DirectLink

Integration Guide for the Server-to-Server Solution v.4.3.3

Table of Contents

1 How Does DirectLink Work?

DirectLink allows you to set up customised links between your applications and our system, as if our system were simply a local server. It provides programme to programme (server to server) access between the merchant's software and our payment and administration functions. The merchant's programme interacts directly with our remote API without human intervention.

Using DirectLink, there is no contact between our system and the merchant's customer. The merchant transmits all the information required to make the payment directly to our system in an HTTPS POST request. Our system requests the financial transaction (synchronously or asynchronously) to the relevant acquirer and returns the response to the merchant in XML format. The merchant's programme reads the response and resumes its processing.

The merchant is therefore responsible for collecting and storing his customer's confidential payment details. He must guarantee the confidentiality and security of these details by means of encrypted web communication and server security. If the merchant does not want to store sensitive information such as card numbers, we recommend using the Alias option in his account (please refer to the Alias Manager integration guide for more information).

The merchant can process new orders, perform maintenance on existing orders and query the status of an order using DirectLink.

Even if the merchant has automated requests with DirectLink, he can consult the history of the transaction manually in the back office, using his web browser or a report download. For the configuration and functionality of the administration site, please refer to the Back-Office User Guide.

2 General Procedures and Security Settings

> Important
>
> The following general procedures and security controls are valid for all DirectLink requests: new order requests, maintenance requests and direct queries.

2.1 Request form

For new order requests, maintenance requests and direct queries, the merchant must send requests with certain parameters to specific URLs. The payment/maintenance/query parameters must be sent in a POST request as follows:

PSPID=value1&USERID=value2&PSWD=value3&...

The type/subtype indicating the Media Type in the Content-Type entity-header field in the POST request needs to be "application/x-www-form-urlencoded".

DirectLink works in “one request-one reply” mode, each payment is processed individually. Our system handles individual transaction requests via DirectLink and can work synchronously (where this option is technically supported), i.e. we wait for the bank’s reply before returning an XML response to the request.

2.2 Security

When we receive a request on our servers, we check the level of encryption and the IP address which the request was sent from.

2.2.1 Encryption

DirectLink is built on a robust, secure communication protocol. DirectLink API is a set of instructions submitted with standard HTTPS POST requests.

At the server end, we use a certificate delivered by Verisign. The TLS encryption guarantees that it is our servers you are communicating with and that your data is transmitted in encrypted form. There is no need for a client TLS certificate.

When we receive a request, we check the level of encryption. We allow merchants to connect to us only in secure https mode using TLS protocols and we strongly recommend to use the most recent and secure versions which are currently TLS 1.1 and 1.2.

Note: At the time of writing we still support SSL v3. However, because of certain vulnerabilities (cf. POODLE), this protocol is being phased out and will eventually not be supported anymore.

2.2.2 IP address

For each request, our system checks the IP address from which the request originates to ensure the requests are being sent from the merchant’s server. In the IP address field of the "Data and origin verification" tab, in the "Checks for DirectLink" section of the Technical Information page of your account you must enter the IP address(es) or IP address range(s) of the servers that send your requests.

If the IP address from which the request originates has not been declared in the IP address field of the "Data and origin verification" tab, checks for DirectLink section of the Technical Information page in your account, you will receive the error message *“unknown order/1/i”*. The IP address the request was sent from will also be displayed in the error message.

2.3 Response parsing

We will return an XML response to your request. Please ensure that your systems parse this XML response as tolerantly as possible to avoid issues in the future, e.g. avoid case-sensitive attribute names, do not prescribe a specific order for the attributes returned in responses, ensure that new attributes in the response will not cause issues, etc.

3 Request a New Order

3.1 Order request

3.1.1 Request URL

The request URL in the TEST environment is https://mdepayments.epdq.co.uk/ncol/test/orderdirect.asp.

The request URL in the PRODUCTION environment is https://payments.epdq.co.uk/ncol/prod/orderdirect.asp.

> Important
>
> Do not forget to replace “test” with “prod” in the request URL when you switch to your PRODUCTION account. If you forget to change the request URL, once you start in production with real orders, your transactions will be sent to the test environment and will not be sent to the acquirers/banks.

3.1.2 Request parameters

The following table contains the request parameters for sending a new order:

Parameter (* = Mandatory)	Usage
PSPID*	Your affiliation name in our system.
ORDERID*	Your unique order number (merchant reference).
USERID*	Name of your application (API) user. Please refer to the User Manager documentation for information on how to create an API user.
PSWD*	Password of the API user (USERID).
AMOUNT*	Amount to be paid MULTIPLIED BY 100, as the format of the amount must not contain any decimals or other separators.
CURRENCY*	ISO alpha order currency code, for example: EUR, USD, GBP, CHF, etc.
CARDNO*	Card/account number.
ED*	Expiry date (MM/YY or MMYY).
COM	Order description.
CN	Customer name.
EMAIL	Customer’s email address.
SHASIGN	Signature (hashed string) to authenticate the data (see section 3.5).
CVC*	Card Verification Code. Depending on the card brand, the verification code will be a 3- or 4-digit

