iPOS

Credit Card Payment Gateway

INTEGRATION PROCEDURES AND SPECIFICATIONS

Revision 7

Contents

Introduction

In this document we describe the process required to connect your web site or e-commerce store to the Digital Age Technologies payment gateway (iPOS). We also describe the flow of a typical transaction through the relevant pages on DAT's secure payment site back to your web site. The technical section describes the requirements in detail and will require some basic HTML coding knowledge in order to implement. However, this is a relatively simple operation and does not require extensive knowledge or experience in order to implement.

Our Client Admin website provides you with an online interface to query your transactions, refund, process manual payments and to generally manage and configure your solution. This system is provided to simplify administration and to allow you, the client, to have all the relevant details at your fingertips in one integrated package, without the need for you own backend systems.

iPOS – the simple online credit card solution

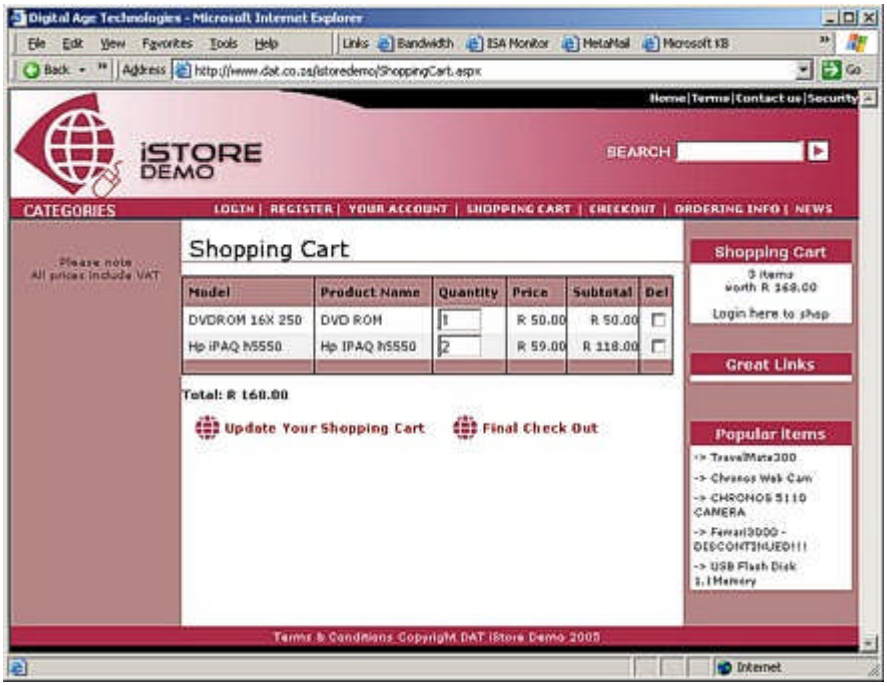
iPOS is the perfect Internet Point-Of-Sale device for your online e-commerce store or web presence. With its real-time processing capabilities, your transactions are instantly authorised through the banking networks and the money made available to you. In a matter of seconds, you can collect money from your clients or business partners and know instantly whether it was successful or not.

Our payment gateway forwards the transaction details to the banking networks on your behalf, and they in turn, respond with the necessary authorisations. Once a transaction has been authorised, the money is reserved on the card holder's account until it is either cancelled or settled. If the transaction is settled, the money is transferred to the merchant's account.

