Payment Gateway Guide

April, 2016

Table of Contents

Introduction

In today's challenging business environment it is fundamental even for small businesses to reach globally and expand their potential. The Internet presents a unique opportunity for this but at the same time businesses need to find a secure, reliable and cost-effective way of accomplishing online transactions.

JCC Payment Systems Ltd's ("JCC") payment gateway offers real-time and batch payment processing. It uses available security measures to prevent fraudulent transactions and ensure data safety yet it's easy to integrate with merchants' systems. In addition, it allows merchants to review and manage transactions, prepare reports, etc. through a user-friendly, intuitive administration interface.

About this Guide

This guide intends to provide an introduction to payment card processing using JCC's payment gateway to both technical and business people. It provides an introduction to general concepts about online credit card processing and describes the integration methods available for the JCC Gateway in a consise way so that it's easy to decide which is the best available method for each business.

Accepting Payments Online

Any business that wants to accept payments online needs to have a merchant account and utilize the services of a Payment Service Provider (PSP). The merchant account will be provided by a so-called Acquirer while the PSP will provide the payment gateway. JCC is both an acquirer and a PSP so the whole process gets simplified a lot as you have a single point of contact for both.

Merchant Account / Acquirer

As mentioned above, the merchant account is offered to the merchant (business that wants to accept credit card payments) by an Acquirer.

An acquirer is a financial institution associated with one or more credit card companies (e.g. Visa, Mastercard, American Express) and is responsible for the settlement of the transactions, i.e. in particular:

1. The acquirer collects credit card data and payment amount from the merchant
2. The acquirer forwards the above information to the credit card issuer/bank (note: the credit card number identifies the type of card, the issuing bank and the cardholder's account)
3. If the cardholder has enough credit in their account to cover the purchase, the credit card issuer/bank authorizes the transaction and generates an authorization code which is sent to the acquirer (note: this puts a hold on the cardholder's account for the amount of the transaction but the cardholder's account has not been actually charged yet)
4. The acquirer sends the approval (or denial) code to the merchant
5. Either immediately or at a later time (but as long as the authorization code is still valid and the amount is on hold in the cardholder’s account) the merchant requests the capture of the authorized amount from the acquirer
6. The acquirer sends the capture request, through the Card Schemes (VISA, Mastercard etc,) to the card issuer/bank and the card issuer transfers the transaction amount, through the Card Schemes, to the acquirer.
7. The acquirer deposits the amount of the transaction (minus any fees) into the merchant account
8. On an agreed regular basis the acquirer transfers the accumulated funds from various transactions to the merchant’s **bank** account.

As it is obvious from the above the services offered by an Acquirer are crucial in credit card processing and in order to be able to receive these services a merchant account with an Acquirer is required.

In simple terms, you can think of a merchant account as a special intermediary account through which all funds from online payments pass before reaching the account of the merchant/business in a bank.

Payment gateway

Following all the above, someone might wonder where a Payment Gateway fits in all these. The Payment Gateway is very simply the technical medium (or channel) which facilitates the communication between the merchant and the acquirer.

As JCC plays the role of both the Acquirer and the Payment Gateway the whole integration process is much simpler compared to other cases where someone would need to check the acquirers supported by a payment gateway and vice versa before deciding who to use for each service. Unlike JCC, in cases where the Acquirer is different from the PSP the whole process (from application for a merchant account to integration and card processing) can be cumbersome.

Security in Credit Card Processing

Security is the biggest fear for all parties, cardholders and merchants, involved in credit card transactions, especially online.

In the case of customers their fear is obvious: whether their credit card information can be "stolen" and used by third parties.

In the case of merchants the concern is transactions unauthorized by the legitimate cardholder which can cause chargebacks. A chargeback occurs when a transaction made on a valid credit card, is disputed by the cardholder, i.e. the cardholder says "I didn't do it". In that case, what basically happens is the following:

1. The cardholder disputes the transaction with the card issuer/bank.
2. The card issuer/bank sends a chargeback (requests money back) from the acquirer.
3. If the chargeback is validated (and also, depending on many other factors) the acquirer gets the money from the merchant account and returns it to the card issuer/bank and subsequently, the cardholder. In some cases, chargebacks might also impose penalties to merchants.