Parameter (* = Mandatory)	Usage
	code on the front or rear of the card, an issue number, a start date or a date of birth.
ECOM_PAYMENT_CARD_VERIFICATION	Alternative to CVC: date of birth / issue number / etc. (depending on country/bank)
OWNERADDRESS	Customer's street name and number.
OWNERZIP	Customer's postcode.
OWNERTOWN	Customer's town/city name.
OWNERCTY	Customer's country, e.g. BE, NL, FR, etc.
OWNERTELNO	Customer's telephone number.
OPERATION *(not strictly required, but strongly recommended)*	Defines the type of requested transaction. You can configure a default operation (payment procedure) in the "Global transaction parameters" tab, "Default operation code" section of the Technical Information page. When you send an operation value in the request, this will overwrite the default value. Possible values: ▪ RES: request for authorisation ▪ SAL: request for direct sale ▪ RFD: refund, not linked to a previous payment, so not a maintenance operation on an existing transaction (you can not use this operation without specific permission from your acquirer). Optional: • PAU: Request for pre-authorisation: In agreement with your acquirer, and once enabled in your ePDQ account, you can use this operation code to temporarily reserve funds on a customer's card. This is a common practice in the travel and rental industry. PAU/pre-authorisation can currently only be used on MasterCard transactions and is supported by selected acquirers. This operation code cannot be set as the default in your ePDQ account. Should you use PAU on transactions via acquirers or with card brands that don't support pre-authorisation, these transactions will not be blocked but processed as normal (RES) authorisations.
WITHROOT	Adds a root element to our XML response. Possible values: 'Y' or empty.
REMOTE_ADDR	Customer's IP address (for Fraud Detection Module only). If a country check does not need to be performed on the IP address, send 'NONE'.

Parameter (* = Mandatory)	Usage
RTIMEOUT	Request timeout for the transaction (in seconds, value between 30 and 90) IMPORTANT: The value you set here must be smaller than the timeout value in your system!
ECI	Electronic Commerce Indicator. You can configure a default ECI value in the "Global transaction parameters" tab, "Default ECI value" section of the Technical Information page. When you send an ECI value in the request, this will overwrite the default ECI value. Possible (numeric) values: 0 - Swiped 1 - Manually keyed (MOTO) (card not present) 2 - Recurring (from MOTO) 3 - Instalment payments 4 - Manually keyed, card present 7 - E-commerce with SSL encryption 9 - Recurring (from e-commerce)

More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

➢ If your business falls under the Merchant Category Code (MCC) 6012, please find extra info and parameters in the Appendix here.

The list of possible parameters to send can be longer for merchants who have activated certain options/functionalities in their accounts. Please refer to the respective option documentation for more information on extra parameters linked to the option.

The following request parameters are mandatory in new orders:

- PSPID and USERID
- PSWD
- ORDERID
- AMOUNT (x 100)
- CURRENCY
- CARDNO
- ED
- CVC
- OPERATION

3.1.3 Test page

A test page for an order request can be found at https://mdepayments.epdq.co.uk/ncol/test/testodl.asp.

3.1.4 Excluding specific payment methods

If there are payment methods you don't want a customer to be able to pay with, you can use a parameter to do so.
This is particularly useful for sub-brands, when you want to accept a brand (e.g. MasterCard) but not one of its sub-brands (e.g. Maestro)

The parameter is the following:

Field	Usage
EXCLPMLIST	List of payment methods and/or credit card brands that should NOT be used, separated by a ";" (semicolon).

More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

If a customer tries paying with a card linked to a payment method and/or (sub)brand you've excluded using the EXCLPMLIST parameter, the error message "Card number incorrect or incompatible" will be returned with the NCERRORPLUS return field.

3.1.5 Split credit/debit cards

The functionality to split VISA and MasterCard into a debit and a credit payment method allows you to offer them to your customers as two different payment methods (e.g. VISA Debit and VISA Credit), or you can decide only to accept one of both split brands.

To use the split of credit and debit cards via DirectLink, you need to include the CREDITDEBIT parameter in the hidden fields you send to the orderdirect.asp page.

Parameter	Format
CREDITDEBIT	"C": credit card "D": debit card

This field has to be included in the SHA-IN calculation

Related error: When the buyer selects the debit card method but next enters a credit card number, an error code will be returned: 'Wrong brand/Payment method was chosen'

If the payment is successfully processed with the CREDITDEBIT parameter, the same parameter will also be returned in the XML response, and/or can be requested with a Direct Query. However, whereas the submitted values are C or D, the return values are "CREDIT" or "DEBIT".

You will also find these return values in transaction overview via "View transactions" and "Financial history", and in reports you may download afterwards.

Configuration in your account

The split functionality can be activated and configured per payment method, in your ePDQ account. Check our Split Credit/Debit Cards guide for more information.

3.2 Order request using 3-D Secure

Our system supports the usage of 3-D Secure with DirectLink. For more information about this feature, please see the DirectLink with 3-D Secure integration guide.

Important

- If you wish to use 3-D Secure with DirectLink, you need to have the D3D option activated in your account.
- Some acquiring banks require the use of 3-D Secure. Please check with your acquirer if this is the case for you.