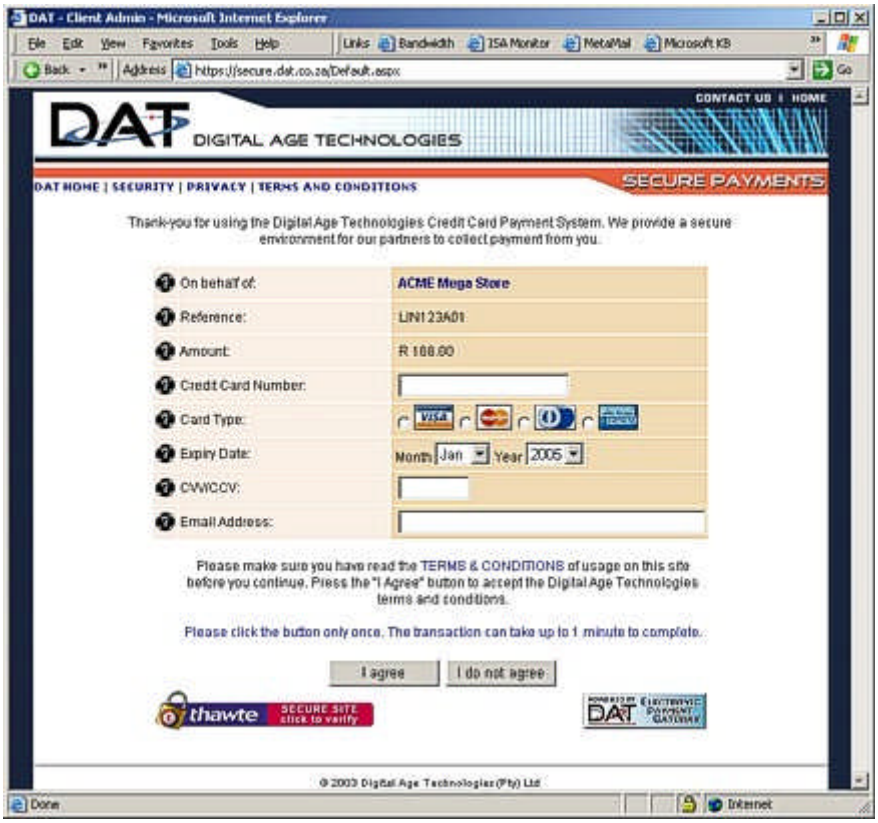
IPOS performs in a similar way to a normal physical Point-Of-Sale device that is used over the counter by businesses everywhere. However, instead of swiping your card and signing the receipt, your card details are filled in on our secure payment page and you acknowledge your intention to process a transaction on your card by clicking on a button and agreeing to the Terms and Conditions.

The Transaction Flow

In a typical transaction, a client browsing online will place an order with the merchant of the website he/she is visiting. This is generally achieved through the use of a virtual shopping basket that collects together the details of the items that the client wishes to purchase. These items will have such information as Unit Price and Quantity. The basket will sum up the amounts of each item and add the relevant taxes and shipping costs to the order. Once complete, the total amount payable is ready to be sent for processing through a credit card capture system. This procedure is called a “checkout”, and most shopping basket systems use a similar method.

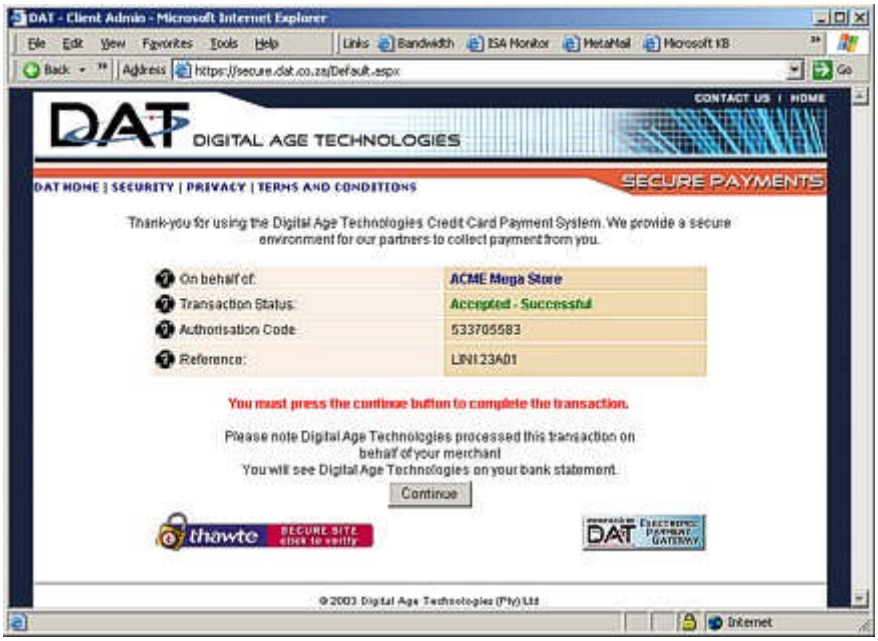


The checkout procedure redirects the client to our **secure*** credit card collection page where they will type in their credit card details. Also displayed on this page is the name of the merchant or person that is being paid, the amount of the transaction and a unique reference number that identifies this particular transaction for later queries. We also collect an e-mail address from the client that is only used for the purposes of verifying and/or authenticating the validity of the transaction, if it is needed.