In the case of chargebacks, the big problem for merchants is that they might have shipped goods or provided the service for which they were paid before a chargeback "hits" them. This is because there is a number of days after the original transaction was performed during which the cardholder may initiate a chargeback. This period is called *Chargeback Period* and can often be quite long, maybe up to 6 months. Acquirers are responsible to fulfill chargebacks, i.e. return money, and thus, will often reserve a percentage from each transaction for the chargeback period as a chargeback reserve; this is basically a guarantee against potential chargebacks. The percentage to be retained by the acquirer as a chargeback reserve may vary depending on the business of the merchant and security measures implemented (e.g. is the merchant using 3D Secure).

In order to address the concerns of both customers and merchants various security measures have been implemented for online credit card payments.

CVV

Another protocol used to prevent the unauthorized use of a credit card online is the CVV (Card Verification Value). This is called CVV2 by VISA, CVC2 by MasterCard and CID by American Express but the idea behind all three is exactly the same. Basically, a 3 or 4 digit number at the signature stripe of the card (at the front for American Express) checksums the rest of the card's information (name, number, expiry date, etc.). This number is extremely difficult to calculate even if you have all the card's information as some encryption keys known only to the issuer are used to calculate it; in fact, the CVV system has never been cracked so far, i.e. nobody managed to generate a valid CVV value for any card just by knowing all the card's information. Therefore, it is assumed that the only way to possess the CVV code is to have the card itself. CVV is a widely used security measure and nearly all banks issue their cards with a CVV code. CVV cannot provide protection in the case that a card is physically stolen and thus, a non-authorized person gets hold of its CVV code.

3D Secure

The real revolution in online transactions security came with the 3DS (3D Secure) protocol (Visa calls it *VerifiedByVisa*, MasterCard calls it *MasterCard SecureCode* and JCB *J/Secure*). 3DS is an XML-based protocol and is called 3D because of the 3 domains involved:

- The Issuer Domain including systems and functions of the issuer and its cardholders;
- The Acquirer Domain including functions of the acquirer and its merchants; and
- The Interoperability Domain systems and functions that enable the Issuer Domain and the Acquirer Domain to interoperate and authenticate each other worldwide.

The three domains involved in 3DS transactions exchange XML messages over SSL encrypted connection. 3DS is facilitated through the use of a special plug-in called MPI (Merchant Plug In) which is installed on the Acquirer's systems.

The idea of 3DS is to introduce another authentication step into the transaction and authenticate not only the card but also the cardholder. This is achieved by "diverting" the transaction to the card issuer who authenticates the cardholder using some authentication mechanism, the most common being a password/PIN. An online credit card transaction/payment can only be completed if 3DS authentication is successful.

3DS has benefits for both merchants and cardholders. In particular:

- Merchants: the advantage for Merchants is the reduction of "unauthorized" ("I didn't do it") transactions and resulting chargebacks. Since the 3DS authentication takes place by the card issuer/bank itself, liability for any chargebacks is shifted to it and not the merchant. This does not apply for all possible chargebacks. There are also cases where merchants are not eligible for chargeback liability shift and also, geographical restrictions; discussion of these exceptional cases is beyond the scope of this document.

- Cardholders enjoy two serious advantages compared to non-3DS transactions:
    - Online card fraud is not possible even if their credit card details or their credit card physically gets into the possession of an unauthorized person.
    - Since 3DS authentication takes place by the card issuer, the merchants are not able to capture and store the 3DS authentication credentials of the cardholder (as mentioned above this is usually a password/PIN). Therefore, even if a merchant's systems are compromised and customers' credit card information is found it will still not be possible for the hackers that get hold of it to perform any 3DS transactions online since they will not have the 3DS credentials.

It is extremely interesting to note that although some issuers/banks worldwide have not yet enrolled their cardholders for 3DS, transactions with such cards on merchants enrolled for 3DS can still be completed without a problem (so merchants do not lose potential customers) and liability for chargebacks is still shifted to the card issuer/bank (again of course there are certain exceptions).

People that hold cards of issuers who are enrolled for 3DS but their cards are not enrolled for 3DS will usually be prompted for online enrollment to 3DS the first time they use their credit card on a merchant that utilizes 3DS.

SSL Certificates

As mentioned above SSL (Secure Socket Layers) is a protocol used to encrypt the communication of messages in a 3DS transaction. SSL is also used to encrypt the transmission of information between the merchant's systems (e.g. online shop) and the cardholder, the payment gateway and the acquirer.