3.3 Order response

Our server returns an XML response to the request:

Example of an XML response to an order request:

```
<?xml version=”1.0”?>
<ncresponse orderID=”99999” PAYID=”1111111” NCSTATUS=”0” NCERROR=””
NCERRORPLUS=”” ACCEPTANCE=”12345” STATUS=”5” ECI=”7” amount="125"
currency="EUR" PM="CreditCard" BRAND="VISA"/>
```

The following table contains a list of default and optional ncresponse tag attributes:

Field	Usage
Returned by default	
NCERROR	Error code.
orderID	Your order reference.
PAYID	Payment reference in our system.
STATUS	Transaction status.
Optionally returned (as per "Dynamic parameters" configuration)	
ACCEPTANCE	Acceptance code returned by acquirer.
amount	Order amount (not multiplied by 100).
BRAND	Card brand or similar information for other payment methods.
currency	Order currency.
ECI	Electronic Commerce Indicator.
NCERRORPLUS	Explanation of the error code.
NCSTATUS	First digit of NCERROR.
PM	Payment method.
> Check for additional return fields in your ePDQ account via Configuration > Technical information > Feedback tab > "Dynamic parameters" (DirectLink section). The list of optional parameters depends on options activated in your account.	

More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

The attribute list may be longer for merchants who have activated certain options (e.g. the Fraud Detection Module) in their accounts. Please refer to the respective option documentation for further information about additional response attributes linked to the option.

3.4 Possible response statuses

Status	NCERROR	NCSTATUS	Explanation
5 Authorised	0	0	The authorisation has been accepted. An authorisation code is available in the field “ACCEPTANCE”. The status will be 5 if you have configured "Authorisation" as default operation code in your

Status	NCERROR	NCSTATUS	Explanation
			Technical Information page or if you send Operation code RES in your transaction request.
9 Payment requested	0	0	The payment has been accepted. An authorisation code is available in the field “ACCEPTANCE”. The status will be 9 if you have configured "Sale" as the default operation code in your Technical Information page or if you have sent Operation code SAL in your transaction request.
0 Invalid or incomplete	500....	5	At least one of the payment data fields is invalid or missing. The NCERROR and NCERRORPLUS fields contains an explanation of the error. After correcting the error, the customer can retry the authorisation process.
2 Authorisation refused	300....	3	The authorisation has been declined by the financial institution. The customer can retry the authorisation process after selecting a different payment method (or card brand).
51 Authorisation waiting	0	0	The authorisation will be processed offline. This is the standard response if you have chosen offline processing in the account configuration. The status will be 51 in two cases: • You have defined “Always offline” in the "Global transaction parameters" tab, "Processing for individual transactions" section of the Technical Information page in your account. • When the online acquiring system is unavailable and you have defined “Online but switch to offline in intervals when the online acquiring system is unavailable” in the "Global transaction parameters" tab, in the "Processing for individual transactions" section of the Technical Information page in your account. You cannot retry the authorisation process because the payment might be accepted offline.
52 Authorisation not known Or 92 Payment uncertain	200...	2	A technical problem arose during the authorisation/ payment process, giving an unpredictable result. The merchant can contact the acquirer helpdesk to establish the precise status of the authorisation/ payment or wait until we have updated the status in our system. The customer should not retry the authorisation process, as the authorisation/payment might already have been accepted.

More information about statuses and error codes can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > User guides > List of the payment statuses and error codes.

3.5 Duplicate request

If you request processing for an already existing (and correctly processed) orderID, our XML response will contain the PAYID corresponding to the existing orderID, the ACCEPTANCE given by the acquirer in the previous processing, STATUS "0" and NCERROR "50001113".

3.6 Additional security: SHA signature

The SHA signature is based on the principle of the merchant's server generating a unique character string for each order, hashed with the SHA-1, SHA-256 or SHA-512 algorithms. The result of this hash is then sent to us in the merchant's order request. Our system reconstructs this signature to check the integrity of the order data sent to us in the request.

This string is constructed by concatenating the values of the fields sent with the order (sorted alphabetically, in the 'parameter=value' format), with each parameter and value followed by a passphrase. The passphrase is defined in the merchant's *Technical information*, under the "Data and Origin Verification" tab, in the "Checks for DirectLink" section. For the full list of parameters to include in the SHA Digest, please refer to Appendix 4. Please note that these values are all case-sensitive when compiled to form the string before the hash!

Important

- All parameters that you send (and that appear in the list in List of Parameters to be included in SHA IN Calculation), will be included in the string to hash.
- All parameter names should be in UPPERCASE (to avoid any case confusion)
- Parameters need to be sorted alphabetically
- Parameters that do not have a value should NOT be included in the string to hash
- When you choose to transfer your test account to production via the link in the account menu, a random SHA-IN passphrase will be automatically configured in your production account.
- For extra safety, we request that you use different SHA passwords for TEST and PROD. Please note that if they are found to be identical, your TEST passphrase will be changed by our system (you will of course be notified).

When you hash the string composed with the SHA algorithm, a hexadecimal digest will be returned The length of the SHA Digest is 40 characters for SHA-1, 64 for SHA-256 and 128 for SHA-512. This result should be sent to our system in your order request, using the "SHASign" field.

Our system will recompose the SHA string based on the received parameters and compare the Merchant's Digest with our generated Digest. If the result is not identical, the order will be declined. This check guarantees the accuracy and integrity of the order data.

You can test your SHASIGN here.