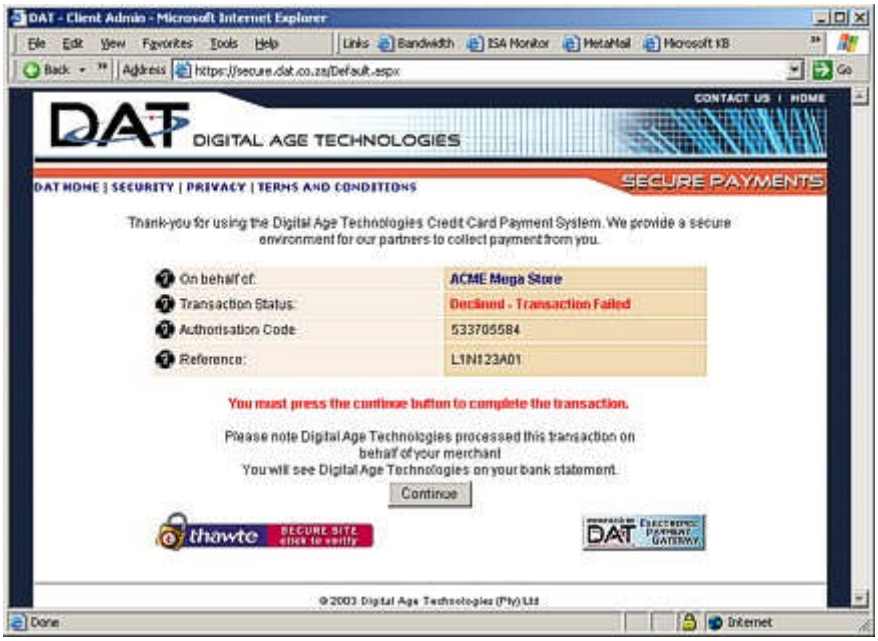


**** [This web page is secured by a digital certificate that uses 128 bit encryption to encrypt all communications between the client and the payment gateway. This protects the client's card details and other personal information while the payment is being processed. See the section on Security for more information.] ****

Once the credit card details have been filled in and the customer has agreed to the Terms and Conditions by pressing the "I Agree" button, the transaction is processed and a results page appears.



This shows that the transaction was processed and was successful. Should there be an error, or should the transaction be declined for any reason, the following result page will be displayed:

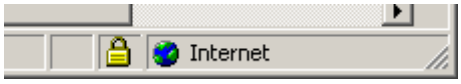


No matter what the result of the transaction, once the client clicks on the “Continue” button, they will be redirected back to your site (to the URL of your choosing).

Security

The DAT credit card collection page is protected by a Thawte digital certificate that uses 128 bit encryption to encrypt all communications between the client's browser and the payment gateway. This prevents the client's card details and other personal information from being intercepted or viewed while the payment is being processed. This is an extremely important and necessary precaution that we have implemented due to the ever-increasing risk of cyber fraud. You should never submit credit card information across the Internet unless the page you are filling in is protected by such a mechanism. ALWAYS CHECK FOR THE USE OF A CERTIFICATE.

It is an easy matter to ascertain whether or not a certificate is being used. The first indication is a lock icon that appears on the bottom right of the browser. This indicates that the browser session is now being "secured" via the use of a digital certificate. If you double-click on the lock icon, you will see a window appear that provides the details of the particular certificate in use.



The second indication of secured page is the use of the HTTPS (HTTP Secure) channel which shows up in the address (or URL) of the browser window as:

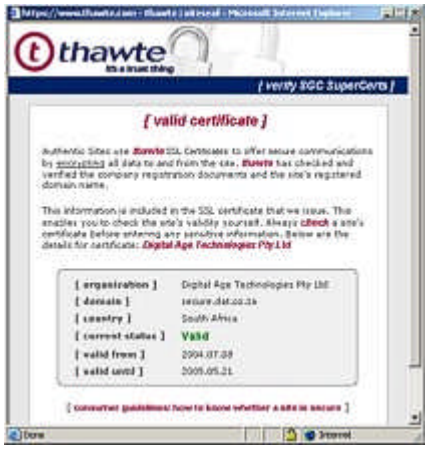
https://www... (note the "s" that is present after the "http")

Rather than the normal:

http://www...

