transaction moves to step 3.
3. The payment gateway contacts the Directory Server to query whether this card is enrolled in the 3D Secure scheme.
4. The Directory Server determines whether the card is enrolled in the 3DS scheme, then passes this information back to the payment gateway.
    a. If the card is enrolled in the 3D Secure Authentication Scheme, the transaction moves to step 5.
    b. If not, the transaction moves to step 10.
5. The payment gateway passes the URL of the cardholder's bank's Access Control Server (ACSURL) and additional data from which a Payment Request string (PaREQ) is created, to the merchant's system (CallbackURL) as part of a transparent redirect. Again, the customer is unaware of this redirect. The data passed to the Merchant's System should be checked for errors at this point.
    a. If errors occur (for example; Variable Tampering), the transaction shouldn't go any further and moves to step 11.
    b. If no errors occurred, the transaction moves to step 6.
6. The customer is then redirected by the merchant's system (CallbackURL) to their bank's Access Control Server (ACSURL) and they are greeted with the last 4 digits of their credit card & the identification text they specified when registering their card for 3D Secure. This redirection is not transparent; it is very much visible to the customer.
7. The customer then validates their card details using their 3D Secure password, which is validated by their bank's Access Control Server.
8. The Access Control Server then initiates a redirect of the customer's browser back to a secure processing page on the merchant's website (TermURL), which forwards the payment response string (PaRES) from the Access Control Server to the payment gateway (Transparent Redirect URL) using a transparent page redirect. The data passed to the payment gateway will be checked for errors at this point.
    a. If errors occur (for example; Variable Tampering), the details will be passed back to the merchant's system (CallbackURL) and the transaction won't go any further.
    b. If no errors occurred, the transaction moves to step 10.
9. The payment gateway checks the contents of the payment response (PaRES).
    a. If the transaction is declined (following a 3D Secure authentication failure), move to step 11.
    b. If not, the transaction moves to step 10.
10. The payment gateway then submits the transaction to the bank for authorisation. The results of the transaction are then passed back to the merchant's system (CallbackURL) in a transparent redirect. The data passed to the Merchant's System should be checked for errors at this point.

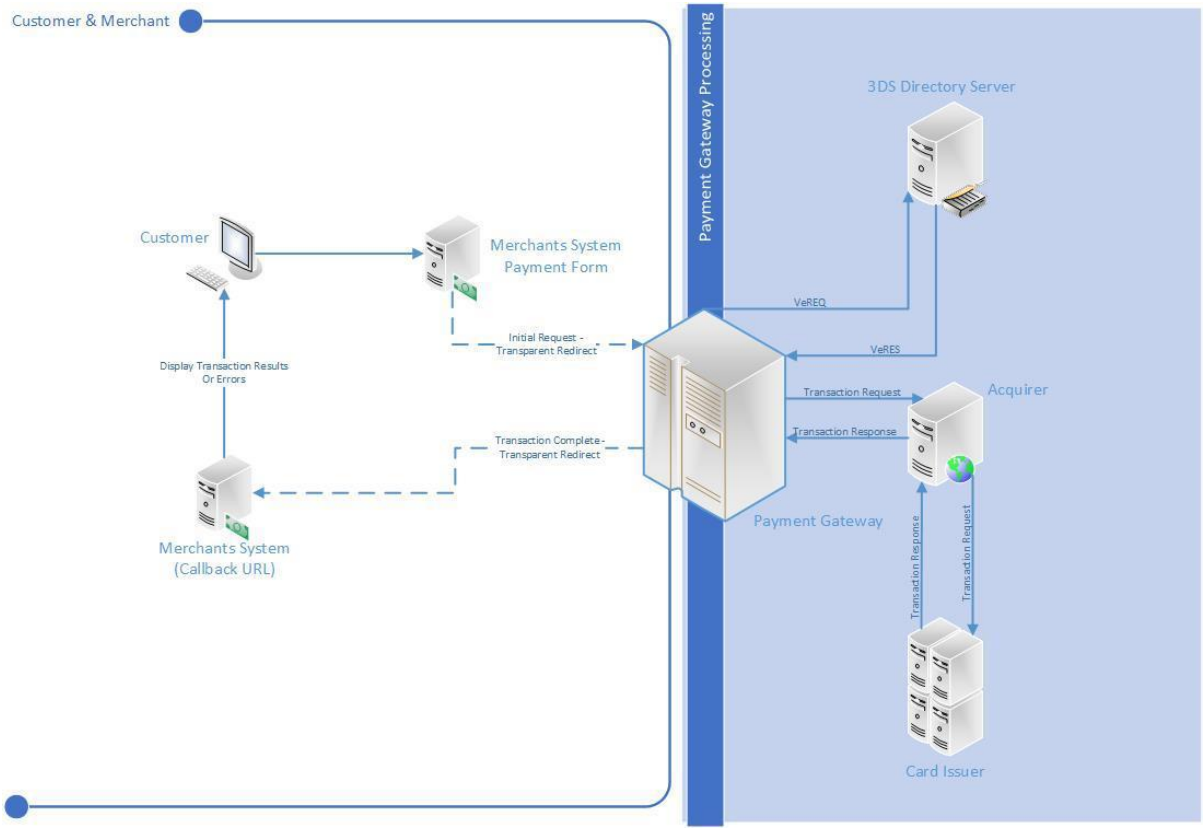
   a. If errors occur (for example; Variable Tampering), the transaction **HAS already been** processed, but the merchant's system should stop the transaction from going any further.