Example of a SHA-1-IN calculation with only basic parameters

Parameters (in alphabetical order)
AMOUNT: 15.00 -> 1500
CARDNO: 4111111111111111
CURRENCY: EUR
OPERATION: RES
ORDERID: 1234
PSPID: MyPSPID

SHA Passphrase (In technical info)
Mysecretsig1875!?

String to hash

AMOUNT=1500Mysecretsig1875!?CARDNO=4111111111111111Mysecretsig1875!?
CURRENCY=EURMysecretsig1875!?OPERATION=RESMysecretsig1875!?
ORDERID=1234Mysecretsig1875!?PSPID=MyPSPIDMysecretsig1875!?

Resulting Digest (SHA-1)
2B459D4D3AF0C678695AE77EE5BF0C83CA6F0AD8

If the SHASIGN sent in your request does not match the SHASIGN which we derived using the details of the order and the passphrase entered in the SHA-IN Signature field in the "Data and origin verification" tab, checks for DirectLink section of the Technical Information page, you will receive the error message *"unknown order/1/s".*

If the "SHASIGN" field in your request is empty but a passphrase has been entered in the SHA-IN Signature field in the "Data and origin verification" tab, checks for DirectLink section of the Technical Information page (indicating you want to use a SHA signature with each transaction), you will receive the error message *"unknown order/0/s".*

4 Direct Maintenance: Maintenance on Existing Orders

A direct maintenance request from your application allows you to: perform a data capture (payment) of an authorised order automatically (as opposed to manually in the back office); cancel an authorisation on an order; renew an authorisation of an order; or refund a paid order.

Data captures, authorisation cancellations and authorisation renewals are specifically for merchants who have configured their account/requests to perform the authorisation and the data capture in two stages.

4.1 Maintenance request

4.1.1 Request URL

The request URL in the TEST environment is https://mdepayments.epdq.co.uk/ncol/test/maintenancedirect.asp.

The request URL in the PRODUCTION environment is https://payments.epdq.co.uk/ncol/prod/maintenancedirect.asp.

> Important
>
> Do not forget to replace “test” with “prod” in the request URL when you switch to your PRODUCTION account. If you forget to change the request URL, once you start working with real orders, your maintenance transactions will be sent to the test environment and will not be sent to the acquirers/banks.

4.1.2 Request parameters

The following table contains the mandatory request parameters for performing a maintenance operation:

Field	Usage
AMOUNT	Order amount multiplied by 100. This is only required when the amount of the maintenance differs from the amount of the original authorisation. However, we recommend its use in all cases. Our system will check that the maintenance transaction amount is not higher than the authorisation/payment amount.
OPERATION	Possible values: ▪ REN: renewal of authorisation, if the original authorisation is no longer valid. ▪ DEL: delete authorisation, leaving the transaction open for further potential maintenance operations. ▪ DES: delete authorisation, closing the transaction after this operation. ▪ SAL: partial data capture (payment), leaving the transaction open for another potential data capture. ▪ SAS: (last) partial or full data capture (payment), closing the transaction (for further data captures) after this data capture. ▪ RFD: partial refund (on a paid order), leaving the transaction open for another potential refund. ▪ RFS: (last) partial or full refund (on a paid order), closing the transaction after this refund. Please note with DEL and DES that not all acquirers support the deletion of an authorisation. If your acquirer does not support DEL/DES, we will

Field	Usage
	nevertheless simulate the deletion of the authorisation in the back office.
ORDERID	You can send the PAYID or the orderID to identify the original order. We recommend the use of the PAYID.
PAYID	
PSPID	Login details: PSPID and (API) USERID with the USERID's password
PSWD	
USERID	

More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

4.1.3 Test page

An example (test page) of a direct maintenance request can be found at: https://mdepayments.epdq.co.uk/ncol/test/testdm.asp

4.2 Maintenance response

Our server returns an XML response to the request:

Example of an XML response to a direct maintenance request:

```
<?xml version="1.0"?>
<ncresponse orderID="99999" PAYID="1111111" PAYIDSUB="3" NCSTATUS="0"
NCERROR="" NCERRORPLUS="" ACCEPTANCE="12345" STATUS="91" amount="125"
currency="EUR"/>
```

The following table contains a list of the ncresponse tag attributes:

Field	Usage
ACCEPTANCE	Acceptance code returned by acquirer
amount	Order amount (not multiplied by 100)
currency	Order currency
NCERROR	Error code
NCERRORPLUS	Explanation of the error code
NCSTATUS	First digit of NCERROR
orderID	Your order reference
PAYID	Payment reference in our system
PAYIDSUB	The history level ID of the maintenance operation on the PAYID

Field	Usage
STATUS	Transaction status

More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

The standard ncresponse tag attributes are the same as those for the XML reply to a new order, except for the extra attribute PAYIDSUB.

4.3 Possible transaction statuses

The maintenance orders are always processed offline (except for authorisation renewals).