We also provide additional clues to advertise our security features, such as the Thawte Secure Site seal that is displayed on the lower left of the credit card collection page as well as other pages within the DAT system.

If you click on this seal, the details of the digital certificate will be displayed:



Technical Information

There are two general ways in which the secure credit card collection facility can be used. The first is after the checkout procedure, initiated from the shopping basket, and the second is from a “Buy Now” type button for each product that calls the payment page directly. There are benefits to using a shopping basket, such as the totalling of item costs, taxes and shipping costs for multiple items. Without the shopping basket products can generally only be sold one at a time, but that might suit certain vendors who only have a small number of products. In this case, a single “Buy Now” button for each product can be used.

(If you would like more information on the DAT shopping basket facility, which is already fully integrated with our payment gateway, please call us on (011) 807-7550, or e-mail us at sales@dat.co.za.)

Both methods however, rely on the same mechanism to call the credit card collection page. This is achieved through the use of an HTML FORM submitted via an HTTP POST (see the sample form as an example).

Submit Values

The DAT credit card collection page can be found at:

https://secure.dat.co.za/default.aspx

Please note that this page cannot be called or viewed without parameters. For a full list of available parameters (fields) see the table below:

FORM INPUT PARAMETERS:

Field Name	Data Type	Description	Optional
CID	String(8)	Client ID, a unique ID given to you by DAT for processing your payments.	NO
BID	Integer	Branch ID for departmental accounting only.	YES (default is “1” if not specified)
Amount	Double	The total amount to be collected from the credit card in South African Rands. (Minimum R10.00)	YES (but only if Donate = “1”)
DisplayAmount	String	The value (including currency symbol) to display on the page regardless of the actual amount being passed in using the “Amount” field, e.g.: “$5.50”	YES
Donate	Boolean	Allow the client to specify the amount. If this field is set to “1” then the Amount field is displayed in an editable input box that the client can fill in or alter.	YES
Ref	String(17)	A unique reference for a transaction. Please use a string of the form "CIDxxxxxxx", where CID is your Client ID given to you by DAT and xxxxxxx is any other string or number sequence.	YES (A date/time stamp will be used if not specified.
Email	String	Default value for the e-mail field on the collection screen. If this is set, the “Email” input box on the collection page is not editable.	YES
SuccessURL	String	The address (URL) to return to after a successful transaction has been processed.	YES

FailureURL	String	The address (URL) to return to after a failed transaction has been processed.	YES
Budget	Boolean	Allow budget payments. If this field is set to “1” then you are able to select a budget payment period. (South African issued cards only).	YES
Basket	Boolean	iBasket clients only. If this field is set to “1” then the transaction is flagged as a basket transaction and the first return URL is an auto-generated invoice page.	YES

Here is an example of a FORM that can be used to call the credit card collection page:

Sample Form:

```
<form action=”https://secure.dat.co.za/default.aspx” method=”post”>
        <input type=”hidden” name=”CID” value=”DATPOS”>
        <input type=”hidden” name=”Ref” value=”TST1045”>
        <input type=”hidden” name=”Amount” value=”123.45”>
        <input type=”hidden” name=”SuccessURL” value=”http://www.domain.co.za/success.htm”>
        <input type=”hidden” name=”FailureURL” value=”http://www.domain.co.za/failure.htm”>
        <input type=”Submit” value=”Buy Now” name=”submit”>
</form>
```

NOTE: The value and name of the submit button are arbitrary.

There are other parameters that could be used in this FORM but this represents a typical grouping of options that is used by most merchants. Having a valid CID is compulsory and generally the Amount field must also be set, unless you specifically want the client to be able to change the amount themselves during the payment process, in which case you can add the additional Donate parameter and set its value to “1”.

The SuccessURL and FailureURL parameters are important if you wish to redirect the client back to your site after processing their payment. These parameters configure the “Continue” button (on the payment result page) to redirect the client to the URL specified. This is important if your purchase process continues after the payment has been made. Most often these URLs are just information pages that confirm the status of the client’s order and perhaps outline additional shipping policies or contact details.

Return Values

Along with redirecting the client back to the Success and Failure URLs, we also pass back a set of parameters (fields) that contain values relevant to the transaction that was just processed. There are two scenarios:

1) The client clicks on the “I Disagree” button on the credit card collection page and therefore does not process a transaction. The client will be redirected to the FailureURL.
2) The client clicks on the “I Agree” button on the credit card collection page and therefore submits a transaction for processing. Depending on the outcome of the transaction, the client will either be redirected to the SuccessURL if the transaction succeeded, or the FailureURL if the transaction failed or was declined.