11. The merchant's system should display the transaction result to the customer (or desired error information if any occurred before this point)

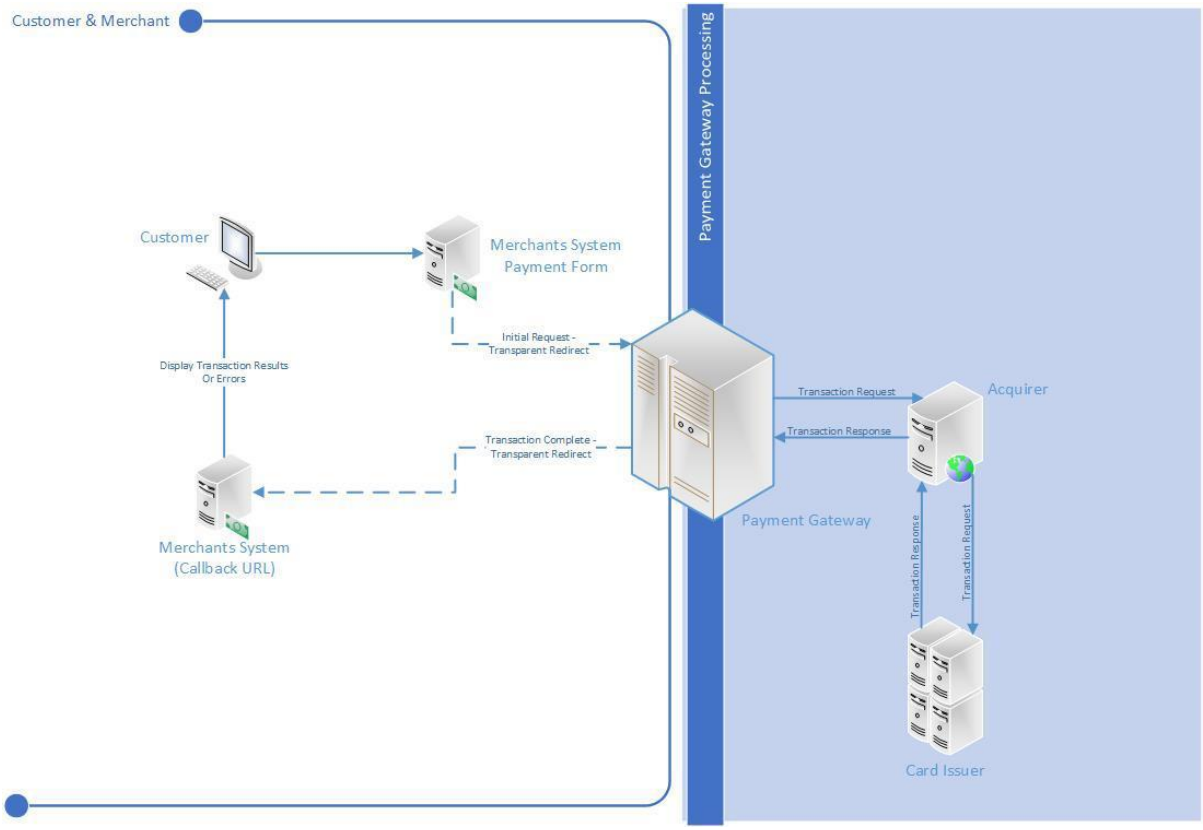
Transaction Flow Maps - Including 3D Secure Authentication



Transaction Flow Maps - 3D Secure Card Not Enrolled



Transaction Flow Maps - 3D Secure Disabled (MMS Setting)



ACS Simulator

The test system comes complete with an ACS simulator, which allows your developer to simulate the most common responses that might come back from the cardholder's bank's access control server

There are 4 possible conditions that can be simulated:

1. Password Correct – the case where the cardholder enters the correct 3D Secure password. Relates to a 3D Secure status of "Y"
2. Password Incorrect – the case where the cardholder enters the wrong 3D Secure password. Relates to a 3D Secure status of "N"
3. Attempted Processing – the case where the cardholder attempted to authenticate themselves, but this could not be completed for some reason. Proof of this attempt is returned with the payment response message. Relates to a 3D Secure status of "A"
4. Unknown Error – the case where an unexpected error occurred whilst trying to authenticate the cardholder. Relates to a 3D Secure status of "U"

Appendix 3: Code examples

StringToHash

This is a sample SALE transaction StringToHash for the transparent redirect URL, this is used to generate the HashDigest.

```
MerchantID=**MERCHANTID**&Password=**PASSWORD**&Amount=9863&CurrencyCode=826&EchoAVSCheckResult=true&EchoCV2CheckResult=true&EchoThreeDSecureAuthenticationCheckResult=true&EchoCardType=true&OrderID=Order-157&TransactionType=SALE&TransactionDateTime=2019-11-07 09:30:16 +00:00&CallbackURL=http://gateway.test/callback.php&OrderDescription=Order description
```

3D Secure Authentication Required – Response

This is an example response for a transaction requiring 3D Secure Authentication. This response would have been sent via POST to the merchant's CallbackURL from the gateway. This contains a HashDigest that can be used to verify that the response is as expected.

```
HashDigest: d6b88898177d86806a322e06f0f3fa544535a3bc
MerchantID: **MERCHANTID**
StatusCode: 3
Message: Issuer authentication required
CrossReference: 191107093208704502245361
OrderID: Order-157
TransactionDateTime: 2019-11-07 09:30:16 +00:00
ACSURL: https://gw2.tponlinepayments2.com:4430/ACS/Default.aspx
PaREQ:
eJxVUttOg0AQfTfxHwjvdlkoFJphmyoaG9NLlD74uC4biimXLmCKX+8sBavJJjvnzGVnziwszvnR+JKqzs
oiNOnEMg1ZiDLJijQ09/HTnW8u2O0NxAclZfQmRaskg7Wsa55KI0tCc7d8laepY1PPnTqWbzLoGQZDVY
ZFJzaQEWKyEgdeNAy4ON2vNozaztT1Zj6QgYBcqlX0ywdALgQUPJdsx7vvspDG/gVIT4Ao26JRHfNtD8g
IoFVHdmiaak5IdUlp8w/FRQlEu4BcG9m12qqx1DlL2DZK6TpadZv4He/Hbv2ZOtt4TxGHQHQEJLyRzLZ
oQKk1M6xg7thzCwfoeeC57oEF/sRzcKgLgko/shxd2vOXAVRWofTjFCMCea6wdYxADX9tSGQt2FYlUhn
aVFnVoLgGdqAdQK4TPTxroUWD+uGG8FDHcy2tdc/p+hnKZbsW7R/QAIjOIsMiybButP59gx8sVrsr
```

3D Secure Authentication Required - StringToHash

This is a sample StringToHash for transaction requiring 3D Secure Authentication, this is used to generate the HashDigest.

```
MerchantID=**MERCHANTID**&Password=**PASSWORD**&StatusCode=3&Message=Issuer
authentication required&CrossReference=191107093208704502245361&OrderID=Order-
157&TransactionDateTime=2019-11-07 09:30:16
+00:00&ACSURL=https://gw2.payzoneonlinepayments.com:4430/ACS/Default.aspx&PaREQ=eJ
xVUttOg0AQfTfxHwjvdlkoFJphmyoaG9NLlD74uC4biimXLmCKX+8sBavJJjvnzGVnziwszvnR+JKqzso
iNOnEMg1ZiDLJijQ09/HTnW8u2O0NxAclZfQmRaskg7Wsa55KI0tCc7d8laepY1PPnTqWbzLoGQZDVY
ZFJzaQEWKyEgdeNAy4ON2vNozaztT1Zj6QgYBcqlX0ywdALgQUPJdsx7vvspDG/gVIT4Ao26JRHfNtD
8gIoFVHdmiaak5IdUlp8w/FRQlEu4BcG9m12qqx1DlL2DZK6TpadZv4He/Hbv2ZOtt4TxGHQHQEJLy
RzLZoQKk1M6xg7thzCwfoeeC57oEF/sRzcKgLgko/shxd2vOXAVRWofTjFCMCea6wdYxADX9tSGQt2
FYlUhnaVFnVoLgGdqAdQK4TPTxroUWD+uGG8FDHcy2tdc/p+hnKZbsW7R/QAIjOIsMiybButP59gx8s
Vrsr
```