Status	NCERROR	NCSTATUS	Explanation
0 - Invalid or incomplete	500....	5	At least one of the payment data fields is invalid or missing. The NCERROR and NCERRORPLUS fields give an explanation of the error.
91 - Payment processing	0	0	The data capture will be processed offline.
61 - Author. deletion waiting	0	0	The authorisation deletion will be processed offline.
92 - Payment uncertain	200...	2	A technical problem arose during the payment process, giving an unpredictable result. The merchant can contact the acquirer helpdesk to establish the precise status of the payment or wait until we have updated the status in our system. You should not repeat the payment process, as the payment might already have been accepted.
62 - Author. deletion uncertain	200...	2	A technical problem arose during the authorisation deletion process, giving an unpredictable result. The merchant can contact the acquirer helpdesk to establish the precise status of the payment or wait until we have updated the status in our system.
93 - Payment refused	300....	3	A technical problem arose.
63 - Author. deletion refused	300....	3	A technical problem arose.

More information about statuses and error codes can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > User guides > List of the payment statuses and error codes.

4.4 Duplicate request

If maintenance is requested twice for the same order, the second one will theoretically be declined with an error “50001127” (this order is not authorised), because the initial successful transaction will have changed the order status.

5 Direct Query: Querying the Status of an Order

A direct query request from your application allows you to query the status of an order automatically (as opposed to manually in the back office). You can only query one payment at a time, and will only receive a limited amount of information about the order.

If you need more details about the order, you can look up the transaction in the back office or perform a manual or automatic file download (please refer to the Back office User Guide and the Advanced Batch Integration Guide).

5.1 Query request

5.1.1 Request URL

The request URL in the TEST environment is https://mdepayments.epdq.co.uk/ncol/test/querydirect.asp

The request URL in the PRODUCTION environment is https://payments.epdq.co.uk/ncol/prod/querydirect.asp

> Important
>
> Do not forget to replace “test” with “prod” in the request URL when you switch to your PRODUCTION account.

5.1.2 Request parameters

The following table contains the mandatory request parameters to perform a direct query:

Field	Usage
PSPID	Login details: PSPID and (API) USERID with the USERID’s password
USERID	
PSWD	
PAYID	You can send the PAYID or the ORDERID to identify the original order. We recommend the use of the PAYID.
ORDERID	
PAYIDSUB	You can indicate the history level ID if you use the PAYID to identify the original order (optional).

More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

5.1.3 Test page

An example (test page) of a direct query request, can be found at: https://mdepayments.epdq.co.uk/ncol/test/testdq.asp.

5.2 Query response

Our server returns an XML response to the request:

Example of an XML response to a direct query:

```
<?xml version="1.0"?>
<ncresponse orderID="99999" PAYID="1111111" PAYIDSUB="3" NCSTATUS="0"
NCERROR="" NCERRORPLUS="" ACCEPTANCE="12345" STATUS="9" ECI="7" amount="125"
currency="EUR" PM="CreditCard" BRAND="VISA" CARDNO="XXXXXXXXXXXX1111"
IP="212.33.102.55"/>
```

The following table contains a list of the ncresponse tag attributes:

Field	Usage
orderID	Your order reference
PAYID	Payment reference in our system
PAYIDSUB	The history level ID of the maintenance operation on the PAYID
NCSTATUS	First digit of NCERROR
NCERROR	Error code
NCERRORPLUS	Explanation of the error code
ACCEPTANCE	Acceptance code returned by acquirer
STATUS	Transaction status
ECI	Electronic Commerce Indicator
amount	Order amount (not multiplied by 100)
currency	Order currency
PM	Payment method
BRAND	Card brand or similar information for other payment methods
CARDNO	The masked credit card number
IP	Customer's IP address, as detected by our system in a 3-tier integration, or sent to us by the merchant in a 2-tier integration

More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

The standard ncresponse tag attributes are identical to those for the XML reply to a new order, except for the additional attributes PAYIDSUB, CARDNO and IP.

The attribute list may be longer for merchants who have activated certain options (e.g. the Fraud Detection Module) in their accounts. Please refer to the respective option documentation for more information on extra response attributes linked to the option.

5.2.1 Transactions processed with e-Commerce

If the transaction whose status you want to check was processed with e-Commerce, you will also receive the following additional attributes (providing you sent these fields with the original e-Commerce transaction).

Field	Usage
complus	A value you wanted to have returned
(paramplus content)	The parameters and their values you wanted to have returned

For more information, please refer to the Advanced e-Commerce integration guide in the Support section of your account.

Example of an XML response to a direct query for an e-Commerce transaction:

```
<?xml version="1.0"?>
<ncresponse orderID="99999" PAYID="1111111" PAYIDSUB="3" NCSTATUS="0" NCERROR=""
NCERRORPLUS="" ACCEPTANCE="12345" STATUS="9" amount="125" currency="EUR"
PM="CreditCard" BRAND="VISA" CARDNO="XXXXXXXXXXXX1111" IP="212.33.102.55"
COMPLUS="123456789123456789123456789" SessionID="126548354"
ShopperID="73541312"/>
```

5.3 Possible response statuses

The STATUS field will contain the status of the transaction.

More information about statuses and error codes can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > User guides > List of the payment statuses and error codes.

Only the following status is specifically related to the query itself:

Status	NCERROR	NCSTATUS	Explanation
88			The query on querydirect.asp failed

5.4 Direct Query as fallback

The response times for a DirectLink transaction request are generally a few seconds; some acquirers may, however, have longer response times. If you want to install a check mechanism to verify that our system is up and running smoothly, we suggest you set the request timeout in orderdirect.asp to 30 seconds (30-40 for Diners).