See the tables below:

“I Disagree” OUTPUT PARAMETERS:

Field Name	Data Type	Description
CID	String(8)	Client ID, a unique ID given to you by DAT for processing your payments.
BID	Integer	Branch ID for departmental accounting only
ErrCode	Integer	Return value of error codes (see Appendix A). Set to 99006 if “I Disagree” button is clicked.
ErrReason	String	A short text description of the errors that occurred.

“I Agree” OUTPUT PARAMETERS:

Field Name	Data Type	Description
CID	String(8)	Client ID, a unique ID given to you by DAT for processing your payments.
BID	Integer	Branch ID for departmental accounting only
Ref	String(17)	The unique transaction reference specified or generated before processing the transaction.
Amount	Double	The total amount collected from the credit card in South African Rands.
Email	String	The e-mail address filled in by the client or passed in by the merchant.
TraceNo	Integer	A unique tracking number used by the bank.
ErrCode	Integer	Error code (see Appendix A). Set to “0” if transaction was successful.
ErrReason	String	A short text description of the errors that occurred. Set to ‘Successful’ if the transaction was successful.
SuccessURL	String	Basket clients only - The address (URL) to return to after the invoice is displayed.
FailureURL	String	Basket clients only - The address (URL) to return to after the invoice is displayed.

These values can be used to update any backend systems that might be keeping track of the payment process. Your Success and Failure URLs can extract the information passed back in these fields, so that you have the outcome of the transaction first-hand without having to go back and check it manually using our Client Admin site. However, you do not have to use any of the information passed back if you don’t need to.

The Testing Process

As with any new system you should test the mechanism before using it as a business tool that you rely on to make money! We provide just such a mechanism so that you can iron out all the problems before you go live. We have set up a demo Client Account that can submit transactions to our payment gateway. You can use this demo account by specifying the Client ID (CID) of “DATPOS” in your FORM. This is linked to a demo company called “Acme Mega Store”.

All transactions that are processed using this Client ID are authorised through the gateway but no money is deducted. You can use this to check the full process end-to-end. You will need a valid credit card however, to test a successfully authorised transaction. To test a declined transaction, you can use the VISA card number 4111 1111 1111 1111 with any non-expired date.

Remember that even though no money is deducted from successfully authorised transactions, the amounts are still reserved on the cardholder’s account for up to 30 days. So make your testing amounts small!

Remember to make sure that the SuccessURL and the FailureURL point to a page or pages on your site that can continue to lead the client through the purchase process after payment.

In order to check the status of transactions that were submitted using the demo account, please go the following website:

https://secure.dat.co.za/clientadmin

Login using the Merchant Code: “DATPOS” and the password: “password”.

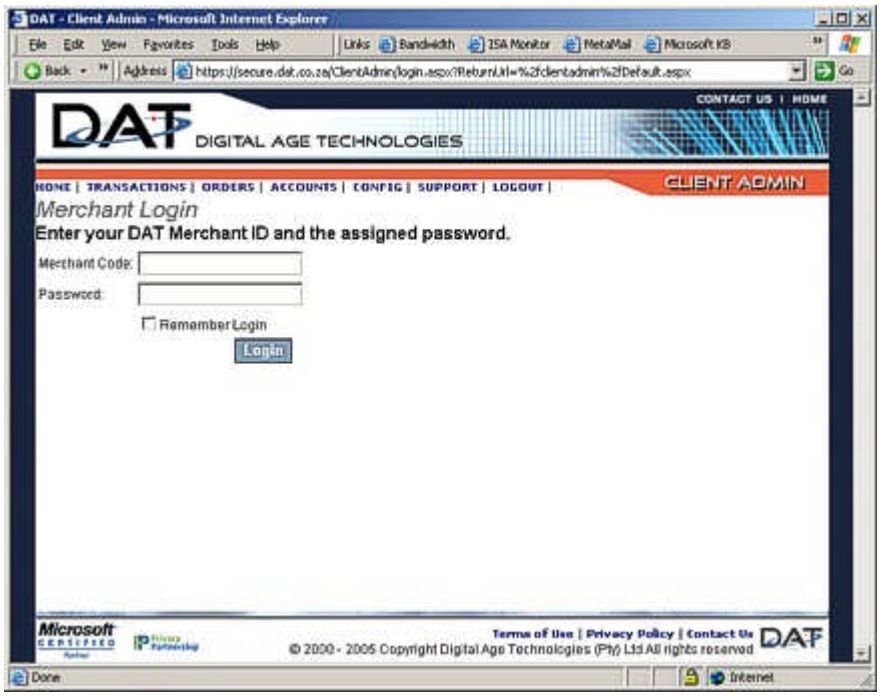
Use the “Transactions” link on the top menu to search or view your transactions. Remember that there might be other transactions listed from other people that are also testing, so please be courteous and don’t interfere with the transactions submitted by other people.