3D Secure Authentication Required – Request

Using the information sent from the gateway a Request is sent to the ACSURL to process and display the 3D Secure authentication screen, the TermURL is used at the CallbackURL once the customer has completed 3D secure authentication.

```
<form method="POST" action="https://gw2.tponlinepayments2.com:4430/ACS/Default.aspx"
target="ACSFrame">
    <input type="hidden" name="PaReq"
value="eJxVUttOg0AQfTfxHwjvdlkoFJphmyoaG9NLlD74uC4biimXLmCKX+8sBavJJjvnzGVnziwszvnR
+JKqzsoiNOnEMg1ZiDLJijQ09/HTnW8u2O0NxAclZfQmRaskg7Wsa55KI0tCc7d8laepY1PPnTqWbzLoG
QZDVYZFJzaQEWKyEgdeNAy4ON2vNozaztT1Zj6QgYBcqlX0ywdALgQUPJdsx7vvspDG/gVIT4Ao26JRH
fNtD8gloFVHdmiaak5IdUlp8w/FRQlEu4BcG9m12qqx1DlL2DZK6TpadZv4He/Hbv2ZOtt4TxGHQHQEJ
LyRzLZoQKk1M6xg7thzCwfoeeC57oEF/sRzcKgLgko/shxd2vOXAVRWofTjFCMCea6wdYxADX9tSGQt2
FYlUhnaVFnVoLgGdqAdQK4TPTxroUWD+uGG8FDHcy2tdc/p+hnKZbsW7R/QAIjOIsMiybButP59gx8sVr
sr">
    <input type="hidden" name="MD" value="191107093208704502245361">
    <input type="hidden" name="TermUrl" value="http://gateway.test/callback.php">
</form>
```

3D Secure Authentication Completed – Response

This is an example response for a transaction requiring 3D Secure Authentication. This response would have been sent via POST to the merchant's TermUrl from the gateway.

```
PaRes:
eJxdkttuwjAMhu8n7R2q3o8cekYmiKkDMQmGtqIBd6WNSid6oAcEbz83Y8CWm9hfHPuPHRiesr12lFW
dFvlAZz2qazKPijjNk4G+DMZPrj4Ujw8Q7Cop/Q8ZtZUUMJN1HSZSS+OBvhi9y4NpcGZbpkFdXUBHanW
WspJVDm+4ifhSRWCRHgfy62KyKtqFeSMgjA7P07lg3DAt23GBXABkspr6V+4B+QFAbncXbWfVKO6UxuL
NT9jMn57nwRr3l/PsKzHegiVDfwCki4A4bKTglHmMUUejXt/gfYo1FYeySzfKihZze65tALkngG2osE9n4X
IbyNUDeSqLXGIEPvBqA7mJK8NcmJ5jGxZVy3Y9hrmRQrAS0KTZP1Fm36JAFIe6CZu2FmsgFwui8HgUm
9Vru52U9Xayt9fGuNhM5jzizSH6NPGxKgRklApqoSjc1a3RPimqtNllndS/AEgnhagxqh6rYXf4/hN8A+Rht
ZU=
```

3D Secure Authentication Completed - StringToHash

This is a sample StringToHash for transaction requiring 3D Secure Authentication, this is used to generate the HashDigest.

```
MerchantID=**MERCHANTID**&Password=**PASSWORD**&CrossReference=191107093208704502245
361&TransactionDateTime=2019-11-07 09:34:54
+00:00&CallbackURL=http://gateway.test/callback.php&PaRES=eJxdkttuwjAMhu8n7R2q3o8cekY
miKkDMQmGtqIBd6WNSid6oAcEbz83Y8CWm9hfHPuPHRiesr12lFWdFvlA
```

3D Secure Authentication Completed – Request

Using the information sent from the gateway a Request is sent to the Transparent Redirect URL to process, please note that the MD variables becomes the CrossReference

```
<form  method="POST"
action="https://mms.tponlinepayments2.com/Pages/PublicPages/TransparentRedirect.aspx"
target="_parent">
    <input type="hidden" name="PaRES"
value="eJxdkttuwjAMhu8n7R2q3o8cekYmiKkDMQmGtqlBd6WNSid6oAcEbz83Y8CWm9hfHPuPHRies
r12lFWdFvlAZz2qazKPijjNk4G+DMZPrj4Ujw8Q7Cop/Q8ZtZUUMJN1HSZSS+OBvhi9y4NpcGZbpkFdX
UBHanWWspJVDm+4ifhSRWCRHgfy62KyKtqFeSMgjA7P07lg3DAt23GBXABkspr6V+4B+QFAbncXbWfV
KO6UxuLNT9jMn57nwRr3l/PsKzHegiVDfwCki4A4bKTglHmMUUejXt/gfYo1FYeySzfKihZze65tALkngG
2osE9n4XIbyNUDeSqLXGIEPvBqA7mJK8NcmJ5jGxZVy3Y9hrmRQrAS0KTZP1Fm36JAFIe6CZu2FmsgF
wui8HgUm9Vru52U9Xayt9fGuNhM5jzizSH6NPGxKgRklApqoSjc1a3RPimqtNllndS/AEgnhagxqh6rYXf
4/hN8A+RhtZU=">
    <input type="hidden" name="CrossReference" value="191107093208704502245361">
    <input type="hidden" name="CallbackURL" value="http://gateway.test/callback.php">
    <input type="hidden" name="HashDigest"
value="db1b3aa4cf8373866c0ed8eec667d02ca2547536">
    <input type="hidden" name="MerchantID" value="**MERCHANTID**">
    <input type="hidden" name="TransactionDateTime" value="2019-11-07 09:34:54 +00:00">
</form>
```