SSL certificates use public key cryptography to confirm each entity's identity and encrypt communication. SSL certificates are supplied by the so-called Certification Authorities.

Digital/Hash Signatures

A digital signature is used in data exchange for two purposes:

1. To verify the identity of the sender to the recipient
2. To ensure the integrity of the data transmitted between different parties.

Hash signatures are a form of digital signatures which are efficient and easy to implement. The two parties that share information have a common secret/password. When one party sends information to the other it also uses some or all of the information sent along with the password to create a hash value (the signature) using a one-way, non-reversible function/algorithm (such as MD5 or SHA1). The use of a one-way non-reversible function is of great importance so that even if a hacker gets hold of the hash, still he/she cannot decrypt it and learn the common secret/password. When information arrives to the recipient, the recipient needs to confirm that it was indeed sent by the sender and has not been tampered with during transition. The recipient knows what information was used to create the hash and this information has been transmitted to the recipient unhashed. He also knows the common secret/password and the algorithm used by the sender to create his signature. So using the unhashed sent information and the password he can re-create the hash using the algorithm used by the recipient.

If the hash created matches the hash received the information has been transmitted by the right sender and has not been tampered with. In case the two hashes do not match then, either the information was not sent by the proper sender (and thus the password used to create the hash is wrong) or information has been tampered with during transmission; in both cases the received data should be discarded.

PCI Compliance

The Payment Card Industry (PCI) Security Standards Council has derived the Data Security Standard (DSS), a set of comprehensive requirements for enhancing payment account data security, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. Any organization, whether a merchant, an acquirer or an issuer, that stores, processes, or transmits cardholder data (credit card numbers, expiration dates, etc.) needs to be certified for PCI DSS compliance.

The PCI DSS compliance requirements applicable for a merchant depends on various parameters including the payment method used, the volume of transactions processed and the use of a PCI DSS compliant service provider.

Going into the details of PCI DSS is beyond the scope of this document, especially as the standard is under continuous evolution to mitigate emerging payment security risks. However, it is built around the following principles:

- Build and Maintain a Secure Network;
- Protect Cardholder Data;
- Maintain a Vulnerability Management Program;
- Implement Strong Access Control Measures;
- Regularly Monitor and Test Networks; and
- Maintain an Information Security Policy.

For further information with regards to the Payment Card Industry Data Security Standard (PCI DSS) and the requirements for certification, please refer to Mastercard, VISA and PCI Security Standards Council websites.

JCC Anti-fraud Control

JCC provides an additional layer of security to merchants by providing a real-time rule-based anti-fraud tool. This tool examines transaction data to measure, monitor and control fraud in real-time. According to collected data, rules can be defined for all merchants, individual merchants or group of merchants (e.g. hotels).

The JCC Anti-fraud Control examines not only financial data but also, information contained in every Internet request (including IP address, browser information and more). The defined rules are combined with other information (such as geo location lookups, blacklists and customer past behaviour), to facilitate a real-time decision in regards of whether the transaction is legitimate or fraudulent and allow it to proceed or block it accordingly.

Additional Security Measures

Merchants who wish to take additional security measures and minimize their exposure can adopt various policies in their systems, e.g.:

- Put a ceiling on individual transaction amount or, if they maintain a user database, limit the total amount that a user is allowed to spend per day/week/month. Such ceilings could be removed upon creation of a positive history by the user.
- Limit the number of transactions or the total amount of transactions for which each credit card is authorized within a certain time interval (e.g. day, week, month).
- Limit the number of transactions or the amount of transactions per IP address.
- Block or impose strict restrictions for IPs from high risk countries.
- Create a "black list" of cards, IP addresses or even computer names.
- Monitor decline ratio and take measures if certain thresholds are exceeded; usually a high decline ratio indicates fraud attempts.

Many of the above measures are offered as a package from certain service providers and can be easily integrated with merchant systems through web services, APIs, etc.

Integration Methods

The JCC Payment Gateway can be used to process online/real time transactions, mail/telephone orders (MOTO) and batches. The methods available to each merchant will depend on his contract with JCC.

Regarding online transaction processing there are few different ways that a merchant can use to integrate his systems with the JCC payment gateway:

- HTTPS Post Redirect;
- HTTPS Post Direct;
- Server to Server (Socket-based);
- Batch Processing;
- Tokenization; and
- Web Services.