Going Live

Once your account has been created we will issue you with your own ClientID (CID). You must change the CID fields in your FORMS to use this new value or otherwise your transactions will continue to be allocated to our demo account. All new accounts are added in test mode, which means all card transactions will be authorised only, so you can continue testing your system with your actual CID.

Once testing has been completed, you can simply instruct us to make your account live. When this is done all transactions will be authorised and captured in real-time. This means that real money will start moving between accounts.

You will be issued with a password, which together with your ClientID, gives you access to the Client Admin site where you can see all the transactions that have been processed. Your Merchant Code is your Client ID. The Client Admin site can be accessed at: https://secure.dat.co.za/clientadmin



Additional Information

We have various other ways of facilitating the transaction such as batch transactions, COM objects and XML Web Services.

Our payment gateway is also available as a Web Service using XML and SOAP. Using this you can connect to us and perform a completely transparent authorisation. This can be customised directly into your web solution without seeing any of our pages. If you do this you will need an SSL server certificate to collect the credit card data securely. You will also need to know how to use SOAP, XML and Web Services.

Along with credit card payments, DAT also specialises in e-commerce applications in general. We provide a full range of e-commerce modules that can be used in an integrated fashion to simplify the creation of an online trading presence on the Internet. Our iBasket solution can be used in conjunction with our credit card payment system. This provides a fully-featured shopping basket that is highly customisable. Not only can it be configured to blend into your online store, but it also manages the many variations on shipping costs and delivery in an easy-to-use manner. All orders and credit card payments can be managed directly from DAT's Client Admin website.

If you need even more functionality than that then iStore is the way to go. This product is a complete online start up store. It can be customised to portray the image that you choose, and it uses our shopping basket and credit card collection system automatically. All products can be uploaded and administered online, and all orders and payments can be managed using the DAT Client Admin website.

Should you be interested in any of these options please do not hesitate to contact us. We will be happy to assist you in any manner that we can.

Contact Us

We are always available to help you with your integration procedure. Please feel free to call us if you have any difficulties.

Postal Address:

PO Box 179,
Sunninghill,
2157.

Physical Address:

Delft House,
376 Rivonia Boulevard,
Rivonia,
2128.

Telephone and Fax:

Tel: (011) 807-7550
Fax: (011) 807-0945

General Enquiries:

E-mail: enquiries@dat.co.za

Other Enquiries:

Administration - accounts@dat.co.za
Sales - sales@dat.co.za
Security - security@dat.co.za
Support - support@dat.co.za
Technical - technical@dat.co.za
Webmaster - webmaster@dat.co.za

Appendix A

Below is a list of common error codes and error descriptions that are found when processing transactions through the DAT payment gateway. If you receive an error that is not listed in this table, please call us to resolve the issue.

Code	Description
0	Successful
50004	Invalid CVV2 received
50005	Invalid Expiry Date received
50006	Invalid Credit Card Number received
50012	Transaction in wrong state from this request
50015	Invalid budget period received
50016	Amount too small for budget transaction
50500	Error in connection to database
51047	Invalid State Change
51051	Invalid currency code - only 710 (SA Rand) accepted at present
51052	Update failed
51055	Duplicate request received (ensure that the date and time is accurate)
60000	Transaction Failed
60001	Transaction Failed - Because communication with backend failed or timed out
99000	Transaction already processed
99001	Exception occurred
99003	Transaction Failed - Merchant cannot process foreign transactions
99004	Transaction Failed - Merchant has a local currency limit set
99005	Transaction Failed - Merchant has a foreign currency limit set
99006	Client did not agree to process the transaction