Transaction Complete – Response

This is an example response for a completed transaction. This response would have been sent via POST to the merchant's CallbackURL from the gateway.

```
HashDigest: 3534d0b78196b65845f7ae38396f60357d5629a9
MerchantID: **MERCHANTID**
StatusCode: 0
Message: AuthCode: 448178
PreviousStatusCode:
PreviousMessage:
CrossReference: 191107093656165702119743
Amount: 9863
CurrencyCode: 826
OrderID: Order-157
TransactionType: SALE
TransactionDateTime: 2019-11-07 09:36:56 +00:00
OrderDescription: Order description
Address1: 113 Broad Street West
Address2:
Address3:
Address4:
City: Oldpine
State: Strongbarrow
PostCode: SB42 1SX
CountryCode: 250
EmailAddress:
PhoneNumber:
AddressNumericCheckResult: PASSED
PostCodeCheckResult: PASSED
CV2CheckResult: PASSED
ThreeDSecureAuthenticationCheckResult: PASSED
FraudProtectionCheckResult:
CardType: VISA
CardClass: PERSONAL
CardIssuer: CREDIT INDUSTRIEL ET COMMERCIA
CardIssuerCountryCode: 250
```

Transaction Complete - StringToHash

This is a sample StringToHash for a complete transaction to verify that the transaction contains the information expected.

```
MerchantID=**MERCHANTID**&Password=**PASSWORD**&StatusCode=0&Message=AuthCode:
448178&PreviousStatusCode=&PreviousMessage=&CrossReference=191107093656165702119743&A
ddressNumericCheckResult=PASSED&PostCodeCheckResult=PASSED&CV2CheckResult=PASSED&Thr
eeDSecureAuthenticationCheckResult=PASSED&CardType=VISA&CardClass=PERSONAL&CardIssuer
=CREDIT INDUSTRIEL ET
COMMERCIA&CardIssuerCountryCode=250&Amount=9863&CurrencyCode=826&OrderID=Order-
157&TransactionType=SALE&TransactionDateTime=2019-11-07 09:36:56
+00:00&OrderDescription=Order description &Address1=113 Broad Street
West&Address2=&Address3=&Address4=&City=Oldpine&State=Strongbarrow&PostCode=SB42
1SX&CountryCode=250&EmailAddress=&PhoneNumber=
```

Appendix 4: Transaction Result Status Codes

The StatusCode is a numerical value representation for the result of the transaction. If any other code is returned not listed here, it should be treated as an error and handled accordingly.

StatusCode	Explanation
0	Transaction Successful
3	Issuer Authentication Required. This means the card is enrolled for 3D Secure Authentication and is required before the transaction can continue.
5	Transaction Declined. You may sometimes get additional information in the Transaction Result Message as to why if we are informed as to why.
20	Duplication Transaction.
30	An Error Occurred.

Appendix 5: Override Policy Codes & Explanations

OverrideAVSPolicy Codes

The OverrideAVSPolicy codes are 4-character codes which instruct the gateway how to handle the AVS checking for that particular transaction.
The first character determines the behaviour when 1 or more of the results of the address numeric or post code check are known.
The second and third characters determine the behaviour when dealing with partial matches – this is where either the address numeric check or the post code check returns partial matches.
The fourth character determines the behaviour when none of the results of the address numeric or the post code check are known.