If you have not received a response from our system after 30 seconds, you can send a request to querydirect.asp, asking for the status of your most recent transaction sent to orderdirect.asp. If you receive an immediate reply containing a non-final status for the transaction, there might be issues at the acquirer's end.

If you have not received an answer to this direct query request after 10 seconds, there might be issues at our end. You can repeat this request to querydirect.asp every 30 seconds until you see you receive a response within 10 seconds.

Please note:

1. This check system will only be able to pinpoint issues at our end if there is also a check at your end to verify that requests are leaving your servers correctly.

2. An issue at our end will not always necessarily be caused by downtime, but could also be as a result of slow response times due to database issues for example.

3. Please use these checks judiciously to avoid bombarding our servers with requests, otherwise we might have to restrict your access to the querydirect.asp page.

> Important
>
> To protect our system from unnecessary overloads, we prohibit system-up checks which involve sending fake transactions or systematic queries, as well as systematic queries to obtain transaction feedback for each transaction.

6 Appendix: Troubleshooting

The following section contains a non-exhaustive list of possible errors you can find in the NCERRORPLUS field, and in the "Error logs" section in your ePDQ Account:

- *Connection to API feature not allowed for this user*

You have sent us a request with only the PSPID/password or PSPID/administrative user/password as login details. You need to create a special API user to send requests to our server. An API is a user specifically designed so that an application can send automatic requests to the payment platform. Please refer to the User Manager documentation for more information on how to create an API user.

- *unknown order/1/i*

This error means that the IP address from which a request was sent is not an IP address the merchant had entered in the IP address field of the "Data and origin verification" tab, checks for DirectLink section of his Technical Information page. The merchant is sending us a request from a different server from the one(s) entered in the IP address field of the "Data and origin verification" tab, checks for DirectLink section.

- *unknown order/1/s*

This error message means that the SHASIGN sent in your transaction request differs from the SHASIGN calculated at our end using the order details and the additional string (password/ passphrase) entered in the SHA-IN Signature field in the "Data and origin verification" tab, checks for DirectLink section of the Technical Information page.

- *unknown order/0/s*

This error message means that the "SHASIGN" field in your request is empty, but an additional string (password/passphrase) has been entered in the SHA-1-IN Signature field in the "Data and origin verification" tab, "Checks for DirectLink" section of the Technical Information page, indicating you want to use a SHA signature with each transaction.

- *PSPID not found or not active*

This error means that the value you entered in the PSPID field does not exist in the respective environment (test or production) or the account has not yet been activated.

- *no <parameter> (for instance: no PSPID)*

This error means that the value you sent for the obligatory <parameter> field is empty. Note: ORDERID is the first field we check, so if you receive the error “no ORDERID”, it can also mean we did not receive any values at all.

- *<parameter> too long (for instance: CURRENCY too long)*

This error means that the value in your <parameter> field exceeds the maximum length.

- *amount too long or not numeric: ... OR AMOUNT not a number*

This error means that the amount you sent in the hidden fields either exceeds the maximum length or contains invalid characters such as ‘.’ (full stop) or ‘,’ (comma) for example.

- *not a valid currency : ...*

This error means that you sent a transaction with a currency code that is incorrect or does not exist.

- *The currency is not accepted by the merchant*

This error means that you sent a transaction in a currency that has not been registered in your account details.

- *ERROR, PAYMENT METHOD NOT FOUND FOR: ...*

This error means that the PM value you sent in your hidden fields does not match any of the payment methods selected in your account, or that the payment method has not been activated in your payment methods page.

7 Appendix: Visa Additional Authorisation Data

(for ePDQ Essential, ePDQ Extra & ePDQ Extra Plus)

In order to reduce fraud, Visa has introduced additional transaction authorisation fields for any UK merchant defined as a Financial Institution. These fields must be captured during your order preparation and submitted to ePDQ, regardless of whether you have integrated via the Hosted Payment Page (e-Commerce) or DirectLink.

Current fraud detection tools may not give card issuing banks sufficient information to validate transactions in this business sector. With this additional data, issuers will be able to make a more informed decision.

To comply with these new requirements you will need to submit the following additional fields in the authorisation requests you send to ePDQ. If you use the SHA-IN passphrase, these fields will need to be appropriately included in the SHA-IN calculation, as described in the e-Commerce and DirectLink guides.

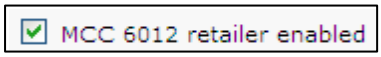
Parameter	Description	Format	Example
RECIPIENTACCOUNTNUMBER	Recipient's account number OR partially masked credit card number	AlphaNum / 10 char. If the number is longer than 10 characters, we only pass the 6 first digits + the last 4 digits.	"12345ABCDZ6789" -> "12345A6789"
RECIPIENTDOB	Recipient's date of birth	DD/MM/YYYY / Num. / 10 char. Division slashes must be entered. Our system will convert the date as follows: YYYYMMDD	"02/03/1982" -> "19820302"
RECIPIENTLASTNAME	Recipient's surname	Alpha / 6 char. If the value is longer than 6 characters, we only pass the 6 first characters.	"Day-O'Reilly" -> "DAYORE"
RECIPIENTZIP	Recipient's postcode	AlphaNum / 6 char. You must only enter the first part of the postcode, up to the space (e.g. 3 or 4 digits).	"MK4 " -> "MK4" "MK46 " -> "MK46"
More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.			