There are no restrictions in the programming language that will be used to carry out the integration. Below we will examine each of the above integration methods and we will also refer to batch processing and MOTO.

As far as the online integration methods it is important to note for which methods 3D Secure is available and for which is not. Also, we need to emphasize that methods which enable the merchant to store, process, or transmit cardholder data (e.g. full credit card number, not padded), require the merchant to be certified for PCI DSS compliance. Finally, for all of the online integration methods the merchant's server needs to be secured using an SSL certificate.

Online/Real Time Processing

HTTPS Post Redirect

The HTTPS Post Redirect method (will refer to it as Redirect) allows processing transactions with and without 3D Secure. It does not enable the merchant to store, process, or transmit cardholder data and thus, does not require the merchant to be certified for PCI DSS compliance.

In the Redirect method the merchant sends to JCC the order details (amount, currency, order id, etc.) and then, a page is displayed to the client from JCC to enter his/her credit card information (this page resides on JCC's servers). Upon submission of credit card information the transaction is processed and the response is returned back to the merchant.

Method Summary	
3D Secure	Compulsory
Merchant SSL Certificate	Required

PCI DSS Certification	Not Required

The steps followed in the Redirect method are as follows and are reflected in Diagram 1:

1. The customer of the merchant completes his shopping on the merchant's website and goes to the checkout page where he is presented with the total purchase amount and clicks on the *Pay* button.
2. At this stage the merchant prepares the request data and sends it to JCC (this is a step transparent to the customer).
3. The customer is presented with the payment form which resides on JCC's servers.
4. The customer enters his credit card details (card number, expiration date and CVV value) on the Payment Form and clicks the submit button, labeled *Proceed*
5. If the merchant utilizes 3DS and the card is enrolled to 3DS the transaction is redirected to the issuer of the customer's card and the customer is presented with a form where he needs to enter his 3DS credentials.
6. The data entered by the customer (and any 3DS data) are sent for authorization by JCC to the issuer or credit card company (this is a step transparent to the customer).
7. If the transaction is approved the amount of the transaction is reserved (and maybe captured) on the customer's card.
8. The result of the transaction is sent back to the merchant.
9. The merchant presents the customer with the transaction/payment result.