Character 1 Codes

Character Code	Explanation
E	This code means fail the transaction if either the address numeric check or post code check has failed
B	This code means fail the transaction only if both the address numeric check and the post code checks have failed
A	This code means fail the transaction only if the address numeric check has failed
P	This code means fail the transaction only if the post code check has failed
N	This code means pass the transaction even if both checks have failed

Character 2 Codes

Character Code	Explanation
P	Treat partial address numeric results as passes
F	Treat partial address numeric results as failures

Character 3 Codes

Character Code	Explanation
P	Treat partial post code results as passes
F	Treat partial post code results as failures

Character 4 Codes

Character Code	Explanation
P	This code means pass the transaction if both results of the AVS check are not known
F	This code means fail the transaction if both results of the AVS check are not known

Examples

- **EFFF** – this is the strongest policy & transactions will only pass if both address numeric & post code checks have passed. Partial matches are treated as failures

- **EPFP** – this policy means that transactions will only pass if both the address numeric & post code checks have passed, but if the results of both are unknown, then pass the transaction. Partial address numeric results are treated as passes, but partial post code checks are treated as failures
- **BPPF** – this policy means that the transaction will fail only if both the address numeric and post code checks have failed, but if the results of both are unknown, then fail the transaction. Both address numeric and post code partial results are treated as passes
- **NPPF** – this policy means that the transaction will pass even if the results of the address numeric and post code checks are failed, but if the results are unknown, then fail the transaction (not a recommended policy!) . Both address numeric and post code partial results are treated as passes
- **NPPP** – this is the weakest policy & transactions will pass regardless of the results of the address numeric & post code checks. Both address numeric and post code partial results are treated as passes.

Questions

Q: Why would the results of the AVS check be unknown?

A: The main reasons for the results of the AVS checks being unknown are:

1. The relevant address data was not passed in with the transaction – the address numeric check is carried out across the Address1, Address1, Address3, Address4, City & State fields – if none of them are present, then the state of the address numeric check will be unknown. Similarly, the post code check is carried out of the field PostCode & if that is not present, then the state of the post code check will be unknown.
2. If the transaction is a cross reference transaction & the respective address information was not submitted with the transaction, or was not submitted or unknown for the transaction being referenced, then the result will carry forward to this transaction
3. If there was a problem contacting the provider, or the provider itself had a problem delivering the results of the AVS checks (least likely reason)

OverrideCV2Policy Codes

The OverrideCV2Policy codes are 2-character codes which instruct the gateway how to handle the CV2 checking for that particular transaction.
The first character determines the behaviour when 1 or more of the results of the address numeric or post code check are known.
The second character determines the behaviour when none of the results of the address numeric or the post code check are known.

Character 1 Codes

Code	Explanation
P	This code means pass the transaction if the CV2 check has failed
F	This code means fail the transaction if the CV2 check has failed

Character 2 Codes

Character Code	Explanation
P	This code means pass the transaction if both results of the CV2 check are not known
F	This code means fail the transaction if both results of the CV2 check are not known

Examples

- **FF** – this is the strongest policy & transactions will only pass if the CV2 check has passed
- **FP** – this policy means that transactions will only pass if the CV2 has passed, but if the results are unknown, then pass the transaction
- **PF** – this policy means that the transaction will pass if the CV2 failed, but if the result of the check is unknown, then fail the transaction (not a recommended policy!)
- **PP** – this is the weakest policy & transactions will pass regardless of the results of the CV2 check

Questions

Q: Why would the CV2 result be unknown?

A: The main reasons for the result being unknown are:

1. The CV2 was not submitted with the transaction
2. If the transaction is a cross reference transaction & the CV2 code was not submitted as an override, or was not submitted or unknown for the original transaction being referenced, then that result will carry forward to this transaction
3. If there was a problem contacting the provider, or the provider itself had a problem delivering the results of the CV2 check (least likely reason)

Appendix 6: Country (ISO 3166-1) Codes

ISO Code	Country
826	United Kingdom
840	United States
036	Australia
004	Afghanistan
248	Åland Islands
008	Albania
012	Algeria
016	American Samoa
020	Andorra
024	Angola
660	Anguilla
010	Antarctica
028	Antigua and Barbuda
032	Argentina
051	Armenia
533	Aruba
040	Austria
031	Azerbaijan
044	Bahamas
048	Bahrain
050	Bangladesh
052	Barbados
112	Belarus
056	Belgium
084	Belize
204	Benin
060	Bermuda
064	Bhutan
068	Bolivia
070	Bosnia and Herzegovina
072	Botswana
074	Bouvet Island
076	Brazil
086	British Indian Ocean Territory
096	Brunei Darussalam
100	Bulgaria
854	Burkina Faso
108	Burundi
116	Cambodia
120	Cameroon
124	Canada
132	Cape Verde
136	Cayman Islands
140	Central African Republic
148	Chad
152	Chile
156	China
162	Christmas Island
166	Cocos (Keeling) Islands
170	Colombia
174	Comoros
178	Congo