Note

If special characters, other than a space, ' (apostrophe), * (asterisk), $ (dollar sign), / (forward slash) or - (hyphen) are inserted in a field, the whole field content will be emptied automatically when submitted.

When setting up your account, Barclaycard will ensure that it is enabled to support these additional fields. If the fields are not available to you and you believe that this Visa requirement applies to your business, then please contact us at epdqsupport@barclaycard.co.uk.

If enabled, the following flag should be visible in the Visa configuration page of your ePDQ account:



8 Appendix: List of Parameters to be included in SHA IN Calculation

ACCEPTANCE
ACCEPTURL
ADDMATCH
ADDRMATCH
AIACTIONNUMBER
AIAGIATA
AIAIRNAME
AIAIRTAX
AIBOOKIND*XX*
AICARRIER*XX*
AICHDET
AICLASS*XX*
AICONJTI
AIDEPTCODE
AIDESTCITY*XX*
AIDESTCITYL*XX*
AIEXTRAPASNAME*XX*
AIEYCD
AIFLDATE*XX*
AIFLNUM*XX*
AIGLNUM
AIINVOICE
AIIRST
AIORCITY*XX*
AIORCITYL*XX*
AIPASNAME
AIPROJNUM
AISTOPOV*XX*
AITIDATE
AITINUM
AITINUML*XX*
AITYPCH
AIVATAMNT
AIVATAPPL
ALIAS
ALIASOPERATION
ALIASPERSISTEDAFTERUSE
ALIASUSAGE
ALLOWCORRECTION
AMOUNT
AMOUNT*XX*
AMOUNTHTVA
AMOUNTTVA
ARP_TRN
BACKURL

BATCHID
BGCOLOR
BLVERNUM
BIC
BIN
BRAND
BRANDVISUAL
BUTTONBGCOLOR
BUTTONTXTCOLOR
CANCELURL
CARDNO
CATALOGURL
CAVV_3D
CAVVALGORITHM_3D
CERTID
CHECK_AAV
CIVILITY
CN
COM
COMPLUS
CONVCCY
COSTCENTER
COSTCODE
CREDITCODE
CREDITDEBIT
CUID
CURRENCY
CVC
CVCFLAG
DATA
DATATYPE
DATEIN
DATEOUT
DBXML
DCC_COMMPERC
DCC_CONVAMOUNT
DCC_CONVCCY
DCC_EXCHRATE
DCC_EXCHRATETS
DCC_INDICATOR
DCC_MARGINPERC
DCC_REF
DCC_SOURCE
DCC_VALID
DECLINEURL
DELIVERYDATE
DEVICE
DISCOUNTRATE

DISPLAYMODE
ECI
ECI_3D
ECOM_BILLTO_COMPANY
ECOM_BILLTO_POSTAL_CITY
ECOM_BILLTO_POSTAL_COUNTRYCODE
ECOM_BILLTO_POSTAL_COUNTY
ECOM_BILLTO_POSTAL_NAME_FIRST
ECOM_BILLTO_POSTAL_NAME_LAST
ECOM_BILLTO_POSTAL_NAME_PREFIX
ECOM_BILLTO_POSTAL_POSTALCODE
ECOM_BILLTO_POSTAL_STREET_LINE1
ECOM_BILLTO_POSTAL_STREET_LINE2
ECOM_BILLTO_POSTAL_STREET_LINE3
ECOM_BILLTO_POSTAL_STREET_NUMBER
ECOM_BILLTO_TELECOM_MOBILE_NUMBER
ECOM_BILLTO_TELECOM_PHONE_NUMBER
ECOM_CONSUMERID
ECOM_CONSUMER_GENDER
ECOM_CONSUMEROGID
ECOM_CONSUMERORDERID
ECOM_CONSUMERUSERALIAS
ECOM_CONSUMERUSERPWD
ECOM_CONSUMERUSERID
ECOM_ESTIMATEDDELIVERYDATE
ECOM_ESTIMATEDELIVERYDATE
ECOM_PAYMENT_CARD_EXPDATE_MONTH
ECOM_PAYMENT_CARD_EXPDATE_YEAR
ECOM_PAYMENT_CARD_NAME
ECOM_PAYMENT_CARD_VERIFICATION
ECOM_SHIPMETHOD
ECOM_SHIPMETHODDETAILS
ECOM_SHIPMETHODSPEED
ECOM_SHIPMETHODTYPE
ECOM_SHIPTO_COMPANY
ECOM_SHIPTO_DOB
ECOM_SHIPTO_ONLINE_EMAIL
ECOM_SHIPTO_POSTAL_CITY
ECOM_SHIPTO_POSTAL_COUNTRYCODE
ECOM_SHIPTO_POSTAL_COUNTY
ECOM_SHIPTO_POSTAL_NAME_FIRST
ECOM_SHIPTO_POSTAL_NAME_LAST
ECOM_SHIPTO_POSTAL_NAME_PREFIX
ECOM_SHIPTO_POSTAL_POSTALCODE
ECOM_SHIPTO_POSTAL_STATE
ECOM_SHIPTO_POSTAL_STREET_LINE1
ECOM_SHIPTO_POSTAL_STREET_LINE2
ECOM_SHIPTO_POSTAL_STREET_NUMBER