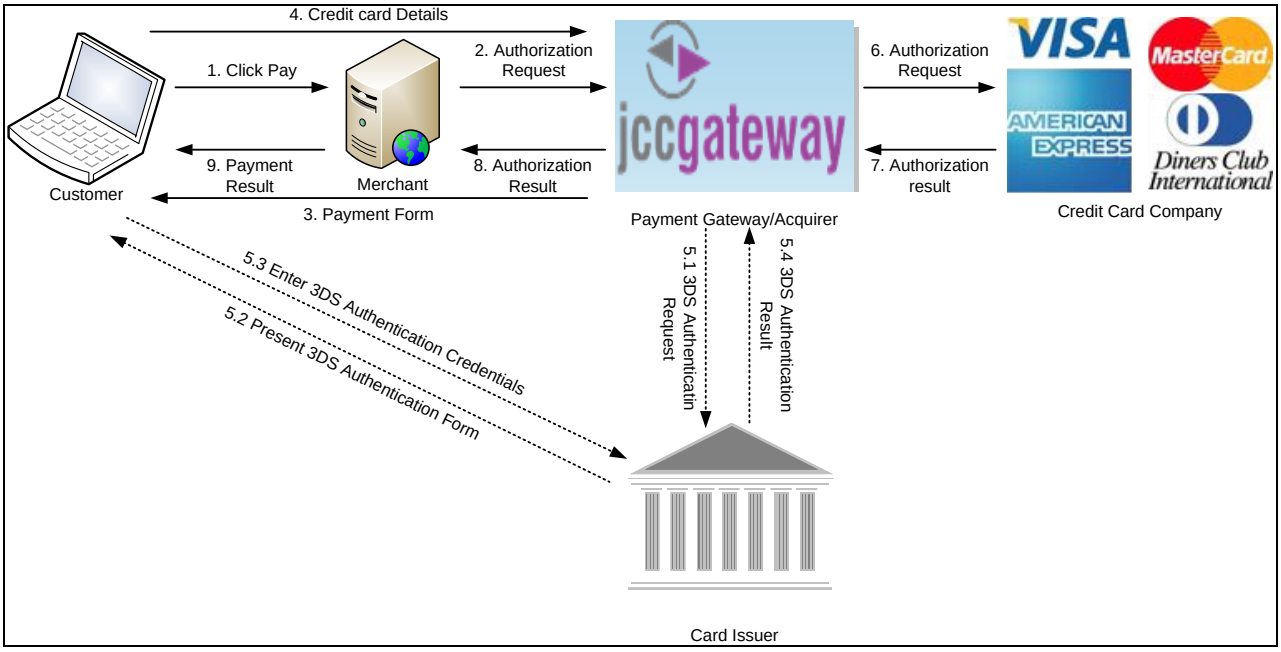

Diagram 1: HTTPS POST Redirect Processing

All that a merchant needs to do to send a Redirect request for processing to JCC is to put all fields an HTML form and submit it to the designated URL.

HTTPS Post Direct

The HTTPS Post Direct method (will refer to it as Direct) is very similar to the Redirect one. Like the Redirect it allows processing transactions with and without 3D Secure. Unlike the Redirect method, the merchant is able to store, process, or transmit cardholder data and may also affect the security of the payment transaction and the integrity of the page that accepts the cardholder data.Therefore, this method requires the merchant to be certified for PCI DSS compliance.

In the Direct method the page on which credit card details are entered resides on the merchant's server and this is why the merchant is able to access and store credit card details. The merchant sends to JCC the order details (amount, currency, order id, etc.) along with credit card details. The transaction is then processed and the result is returned back to the merchant.

Method Summary	
3D Secure	Compulsory
Merchant SSL Certificate	Required
PCI DSS Certification	Required

The steps followed in the Direct method are very similar to the Redirect. The only difference is that since credit card details are collected from the customer on the merchant's website they are sent along with the transaction details to JCC and there is no Payment form presented to the customer from JCC. In detail, the steps are as follows and are reflected in Diagram 2:

1. The customer of the merchant completes his shopping on the merchant website and goes to the checkout page where he is presented with the total purchase amount and fields to enter his credit card details (card number, expiration date and CVV value); the customer enters his card details and then, clicks on the *Pay* button.
2. At this stage the merchant prepares the request data (which includes card details) and sends it to JCC (this is a step transparent to the customer)
3. If the merchant utilizes 3DS and the card is enrolled to 3DS the transaction is redirected to the issuer of the customer's card and the customer is presented with a form where he needs to enter his 3DS credentials.
4. The data entered by the customer (and any 3DS data) are sent for authorization by JCC to the issuer or credit card company (this is a step transparent to the customer).
5. If the transaction is approved the amount of the transaction is reserved (and maybe captured) on the customer's card.
6. The result of the transaction is sent back to the merchant.
7. The merchant presents the customer with the transaction/payment result.