ISO Code	Country
180	Congo, Democratic Republic of the
184	Cook Islands
188	Costa Rica
384	Côte d'Ivoire
191	Croatia
192	Cuba
196	Cyprus
203	Czech Republic
208	Denmark
262	Djibouti
212	Dominica
214	Dominican Republic
218	Ecuador
818	Egypt
222	El Salvador
226	Equatorial Guinea
232	Eritrea
233	Estonia
231	Ethiopia
238	Falkland Islands (Malvinas)
234	Faroe Islands
242	Fiji
246	Finland
250	France
254	French Guiana
258	French Polynesia
260	French Southern Territories
266	Gabon
270	Gambia
268	Georgia
276	Germany
288	Ghana
292	Gibraltar
300	Greece
304	Greenland
308	Grenada
312	Guadeloupe
316	Guam
320	Guatemala
831	Guernsey
324	Guinea
624	Guinea-Bissau
328	Guyana
332	Haiti
334	Heard Island and McDonald Islands
336	Holy See (Vatican City State)
340	Honduras
344	Hong Kong
348	Hungary
352	Iceland
356	India
360	Indonesia
364	Iran, Islamic Republic of
368	Iraq

ISO Code	Country
372	Ireland
833	Isle of Man
376	Israel
380	Italy
388	Jamaica
392	Japan
832	Jersey
400	Jordan
398	Kazakhstan
404	Kenya
296	Kiribati
408	Korea, Democratic People's Republic of
410	Korea, Republic of
414	Kuwait
417	Kyrgyzstan
418	Lao People's Democratic Republic
428	Latvia
422	Lebanon
426	Lesotho
430	Liberia
434	Libyan Arab Jamahiriya
438	Liechtenstein
440	Lithuania
442	Luxembourg
446	Macao
807	Macedonia, the former Yugoslav Republic of
450	Madagascar
454	Malawi
458	Malaysia
462	Maldives
466	Mali
470	Malta
584	Marshall Islands
474	Martinique
478	Mauritania
480	Mauritius
175	Mayotte
484	Mexico
583	Micronesia, Federated States of
498	Moldova
492	Monaco
496	Mongolia
499	Montenegro
500	Montserrat
504	Morocco
508	Mozambique
104	Myanmar
516	Namibia
520	Nauru
524	Nepal
528	Netherlands
530	Netherlands Antilles
540	New Caledonia
554	New Zealand

ISO Code	Country
558	Nicaragua
562	Niger
566	Nigeria
570	Niue
574	Norfolk Island
580	Northern Mariana Islands
578	Norway
512	Oman
586	Pakistan
585	Palau
275	Palestinian Territory, Occupied
591	Panama
598	Papua New Guinea
600	Paraguay
604	Peru
608	Philippines
612	Pitcairn
616	Poland
620	Portugal
630	Puerto Rico
634	Qatar
638	Reunion Réunion
642	Romania
643	Russian Federation
646	Rwanda
652	Saint Barthélemy
654	Saint Helena
659	Saint Kitts and Nevis
662	Saint Lucia
663	Saint Martin (French part)
666	Saint Pierre and Miquelon
670	Saint Vincent and the Grenadines
882	Samoa
674	San Marino
678	Sao Tome and Principe
682	Saudi Arabia
686	Senegal
688	Serbia
690	Seychelles
694	Sierra Leone
702	Singapore
703	Slovakia
705	Slovenia
90	Solomon Islands
706	Somalia
710	South Africa
239	South Georgia and the South Sandwich Islands
724	Spain
144	Sri Lanka
736	Sudan
740	Suriname
744	Svalbard and Jan Mayen
748	Swaziland
752	Sweden

ISO Code	Country
756	Switzerland
760	Syrian Arab Republic
158	Taiwan, Province of China
762	Tajikistan
834	Tanzania, United Republic of
764	Thailand
626	Timor-Leste
768	Togo
772	Tokelau
776	Tonga
780	Trinidad and Tobago
788	Tunisia
792	Turkey
795	Turkmenistan
796	Turks and Caicos Islands
798	Tuvalu
800	Uganda
804	Ukraine
784	United Arab Emirates
581	United States Minor Outlying Islands
858	Uruguay
860	Uzbekistan
548	Vanuatu
862	Venezuela
704	Viet Nam
92	Virgin Islands, British
850	Virgin Islands, U.S.
876	Wallis and Futuna
732	Western Sahara
887	Yemen
894	Zambia
716	Zimbabwe