ECOM_SHIPTO_TELECOM_FAX_NUMBER
ECOM_SHIPTO_TELECOM_MOBILE_NUMBER
ECOM_SHIPTO_TELECOM_PHONE_NUMBER
ECOM_SHIPTO_TVA
ED
EMAIL
EXCEPTIONURL
EXCLPMLIST
EXECUTIONDATE*XX*
FACEXCL*XX*
FACTOTAL*XX*
FIRSTCALL
FLAG3D
FONTTYPE
FORCECODE1
FORCECODE2
FORCECODEHASH
FORCEPROCESS
FORCETP
FP_ACTIV
GENERIC_BL
GIROPAY_ACCOUNT_NUMBER
GIROPAY_BLZ
GIROPAY_OWNER_NAME
GLOBORDERID
GUID
HDFONTTYPE
HDTBLBGCOLOR
HDTBLTXTCOLOR
HEIGHTFRAME
HOMEURL
HTTP_ACCEPT
HTTP_USER_AGENT
INCLUDE_BIN
INCLUDE_COUNTRIES
INITIAL_REC_TRN
INVDATE
INVDISCOUNT
INVLEVEL
INVORDERID
ISSUERID
IST_MOBILE
ITEM_COUNT
ITEMATTRIBUTES*XX*
ITEMCATEGORY*XX*
ITEMCOMMENTS*XX*
ITEMDESC*XX*
ITEMDISCOUNT*XX*

ITEMFDMPRODUCTCATEG*XX*
ITEMID*XX*
ITEMNAME*XX*
ITEMPRICE*XX*
ITEMQUANT*XX*
ITEMQUANTORIG*XX*
ITEMUNITOFMEASURE*XX*
ITEMVAT*XX*
ITEMVATCODE*XX*
ITEMWEIGHT*XX*
LANGUAGE
LEVEL1AUTHCPC
LIDEXCL*XX*
LIMITCLIENTSCRIPTUSAGE
LINE_REF
LINE_REF1
LINE_REF2
LINE_REF3
LINE_REF4
LINE_REF5
LINE_REF6
LIST_BIN
LIST_COUNTRIES
LOGO
MANDATEID
MAXITEMQUANT*XX*
MERCHANTID
MODE
MTIME
MVER
NETAMOUNT
OPERATION
ORDERID
ORDERSHIPCOST
ORDERSHIPMETH
ORDERSHIPTAX
ORDERSHIPTAXCODE
ORIG
OR_INVORDERID
OR_ORDERID
OWNERADDRESS
OWNERADDRESS2
OWNERCTY
OWNERTELNO
OWNERTELNO2
OWNERTOWN
OWNERZIP
PAIDAMOUNT

PARAMPLUS
PARAMVAR
PAYID
PAYMETHOD
PM
PMLIST
PMLISTPMLISTTYPE
PMLISTTYPE
PMLISTTYPEPMLIST
PMTYPE
POPUP
POST
PSPID
PSWD
RECIPIENTACCOUNTNUMBER
RECIPIENTDOB
RECIPIENTLASTNAME
RECIPIENTZIP
REF
REFER
REFID
REFKIND
REF_CUSTOMERID
REF_CUSTOMERREF
REGISTRED
REMOTE_ADDR
REQGENFIELDS
RNPOFFERT
RTIMEOUT
RTIMEOUTREQUESTEDTIMEOUT
SCORINGCLIENT
SEQUENCETYPE
SETT_BATCH
SID
SIGNDATE
STATUS_3D
SUBSCRIPTION_ID
SUB_AM
SUB_AMOUNT
SUB_COM
SUB_COMMENT
SUB_CUR
SUB_ENDDATE
SUB_ORDERID
SUB_PERIOD_MOMENT
SUB_PERIOD_MOMENT_M
SUB_PERIOD_MOMENT_WW
SUB_PERIOD_NUMBER

SUB_PERIOD_NUMBER_D
SUB_PERIOD_NUMBER_M
SUB_PERIOD_NUMBER_WW
SUB_PERIOD_UNIT
SUB_STARTDATE
SUB_STATUS
TAAL
TAXINCLUDED*XX*
TBLBGCOLOR
TBLTXTCOLOR
TID
TITLE
TOTALAMOUNT
TP
TRACK2
TXTBADDR2
TXTCOLOR
TXTOKEN
TXTOKENTXTOKENPAYPAL
TXSHIPPING
TXSHIPPINGLOCATIONPROFILE
TXURL
TXVERIFIER
TYPE_COUNTRY
UCAF_AUTHENTICATION_DATA
UCAF_PAYMENT_CARD_CVC2
UCAF_PAYMENT_CARD_EXPDATE_MONTH
UCAF_PAYMENT_CARD_EXPDATE_YEAR
UCAF_PAYMENT_CARD_NUMBER
USERID
USERTYPE
VERSION
WBTU_MSISDN
WBTU_ORDERID
WEIGHTUNIT
WIN3DS
WITHROOT