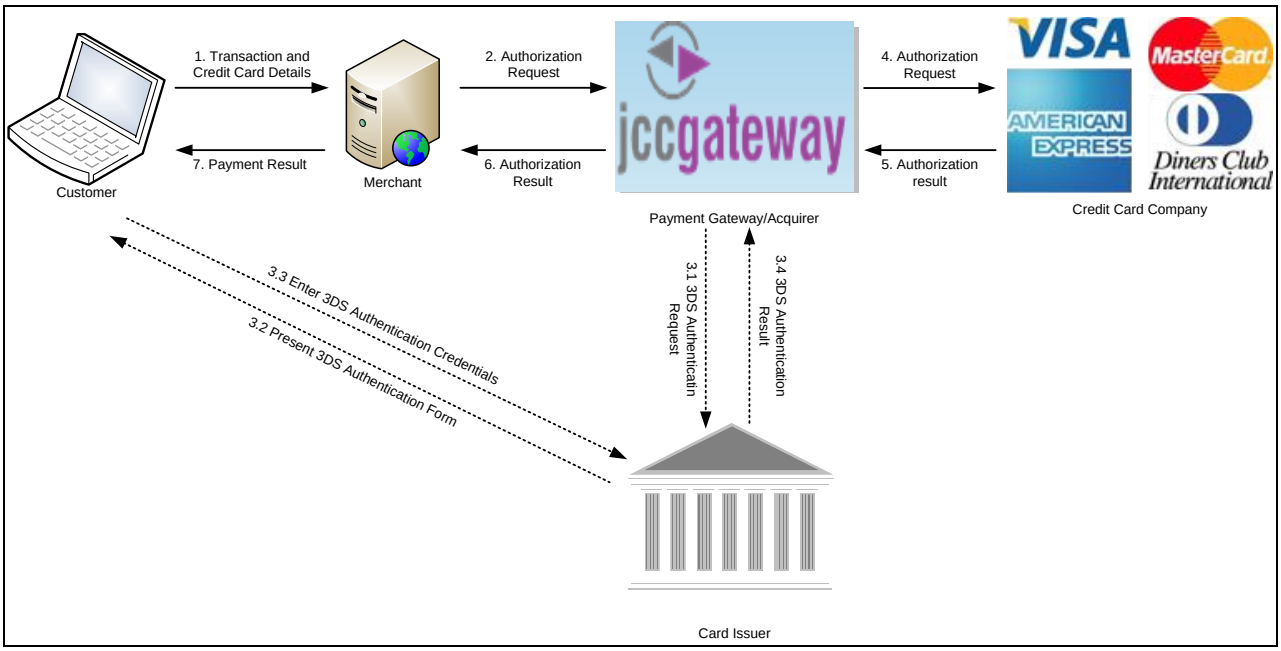

Diagram 2: HTTPS POST Direct Processing

Like with the Redirect method, all that a merchant needs to do in order to send a Direct request for processing to JCC is to put all fields in an HTML form and give the opportunity to the customer to enter his credit card details on the same form. When the customer submits the form the request will be sent to JCC for processing.

Server to Server (Socket-based)

The Server to Server is a socket based integration method (will refer to it as S2S). Like with the Direct method, credit card details are collected by the customer on a page residing on the merchant's server. The merchant then forms the authorization request and opens a socket connection to JCC through which it sends the authorization request and receives the authorization response.

Since credit card details are entered on a page residing on the merchant's website, the merchant is able to store, process, or transmit cardholder data and may also affect the security of the payment transaction and the integrity of the page that accepts the cardholder data. Therefore, this method requires the merchant to be certified for PCI DSS compliance.

Unlike the HTTPS POST Redirect and Direct methods, in the S2S method there is no browser-level interaction between the customer/merchant and JCC and thus, it is not possible to redirect the customer's browser for 3DS authentication; consequently, 3DS is NOT available for this method.

Method Summary	
3D Secure	Not Available
Merchant SSL Certificate	Required
PCI DSS Certification	Required

The steps followed in the S2S method are very similar to the ones of Direct, without of course the steps related to 3DS which is not available, and are shown in Diagram 3:

1. The customer of the merchant completes his shopping on the merchant website and goes to the checkout page where he is presented with the total purchase amount and fields to enter his credit card details (card number, expiration date and CVV value); the customer enters his card details and then, clicks on the *Pay* button.
2. At this stage the merchant prepares the request data (which includes card details), opens a socket and sends it to JCC (this is a step transparent to the customer).
3. The data entered by the customer is sent for authorization by JCC to the issuer or credit card company (this is a step transparent to the customer).
4. If the transaction is approved the amount of the transaction is reserved (and maybe captured) on the customer's card.
5. The result of the transaction is sent back to the merchant who receives it through the socket opened at step 2.
6. The merchant presents the customer with the transaction/payment result.

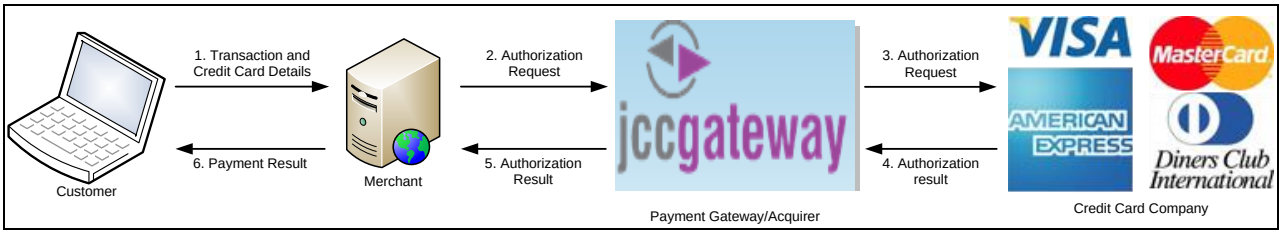

Diagram 3: Server to Server Processing

Despite of the fact that the steps involved in the S2S method are pretty similar to those of the Direct method, the implementation of communication between the merchant and JCC is completely different since it is socket-based instead of HTTPS POST. The merchant still needs to present the customer with a form in which the customer will enter his credit card details; this form however, is not submitted to JCC but to a script residing on the merchant's server. This script will take credit card data along with the rest of the transaction details, formulate a request and open a socket to JCC to send the authorization request. Then, through the same socket, in the same script, the merchant will receive and process the response of JCC before presenting the transaction/payment result to the customer.