Appendix 7: Currency (ISO 4217) Codes

ISO Code	Currency
826	Pound Sterling
840	US Dollar
978	Euro
971	Afghani
12	Algerian Dinar
32	Argentine Peso
51	Armenian Dram
533	Aruban Guilder
36	Australian Dollar
944	Azerbaijanian Manat
44	Bahamian Dollar
48	Bahraini Dinar
764	Baht
590	Balboa
50	Bangladeshi Taka
52	Barbados Dollar
974	Belarusian Ruble
84	Belize Dollar
60	Bermudian Dollar
984	Bolivian Mvdol (Funds code)
68	Boliviano
986	Brazilian Real
96	Brunei Dollar
975	Bulgarian Lev
108	Burundian Franc
124	Canadian Dollar
132	Cape Verde Escudo
136	Cayman Islands Dollar
288	Cedi
952	CFA Franc BCEAO
950	CFA Franc BEAC
953	CFP franc
152	Chilean Peso
963	Code reserved for testing purposes
170	Colombian Peso
174	Comoro Franc
977	Convertible Marks
558	Cordoba Oro
188	Costa Rican Colon
191	Croatian Kuna
192	Cuban Peso
196	Cyprus Pound
203	Czech Koruna
270	Dalasi
208	Danish Krone
807	Denar
262	Djibouti Franc
678	Dobra
214	Dominican Peso
951	East Caribbean Dollar
818	Egyptian Pound
230	Ethiopian Birr

takepayments
we make it easy

ISO Code	Currency
955	European Composite Unit (EURCO)
956	European Monetary Unit
958	European Unit of Account 17 (E.U.A.-17)
957	European Unit of Account 9 (E.U.A.-9)
238	Falkland Islands Pound
242	Fiji Dollar
348	Forint
976	Franc Congolais
292	Gibraltar pound
959	Gold (one Troy ounce)
600	Guarani
324	Guinea Franc
328	Guyana Dollar
332	Haiti Gourde
344	Hong Kong Dollar
980	Hryvnia
352	Iceland Krona
356	Indian Rupee
364	Iranian Rial
368	Iraqi Dinar
388	Jamaican Dollar
392	Japanese yen
400	Jordanian Dinar
404	Kenyan Shilling
598	Kina
418	Kip
233	Kroon
414	Kuwaiti Dinar
894	Kwacha
454	Kwacha
973	Kwanza
104	Kyat
981	Lari
428	Latvian Lats
422	Lebanese Pound
8	Lek
340	Lempira
694	Leone
430	Liberian Dollar
434	Libyan Dinar
748	Lilangeni
440	Lithuanian Litas
426	Loti
969	Malagasy Ariary
458	Malaysian Ringgit
470	Maltese Lira
795	Manat
480	Mauritius Rupee
943	Metical
484	Mexican Peso
979	Mexican Unidad de Inversion (UDI)
498	Moldovan Leu
504	Moroccan Dirham
566	Naira

ISO Code	Currency
232	Nakfa
516	Namibian Dollar
524	Nepalese Rupee
532	Netherlands Antillian Guilder
376	New Israeli Shekel
901	New Taiwan Dollar
949	New Turkish Lira
554	New Zealand Dollar
64	Ngultrum
999	No currency
408	North Korean Won
578	Norwegian Krone
604	Nuevo Sol
478	Ouguiya
776	Pa'anga
586	Pakistan Rupee
964	Palladium (one Troy ounce)
446	Pataca
858	Peso Uruguayo
608	Philippine Peso
962	Platinum (one Troy ounce)
72	Pula
634	Qatari Rial
320	Quetzal
512	Rial Omani
116	Riel
642	Romanian Leu
946	Romanian New Leu
462	Rufiyaa
360	Rupiah
643	Russian Ruble
646	Rwanda Franc
654	Saint Helena Pound
882	Samoan Tala
682	Saudi Riyal
941	Serbian Dinar
690	Seychelles Rupee
961	Silver (one Troy ounce)
702	Singapore Dollar
703	Slovak Koruna
90	Solomon Islands Dollar
417	Som
706	Somali Shilling
972	Somoni
710	South African Rand
410	South Korean Won
960	Special Drawing Rights
144	Sri Lanka Rupee
938	Sudanese Pound
968	Surinam Dollar
752	Swedish Krona
756	Swiss Franc
760	Syrian Pound
834	Tanzanian Shilling

ISO Code	Currency
398	Tenge
780	Trinidad and Tobago Dollar
496	Tugrik
788	Tunisian Dinar
800	Uganda Shilling
970	Unidad de Valor Real
990	Unidades de formento
784	United Arab Emirates dirham
860	Uzbekistan Som
548	Vatu
862	Venezuelan bolívar
704	Vietnamese đồng
947	WIR Euro
948	WIR Franc
886	Yemeni Rial
156	Yuan Renminbi
716	Zimbabwe Dollar
985	Zloty
997	No currency
998	No currency