Web Services

Web services is another integration method where the credit card details are collected by the customer on a page residing on the merchant's server. The merchant then forms the authorization request and sends it over to JCC using a SOAP XML Request and receives the authorization response through a SOAP XML Response.

Since credit card details are entered on a page residing on the merchant's website, the merchant is able to store, process, or transmit cardholder data and may also affect the security of the payment transaction and the integrity of the page that accepts the cardholder data. Therefore, this method requires the merchant to be certified for PCI DSS compliance.

Like the Server to Server method there is no browser-level interaction between the customer/merchant and JCC and thus, it is not possible to redirect the customer's browser for 3DS authentication; consequently, 3DS is NOT available for this method.

It is important to say that Web Services do not only allow processing of online Authorizations or Authorizations/Captures like other processing methods but also, provide a lot of other functionalities. In particular, there are three different Web Services allowing the following:

- Online Service:
  - Authorization
  - Authorization and capture
- Financial Service:
  - Capture a previously authorized transaction
  - Reverse a previously authorized but NOT captured amount
  - Refund a previously authorized and captured amount
- Query Service:
  - Search transactions by date
  - Search transactions by order number/ID
  - Search transactions by status

OnlineService – Authorization/Capture

Method Summary	
3D Secure	Not Available
Merchant SSL Certificate	Required
PCI DSS Certification	Required

The steps followed for authorizing a transaction using Web Services are nearly identical to the ones of Server to Server and are shown in Diagram 4:

1. The customer of the merchant completes his shopping on the merchant website and goes to the checkout page where he is presented with the total purchase amount and fields to enter his credit card details (card number, expiration date and CVV value); the customer enters his card details and then, clicks on the *Pay* button.
2. At this stage the merchant prepares the request data (which includes card details) and sends the SOAP XML Authorization Request to JCC (this is a step transparent to the customer).
3. The data entered by the customer is sent for authorization by JCC to the issuer or credit card company (this is a step transparent to the customer).
4. If the transaction is approved the amount of the transaction is reserved (and maybe captured) on the customer's card.
5. The result of the transaction is sent back to the merchant using a SOAP XML Response.
6. The merchant presents the customer with the transaction/payment result.

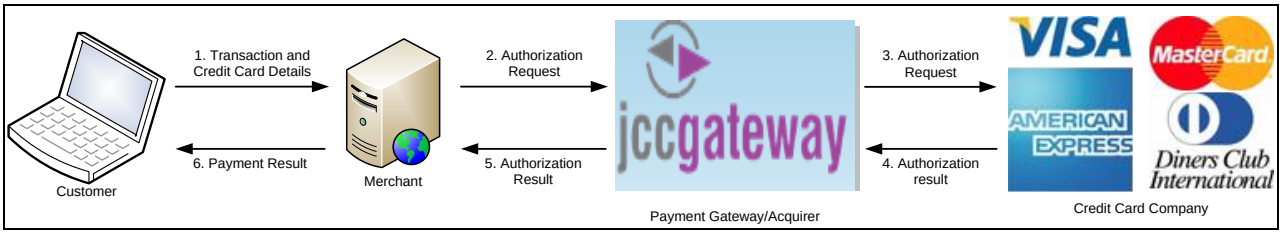

Diagram 4: Authorization using Web Services

The easiest way to implement Web Services integration with JCC's Payment Gateway is by utilizing the facilities of a modern IDE (Integrated Development Environment) such as NetBeans, Eclipse, Visual Studio, etc. (choice of IDE to use depends on programming language).

Financial Service – Capture, Refund, Reversal

The Financial Service allows capturing a previously authorized transaction, reversing a previously authorized but NOT captured amount or refunding a previously authorized and captured amount. An SSL certificate is required for all three operations of the Financial Service in order to encrypt the communication with JCC.

Reversals and Refunds are very frequently confusing and thus, it's important to clarify the difference: the only difference between Reversals and Refunds is that Reversals are applicable when a transaction has been authorized but NOT captured while Refunds are applicable when a transaction has been both Authorized and Captured.

Query Service – Search by Date, Search by ID, Search by Status

The Query Service, as its name suggests, allows querying transactions, either by Date, or by ID or by Status. Like with the Financial Service, an SSL certificate is required in order to encrypt the communication with JCC.

The Search by Date will retrieve a list of orders between two dates. The Search by ID will retrieve a single transaction matching the ID searching for. The Search by Status will retrieve a list of transactions

with the status searching for (e.g. Authorized, Captured, Refunded, etc.) while it also allows to limit the search scope between two dates.

Batch Processing

As mentioned earlier, JCC's payment gateway allows processing transactions offline in batches. Using batch processing, merchants can perform the following transactions:

- Authorization
- Capture
- Authorization and capture
- Refund
- Reversal.

When processing transactions in batches, the merchant prepares a file according to the specification required by the JCC Gateway. The file is uploaded through the Merchant Backoffice System and is parsed/validated instantly to check correctness of structure and format. Then, given that a batch file has been successfully validated upon upload, at a specific scheduled time the transactions in the file are processed and through the Merchant Backoffice System one can see the results of the processing.

It is important to mention that batch processing is an offline processing method. This means that cardholder is not interacting during the transaction and thus, 3D Secure is not available. Also, since the merchant needs to collect credit card data from cardholders while preparing a batch, it means that the merchant is able to store, process, or transmit cardholder data and needs to be certified for PCI DSS compliance.

Tokenization

Tokenization allows recurrent processing of transactions using a card which has been previously registered with JCC as part of an authorization transaction and for which JCC has issued a unique hash. Tokenization allows merchants who are not certified for PCI DSS compliance, to process recurrent transactions without the need to store card data and thus, without the need to be certified.

The steps required in order to implement tokenization are the following:

1. Registration of credit card/creation of token/hash:
    a. Send a regular authorization request including request to register credit card.
    b. Receive authorization response from JCC (i.e. authorization is processed like in a normal transaction); if successful then the token/hash for the credit card will be included in the response and should be stored by the merchant so that he is able to process subsequent transactions using the same credit card which will be identified in future transactions from the unique token/hash created for it.

2. Processing of subsequent transactions using the created token:
    a. Send an authorization request where instead of credit card data, the token representing the credit card is sent instead.
    b. Regular authorization response is returned from JCC.

3. Update of credit card details - this is required when a card for which a token has been previously issued by JCC has expired and thus, it is necessary to send the new expiration date to JCC which will update the credit card details in its systems:
    a. Send a regular authorization request with true credit card data (i.e. card number, expiration date and CVV, not token) along with request to update credit card data stored by JCC (JCC will identify the card from the card number which is not changing upon renewal).
    b. If authorization is successful (authorization is processed like in a normal transaction), then the response will contain a token/hash that the merchant should store to use for future transactions.

4. Deactivation of token - this is required to disallow further processing using the specific token:
    a. Send a deactivation request containing only the token (no credit card details). The fields required are the same as for an authorization request.
    b. Confirmation is returned from JCC. Authorization is NOT processed.

Credit card registration (to get a token the very first time) as well as update of credit card details and creation of new token are available using the following integration methods:

- HTTPS Post Redirect;

- HTTPS Post Direct;
- Server to Server (Socket-based); and
- Web Services.

3D Secure is available as if processing a regular authorization (i.e. in the cases of HTTPS Post Redirect and Direct with the cardholder being present/processing the transaction).

Processing of transactions using a token or deactivation of a token is available using the following integration methods:

- HTTPS Post Direct;
- Server to Server (Socket-based);
- Web Services; and
- Batch Processing.

3D Secure is not available when processing transactions using a token.

Virtual POS (Mail Order/Telephone Order – MOTO)

MOTO Transactions can be processed through the Virtual POS system residing within the Merchant Backoffice System.

Apart from processing MOTO transactions JCC's Merchant Backoffice System allows merchants to perform a number of other functions such as viewing reports of transactions, viewing details of each transaction, capture, reverse or refund transactions, etc.